CYFRYZACJA RYNKU PRACY

Moduł szkoleniowy opracowany w ramach projektu „Inicjowanie Działań Wdrażających Porozumienie Ramowe Europejskich Partnerów Społecznych w sprawie cyfryzacji” dofinansowany ze środków Unii Europejskiej

PL

Dofinansowane przez Unię Europejską

NSZZ Solidarność Komisja Krajowa

instrat

NSZZ Solidarność Komisja Krajowa

instrat

Cyfryzacja rynku pracy

Moduł szkoleniowy opracowany w ramach projektu

Inicjowanie działań wdrażających Porozumienie Ramowe Europejskich Partnerów Społecznych w sprawie cyfryzacji

dofinansowany ze środków Unii Europejskiej

Dofinansowane przez Unię Europejską

Czerwiec 2023

Autorki:

Blanka Wawrzyniak

Marta Musidłowska

Wsparcie merytoryczne:

Hanna Sakowicz-Daszczyńska

Redakcja:

Julia Zaleska

Opracowanie graficzne, skład, druk:

PP WiB Piotr Winczewski

tel. +48 58 341 99 89, e-mail: wib1@wp.pl

Okładka źródła:

palec dloni robota /rawpixel.com/freepik.com

Tesla Robot Dance / wikimedia.org

portret pracownika fabryki/ aleksandarlittlewolf/ freepik.com

grafiki AI użyte w publikacji freepik.com

Publikacja bezpłatna, sfinansowana ze środków Unii Europejskiej w ramach projektu nr 101051759 **„Inicjowanie działań wdrażających Porozumienie Ramowe Europejskich Partnerów Społecznych w sprawie cyfryzacji (EFAD)”.** Tytuł oryginalny: “Initiating activities to implement the European Social Partners Framework Agreement on Digitalisation (EFAD)”.

Nota wstępna

Niniejsza publikacja powstała w ramach projektu „Inicjowanie działań wdrażających Porozumienie Ramowe Europejskich Partnerów Społecznych w sprawie cyfryzacji”. Stanowi ona podręcznik, który będzie wykorzystywany zarówno podczas szkoleń projektowych jak i po jego zakończeniu. Moduł szkoleniowy ma na celu przygotowanie partnerów społecznych na dynamiczne zmiany zachodzące na rynku pracy w związku z transformacją cyfrową. Są to zmiany dotyczące m.in. automatyzacji produkcji, nowych modeli biznesowych, pracy zdalnej i innowacyjnych metod zarządzania w firmach. Publikacja zawiera także omówienie praw pracowniczych w dobie cyfrowej. Jej celem jest wyposażenie pracowników w narzędzia pozwalające na odłączenie się i zachowanie równowagi między życiem prywatnym a zawodowym.

Spis treści

Wstęp

Choć sztuczna inteligencja (AI) jest szerokim terminem obejmującym grupę algorytmów, które mogą modyfikować swoje parametry i tworzyć nowe wyniki, w najprostszych słowach można określić ją jako zdolność maszyn do rozumienia, uczenia się, planowania i wykazywania kreatywności.

Dla wielu ekspertów tempo rozwoju sztucznej inteligencji i jej wpływ na otaczający nas świat wydają się niepokojące. Wpływ na to ma m.in. fakt, że systemy AI tworzone są przez największe spółki technologiczne z USA i Chin, które za priorytet stawiają swoje komercyjne zyski. Przed niebezpieczeństwami związanymi z nieskrępowanym rozwojem AI przestrzegają też sami przedstawiciele branży technologicznej. Pod listem otwartym nawołującym do wstrzymania eksperymentów nad systemami sztucznej inteligencji i systemów potężniejszych od Czatu GPT-4 podpisały się m.in. takie osoby, jak Elon Musk (dyrektor generalny SpaceX, Tesli i Twittera), Steve Wozniak (współzałożyciel firmy Apple), czy Yuval Noah Harari (futurysta, profesor Uniwersytetu Hebrajskiego w Jerozolimie).

Kontrolowanie rozwoju AI jest niezbędne do tego, aby zapewnić bezpieczeństwo systemów sztucznej inteligencji i zagwarantować, że uwzględniają one wpływ dobrostan człowieka. Jednak w powszechnym natłoku informacji dotyczących AI, na pierwszy plan wysuwają się najbardziej alarmistyczne wizje, niekoniecznie mające oparcie w rzeczywistości. To natomiast prowadzi do sceptycznych opinii na temat nowych technologii, lęku przed masowym bezrobociem i niechęci do wykorzystywania narzędzi cyfrowych. Należy jednak pamiętać, że w technologie stanowią obecnie nieodłączną część codzienności. To nie tylko źródła rozrywki, ale także narzędzia ułatwiające wykonywanie obowiązków domowych i zawodowych. Z tego względu przyswajanie innowacyjnych rozwiązań oraz edukowanie społeczeństwa w zakresie właściwego korzystania z nich jest niezmiernie ważne.

Działania uświadamiające powinny dotyczyć także (albo i przede wszystkim) narzędzi cyfrowych stosowanych w miejscach pracy. Jak zostanie wskazane w dalszej części podręcznika, nowe technologie wykorzystywane są w wielu sektorach i na różnych etapach zatrudnienia (od rekrutacji po ewaluację pracownika). Ułatwiają one zarówno procesy zarządzania przedsiębiorstwem, jak również codzienną pracę wielu ludzi (zarówno pracowników fizycznych, jak i umysłowych). Najlepszym przykładem tego jest powszechne wykorzystywanie maszynowych tłumaczy języka typu Google Translator czy Deepl, które usprawniają komunikację transgraniczną pomiędzy firmami czy umożliwiają przekład tekstów branżowych bez konieczności korzystania z usług profesjonalnego tłumacza.

Coraz większe nadzieje na usprawnianie pracy pokłada się też w generatywnej sztucznej inteligencji. Aplikacje takie jak Czat GPT czy DALL-E już teraz wykorzystywane są do kreatywnych zadań, np. pisania e-maili lub przeprowadzania analiz danych. Przykładowo, za pomocą generatywnego AI możliwe są szybsza analiza treści artykułu czy zapis przebiegu spotkania w zaledwie chwilę. Po wydaniu odpowiedniej komendy (np. „podaj główne wnioski z dyskusji") i wprowadzeniu w system podstawowych parametrów, można spodziewać się wygenerowania oczekiwanych wyników (wniosków).

Równocześnie należy pamiętać, że duże modele językowe (LLM, ang. *Large Language Model*), takie jak Czat GPT, pomimo że tworzą treści brzmiące naturalnie, to jednak generują je automatycznie i bezrefleksyjnie. To natomiast może powodować, że teksty są produkowane przez algorytm, choć bardzo wiarygodne, zawierają wiele błędów. Dlatego tak ważne jest wyrobienie wśród użytkowników umiejętności krytycznego myślenia, zdolności analizy rzeczywistego otoczenia i odsiewania tego, co nieprawdziwe (np. *fake news*). Co więcej, w pracy w dobie cyfrowej, poza przygotowaniem zatrudnionych w różnych sektorach do automatyzacji i wyposażeniem ich w nowe kompetencje, konieczne jest nauczenie pracowników koegzystowania z technologiami oraz umiejętności „odłączenia się". To warunki odpowiedniego balansu pomiędzy życiem prywatnym a życiem zawodowym.

Niniejsza praca powstawała na przełomie lat 2022 i 2023. Mając na uwadze dynamiczny rozwój innowacji, a w szczególności narzędzi sztucznej inteligencji (AI), autorki podręcznika chcą zaznaczyć, iż niektóre treści mogą ulec dezaktualizacji w nadchodzących miesiącach i latach w związku z postępem technicznym.

Słownik pojęć

AI Act/akt w sprawie sztucznej inteligencji

– unijne rozporządzenie ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji.

Algorytm

– zestaw instrukcji (formuła obliczeniowa), które autonomicznie podejmują decyzje na podstawie modeli statystycznych lub reguł decyzyjnych bez wyraźnej interwencji człowieka.

Anonimizacja

– proces polegający na przekształceniu danych osobowych w sposób uniemożliwiający ich przyporządkowanie do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Automatyzacja

– stosowanie technologii do kontrolowania produkcji oraz tworzenia produktów i usług z wykorzystaniem narzędzi cyfrowych.

Blockchain

– tzw. łańcuch bloków, technologia służąca do przesyłania i przechowywania informacji o transakcjach internetowych; rejestr zdecentralizowanych danych, które są bezpiecznie współużytkowane. Technologia blockchain umożliwia grupie wybranych uczestników dzielenie się danymi.

Bring your own device (BYOD)

– trend polegający na wykorzystywaniu prywatnych urządzeń, takich jak laptopy, smartfony czy tablety do wykonywania obowiązków zawodowych.

Czat GPT

– narzędzie wykorzystujące sztuczną inteligencję (chatbot), które w formule przypominającej dialog, pozwala otrzymywać odpowiedzi na pytania zadawane w języku naturalnym przez użytkownika.

Dane osobowe

– wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej (poszczególne informacje, które w połączeniu ze sobą mogą prowadzić do zidentyfikowania tożsamości danej osoby, także stanowią dane osobowe).

Deep fake

– od dwóch angielskich zwrotów: *deep learning* (głębokie uczenie) oraz *fake* (fałsz, podróbka). To obróbka dźwięku i obrazu mająca na celu stworzenie fałszywego przekazu przy użyciu technik z zakresu sztucznej inteligencji. Pozwala to na przygotowanie materiałów, które będą trudne lub niemożliwe do odróżnienia od filmów lub zdjęć stworzonych tradycyjnymi sposobami oraz z udziałem realnych osób.

Duże modele językowe (LLM, ang. *Large Language Models*)

– modele uczenia maszynowego zdolne do wykonywania różnorodnych zadań z zakresu przetwarzania języka naturalnego. Szkolenie takiego systemu polega na dostarczaniu im dużych ilości danych (np. książek, artykułów, stron internetowych), dzięki którym może on uczyć się wzorów i połączeń między słowami w celu generowania nowych treści w przyszłości. Przykładem LLM jest Czat GPT, który został opracowany przez OpenAI i udostępniony publiczności w listopadzie 2022 r. Model ten jest w stanie przetwarzać informacje i wygenerować tekst podobny do tekstu napisanego przez człowieka w odpowiedzi na monity użytkownika.

Fake news

– nieprawdziwa bądź częściowo nieprawdziwa informacja o charakterze sensacyjnym, która celowo wprowadza w błąd odbiorcę.

Gospodarka współdzielenia/na żądanie (*sharing economy*; *on-demand economy*)

– zbiór modeli biznesowych opartych na pośrednictwie platform współpracy, tworzących

ogólnodostępny rynek czasowego korzystania z dóbr lub usług często dostarczanych przez osoby prywatne.

Kompetencje przyszłości

– konkretne umiejętności umożliwiające podejmowanie i realizowanie zadań w środowisku pracy, które jest z gruntu elastyczne, rozproszone geograficznie, podatne na częste i szybkie zmiany oraz zakłada konieczność operowania technologiami cyfrowymi i współpracę ze zautomatyzowanymi systemami oraz maszynami wykorzystującymi sztuczną inteligencję.

Mobbing

– działania lub zachowania skierowane wobec pracownika, polegające na uporczywym i długotrwałym nękaniu lub zastraszaniu go.

Praca platformowa

– forma zatrudnienia, w ramach której pracownik korzysta z platformy cyfrowej, aby uzyskać dostęp do innych organizacji lub osób w celu świadczenia określonych usług i w zamian za wynagrodzenie. Do zadań wykonywanych odpłatnie za pośrednictwem platform cyfrowych należą m.in. przewozy taksówkarskie i kurierskie, dostawy, serwis napraw domowych, jak i prace umysłowe, takie jak copywriting czy księgowość.

Praca wspomagana

– praca, podczas wykonywania której pewne działania mogą być zastąpione przez roboty, podczas gdy inne wymagają udziału czynnika ludzkiego.

Prawo do odłączenia się

– prawo do nieangażowania się poza czasem pracy w zadania związane z pracą i nieuczestniczenie w komunikacji za pomocą narzędzi cyfrowych.

Profilowanie

– dowolna forma zautomatyzowanego przetwarzania danych osobowych polegająca na wykorzystaniu ich do oceny niektórych czynników osobowych osoby fizycznej. Profilowanie wykorzystuje się w szczególności do analizy lub prognoz dotyczących efektów pracy tej osoby,

jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Pseudonimizacja

– przetwarzanie danych osobowych w taki sposób, aby nie było możliwe zidentyfikowanie, do kogo one należą bez dostępu do innych informacji, które są przechowywane bezpiecznie w innym miejscu.

RODO

– *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (dalej: rozporządzenie RODO).

Roboty współpracujące (*collaborative robots*; co-boty)

– urządzenia, których zadaniem jest ograniczanie obciążenia pracowników zakładów przemysłowych poprzez wykonywanie części ich zadań.

Samouczenie się (ML; *machine learning*)

– obszar sztucznej inteligencji poświęcony algorytmom, które nieustannie poprawiają swoje funkcjonowanie poprzez doświadczenie, czyli ekspozycję na dane. Algorytmy uczenia maszynowego budują model matematyczny na podstawie przykładowych danych (zwanych zbiorem uczącym) w celu prognozowania lub podejmowania decyzji bez potrzeby zaprogramowania do tego celu przez człowieka.

Spoofing

– rodzaj ataku, w którym przestępcy podszywają się pod banki, instytucje i urzędy państwowe, firmy, a nawet osoby fizyczne w celu wyłudzenia od swoich ofiar danych lub pieniędzy.

Start-up

– nowo utworzone przedsiębiorstwo lub tymczasowa organizacja poszukująca modelu biznesowego, który zapewniłby jej zyskowny rozwój.

Sztuczna inteligencja (SI, AI)

– zdolność maszyn do rozumienia, uczenia się, planowania i wykazywania kreatywności. Zgodnie z definicją zaproponowaną przez projekt aktu w sprawie sztucznej inteligencji (AI Act) system sztucznej inteligencji oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść określonych szczegółowo w rozporządzeniu, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję. Definicja ta jest bardzo szeroka i mało precyzyjna, co jest jednak zrozumiałe w kontekście tak szybko rozwijającej się technologii, jaką jest sztuczna inteligencja.

Szyfrowanie danych

– zbiór technik służących do kodowania informacji wrażliwych lub osobistych w celu zapewnienia ich poufności.

Wearables

– urządzenia elektroniczne „do ubrania", czyli noszone są blisko skóry. Mogą one monitorować i analizować parametry zdrowotne użytkownika lub jego zachowanie. Do najpopularniejszych urządzeń tego typu zaliczają się obecnie urządzenia typu smartwatch, opaski sportowe (tzw. smartbandy) oraz zegarki sportowe.

Work-life balance

– zachowywanie równowagi pomiędzy pracą (zarówno płatną, jak i nieodpłatną) a życiem rodzinnym oraz czasem wolnym.

Zautomatyzowane podejmowanie decyzji

– działanie oparte na zaawansowanych obliczeniach i wyłącznie technicznych środkach przetwarzania informacji. Wydawanie decyzji przez komputer bez udziału elementu ludzkiego.

1. Wpływ cyfryzacji na procesy pracy

1.1. Porozumienie Ramowe Europejskich Partnerów Społecznych w sprawie cyfryzacji – uwagi ogólne

Cyfrowa transformacja gospodarki ma ogromny wpływ na pracodawców, pracowników i przebieg samej pracy. Aby ułatwić integrację technologii cyfrowych w miejscach pracy, w czerwcu 2020 r. zawarto autonomiczne Porozumienie Ramowe Europejskich Partnerów Społecznych (EFAD). Jego celem jest zapobieganie i minimalizowanie ryzyk, które mogą ponosić pracownicy i pracodawcy. Porozumienie obejmuje wszystkie osoby zatrudnione lub zatrudniające pracowników w sektorze publicznym i prywatnym oraz we wszystkich rodzajach działalności gospodarczej.

Porozumienie EFAD jest niezależną inicjatywą i wynikiem negocjacji między europejskimi partnerami społecznymi w ramach szóstego wieloletniego programu prac na lata 2019–2021. W świetle art. 155 traktatu o funkcjonowaniu Unii Europejskiej (TFUE) to autonomiczne europejskie porozumienie ramowe zobowiązuje członków BusinessEurope, SMEunited, CEEP i EKZZ (oraz komitet łącznikowy EUROCADRES/CEC) do promowania i wdrażania narzędzi oraz środków (w razie potrzeby na poziomie krajowym, sektorowym lub przedsiębiorstw) zgodnie z procedurami i praktykami właściwymi dla partnerów społecznych w państwach członkowskich i państwach Europejskiego Obszaru Gospodarczego.

Przykładem innych autonomicznych porozumień zawieranych w ostatnich latach jest chociażby Autonomiczne porozumienie ramowe europejskich partnerów społecznych dotyczące aktywnego starzenia się oraz podejścia międzypokoleniowego czy Europejskie porozumienie ramowe dotyczące stresu związanego z pracą.

I. Główne cele porozumienia EFAD

1. Zwiększenie świadomości oraz lepsze zrozumienie pracodawców, pracowników i ich przedstawicieli w kwestii szans i wyzwań w pracy, które wynikają z transformacji cyfrowej.
2. Zapewnienie pracownikom i ich przedstawicielom oraz pracodawcom pomocy w opracowywaniu środków i działań mających na celu wykorzystanie nowych możliwości technologii cyfrowej, a następnie radzenie sobie z wyzwaniami, przy jednoczesnym uwzględnieniu istniejących inicjatyw, praktyk i układów zbiorowych.
3. Zachęcenie do partnerskiego podejścia między pracodawcami i związkami zawodowymi.

II. Etapy tworzenia partnerstwa w celu ułatwienia przejścia przez proces transformacji cyfrowej w przedsiębiorstwie

Przedstawiciele pracowników otrzymają takie udogodnienia i informacje, jakie są niezbędne do skutecznego zaangażowania się na różnych etapach procesu.

Etap 1.

„Wspólna eksploracja/przygotowanie/wsparcie", które dotyczą podnoszenia świadomości i stworzenia warunków oraz atmosfery wsparcia i zaufania. Działania te mają umożliwić otwarte omówienie możliwości i wyzwań/zagrożeń związanych z cyfryzacją, a także ich wpływu na miejsce pracy oraz rozmowy o możliwych działaniach i rozwiązaniach.

Etap 2.

„Wspólne mapowanie/regularna ocena/analiza" to zadanie polegające na mapowaniu obszarów tematycznych pod kątem korzyści i możliwości oraz wyzwań i ryzyk, jakie może przynieść pracownikom i przedsiębiorstwu skuteczna integracja technologii cyfrowych.

Etap 3.

„Wspólny przegląd sytuacji i przyjęcie strategii transformacji cyfrowej", który jest wynikiem pierwszych dwóch etapów. Chodzi tutaj o podstawowe zrozumienie możliwości i wyzwań/ryzyk, różnych elementów składających się na ucyfrowienie firmy i ich wzajemnych powiązań, a także uzgodnienie strategii cyfrowych wyznaczających cele dla przedsiębiorstwa na przyszłość.

Etap 4.

„Przyjęcie odpowiednich środków/działań" opierające się na wspólnym przeglądzie sytuacji. Obejmuje ono: możliwość testowania i pilotowania przewidywanych rozwiązań, ustalenie priorytetów, realizację działań w kolejnych fazach czasowych, wyjaśnienie i zdefiniowanie ról i obowiązków kierownictwa oraz pracowników i ich przedstawicieli, a także zasoby i środki towarzyszące (np. wsparcie eksperckie, monitorowanie).

Etap 5.

„Regularne wspólne monitorowanie/działania następcze, uczenie się, ocena" to wspólna ocena skuteczności działań i dyskusja na temat tego, czy dalsza analiza, podnoszenie świadomości, wsparcie lub inne działania są konieczne.

III. Zakres porozumienia obejmuje:

1. Umiejętności cyfrowe i zabezpieczenie zatrudnienia

Partnerzy społeczni powinni być zainteresowani ułatwianiem dostępu do wysokiej jakości szkoleń i rozwoju umiejętności pracowników. Kluczowym wyzwaniem będzie tutaj określenie, jakie umiejętności cyfrowe i zmiany procesów należy wprowadzić w danym przedsiębiorstwie.

Środki, które należy rozważyć obejmują:

- Zobowiązanie stron do przekwalifikowania się.
- Dostęp do szkoleń i ich organizację, wysoką jakość i skuteczność szkoleń, wprowadzenie możliwości pracy w niepełnym wymiarze i przeznaczenia określonego czasu pracy na szkolenia.
- Jasno określone warunki uczestnictwa, w tym: czas trwania, aspekty finansowe, zaangażowanie pracowników oraz rekompensaty, jeśli szkolenie odbywa się poza czasem pracy.

2. Sposoby podłączania i odłączania się

Obowiązkiem pracodawcy jest zapewnienie bezpieczeństwa i zdrowia pracowników w każdym aspekcie związanym z pracą. Dlatego prawo do odłączania się jest jednym z głównych aspektów niniejszego podręcznika. Namawiamy związkowców, aby określenie pełnej i uzasadnionej jasności, co do oczekiwań pracodawcy wobec pracownika podczas korzystania z urządzeń cyfrowych, wspierać przez rokowania zbiorowe na odpowiednich szczeblach.

Wprowadzanie nowych urządzeń cyfrowych może zapewnić elastyczną organizację pracy z korzyścią dla pracowników i pracodawców. Jednocześnie może to generować poważne ryzyko związane z utrudnionym rozgraniczeniem pracy zawodowej i życia osobistego. Dlatego należy skupić się na zapobieganiu negatywnym zjawiskom, wpływającym na zdrowie i bezpieczeństwo pracowników. Do tego potrzebne jest jasne określenie praw, obowiązków i zadań, w których zasada zapobiegania jest najwyższym priorytetem.

Środki, które należy rozważyć obejmują:

- Szkolenia i inne działania podnoszące świadomość pracowników.
- Tworzenie wśród kierownictwa nowej kultury pracy, która pozwala unikać kontaktu z pracownikiem poza godzinami pracy.
- Dostarczanie jasnych wytycznych na temat istniejących przepisów prawa dotyczących czasu pracy, telepracy oraz pracy mobilnej.
- Skuteczna organizacja pracy, w tym zapewnienie takiej liczby pracowników, która nie wymusza na zatrudnionych pracy po godzinach.
- Odpowiednia rekompensata za dodatkowo przepracowany czas.
- Procedury ostrzegania i wsparcia, które pozwalają na odłączenie się i zabezpieczają przed sankcjami z powodu braku kontaktu z pracownikiem po godzinach pracy.
- Zapobieganie izolacji w pracy.

3. Sztuczna inteligencja i zagwarantowanie zasady kontroli człowieka

Nie ma wątpliwości, że AI będzie miało coraz większy wpływ na ludzką pracę. Dlatego europejskie porozumienie autonomiczne określa pewne zasady i kierunki dotyczące wprowadzania jej na rynek pracy. Ważnym elementem, który powinien być gwarantowany w każdym miejscu pracy, jest kontrola człowieka nad SI, stanowiąca podstawę stosowania robotyki i aplikacji opartych na sztucznej inteligencji. System powinien być legalny i sprawiedliwy, a także przestrzegać norm etycznych, zgodnych z prawami człowieka. Z technicznego i społecznego punktu widzenia powinien być natomiast bezpieczny i transparentny.

4. Poszanowanie godności ludzkiej i inwigilacja

Ze względu na znaczną ingerencję nowoczesnych technologii w proces pracy, istnieje ryzyko, że będzie dochodziło do naruszania podstawowych wartości człowieka pracującego (np. poprzez pobieranie danych wrażliwych – dostęp do pomieszczeń lub dokumentów przez skan odcisku palca, źrenicy czy wszczepiony chip). Technologie takie zwiększają ryzyko naruszenia godności człowieka szczególnie w przypadku osobistego monitorowania. Może to prowadzić do pogorszenia warunków pracy.

Minimalizacja i przejrzystość danych osobowych, wraz z jasnymi zasadami ich przetwarzania, ograniczają ryzyko ingerencyjnego monitorowania i niewłaściwego wykorzystywania danych.

W kontekście zatrudnienia zasady dotyczące przetwarzania danych osobowych pracowników określa rozporządzenie RODO. Również partnerzy społeczni w porozumieniu EFAD przypominają, że art. 88 RODO odnosi się do możliwości ustanowienia w drodze układów zbiorowych bardziej szczegółowych zasad przechowywania danych osobowych pracowników. Ma to zapewnić ochronę praw i wolności pracowników w związku z przetwarzaniem ich danych osobowych w kontekście stosunku pracy.

Środki, które należy rozważyć obejmują:

- Umożliwianie przedstawicielom pracowników rozwiązywania problemów związanych z danymi, zgodami na przetwarzanie danych osobowych, ochroną prywatności i nadzorem.
- Gromadzenie danych w konkretnym i przejrzystym celu. Dane nie powinny być gromadzone ani przechowywane po prostu dlatego, że jest to możliwe lub w nieokreślonym celu.
- Informowanie pracowników, że mogą nie wyrazić zgody na przetwarzanie określonej grupy danych osobowych czy też w każdym momencie wycofać daną wcześniej zgodę.
- Zapewnienie przedstawicielom pracowników udogodnień i narzędzi (cyfrowych), np. cyfrowych tablic ogłoszeń do wypełniania swoich obowiązków.

5. Wdrożenie i działania następcze

Organizacje członkowskie złożą sprawozdanie z realizacji porozumienia komitetowi do spraw dialogu społecznego. W ciągu pierwszych trzech lat od daty podpisania tej umowy, komitet dialogu społecznego został zobligowany do przygotowania i przyjęcia corocznego pakietu podsumowującego bieżące wdrażanie umowy. Pełen raport z podjętych działań wdrożeniowych zostanie przygotowany przez komitet i przyjęty przez europejskich partnerów społecznych w następnych latach. Umowa nie narusza prawa partnerów społecznych do zawierania umów dostosowujących lub uzupełniających w sposób, który będzie uwzględniać szczególne potrzeby zainteresowanych partnerów społecznych.

1.2. Nowe technologie w miejscu pracy – praca wspomagana technologiami (współpracująca) i w pełni zautomatyzowana

Stosunek do robotyzacji zmienia się zarówno z perspektywy przedsiębiorców, jak i samych pracowników. Robot nie pozostaje już jedynie w sferze wyobrażeń, ale występuje jako narzędzie produkcyjne, które może odciążyć człowieka i pomóc mu w rozwiązywaniu konkretnych

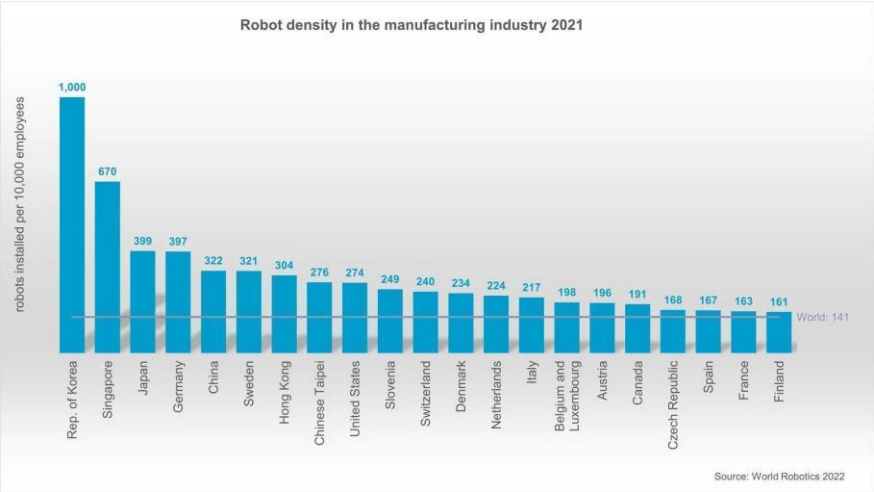
problemów. W zależności od sektora i etapu produkcji, automatyzacja może być wprowadzana jednak w różnym stopniu. Poza poziomem zaangażowania w zadania, roboty można podzielić na wykonujące głównie pracę intelektualną (np. wszelkie narzędzia AI), jak i te odciążające człowieka w powtarzalnych czynnościach (np. pakowanie pro duktów).

Czym jest zautomatyzowany system produkcyjny?

Automatyzacją produkcji nazywamy kierunek rozwoju firm, który polega na znacznym ograniczeniu lub całkowitym zastąpieniu ludzkiej pracy fizycznej i umysłowej pracą maszyn. Początki tego zjawiska sięgają XX wieku, kiedy to w 1913 r. Henry Ford na zawsze zmienił świat dzięki ruchomej linii montażowej, obsługiwanej przez wyspecjalizowanych pracowników. Założeniem takiej pracy było zwiększenie skali produkcji, przy równoczesnym obniżeniu ceny za produkt końcowy.

Obecnie mamy do czynienia z kolejnym etapem ewolucji produkcji – usprawnieniem automatyzacji poprzez digitalizację. Dzięki technologiom, takim jak intuicyjne moduły programowania, tworzenie szczegółowych instrukcji dla robotów staje się coraz łatwiejsze. Zaawansowane czujniki umożliwiają maszynom rozumienie otaczającego ich środowiska i lepszą reaktywność. Według Międzynarodowej Federacji Robotyki (International Federation of Robotics), od 2015 do 2020 r. gęstość robotów[1] prawie podwoiła się na całym świecie, rosnąc z 66 jednostek w 2015 r. do 126 jednostek w 2020 r.

Kraje z najbardziej zautomatyzowaną produkcją (2021 r.)



Źródło: International Federation of Robotics (*The Robot Report*, 2021).

[1] Metryka stosowana przez Międzynarodową Federację Robotyki, mierząca liczbę robotów na 10 tys. pracowników w danej branży.

Praca wspomagana

Z pracą wspomaganą mamy do czynienia w przypadku, gdy pewne czynności w produkcji mogą być zastąpione przez roboty, podczas gdy inne wymagają udziału czynnika ludzkiego. Do wspierania procesów wytwórczych wykorzystuje się najczęściej roboty współpracujące (*collaborative robots*; tzw. co-boty), których zadaniem jest odciążanie pracowników zakładów przemysłowych poprzez wykonywanie części zadań. Ważną cechą odróżniającą tzw. co-boty od standardowych systemów przemysłowych (które zwykle są odseparowane od ludzi), jest to, że w przypadku robotyki współpracującej automatycznie, sterowane systemy robotów współdzielą z ludźmi tę samą przestrzeń pracy.

Sposoby przebiegu współpracy robotów z ludźmi:

1. **Ograniczona interakcja z człowiekiem –** całkowite zatrzymanie się robota, kiedy w wyznaczonym obszarze pojawia się człowiek oraz samodzielnie wznowienie działania po opuszczeniu przestrzeni przez pracownika.
2. **Współpraca z człowiekiem –** dzięki wbudowanym czujnikom co-bot spowalnia działania bądź przerywa pracę, kiedy ktoś znajdzie się w jego pobliżu, co pozwala na bezpieczne współdziałanie człowieka z maszyną.
3. **Prowadzenie ręczne** – co-bot przez cały czas jest sterowany przez operatora. Przykładowo, urządzenie utrzymuje ładunek, gdy człowiek kieruje jego ramieniem.

Praca w pełni zautomatyzowana

Automatyzacja w przemyśle rozumiana jest jako stosowanie technologii do kontrolowania produkcji oraz tworzenia produktów i usług z wykorzystaniem narzędzi cyfrowych. W przypadku pełnej automatyzacji ludzie i maszyny przestają wykonywać dopełniające się zadania i zaczynają działać w tych samych zakresach. Na skutek robotyzacji udział pracowników w procesach produkcyjnych znacznie maleje bądź całkowicie zanika. Wszelkie procesy produkcji stają się w pełni zautomatyzowane, a interwencja człowieka nie jest potrzebna na jakimkolwiek etapie tworzenia produktu.

Pomimo powszechnego lęku wywołanego pogłębiającą się automatyzacją procesów przemysłowych, wprowadzenie tego typu technologii może przynieść korzyści na różnych płaszczyznach związanych z procesami produkcji – m.in. wtedy, gdy praca jest ryzykowna dla życia i zdrowia człowieka.

Dyskusja – czy należy opodatkować pracę robota?

Wraz z malejącymi kosztami automatyzacji procesów produkcyjnych zwiększa się skala robotyzacji przemysłu. Wśród przewidywanych skutków tego stanu rzeczy można wymienić zarówno pozytywne aspekty, takie jak wzrost gospodarczy czy zwiększenie produktywności, jak również negatywne – m.in. redukcję zatrudnienia w różnych gałęziach sektora produkcyjnego.

Przekształcanie się dotychczasowych modeli biznesowych budzi liczne kontrowersje, a przed ustawodawcami państw, w których automatyzacja już teraz rozwinęła się w zaskakującym tempie, stoją nowe wyzwania.

Wobec znacznej redukcji kosztów związanych z zatrudnieniem i osiągania zysków spowodowanych wykorzystaniem robotów w przemyśle, jednym z trudnych do rozstrzygnięcia zagadnień stała się **kwestia podatków nakładanych na pracę robotów**. Jeżeli natomiast chodzi o nabywanie nowych maszyn i urządzeń, poszczególne rządy wykorzystują zachęty podatkowe, które mają sprzyjać cyfrowej transformacji i modernizacji sektora przemysłu. Przykładowo w Polsce od 2022 r. przedsiębiorcom przysługuje możliwość odliczenia nawet do 150% kosztów zakupu maszyn i urządzeń funkcjonalnie z nimi związanych i służących bezpieczeństwu pracy na stanowiskach, gdzie zachodzi interakcja człowieka z robotem.

Pozytywne i negatywne konsekwencje robotyzacji

1. **Gospodarka**

a) **Pozytywne:**

- Możliwość szybszego ulepszania produktów i ich wprowadzenia na rynek.
- Szybszy rozwój nowych technologii.
- Poprawa konkurencyjności firm.

b) **Negatywne:**

- Zwiększenie bezrobocia – zgodnie z szacunkami autorów raportu *Future of Jobs* z 2023 r. (World Economic Forum), w niedalekiej przyszłości maszyny będą wykonywać procentowo więcej zadań aniżeli ludzie. O ile w 2018 r. średnio 71% czasu pracy stanowiły zadania wykonywane z udziałem czynnika ludzkiego, o tyle w 2025 r. proporcje te ulegną istotnej zmianie. Ludzie będą odpowiedzialni za ok. 48% działań, podczas gdy pozostałe 52% będą w pełni zautomatyzowane.

- Zwiększone zużycie energii, a także przyczynienie się do zwiększenia zanieczyszczenia środowiska.

2. **Pracodawca**

a) **Pozytywne:**

- Obniżenie kosztów produkcji.
- Zmniejszenie ryzyka błędów.
- Możliwość lepszego ewidencjonowania wydajności.
- Szybsze wyłapywanie „wąskich gardeł”, co ułatwia optymalizację pracy.
- W niektórych państwach (np. w Polsce) – możliwość odliczenia kosztów zakupu robotów przemysłowych o określonym przeznaczeniu.

b) **Negatywne:**

- Wysokie koszty początkowe instalacji sprzętu.
- Konieczność inwentaryzacji i wysokie koszty napraw.
- Jeżeli procesy są wysoko zautomatyzowane, awarie sprzętu powodują przestoje w produkcji.
- Zmniejszona elastyczność reakcji na nieoczekiwane problemy czy błędy w porównaniu do reakcji pracownika.
- Konieczność zgodności z wymagającymi regulacjami.
- Wysokie koszty zużycia energii.

3. **Pracownik**

a) **Pozytywne:**

- Uproszczenie obsługi procesu produkcyjnego.
- Wsparcie w trudniejszych lub bardziej powtarzalnych czynnościach.
- Wzrost wydajności produkcji przy mniejszym zaangażowaniu pracownika.
- Możliwość poświęcenia czasu na bardziej rozwijające czynności ze względu na oddanie tych powtarzalnych narzędziom automatycznym.
- Pojawienie się nowych miejsc pracy związanych z tworzeniem, obsługą czy naprawą maszyn.

b) **Negatywne:**

- Możliwość utraty pracy ze względu na zautomatyzowanie procesu.
- Wyższe prawdopodobieństwo wypalenia zawodowego wywołane lękiem o utratę pracy.
- W razie awarii maszyn lub niewłaściwego z nich korzystania – narażenie na pogorszenie stanu zdrowia/zagrożenie życia.

1.3. Zapobieganie nieproporcjonalnemu i nadmiernemu nadzorowi w miejscu pracy

Nadzór w miejscu pracy – szanse i zagrożenia

Firmy technologiczne chętnie odpowiadają na rosnące zapotrzebowanie pracodawców w zakresie nowych technologii. Kierunek rozwoju narzędzi AI stwarza natomiast możliwości obejmowania pracowników pełną kontrolą – niezależnie od ich wiedzy i zgody. Istnieją także silne tendencje zmierzające ku zaakceptowaniu nowego stanu rzeczy jako „naturalnej" konsekwencji rozwoju firm.

Szanse:

- monitoring wykorzystywany w sytuacjach zagrożenia i w razie wypadku w pracy może działać na korzyść pracownika (np. w przypadku konieczności udowodnienia, iż stanowisko pracy nie było dostatecznie bezpieczne),
- w niektórych sektorach monitorowanie jest konieczne, aby zapewnić zgodność z przepisami (np. w bankowości może służyć do zapobiegania wykorzystywaniu informacji poufnych),
- nadzór wykorzystywany podczas szkolenia pracownika może przyspieszyć procesy wdrażania go w struktury firmy (np. *wearables* w branży budowlanej stanowią inteligentne kaski z czujnikami wibracji, które ostrzegają pracowników przed potencjalnie niebezpiecznymi obiektami w otoczeniu).

Przykład Stellate

Stellate, start-up z San Francisco zajmujący się analizą danych, posiada zespół pracowników rozproszonych w różnych zakątkach globu. Oprócz narzędzi wykorzystywanych do wspólnej pracy zdalnej, firma monitoruje rozwój swoich pracowników za pomocą programów szkoleniowych i mentoringu. Zamiast kar za nieodpowiednio wysoką wydajność pracownika czy inne niewłaściwe zachowanie, głównym celem tego rodzaju inicjatyw jest promowanie wśród pracowników firmy narzędzi służących do zwiększenia efektywności swojej pracy.

Zagrożenia:

- nadużywanie lub niewłaściwe wykorzystywanie technologii cyfrowych może prowadzić do naruszania prawa do prywatności i ochrony danych osobowych pracowników,
- zagrożenie dla zdrowia psychicznego i fizycznego pracowników z powodu stresu związanego z nadmiernym nadzorem oraz narzuconymi normami pracy,
- utrudnianie zrzeszania się pracowników – śledzenie pracowników i rozpoznawanie nastrojów w firmie pozwala na wyłapywanie ruchów na rzecz zrzeszania się (np. w dużych zakładach pracy zdarza się, że dane pracowników są wykorzystywane do tego, aby rozpoznawać ich nastawienie do pracodawcy i określać, gdzie jest największe prawdopodobieństwo sprzeciwu pracowników wobec polityki firmy).

Główne zasady dotyczące monitoringu w miejscu pracy

Uznaje się, że pracodawcy powinni mieć możliwość nadzorowania miejsc pracy i oceny efektywności swoich pracowników w celu zapewnienia lepszego zarządzania firmą oraz ochrony tajemnicy przedsiębiorstwa, egzekwowania przestrzegania przepisów prawa i zapobiegania popełnieniu przestępstwa przez pracownika. Równocześnie Unia Europejska i poszczególne państwa członkowskie kładą duży nacisk na kwestie prywatności pracowników i poszanowania ich życia osobistego.

Monitorowanie miejsca pracy jest legalne, jednak…[2]

- przed rozpoczęciem korzystania z monitoringu wizyjnego należy szczegółowo określić cele przetwarzania informacji (np. zapewnienie bezpieczeństwa pracowników),
- pracodawca ma obowiązek poinformować osoby, które potencjalnie mogłyby zostać objęte monitoringiem, o tym, że monitoring jest stosowany i jaki obszar jest nim objęty.

Co również ważne, cele, zakres oraz sposób zastosowania monitoringu powinny zostać ustalone w układzie zbiorowym pracy lub w regulaminie pracy, np. w ramach negocjacji zbiorowych. W sytuacji, gdy pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy, zasady te zapisuje się w obwieszczeniu.

Ukryty nadzór wideo jest dozwolony tylko w ograniczonym zakresie w przypadku, gdy istnieje uzasadnione podejrzenie, że popełniono poważne wykroczenie lub przestępstwo, powodujące znaczną szkodę dla pracodawcy.

Pracodawca może ponadto zastosować inne rodzaje monitoringu. Przykładowo mogą być to:

- GPS zamontowany w służbowym samochodzie,
- monitoring internetu i komunikatorów używanych na sprzęcie firmowym,
- geolokalizator służbowego telefonu komórkowego czy laptopa.

Do wszystkich form monitoringu stosuje się odpowiednio przepisy dotyczące monitoringu wizyjnego (np. pracodawca może monitorować pocztę e-mail pracownika tylko po wcześniejszym powiadomieniu o tym pracownika).

Monitoring w pracy a prawo – przykłady z krajów partnerskich

Polska

Zgodnie z polskim Kodeksem pracy, monitoring to szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu.

[2] Zasady dotyczące monitoringu w miejscu pracy wynikające z prawa wspólnotowego (art. 8 Europejskiej Konwencji Praw Człowieka, rozporządzenie RODO), orzeczeń sądów i trybunałów, Kodeksów pracy poszczególnych państwach członkowskich.

Monitoring w Polsce jest dozwolony, jeżeli jest to niezbędne do:

- zapewnienia bezpieczeństwa pracowników,
- ochrony mienia lub kontroli produkcji,
- zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę,
- monitoringu poczty elektronicznej (art. 223 Kodeksu pracy), który jest dozwolony, o ile jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy; monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

Nagrania obrazu pracodawca może wykorzystywać wyłącznie do celów, dla których zostały zebrane i przechowywać przez okres nieprzekraczający trzech miesięcy od dnia nagrania.

Jak prowadzić monitoring w sposób zgodny z prawem? Postępowanie w sześciu krokach

Prowadzenie monitoringu zgodnego z prawem wymaga od pracodawcy ocenienia, jaki wpływ mogą mieć jego działania na pracowników. Poniższe kroki wskazują, na jakich pytaniach powinna opierać się taka analiza.

Kroki	Pytanie	Działanie
Krok 1	Jeżeli wprowadzony został już monitoring, to na czym on w tym momencie polega?	Przeprowadzenie audytu ustalającego, jakie rodzaje monitoringu są wykorzystywane w miejscu pracy oraz kto w organizacji ma uprawnienia do monitorowania pracowników
Krok 2	Dlaczego monitoring jest lub ma być prowadzony?	• Zrozumienie celu monitorowania pracowników. • Dokładne określenie funkcji monitoringu (dane zbierane z konkretnego monitorowania mogą być wykorzystywane wyłącznie do celów, dla których zostały zebrane). **Wyjątek**: jeżeli w trakcie monitoringu organizacja wejdzie w posiadanie informacji o aktywności, której nie można zignorować (np. potencjalna działalność przestępcza, mobbing), zebrane dane mogą posłużyć do pociągnięcia do odpowiedzialności osób odpowiedzialnych

Krok 3	Czy można osiągnąć ten cel bez monitorowania?	• Po zidentyfikowaniu powodu, dla którego ma zostać wprowadzony monitoring, należy określić, czy ten sam cel można osiągnąć bez monitorowania pracowników. **Przykład:** wprowadzenie monitorowania witryn odwiedzanych przez pracowników można zastąpić blokowaniem nieodpowiednich stron lub poprzez umożliwianie pracownikom przesyłania plików jedynie z określonych kont i w ramach określonego rozmiaru
Krok 4	Jeżeli nie można osiągnąć danego celu bez monitorowania, czy istnieje mniej inwazyjny sposób kontroli niż ten aktualnie rozważany?	**Przykład**: sprawdzenie tego, czy pracownicy nie naruszają polityki poufności informacji w firmie może być monitorowane zarówno poprzez kontrolowanie treści e-maili wysyłanych przez pracowników, jak i poprzez automatyczne monitorowanie, polegające np. na sprawdzeniu adresów e-mail i tematyki wiadomości lub blokowaniu wiadomości z załącznikami o określonym rozmiarze

Krok 5	W jaki sposób monitoring będzie wpływał na pracowników?	• Potrzeba odpowiedzi na następujące pytania:
		  ○ Czy monitorowanie można uznać za deprecjonujące lub niesprawiedliwe?
		  ○ Czy monitoring będzie miał wpływ na wzajemne zaufanie pracodawcy i pracowników?
		  ○ Czy jakiekolwiek poufne lub wrażliwe informacje można udostępnić osobom, które nie mają potrzeby biznesowej, by o nich wiedzieć?
		
		Przykład: zespół księgowy może uzyskać informację, że dana osoba była nieobecna w pracy ze względu na zwolnienie chorobowe (aby umożliwić wypłatę zasiłku chorobowego), ale tylko kierownik działu HR musi znać medyczne powody zwolnienia

Krok 6	Czy wprowadzenie monitoringu jest zasadne?	• Podjęcie decyzji, czy wprowadzenie monitorowania jest uzasadnione (łatwiej uzasadnić monitorowanie mniej inwazyjne, o którym powiadomieni są pracownicy). • Przed wprowadzeniem monitorowania można przeprowadzić konsultacje z pracownikami, by wspólnie wypracować uzasadnienie dla monitorowania

Nadzór nad pracownikiem a praca zdalna

Nadzór zatrudnionych osób może odbywać się poprzez instalowanie aplikacji kontrolujących na komputerach pracowniczych, o czym często nie powiadamia się pracowników. Tak zwane oprogramowania bossware[3] mogą rejestrować naciśnięcia klawiszy, robić zrzuty ekranu, a nawet aktywować kamery internetowe pracowników w trakcie pracy zdalnej.

Warto zauważyć, że nieustanna obawa o bycie obserwowanym przez pracodawcę może prowadzić do pogorszenia się stanu psychicznego pracowników. Jak wskazują badania, aż 56% respondentów odczuwa stres i niepokój o to, że pracodawca nadzoruje ich komunikację elektroniczną, 41% stale zastanawia się, czy jest obserwowana, a 32% z tego powodu rzadziej robi sobie przerwy w pracy.

Jak efektywnie kontrolować pracę bez naruszania dobra pracownika?

Wskazówki dla pracodawcy:

- poinformuj pracownika o stosowanych narzędziach nadzoru,
- wyjaśnij zasady stosowania monitoringu i wyznacz jego granice (np. dotyczące rodzaju przetwarzanych danych),
- zamiast nadmiernego nadzoru i wglądu w codzienne czynności pracownika, wprowadź system rozliczalności za efekty (np. cotygodniowy przegląd i ewaluacja zadań),
- wykorzystuj aplikacje służące do monitorowania i zarządzania przepływem zadań (np. Connecteam) oraz usprawniaj zdalną komunikację międzyzespołową i wspólne planowanie.

1.4. Różnica między pracą zdalną a telepracą – wpływ na relacje pracownicze

Według badań Komisji Europejskiej w roku poprzedzającym wybuch pandemii COVID-19 tylko 5,4% osób zatrudnionych w UE-27 pracowało z domu – to udział, który nie zmienił się od 2009 r. Na skutek pandemii odsetek ten wzrósł ponad dwukrotnie, osiągając 12,3%. W niektórych państwach członkowskich liczba ta przekroczyła łącznie nawet 1/4 zatrudnionych osób bez względu na branżę czy sektor gospodarki.

[3] Nazwa pochodzi od angielskich słów *boss* oraz *software* i oznacza oprogramowania dla pracodawców.

Pomimo początkowych trudności z przystosowaniem się do nowej rzeczywistości (spowodowanych przede wszystkim brakiem odpowiedniej infrastruktury teleinformatycznej czy szkoleń w zakresie cyfryzacji procesów pracy), pracownicy nie wyobrażają sobie dziś powrotu do formy pracy sprzed pandemii. Doceniają oni większą elastyczność w pracy, możliwość spędzenia czasu z rodziną oraz wzrost efektywności pracy.

Jednak, pomimo popularności pracy hybrydowej, w dalszym ciągu wielu pracodawców i pracowników decyduje się na powrót do biur. Decyzję taką argumentują poprawą relacji pracowniczych i współpracy, a także możliwością stworzenia środowiska sprzyjającego zbiorowej innowacyjności i lepszej produktywności, oddzielając wyraźnie życie prywatne od zawodowego.

Praca zdalna – podstawowe pojęcia

Wzrost popularności pracy przy użyciu narzędzi cyfrowych i wielość możliwości, które one dają, wymusiły konieczność posługiwania się wachlarzem nowych pojęć. Aby ułatwić odnalezienie się w gąszczu definicji, powstała tabela prezentująca różnice między poszczególnymi trybami pracy.

Rodzaj pracy przy użyciu narzędzi cyfrowych	Definicja
Praca zdalna	Praca zdalna odnosi się do każdej pracy wykonywanej poza siedzibą pracodawcy, niezależnie od zastosowanej technologii. Według nowelizacji polskiego Kodeksu pracy jest to: praca wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą
Telepraca	Telepraca to każda forma organizowania i/lub wykonywania pracy przy użyciu technologii informacyjnych, w kontekście umowy o pracę/stosunku, w której praca, mogąca być wykonywana również w siedzibie pracodawcy, jest regularnie wykonywana poza tą siedzibą
Telepraca w niepełnym wymiarze godzin	Taki układ pracy łączy dni pracy zdalnej z dniami pracy w biurze i został po raz pierwszy zastosowany w praktyce przez Jacka Nillesa na początku lat 70. w USA
Telepraca i praca mobilna oparta na technologiach informacyjno-komunikacyjnych (TICTM)	TICTM odnosi się do wykorzystania technologii informacyjno-komunikacyjnych, takich jak smartfony, tablety, laptopy i komputery stacjonarne do pracy poza siedzibą pracodawcy.

	Obejmuje on wszystkie formy telepracy, ale stara się odróżnić pracę z domu lub stałego miejsca (telepraca) od pracy mobilnej opartej na technologiach informacyjno-komunikacyjnych. Ten ostatni termin jest stosowany w Niemczech dla odróżnienia telepracy wykonywanej w domu od bardziej mobilnej formy pracy
Inteligentna praca/praca zwinna	Inteligentna praca odnosi się do elastycznego systemu pracy, który umożliwia pracownikom wygodną i efektywną pracę bez ograniczeń czasowych i przestrzennych (w dowolnym czasie i miejscu) z wykorzystaniem technologii informacyjno-komunikacyjnych w sieci. Podobny termin („praca zwinna") stosowany jest we Włoszech
Elastyczne warunki pracy	Elastyczna organizacja pracy to alternatywne opcje pracy, które pozwalają na wykonywanie pracy poza tradycyjnymi granicami czasowymi i/lub przestrzennymi standardowego dnia pracy
Praca wirtualna	Praca wirtualna to praca odpłatna lub nieodpłatna, która jest wykonywana przy użyciu kombinacji technologii cyfrowych i telekomunikacyjnych lub produkuje treści dla mediów cyfrowych
Praca hybrydowa	Jest to taki układ pracy, w którym praca może być wykonywana częściowo z siedziby pracodawcy, a częściowo z domu lub innych miejsc

Praca zdalna i telepraca – co na to prawo?

Regulacje na poziomie unijnym

Na ten moment brak wiążących aktów prawnych koncentrujących się na telepracy, choć kilka dyrektyw i rozporządzeń dotyczy kwestii mających zapewnić dobre warunki pracy telepracownikom. Istnieje jednak europejskie *Porozumienie ramowe w sprawie telepracy* (2002). Dokument ten stanowi autonomiczne porozumienie między europejskimi partnerami społecznymi (ETUC, UNICE, UEAPME i CEEP) i zobowiązuje zrzeszone organizacje krajowe do wdrożenia go zgodnie z „procedurami i praktykami" właściwymi dla każdego państwa członkowskiego.

Praca zdalna/telepraca a prawo – przykład Polski

Ustawa z dnia 1 grudnia 2022 r. o zmianie ustawy Kodeks pracy oraz niektórych innych ustaw wprowadziła do polskiego prawa pracy pojęcie pracy zdalnej, jednocześnie uchylając przepisy dotyczące telepracy. Zgodnie z tą nowelizacją praca zdalna **to praca wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą**, w tym pod adresem zamieszkania pracownika, m.in. z wykorzystaniem środków bezpośredniego porozumiewania się na odległość.

Telepraca to natomiast każda forma organizowania i/lub wykonywania pracy przy użyciu technologii informacyjnych, w kontekście umowy o pracę/stosunku, w której praca, **która mogłaby być również wykonywana w siedzibie pracodawcy, jest regularnie wykonywana poza tą siedzibą**. O ile praca zdalna może mieć więc charakter tymczasowy, telepraca co do zasady opiera się na stałym wykonywaniu obowiązków z domu.

Zasady wykonywania pracy zdalnej powinny zostać określone w porozumieniu z organizacjami związkowymi w regulaminie pracy lub w indywidualnym porozumieniu z pracownikiem. Co więcej, pracodawca nie może odmówić pracy zdalnej rodzicom, którzy wychowują dziecko do czwartego roku życia, rodzicom lub opiekunom osób z niepełnosprawnościami lub kobietom w ciąży (chyba że charakter wykonywanych obowiązków na to nie pozwala). Pracodawca ma też obowiązek wyposażyć pracownika w niezbędny sprzęt i narzędzia do wykonywania pracy zdalnej oraz zrekompensować m.in. koszty zużycia energii elektrycznej czy internetu.

Praca zdalna może być wykonywana na wniosek pracownika lub polecenie pracodawcy. Pracodawca może również polecić pracę zdalną w przypadku obowiązywania stanu nadzwyczajnego, stanu zagrożenia epidemicznego lub stanu epidemii oraz z powodu działania siły wyższej, np. zniszczenia miejsca pracy na skutek pożaru czy zalania.

Nowelizacja Kodeksu pracy zawiera również propozycję tzw. okazjonalnej pracy zdalnej, zgodnie z którą na wniosek pracownika będzie on mógł wykonywać pracę zdalną w wymiarze do 24 dni w roku kalendarzowym. Wniosek pracownika dotyczący pracy zdalnej okazjonalnej nie jest jednak wiążący i pracodawca może odmówić jego uwzględnienia.

Co istotne, na pracodawcę został nałożony zakaz dyskryminacji pracownika z powodu wykonywania pracy zdalnej, jak również z powodu odmowy wykonywania takiej pracy. Ponadto pracodawca ma obowiązek umożliwić pracownikowi wykonującemu pracę zdalną przebywanie na terenie zakładu pracy, kontaktowanie się z innymi pracownikami oraz korzystanie z pomieszczeń i urządzeń pracodawcy, zakładowych obiektów socjalnych i prowadzonej działalności socjalnej – na takich samych zasadach, jak w przypadku reszty pracowników.

1.5. Algorytmy a dyskryminacja w miejscu pracy

W świecie napędzanym przez informacje coraz częściej słyszymy o sztucznej inteligencji (*artificial intelligence* – AI), której zastosowania można znaleźć niemal wszędzie. Można spodziewać się, że coraz częściej wykorzystywana będzie ona także w sferze pracy. Zgodnie z badaniami Forbesa, ok. 4 na 5 firm uznaje AI za najwyższy priorytet w swojej strategii biznesowej. Nadziejom na optymalizację kosztów i zwiększenie efektywności w produkcji towarzyszy jednak lęk pracowników o utratę zatrudnienia – jak podaje Forrester w raporcie „Future of Jobs Forecast", liczba miejsc pracy utraconych na rzecz automatyzacji sięgnie 12 milionów w samej Europie do 2040 r.

Pomimo rozbudzania licznych emocji, w debacie publicznej w dalszym ciągu brakuje rzetelnego wyjaśnienia, w jaki sposób działa sztuczna inteligencja oraz czy na pewno każdy rodzaj automatyzacji można zaliczyć do AI. Dla pełnego zrozumienia problemu konieczne jest również zastanowienie się, jaka jest różnica pomiędzy systemem sztucznej inteligencji a algorytmami, ponieważ pojęcia te często używane są naprzemiennie.

AI jest niezwykle szerokim terminem obejmującym grupę algorytmów, które mogą modyfikować swoje parametry i tworzyć nowe algorytmy w odpowiedzi na wyuczone dane wejściowe. Ta zdolność do zmiany, adaptacji i wzrostu w oparciu o nowe dane jest określana właśnie jako „inteligencja".

W najprostszych słowach sztuczną inteligencję można określić więc jako **zdolność maszyn do rozumienia, uczenia się, planowania i wykazywania kreatywności.** Zgodnie natomiast z definicją zaproponowaną przez projekt rozporządzenia w sprawie sztucznej inteligencji (AI Act) system sztucznej inteligencji oznacza oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w rozporządzeniu[4], które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję.

[4] Techniki i podejścia z zakresu sztucznej inteligencji wymienione w rozporządzeniu:

a) mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego,

b) metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) i systemy ekspertowe,

c) podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji.

Algorytm to zestaw instrukcji, a dokładniej formuła obliczeniowa, która autonomicznie podejmuje decyzje na podstawie modeli statystycznych lub reguł decyzyjnych bez wyraźnej interwencji człowieka. Stanowi on sekwencję instrukcji mówiących komputerowi, co ma robić w ramach zestawu precyzyjnie określonych kroków i reguł zaprojektowanych w celu wykonania zadania. Jest to zatem wstępnie ustalony, sztywny, zakodowany sposób postępowania, który zostaje uruchomiony po napotkaniu określonego elementu.

Zagadnieniem należącym do obszaru sztucznej inteligencji jest **samouczenie się** (*machine learning*, ML). Jego głównym celem jest stworzenie systemu działającego automatycznie, który będzie potrafił doskonalić się na bazie doświadczenia w postaci danych oraz zdobywać na tej podstawie nową wiedzę. Proces ten opiera się na znalezieniu wzorca w dostarczonych danych, który ma posłużyć do odpowiedzi na pytanie o nieznany zbiór. Jest to więc swego rodzaju przewidywanie przyszłości za pomocą prawdopodobieństwa i statystyki.

Nie każda sztuczna inteligencja wykazuje się zdolnością samouczenia. Niekiedy algorytm może być bowiem tak napisany, że program, w którym jest umieszczony, wykonuje polecenia bez konieczności uczenia się na nowych danych (jak w przypadku ML).

Przykładem algorytmu, który był już odpowiednio zaprogramowany, był ten, którym dysponował słynny superkomputer IBM Deep Blue. Maszyna ta stała się znana po tym, jak 25 lat temu udało jej się wygrać w szachy z mistrzem Garrim Kasparowem. Deep Blue miał bowiem zapisane wszystkie możliwości ruchów w zależności od ustawienia figur na szachownicy i strategii przeciwnika. Dzięki temu oraz dużej mocy obliczeniowej mógł działać skutecznie w każdej sytuacji.

Przeciwieństwem algorytmu zaimplementowanego w programie IBM Deep Blue, był stworzony przez DeepMind program AlphaGo. Wykorzystując mechanizmy samouczenia się, system ten nauczył się grać w GO (starochińską grę planszową, w której celem jest otoczenie własnymi kamieniami jak największego terytorium na pustej początkowo planszy) i pokonał nawet gracza uznanego za najlepszego na świecie.

Ogólna sztuczna inteligencja to z kolei samoświadomy i dysponujący wszechstronną wiedzą czy umiejętnościami poznawczymi system, zdolny do samodzielnego myślenia i wykonywania zadań. Stworzenie osobliwości technologicznej od lat wzbudza liczne kontrowersje – przede wszystkim dotyczące tego, czy jest to w ogóle możliwe. Zdaniem jednego z czołowych krytyków powstania ogólnej sztucznej inteligencji, filozofa Huberta Dreyfusa, komputery, które nie mają ciała, nie przechodzą okresu dzieciństwa i dojrzewania, a także nie uczestniczą w doświadczeniach kulturowych, nie mogą w ogóle nabyć inteligencji w ludzkim rozumieniu. Jednym z głównych argumentów Dreyfusa było to, że rozwój inteligencji człowieka odbywa się

częściowo w nieświadomy sposób, a zatem nie może być ona wyartykułowana i włączona do programu komputerowego.

Algorytmy w pracy

1. Analiza CV kandydata przy użyciu algorytmu przed nawiązaniem stosunku pracy

Algorytmiczne zatrudnianie polega na wykorzystaniu systemów sztucznej inteligencji i uczenia maszynowego do pozyskiwania kandydatów, rekrutowania, przeprowadzania rozmów kwalifikacyjnych i zatrudniania na stanowiska pracy. Technika ta wykorzystuje wiele kryteriów do oceny kandydata, m.in. jego doświadczenie i wykształcenie, a ponadto często filtruje otrzymane CV, używając słów kluczowych. Algorytmy mogą również pomóc w ocenie bardziej miękkich umiejętności, takich jak skłonność kandydata do szybkiego uczenia się i pracy zespołowej.

Firmy wykorzystujące różne narzędzia AI podczas rekrutacji, chcą w ten sposób zapewnić, że proces prowadzony jest sprawiedliwie. Teoretycznie bowiem, przy pierwszej automatycznej ocenie, nie ma miejsca na działanie czynnika ludzkiego i ewentualną dyskryminację. Systemy te jednak bywają często krytykowane za odzwierciedlanie uprzedzeń osób, które je programowały.

Co ważne, algorytmy nie podejmują ostatecznej decyzji o zatrudnieniu. Mają przede wszystkim zawęzić duże pole kandydatów.

Metody analizowania CV przez algorytm:

- **punktacja CV** – algorytm przyznaje punkty według wcześniej ustalonych przez rekrutera kryteriów,
- **ranking** – porządkowanie CV na podstawie występowania słów kluczowych,
- **dopasowywanie** – identyfikacja słów kluczowych, które pasują do tych z ogłoszenia o pracę,
- **analiza** – algorytm analizuje semantykę CV, wyodrębnia główne informacje i dzieli je na różne kategorie: doświadczenie, umiejętności, dane kontaktowe.

2. Charakterystyka i obszary wykorzystywania algorytmów w miejscu pracy

Rodzaje algorytmów:

- **Opisowe** – służą do rejestrowania zdarzeń przeszłych i analizowania ich wpływu na zdarzenia teraźniejsze, jak np. algorytmy oceny wydajności, mające na celu zebranie różnego rodzaju danych związanych z efektywnością pracownika i wskazanie ogólnej oceny.

- **Predykcyjne** – mają na celu przewidywanie przyszłych zachowań lub szacowanie prawdopodobieństwa wystąpienia zdarzenia (np. przewidywanie wzrostu zapotrzebowania na nowych pracowników).
- **Preskryptywne/zalecające** – ich zadaniem jest wybranie najlepszego scenariusza spośród różnych możliwości i zarekomendowanie określonego działania lub po prostu jego zrealizowanie (np. podejmowanie decyzji dotyczących zasobów ludzkich, przydziału zadań czy harmonogramu).

Wykorzystywanie algorytmów w pracy wiąże się z tzw. **zarządzaniem algorytmicznym**. Odnosi się ono do „systemu kontroli, w którym algorytmom powierza się odpowiedzialność za podejmowanie i wykonywanie decyzji wpływających na pracę, ograniczając w ten sposób udział człowieka i nadzór nad procesem pracy".

Sześć kluczowych funkcji w zakresie zarządzania procesami pracy, do których realizacji wykorzystano algorytmy:

1. Monitorowanie/kontrolowanie pracowników.
2. Ustalanie celów.
3. Zarządzanie wynikami.
4. Tworzenie harmonogramów.
5. Wynagrodzenie.
6. Zakończenie stosunku pracy.

Zwiększenie kontroli pracodawcy nad pracownikami przy pomocy algorytmów

- **Rekomendowanie algorytmiczne** – pracodawcy wykorzystują algorytmy do oceny danej sytuacji oraz wydawania sugestii mających skłonić pracownika do podejmowania czynności wskazywanych przez algorytm.
- **Algorytmiczne ograniczanie** – wykorzystanie algorytmów do wyświetlania tylko niektórych informacji i zezwalania na określone zachowania przy jednoczesnym uniemożliwieniu innych.

Takie wykorzystywanie algorytmów może zwiększać frustrację pracowników, którzy ze względu na konieczność dostosowania się do niezrozumiałych rekomendacji, mogą mieć poczucie zmniejszenia wagi ich głosu.

Algorytmy stosowane do ewaluowania pracy

- **Ewidencja algorytmiczna** – wykorzystanie procedur obliczeniowych do monitorowania, agregowania i raportowania, często w czasie rzeczywistym, szerokiego zakresu precyzyjnie dobranych danych ze źródeł wewnętrznych i zewnętrznych.
- **Technologie obliczeniowe** – wykorzystywane do gromadzenia ocen i rankingów w celu obliczenia pewnej miary wydajności pracowników; także analityka predykcyjna w celu przewidywania ich przyszłej wydajności.

Ewaluacja pracy przy pomocy algorytmów może rodzić określone problemy – nie tylko związane z dyskryminacją, ale również z utratą poczucia prywatności pracowników, bezpieczeństwa informacji itd.

Algorytmy stosowane do wynagradzania

Algorytmiczne premiowanie może dostarczać nagrody w czasie rzeczywistym za zachowania zgodne z wcześniej zdefiniowanymi wytycznymi. Może również wykorzystywać zasady grywalizacji, aby doświadczenie pracy było bardziej pozytywne i rozrywkowe dla pracowników.

Dyscyplina w miejscu pracy

Algorytmiczne zastępowanie (*algorithmic replacing*) polega na szybkim lub nawet automatycznym zwalnianiu z organizacji pracowników osiągających słabe wyniki i zastępowaniu ich wydajniejszymi pracownikami.

Zautomatyzowane podejmowanie decyzji i profilowanie

Artykuł 22 rozporządzenia o RODO stwierdza, że osoba, której dotyczą dane, ma prawo nie podlegać decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołującej wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływające. Prawo do podważenia przez człowieka zautomatyzowanej decyzji dotyczącej jego osoby opiera się na dwóch przesłankach profilowania kwalifikowanego: zautomatyzowanym przetwarzaniu i skutkach prawnych lub czynnikach istotnie wpływających na daną osobę.

Czym jest zautomatyzowane podejmowanie decyzji?

Dzięki skodyfikowanej wiedzy oraz precyzyjnej analizie warunków otoczenia, komputer może wydawać instrukcje bez udziału elementu ludzkiego. Działanie to opiera się na zaawansowanych obliczeniach i wyłącznie technicznych środkach przetwarzania. Tym samym następuje zminimalizowanie udziału człowieka w procesach decyzyjnych, a wyniki podawane są w sposób zautomatyzowany.

Aby jednak przetwarzanie danych zostało uznane za całkowicie zautomatyzowane, w procesie podejmowania decyzji nie może występować żadna ludzka interwencja. Należy zauważyć, że pozorny udział człowieka w podejmowaniu decyzji, polegający np. jedynie na zatwierdzaniu werdyktu wskazywanego przez algorytm, nie będzie stanowić przesłanki do wyłączenia z zakresu stosowania zakazu z art. 22 RODO. Gdyby jednak osoba, mająca uprawnienia i kompetencje do zmiany rozstrzygnięcia, podjęła działania w celu jego modyfikacji, zautomatyzowane podejmowanie decyzji nie będzie miało miejsca.

Jeżeli chodzi o katalog sytuacji objętych art. 22 rozporządzenia o RODO, to jest on szeroki i obejmuje zarówno sytuacje, w których decyzja wywołuje skutki prawne (tj. wpływa na prawa jednostki wynikające z przepisów; np. na prawo do zasiłku dla bezrobotnych) lub ma „podobnie istotny wpływ" (np. dotyczy sytuacji finansowej lub stanu zdrowia danego podmiotu).

Czym jest profilowanie?

W art. 22 RODO uwzględniono także szczególną kategorię zautomatyzowanego podejmowania decyzji, tj. opartego na profilowaniu. Terminem „profilowanie" (art. 4 RODO) określa się dowolną formę zautomatyzowanego przetwarzania danych osobowych polegającą na wykorzystaniu ich do oceny niektórych czynników osobowych osoby fizycznej. W szczególności dotyczy to analizy lub prognozy aspektów dotyczących **efektów pracy tej osoby fizycznej**, jej sytuacji ekonomicznej, stanu zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się[5].

Praktyczne przykłady profilowania:

- **marketing** – tworzenie profili konsumenckich poprzez zbieranie informacji o preferencjach zakupowych i proponowanie przez system produktów indywidualnie dopasowanych do klienta,
- **pożyczki i kredyty** – tworzenie profili kandydatów i uzależnienie pozytywnej decyzji kredytowej od analizy dostarczonych algorytmowi danych osobowych,
- **świadczenia pomocy społecznej** – wykorzystywanie profilowania celem sprawiedliwej alokacji środków pomocy publicznej,
- **rekrutacja i HR** – masowe procesy rekrutacyjne często prowadzone są z wykorzystaniem systemów, które samodzielnie analizują CV oraz inne dane kandydata i na podstawie takiej analizy podejmują decyzje o jego odrzuceniu bądź przyjęciu (np. po przeszukaniu CV

[5] Należy zaznaczyć, że pomimo podobieństw, profilowanie i podejmowanie zautomatyzowanych decyzji to dwie odmienne czynności, które mogą, ale nie muszą być ze sobą powiązane.

według słów kluczowych). W obszarze HR profilowanie wykorzystywane jest także do ewaluacji pracy.

Zagrożenia związane z profilowaniem

- **Naruszanie prywatności i brak transparentności** – o ile wiele osób jest świadomych, że pewnego rodzaju dane (np. medyczne) są szczególnie wrażliwe i powinny być chronione, o tyle część społeczeństwa nie zdaje sobie sprawy z faktu, ile informacji na ich temat można uzyskać z danych behawioralnych wykorzystywanych do niepożądanego profilowania. Co więcej, sam proces profilowania często bywa nietransparentny i niezrozumiały dla osób, których dotyczy.
- **Dyskryminacja** – algorytmy projektowane przez ludzi mogą przenosić uprzedzenia swoich twórców. Tym samym system może mniej korzystnie traktować np. osoby o odmiennych poglądach religijnych, orientacji seksualnej czy kolorze skóry.
- **Ograniczanie różnorodności** – profilowanie ma za zadanie ocenić, scharakteryzować i wyodrębnić grupy odbiorców danych treści po to, by dopasować materiały pod kątem zainteresowań czy przekonań (np. politycznych) danych osób. Uszczupla więc katalog informacji przekazywanych użytkownikowi, ograniczając tym samym różnorodność treści i tworząc tzw. bańki informacyjne oraz zawężając wirtualny horyzont odbiorcy.

Profilowanie w procesie pracy – studium przypadku

Od 2020 r. Austriacka Publiczna Służba Zatrudnienia (AMS) wykorzystuje algorytmiczne profilowanie osób poszukujących pracy, aby zwiększyć skuteczność procesu doradczego i dopasować aktualne programy do potrzeb rynku pracy. System ma na celu klasyfikację osób poszukujących pracy na trzy kategorie:

• Grupa A. Dobre perspektywy na znalezienie pracy w nadchodzącym okresie.

• Grupa B. Przeciętne perspektywy.

• Grupa C. Niskie perspektywy w dłuższej perspektywie.

Następnie, w zależności od przyznanej kategorii, algorytm dopasowuje program pomocowy do potrzeb danej jednostki.

Pytanie do dyskusji: Czy algorytmiczne profilowanie osób bezrobotnych w celu dopasowywania programów wsparcia do ich potrzeb jest uzasadnione?

Przykład: w Nowym Jorku zapowiedziano prawo ograniczające wykorzystanie narzędzi sztucznej inteligencji w procesach rekrutacji. Jak wskazano, głównym problemem występującym w przypadku dokonywania oceny przez sztuczną inteligencję było wykluczanie z procesu grup, które nie pasują do zaprogramowanego klucza. Jako przykład podano dyskwalifikowanie osób z wadą wymowy podczas rozmowy wideo ocenianej przez komputer czy odrzucanie kandydatów z zapaleniem stawów lub innymi schorzeniami ograniczającymi ich sprawność fizyczną (w przypadku testów na czas).

Pytanie do dyskusji: Czy wszelkie rodzaje algorytmicznej oceny w procesie rekrutacyjnym powinny być zakazane?

Przykład: pewien przedsiębiorca pracował nad stworzeniem i wdrożeniem w swojej firmie narzędzia sztucznej inteligencji, które miało pomagać w zatrudnianiu osób odpowiednio przystosowanych do danego stanowiska. Prace zostały wstrzymane w momencie, kiedy firma zdała sobie sprawę z tego, że system dyskryminuje kobiety. Powodem dla częstszego odrzucania damskich profili było opieranie się sztucznej inteligencji na danych z życiorysów osób pracujących w firmie w ostatnich 10 latach (w większości mężczyzn). W konsekwencji komputer ocenił, że powinien traktować mężczyzn priorytetowo, co automatycznie obniżało szanse aplikacji przejawiających cechy żeńskie.

Pytanie do dyskusji: Czy można zidentyfikować inne przykłady dyskryminacji, które mogłyby wystąpić podczas rekrutacji przy zastosowaniu algorytmów profilujących?

Zagrożenia i korzyści płynące z wykorzystywania algorytmów wobec pracowników

Zagrożenia:

- większa kontrola pracodawcy kosztem prywatności pracownika (brak odpowiedniej zgody pracownika),
- erozja ludzkiej autonomii poprzez zastąpienie bezpośredniego kontaktu kierowników z ich podwładnymi, czyli „odczłowieczenie" systemów zarządzania,
- algorytmiczne uprzedzenia i dyskryminacja.

Korzyści:

- zwiększona produktywność dzięki zaoszczędzonemu czasowi i sprawniejszemu podejmowaniu decyzji,
- efektywniejsze planowanie zmian i przydzielanie obowiązków,
- możliwość przeprowadzenia szybszej rekrutacji,

- zrozumienie problemów pojawiających się w miejscu pracy poprzez lepszy wgląd w środowisko pracownicze,
- rzadsze faworyzowanie pracowników i eliminowanie uprzedzeń, jakie mogą mieć miejsce w bezpośrednich relacjach pracowniczych,
- automatyczne podejmowanie decyzji ogranicza możliwość ingerencji w decyzje kierownictwa dotyczące wynagrodzenia, zatwierdzenia urlopu lub przydziału zmiany.

Algorytmizacja relacji pracownik–pracodawca

Algorytmizacja procesów pracy jest już rzeczywistością w wielu firmach. Często jednak działa ona na niekorzyść pracowników w kwestiach, takich jak:

- **Automatyczne zwalnianie pracowników** (zagadnienie do omówienia w ramach dyskusji podczas warsztatów).
- **Algorytmiczne rozliczanie pensji:**
    - Algorytm aplikacji kurierskiej zlecał dostawcom realizację zamówień niezależnie od odległości od punktu odbioru zamówienia. Za dystans do punktu odbioru kierowcy nie otrzymywali wynagrodzenia. Przedsiębiorca pokrywał jedynie koszty przejazdu krótszego dystansu, w wyniku czego, odliczając koszty paliwa i amortyzacji samochodu, kierowcy nie generowali żadnego zysku.
    - Firma podtrzymywała, że zarobki zależą od liczby przejechanych kilometrów, a za każde zamówienie przysługuje stała stawka zwana „stawką podstawową", która może różnić się w zależności od miasta.
    - Problemem jednak była również niepewność pracowników co do stawki godzinowej – w okresie pandemii kurierzy w ciągu jednego dnia otrzymywali informację o zmianie stawki, w konsekwencji czego często zmuszeni byli „dopłacać" zamiast zarabiać za wykonaną pracę.
    - Po strajku obiecano kurierom kilka zmian, w tym m.in. możliwość odrzucenia zlecenia trzy razy dziennie, a nie tylko raz. W przypadku zatem niekorzystnej zmiany stawki podstawowej, kurierzy mają możliwość odmowy realizacji zamówienia. Nie zadeklarowano jednak większej stabilizacji stawki.
- **Algorytmiczna identyfikacja pracowników**
    - Aplikacje taksówkarskie korzystają z oprogramowania służącego do weryfikacji tożsamości swoich kierowców na podstawie przesłanych przez nich selfie. W 2018 r. stwierdzono, że tego rodzaju oprogramowanie, używane przez jedną

z firm, ma skłonności do popełniania błędów w przypadku ciemnoskórych osób (warto podkreślić, że zdecydowana większość kierowców korzystających z aplikacji taksówkarskich to mężczyźni, a wielu z nich pochodzi ze środowisk BAME (*Black, Asian and minority ethnic)*.

- W związku z weryfikacją tożsamości kilkunastu kurierów doniosło, że przez problemy z algorytmem grożono im wypowiedzeniem umowy, zamrożono ich konta lub zwolniono na stałe po tym, jak zrobione przez nich selfie nie przeszło testu *Real Time ID Check*. Niektóre osoby zostały zwolnione po tym, gdy funkcja selfie w ogóle odmówiła działania. Proces ten nie uwzględniał prawa do odwołania.

- **Algorytmiczna ocena (wydajności i nie tylko) pracowników** (zagadnienie do omówienia w ramach dyskusji podczas warsztatów).

Algorytmizacja a ochrona danych osobowych

Jak już wspomniano, algorytm to seria instrukcji mówiących o tym, jak przekształcić zbiór faktów o świecie w przydatne informacje. Mówiąc jeszcze prościej, fakty traktowane są jako dane, zaś informacje to wiedza, którą w dalszej kolejności mogą wykorzystać ludzie lub inne maszyny.

Dane w miejscu pracy i ich ochrona

Aby uniknąć konfliktu na tle prywatności, pracodawcy powinni wdrażać odpowiednie środki ochrony danych osobowych, w szczególności w przypadku wykorzystywania tych danych do zautomatyzowanego podejmowania decyzji, mającego bezpośredni wpływ na pracownika. Koniecznym jest więc odpowiednie wyważenie interesu pracodawcy, któremu zależy na wdrożeniu opartych na danych technologii, jak i dobra osoby, której dane dotyczą oraz działanie zgodne z podstawowymi zasadami wynikającymi z RODO.

- **Pracodawcy powinni gromadzić dane o zatrudnionych tylko wtedy, gdy jest to niezbędne do zarządzania miejscem pracy i wykonywania zadań przez pracowników**

Zgodnie z zasadą minimalizacji ilości danych, pracodawcy powinni ograniczać gromadzenie danych pracowników, tj. wszelkich informacji dotyczących ich tożsamości, zdrowia i biometrii, danych związanych z czynnościami podejmowanymi w miejscu pracy (np. dotyczącymi wydajności), ale też informacji wynikających z aktywności pracowników w mediach społecznościowych. Nieograniczone gromadzenie danych niepotrzebnie naraża pracowników na ryzyka, takie jak chociażby niewłaściwe wykorzystanie danych osobowych przez pracodawców czy ich niekontrolowany wyciek.

- **Pracownicy powinni mieć prawo do wglądu, korekty i pobierania swoich danych**

Pracownicy powinni mieć możliwość otrzymania wszystkich istotnych informacji dotyczących ich danych – w tym informację, dlaczego i jak zostały zebrane ich dane, co zostało wywnioskowane o pracowniku na ich podstawie i czy dane zostały wykorzystane do podjęcia decyzji związanej z jego zatrudnieniem. Pracodawcy powinni być natomiast odpowiedzialni za korektę wszelkich niedokładnych danych.

- **Dane pracowników powinny być chronione przed niewłaściwym wykorzystaniem**

Pracodawca w żadnym wypadku nie powinien zezwalać na sprzedaż lub udzielanie licencji na wykorzystanie danych pracowników osobom trzecim. Gdyby nie to zastrzeżenie, obietnica zysku z monetyzacji danych o pracownikach stwarzałaby zbyt duże ryzyko, iż pracodawcy będą korzystać z danych w sposób niewłaściwy w celu dodatkowego zarobku.

- **Zgoda na przetwarzanie danych osobowych**

W relacjach pracowniczych zgoda na przetwarzanie danych osobowych wzbudza wiele kontrowersji, ponieważ ze względu na brak równowagi stron, łatwo zakwestionować dobrowolność udzielenia tej zgody przez pracownika. Należy zauważyć, że pracodawca mógłby z łatwością wymusić na pracowniku dostosowanie się do jego oczekiwań pod groźbą negatywnych konsekwencji związanych z zatrudnieniem. Jednak zgodnie z art. 155 RODO, państwa członkowskie mogą wprowadzić szczegółowe regulacje dotyczące przetwarzania danych osobowych pracowników w kontekście zatrudnienia, a w szczególności warunki, w oparciu o które można przetwarzać dane osobowe za zgodą pracownika.

Przykładowo, w Polsce pracodawca może zbierać dane osobowe wymienione w Kodeksie pracy, jeżeli pracownik na to przystanie. Należy jednak zaznaczyć, że zgoda powinna być udzielona dobrowolnie, a zatem nie będzie skuteczna, jeżeli pracownik nie będzie miał możliwości odmowy jej udzielenia w obawie, że spotkają go z tego tytułu negatywne konsekwencje. Co więcej, może ona zostać odwołana w każdym czasie.

Rodzaje danych wykorzystywanych na różnych etapach pracy

Etap I. Poszukiwanie pracy

Czego może oczekiwać pracodawca?

Pracodawca może oczekiwać od kandydata przekazania mu podstawowych danych, niezbędnych do podjęcia działań zmierzających do zawarcia umowy. Mogą być to dane:

- identyfikacyjne (imię, nazwisko, imiona rodziców, data urodzenia),

- kontaktowe wskazane przez taką osobę;
- dotyczące wykształcenia, umiejętności, doświadczenia zawodowego (o ukończonych szkołach oraz studiach, przebytych szkoleniach i kursach, poprzednich pracodawcach, zajmowanych stanowiskach oraz obowiązkach zawodowych).

Co ważne, w przypadku uczestnictwa w procesie rekrutacji, pomimo przekazania danych, do zawarcia umowy wcale nie musi ostatecznie dojść.

Czego może oczekiwać kandydat?

Już na pierwszym etapie rekrutacji potencjalny pracodawca, który zbiera dane od kandydatów, jest zobowiązany poinformować te osoby o:

- pełnej nazwie i adresie siedziby firmy,
- danych kontaktowych inspektora ochrony danych (o ile go wyznaczył),
- celu przetwarzania danych oraz podstawie prawnej ich przetwarzania, znanych mu w chwili gromadzenia danych odbiorcach danych (rozumianych szeroko) lub ich kategoriach,
- zamiarze transgranicznego przetwarzania danych (o ile taki istnieje),
- okresie, przez który dane będą przetwarzane bądź kryteriach ustalania tego okresu,
- przysługującym kandydatowi prawie żądania dostępu do danych, w tym otrzymania ich kopii, a także ich sprostowania, usunięcia lub ograniczenia ich przetwarzania,
- prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem do przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli dane są zbierane na podstawie zgody),
- prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
- dobrowolności lub obowiązku podania danych i konsekwencjach ich niepodania.

Etap II. Proces rekrutacji

Podczas rozmowy kwalifikacyjnej rekruter może zadawać wiele szczegółowych pytań w zakresie informacji, jakie kandydat na pracownika zamieścił w swoim CV. Ważne jednak, aby odnosiły się one wyłącznie do kwestii związanych ze stanowiskiem, na które ten aplikuje. Niedopuszczalne są pytania, które mogą zawstydzić kandydata, naruszyć jego prawo do prywatności bądź dobra osobiste (np. dotyczących życia prywatnego, wyznania, orientacji seksualnej, przekonań politycznych itp.).

Czas przechowywania danych

Okres przechowywania danych kandydata powinien być zgodny z zasadami przetwarzania danych z góry określonymi przez administratora. Co do zasady pracodawca powinien więc trwale usunąć dane osobowe kandydata, z którym nie zdecydował się zawrzeć umowy o pracę, niezwłocznie po zakończeniu procesu rekrutacji, tj. po podpisaniu umowy o pracę z nowo zatrudnionym pracownikiem (np. poprzez usunięcie bądź odesłanie danych).

Etap III. Okres zatrudnienia

Wraz z nawiązaniem stosunku pracy, zarówno po stronie pracodawcy, jak i pracownika, rodzą się określone prawa i obowiązki. Ich realizacja w sposób oczywisty wiąże się z koniecznością przetwarzania danych osobowych pracownika. Administrowanie danymi osobowymi, choć zasadniczo uregulowane w rozporządzeniu o RODO, w przypadku pracy doprecyzowane jest dodatkowo w przepisach krajowych.

Przykładowo w Polsce, zgodnie z art. 221 § 2 i 4 Kodeksu pracy, pracodawca ma prawo żądać od pracownika, którego zdecydował się zatrudnić, podania (niezależnie od danych osobowych, które mógł od niego pozyskać w toku rekrutacji) także:

- adresu zamieszkania,
- numeru PESEL,
- innych danych osobowych, m.in. imion i nazwisk oraz dat urodzenia jego dzieci, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez niego ze szczególnych uprawnień przewidzianych w prawie pracy,
- wykształcenia i przebiegu dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie,
- numeru rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

Obowiązki informacyjne pracodawcy względem pracownika

Ponieważ dane pracownika pracodawca będzie przetwarzał w innym celu niż w przypadku kandydata, pracownik powinien uzyskać informacje w tym zakresie. Cel ten można spełnić poprzez umieszczenie takiej informacji w klauzuli informacyjnej przekazywanej kandydatom w toku rekrutacji poprzez uzupełnienie jej o informacje dotyczące celu przetwarzania danych i wskazanie odbiorców danych w razie zatrudnienia kandydata lub też poprzez uzupełnienie tych informacji tuż po zatrudnieniu pracownika.

Kontrola algorytmów wykorzystywanych w pracy (transparentność algorytmów)

Przytoczone dalej przykłady wykorzystania sztucznej inteligencji w miejscu pracy pokazują, że niekontrolowane wykorzystywania narzędzi AI przez firmy może prowadzić do wzrostu niepewności zatrudnienia, a tym samym wywierać negatywny wpływ na życie pracowników. Równocześnie, zgodnie z szacunkami McKinsey Global Institute, aż 70% firm wdroży pewne formy systemów sztucznej inteligencji do 2030 r. Z tego względu tak ważne jest, aby krytycznie oceniać nowe technologie i umożliwiać organom nadzoru i niezależnym organizacjom przeprowadzanie audytów w zakresie AI.

- W Wielkiej Brytanii wykorzystywane przez pocztę krajową oprogramowanie Horizon fałszywie posądzało poszczególnych pracowników o kradzież nawet kilkudziesięciu tysięcy brytyjskich funtów. Na skutek błędu sztucznej inteligencji aż 736 pracowników poczty zostało oskarżonych, a części z nich postawiono zarzuty i skazano.
- W Holandii kierowcy jednej z aplikacji taksówkarskich pozwali firmę po tym, jak algorytm zablokował ich konta za rzekome dopuszczanie się oszustw. Sąd odrzucił ich roszczenia, ponieważ stwierdził, iż naruszenia nie mieszczą się w zakresie definicji w pełni zautomatyzowanego podejmowania decyzji przewidzianego w RODO. W efekcie pracownicy zostali pozostawieni bez jakiejkolwiek ochrony prawnej.
- We Włoszech sąd nakazał jednej z firm dowożących jedzenie ujawnienie algorytmu aplikacji i wyeliminowanie elementów, które ze względu na brak uwzględnienia kwestii regulowanych w prawie pracy (takich jak np. zwolnienia lekarskie czy prawo do strajku), czyniły go dyskryminującym.

Algorytm a tajemnica przedsiębiorstwa

Zgodnie z prawem unijnym, informacje na temat technologii lub jakichkolwiek innych aspektów dotyczących firmy mogą być chronione jako tajemnica przedsiębiorstwa. Muszą jednak spełniać następujące warunki:

- informacje o algorytmie nie są znane powszechnie ani wśród ekspertów z danego sektora,
- informacje o algorytmie mają wartość handlową,
- podjęto działania, aby zapewnić poufność informacji, np. przechowywane są one w bezpiecznym miejscu i każdy, kto ma do nich dostęp lub komu udostępniane są te informacje, podpisał umowę o poufności.

W przypadku nowych technologii wykorzystywanych w procesach pracy, spełnienie tych przesłanek nie jest trudne. Firmy często powołują się na tajemnice handlowe, podkreślając swoje obawy o utratę konkurencyjności wskutek ujawnienia ich wewnętrznych systemów. Z tego

względu wgląd w algorytmy i weryfikowanie narzędzi AI w sektorze prywatnym są szczególnie problematyczne. Co więcej, dodatkowe formy zabezpieczeń prawnych w postaci klauzul poufności zapobiegają przekazywaniu przez osoby z wewnątrz (obecnych lub byłych pracowników) informacji na temat mechanizmów koordynujących ich pracę.

Akt w sprawie sztucznej inteligencji (AI Act)

Wielokrotne oskarżenia sztucznej inteligencji o powielanie uprzedzeń, niedokładność czy dyskryminowanie przez algorytmy poskutkowały tym, że Komisja Europejska podjęła się wprowadzenia regulacji mającej za zadanie kontrolować narzędzia sztucznej inteligencji i zapobiegać negatywnym skutkom ich wykorzystania.

12 kwietnia 2021 r. KE przedstawiła projekt unijnego rozporządzenia w sprawie sztucznej inteligencji – pierwszego tak kompleksowego aktu prawnego dotyczącego narzędzi AI. Celem regulacji jest zapewnienie odpowiedniego środowiska do rozwoju sztucznej inteligencji w Unii Europejskiej, przy równoczesnym uwzględnieniu zagrożeń związanych z rozwojem najnowszych technologii. Przede wszystkim jednak AI Act ma sprawić, że algorytmy wdrażane na terenie UE staną się bezpieczne, przejrzyste, etyczne, bezstronne i będą kontrolowane przez ludzi.

Podejście oparte na ryzyku

Głównym założeniem aktu jest określenie ryzyka, jakie stwarza dany system sztucznej inteligencji oraz uzależnienie od niego, jakim obowiązkom regulacyjnym i wymogom podlegać będą zarówno twórcy, jak i podmioty wdrażające AI.

- **Niedopuszczalne ryzyko** – zakaz stosowania AI

Zakaz szczególnie szkodliwych, sprzecznych z wartościami UE zastosowań sztucznej inteligencji, które stwarzają ryzyko naruszenia praw podstawowych jednostki, np.: dokonywania oceny obywateli (tzw. *social scoring*), wykorzystywania słabości określonej grupy osób ze względu na wiek, niepełnosprawność ruchową lub zaburzenie psychiczne, stosowania technik podprogowych, wykorzystywania identyfikacji biometrycznej w przestrzeni publicznej i do celów egzekwowania prawa (poza kilkoma wyjątkami).

- **Wysokie ryzyko** – AI dopuszczalne, ale pod pewnymi warunkami

Jako systemy o wysokim ryzyku zaklasyfikowano narzędzia mające negatywny wpływ na bezpieczeństwo ludzi lub ich prawa podstawowe, tj. systemy z następujących obszarów:

  - identyfikacja biometryczna i kategoryzacja osób fizycznych,
  - zarządzanie infrastrukturą krytyczną,

- kształcenie lub szkolenie zawodowe – możliwość decydowania o dostępie do kształcenia i szkolenia zawodowego danej osoby (np. ocenianie egzaminów),
- bezpieczeństwo produktów (np. zastosowanie sztucznej inteligencji w chirurgii wspomaganej robotami),
- zatrudnianie, zarządzanie pracownikami i dostęp do samozatrudnienia (np. oprogramowanie do analizowania CV na potrzeby procedur rekrutacji),
- podstawowe usługi prywatne i publiczne (np. ocena zdolności kredytowej, scoring kredytowy),
- egzekwowanie prawa – kolizja z prawami podstawowymi osób (np. weryfikacja autentyczności dokumentów),
- zarządzanie migracją, azylem i kontrolą granic (np. ocenianie wniosków o udzielenie azylu),
- sprawowanie wymiaru sprawiedliwości i procesy demokratyczne (np. sugerowanie rodzaju kary i wymiaru kary dla osoby skazanej za przestępstwo).

Przykłady szczególnych wymagań względem systemów wysokiego ryzyka:

- **Wymogi dotyczące transparentności** – działanie systemów AI wysokiego ryzyka powinno być wystarczająco przejrzyste, aby umożliwić użytkownikom interpretację dotyczących ich wyników. Dla systemów AI wysokiego ryzyka powinny być opracowywane instrukcje użytkowania.
- **Obowiązkowy nadzór człowieka nad systemami wysokiego ryzyka** – konieczne zapewnienie ludziom skutecznego nadzoru nad AI wysokiego ryzyka, w tym zrozumienie możliwości i ograniczeń danego systemu sztucznej inteligencji. Odpowiednie środki nadzoru mogą obejmować podjęcie decyzji o nieużywaniu systemu AI w danej sytuacji, zignorowanie decyzji podjętej przez system AI lub przerwanie działania systemu za pomocą przycisku STOP.

Kwestie pracy podniesione w akcie AI w sprawie sztucznej inteligencji

Systemy wysokiego ryzyka, mające wpływ na rynek pracy i podlegające szczególnemu nadzorowi, zostały wymienione w Załączniku III do projektu aktu w sprawie sztucznej inteligencji. Są to systemy AI:

1. Stosowane w procesie rekrutacji lub wyboru konkretnych osób, a w szczególności te wykorzystywane do publikowania ofert pracy, wstępnej selekcji lub odfiltrowywania aplikacji, oceny kandydatów podczas rozmów kwalifikacyjnych lub testów.

2. Podejmujące decyzje o czyimś awansie bądź zwolnieniu z pracy, wyznaczające podział zadań oraz monitorujące efektywność pracowników i ich zachowania.
3. Decydujące o dostępie do szkolenia zawodowego lub oceniające uczestników szkolenia.

Jak stwierdzono, wymienione wcześniej systemy sztucznej inteligencji mogą mieć istotny wpływ na perspektywy zawodowe osób, których dane przetwarzają, a tym samym mogą rzutować na ich źródło utrzymania i wysokość dochodów. Komisja Europejska zwróciła także uwagę na to, że systemy źle zaprojektowane i wykorzystywane, mogą utrwalać dyskryminacyjne wzorce (np. względem kobiet, osób starszych, niepełnosprawnych, o odmiennym pochodzeniu rasowym, etnicznym czy innej orientacji seksualnej). Co więcej, systemy AI używane do sprawdzania wydajności (w szczególności te oparte na biometrii) mogą mieć wpływ na ochronę danych osobowych i prawo do prywatności. Z tego względu powinny być objęte szczególnie restrykcyjnymi wymogami, a pracownicy zawsze powinni dysponować ścieżką odwoławczą od decyzji algorytmu.

Krytyka AI Act

W odniesieniu do stosowania AI Act w przypadku kwestii dotyczących zatrudnienia pojawiło się także wiele głosów krytycznych. Jak twierdzą eksperci, w rozporządzeniu zbyt mało uwagi poświęcono kwestiom pracowniczym, a kontrola przejrzystości algorytmów sprowadza się do ogólnych wymogów transparentności wymienionych w art. 52 projektu regulacji. Co więcej, wątpliwym jest, aby rozporządzenie weszło w życie jeszcze przed rokiem 2025.

Lęk przed utratą pracy z powodu algorytmizacji/robotyzacji

Zgodnie z szacunkami McKinsey, do 2030 r. automatyzacja w różnych gałęziach gospodarki doprowadzi do konieczności przekwalifikowania się aż 375 milionów pracowników. Nieco inne prognozy, choć równie niepokojące, przedstawiło w swoim raporcie Światowe Forum Ekonomiczne, które w publikacji *Future of Jobs* wskazało, że postępy w obszarach algorytmizacji i technik obliczeniowych mogą spowodować, w najbliższych latach na świecie maszyny mogą zastąpić 75 milionów stanowisk pracy.

Jeżeli chodzi o skutki robotyzacji, można zakładać, że najbardziej odczują je osoby wykonujące pracę fizyczną, zwłaszcza tę opartą na przewidywalnych sekwencjach. Automatyzacja może jednak negatywnie wpłynąć także na sytuację niektórych specjalistów. Według przytoczonego raportu *Future of Jobs*, pośród wypieranych przez AI zawodów, takich jak mechanik, magazynier i kierownik produkcji, znajdziemy także profesję prawnika czy analityka finansowego. Co więcej, skutki automatyzacji odczują osoby, których zawody polegają na zbieraniu i procesowaniu danych, czyli zadaniach wykonywanych znacznie szybciej i precyzyjniej przez maszyny.

Aż 60% pracowników świadkami tego, że 1/3 zadań w ich obecnej pracy ulega automatyzacji. Nie powinno więc dziwić, że zatrudnieni martwią się o swoje dotychczasowe posady. Jak wynika z raportu Procontent Communication *Pandemia automatyzuje Polskę?*, prawie co piąty badany (18,7%) obawia się zautomatyzowania jego stanowiska, a w dalszej kolejności utraty pracy. Jednak eksperci studzą obawy – patrząc globalnie, jedynie 5% zawodów może zniknąć całkowicie. Co więcej, choć wiele posad zostanie wypartych przez maszyny, to można spodziewać się, iż w ich miejsce pojawią się nowe profesje związane ze wzrostem popytu na umiejętności miękkie, które wymagają kreatywności, inteligencji emocjonalnej i krytycznego myślenia.

Ponadto, rozwój technologii będzie przyczyniał się do ciągłego tworzenia nowych, wysoko opłacanych stanowisk w sektorze IT – w skali globalnej może to być aż 50 milionów miejsc pracy do końca dekady. Powyższe optymistyczne podejście zdaje się potwierdzać wspomniana już analiza Światowego Forum Ekonomicznego, w której wskazano, iż wraz z postępującą automatyzacją, pojawi się nawet 133 milionów miejsc pracy. O ile ze względu na dynamizm wywoływanych digitalizacją zmian trudno jest precyzyjnie określić kształt przyszłego poziomu zatrudnienia, o tyle zgodnie z oceną ekspertów wątpliwym jest, aby w najbliższym czasie mogło wystąpić zjawisko technologicznego bezrobocia strukturalnego.

Technologia w służbie inkluzywności

Digitalizacja miejsc pracy przyczynia się do skuteczniejszego włączania w rynek pracy tych grup społecznych, które wcześniej były czasowo lub permanentnie z niego wykluczane.

W przypadku **osób z niepełnosprawnościami** zaobserwować można następujące korzyści:

- brak utrudnień związanych z transportem na miejsce pracy, z jakimi wcześniej borykały się osoby o pewnych ograniczeniach fizycznych,
- mniejsza ekspozycja na bodźce i spokojniejszy tryb pracy zdalnej sprzyjają efektywniejszej pracy osób z niepełnosprawnością intelektualną, nadpobudliwością bądź mających trudności ze skupieniem i uczeniem się,
- korzystanie z środków telekomunikacji elektronicznej (e-mail, komunikatory) pozwala na aktywny udział w dyskusji osób cierpiących na wady wymowy.

Przykłady korzyści dla **rodziców**:

- możliwość spędzania większej ilości czasu z dziećmi,
- zmniejszenie ekspozycji całej rodziny na popularne choroby zakaźne (grypa, przeziębienie, COVID-19),

- możliwość efektywnego godzenia życia prywatnego i zawodowego przez młodych rodziców.

Praca zdalna ma także duży wpływ na pozostawanie na rynku pracy młodych matek (aż 49% pracujących mam przyznaje, że zna przynajmniej jedną osobę, która rzuciła pracę lub planuje to zrobić ze względu na wymóg powrotu do biura).

Przykłady korzyści płynących z wykorzystania **aplikacji taksówkarskich**:

- działanie na rzecz równości płci (w większości amerykańskich miast kobiety stanowiły dotychczas mniej niż 5% taksówkarzy, w przypadku aplikacji gospodarki współdzielenia jest to już ok. 20–30%),
- ułatwianie wejścia na rynek pracy imigrantom (np. z Ukrainy),
- oferowanie bardziej przystępnych cenowo przejazdów – przykładowo aplikacja Uber w Los Angeles jest dostępna w 21 dzielnicach o niskich dochodach, gdzie umożliwia znacznie tańsze przejazdy niż tradycyjne firmy taksówkarskie.

1.6. Wpływ nowych technologii na relacje kontraktualne – dyskusja wokół smart contracts i ich przyszłego zastosowania w relacji pracownik–pracodawca

Cyfryzacja objęła już niemal wszystkie obszary naszego życia codziennego i prywatnego. Dotyczy to również relacji kontraktualnych zawieranych dotychczas ustnie lub na piśmie, które teraz często wzmacniane są lub uzupełniane przy użyciu narzędzi cyfrowych. Z uwagi na ogromną ilość informacji w sieci i coraz częstsze zawieranie wzajemnych zobowiązań z udziałem elementu cyfrowego, w najbliższej przyszłości największy wpływ na relacje kontraktualne z pewnością będą miały narzędzia wykorzystujące technologię blockchain, m.in. inteligentne kontrakty (*smart contracts*).

Czym jest blockchain?

Łańcuch bloków (ang. *blockchain*) to technologia służąca do przesyłania oraz przechowywania informacji o transakcjach zawartych za pośrednictwem internetu. Poszczególne informacje układane są w kolejnych blokach danych. Po nasyceniu bloku określoną liczbą transakcji, kolejne informacje o transakcjach zapisują się w następnym bloku. Dzięki odwołaniu do poprzedniego bloku i łańcuchowemu połączeniu informacji w nich zawartych, niemożliwe staje się zmienienie lub usunięcie zapisu jednej transakcji bez odnotowania takiej zmiany we wszystkich pozostałych

blokach. Rozwiązanie to sprzyja transparentności dokonywanych transakcji i przeciwdziała oszustwom w zakresie manipulowania informacjami.

Czym są *smart contracts*?

Inteligentny kontrakt to „samowykonujący się" program oparty na logice *if-then*. Jest napisany całkowicie w języku programowania i może działać za pomocą technologii rozproszonego rejestru (DLT) czy blockchain. W tym drugim przypadku program jest przechowywany na blockchainie i uruchamia się, gdy określone warunki wyzwalają kolejne działanie – np. może on wywołać płatność lub dostarczyć określoną usługę. Jest to więc **połączenie rzeczywistości wykreowanej na podstawie danej umowy ze światem rzeczywistym za pomocą technologii.** Dzięki temu umowa jest bardziej przejrzysta i wiarygodna, zapewniając stronom pewność co do wykonania jej warunków, gdy zaistnieje określona sytuacja.

Przykłady wykorzystania inteligentnych kontraktów:

- Zakup nieruchomości – dzięki inteligentnym kontraktom proces, który zwykle jest bardzo złożony i wymaga zaangażowania wielu pośredników (notariusz, agent nieruchomości, radca prawny, instytucja udzielająca kredytu), ulega znacznemu uproszczeniu i nie wymaga udziału wyżej wymienionych podmiotów, umożliwiając zdobycie tytułu własności w postaci elektronicznej.
- Zakupy online – w tym przypadku inteligentne kontrakty zapewniają natychmiastowe wykonanie płatności, a w związku z tym szybsze przesłanie produktu do kupującego.
- Przetwarzanie danych osobowych – z uwagi na zapisywanie danych osobowych i cyfrowych ID na blockchainie, ryzyko kradzieży tożsamości jest znacznie mniejsze.
- Rejestrowanie wyników wyborów lub referendów – minimalizacja ryzyka fałszowania wyników głosowania. Zastosowanie inteligentnych kontraktów w tym celu można w praktyce obserwować m.in. w Estonii.
- Wypłacanie odszkodowań i opłacanie składek – automatyczne rozliczanie szkód, obliczanie wysokości składek.

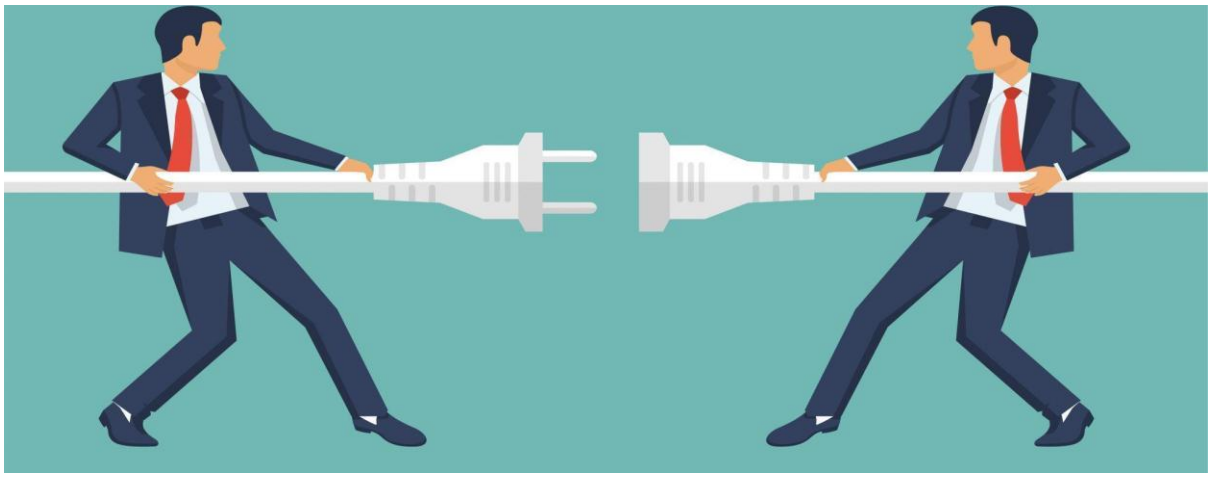
2. Wpływ cyfryzacji na życie prywatne pracowników

2.1. Ochrona czasu pracy pracowników w pracy zdalnej. Praca zdalna a work-life balance

Jak wynika z badań Eurofound, 1/3 pracowników w Unii Europejskiej zaczęła pracować z domu w czasie pandemii, a w związku z przejściem na tryb pracy zdalnej, aż 27% z nich zadeklarowało wykonywanie obowiązków służbowych w czasie wolnym. Podczas lockdownu granica pomiędzy życiem prywatnym a zawodowym zaczęła się zacierać. Pracownicy zyskali możliwość samodzielnego organizowania swojego czasu, ale zostali też wystawieni na ryzyko bycia ciągle dostępnym oraz braku możliwości całkowitego odłączenia się od elektronicznych środków przekazu poza godzinami pracy.

Co istotne, w trybie zadaniowym (nieopartym na sztywnych godzinach pracy) obowiązują takie same zasady, jak w systemie tradycyjnym, tj. zatrudniony powinien wykonywać swoje obowiązki przez 8 godzin na dobę w ciągu pięciodniowego tygodnia pracy. Zadania wykonywane poza tymi ramami powinny być uznawane za pracę w nadgodzinach. O ile jednak elastyczny czas pracy jest niewątpliwie korzystny dla zatrudnionych, o tyle często błędnie sądzą oni, że skoro nie przebywają w biurze w stałych godzinach, to powinni wykazywać się dostępnością o każdej porze dnia.

2.1.1. Prawo do odłączenia się



Źródło: Shutterstock.

Jak stanowi przepis art. 24 Powszechnej Deklaracji Praw Człowieka, każdy człowiek ma prawo do odpoczynku i czasu wolnego, włączając w to rozsądne ograniczenie godzin pracy i okresowe płatne urlopy. Co więcej, zgodnie z art. 31 Karty Praw Podstawowych, każdy pracownik ma prawo do warunków pracy szanujących jego zdrowie, bezpieczeństwo i godność oraz uprawniony jest do okresów dziennego i tygodniowego odpoczynku, do corocznego płatnego urlopu, a przede wszystkim do ograniczenia maksymalnego wymiaru czasu pracy.

Nowa, postpandemiczna rzeczywistość, w której często zatarciu ulega granica między życiem prywatnym a zawodowym, uwydatniła potrzebę wdrożenia regulacji dającej pracownikom pewność, że mogą wylogować się z pracy i nie odpowiadać na maile przełożonych po godzinach bez negatywnych konsekwencji. Z tego względu, w roku 2021 Parlament Europejski przyjął rezolucję opowiadającą się za prawem do odłączenia, wzywając tym samym Komisję Europejską, aby zajęła się przygotowaniem dyrektywy w sprawie prawa do bycia offline.

Warto zauważyć, że rezolucje Parlamentu Europejskiego nie mają mocy wiążącej. Tym samym Komisja Europejska nie jest zobowiązana do podjęcia działań w zakresie implementacji dyrektywy zaproponowanej przez Parlament. Jednakże, mając na uwadze istotę sprawy, można spodziewać się, że Komisja będzie dążyć do uregulowania prawa do odłączenia się i zapewnienia jednolitego poziomu ochrony pracowników w całej Unii Europejskiej.

W kształcie zaproponowanym przez Parlament Europejski dyrektywa w sprawie prawa do bycia offline ma gwarantować:

1) minimum zasad gwarantujących pracownikom, którzy wykorzystują w codziennej pracy środki umożliwiające komunikowanie się na odległość, prawo do bycia offline,
2) zakaz dyskryminacji lub mniej korzystnego traktowania pracowników (w tym zakaz rozwiązywania umów o pracę) korzystających z prawa do odłączenia,
3) równe traktowanie wszystkich pracowników, zarówno tych z sektora publicznego, jak i prywatnego, pracowników niższego szczebla i kadry menedżerskiej (choć w ostatnim przypadku może być to utrudnione, z uwagi na szczególne regulacje dotyczące kadry kierowniczej),
4) sprawną procedurę sądową i możliwość dochodzenia roszczeń związanych z naruszeniem przyznanych praw (dostęp do ochrony sądowej przed reperkusjami).

Obowiązki pracodawców w związku z prawem pracowników do bycia offline

Nowe uprawnienia dla pracowników wiążą się także z dodatkowymi obowiązkami po stronie pracodawców. Należy do nich m.in. konieczność zapewnienia wewnętrznego systemu umożliwiającego precyzyjny pomiar czasu przepracowanego każdego dnia przez pracownika

(z poszanowaniem prawa do prywatności i ochrony danych osobowych). Co więcej, ważną kwestią jest także wspieranie pracowników w byciu offline – jasne komunikowanie nowego prawa w polityce firmy, prowadzenie szkoleń i kampanii informacyjnych w tym obszarze. Jednak w zakresie podnoszenia świadomości najistotniejszy i najbardziej obiecujący wydaje się obowiązek pisemnego poinformowania każdego z pracowników o jego prawach.

Dodatkowo, pracodawcy powinni unikać promowania kultury ciągłej dostępności i wynagradzania pracowników, którzy nie korzystają z prawa do odłączenia się. Ważną kwestią powinna być także ocena w zakresie bezpieczeństwa i higieny pracy w odniesieniu do prawa do odłączenia się (np. pod kątem zagrożeń psychospołecznych).

2.1.2. Równowaga między życiem prywatnym a zawodowym – rola państwa

Źródło: Technology Headlines.

Istotną rolę w kształtowaniu relacji na linii pracownik–pracodawca ma państwo i jego polityka w zakresie pracy. W kwestii równowagi pomiędzy życiem prywatnym a zawodowym niektóre kraje podejmują inicjatywy propagujące dobre praktyki w obszarze zatrudnienia. Z jednej strony dotyczy to wdrażania krajowych regulacji, z drugiej – pokrewnych prawu instrumentów, które nie posiadają prawnie wiążących mocy, ale dążą do kształtowania pewnych zachowań.

Takie „miękkie” środki mogą polegać np. na wdrażaniu kodeksów dobrego postępowania bądź dawaniu dobrego przykładu innym pracodawcom poprzez promowanie propracowniczego podejścia w strukturach administracji państwowej. Tę ścieżkę wybrała Malta, która w 2020 r. wydała *Podręcznik w zakresie środków dążących do zachowania równowagi pomiędzy życiem prywatnym a zawodowym*. W publikacji tej zebrano i dokładnie opisano przysługujące pracownikom prawa, wraz z instrukcjami, jak właściwie pracować w dobie digitalizacji (np. jak zorganizować swoją pracę podczas zdalnego wykonywania obowiązków). Użyteczność podręcznika polega jednak nie tylko na lepszej znajomości przywilejów pracowniczych czy dodatkowej wiedzy w zakresie cyfryzacji. Tego typu kodeksy dobrych praktyk, obowiązujące w miejscu pracy (bądź danym sektorze), mogą stanowić również swoistą kartę przetargową w negocjacjach z pracodawcą.

W przypadku maltańskiego podręcznika, inicjatorzy przedsięwzięcia wskazali, że ich nadrzędnym celem było zapewnienie równowagi między życiem zawodowym a prywatnym osób zatrudnionych w sektorze publicznym poprzez zwiększenie świadomości pracowników. Warto jednak zaznaczyć, iż podręcznik nie rozszerza w żaden sposób katalogu praw pracowniczych, a jedynie zwraca uwagę na właściwe praktyki w obszarze zatrudnienia i uświadamia pracownikom możliwość negocjowania warunków pracy zgodnych z zapisami dokumentu.

Przykłady propagowania prawa do odłączenia się w krajach UE

Chociaż na ten moment nie istnieją jeszcze ogólnoeuropejskie ramy prawne regulujące prawo do odłączenia się, na arenie unijnej występują już pewne przykłady działań legislacyjnych w tym zakresie. Połączone jest to z promowaniem prawa do odłączenia się za pośrednictwem zbiorowych układów pracy. Co więcej, część państw członkowskich wdrożyła już własne ustawodawstwo dotyczące prawa do bycia offline.

Francja

Francja uważana jest za pioniera w zakresie prawa do odłączenia się. Już w 2013 r. w przyjęto tam międzysektorowe porozumienie w sprawie jakości życia w pracy, które zachęcało firmy do unikania ingerencji w życie prywatne pracowników oraz określało czas, w którym urządzenia służące do kontaktu z pracownikiem powinny być wyłączane. Postanowienia te zostały następnie uchwalone 8 sierpnia 2016 r. oraz włączone do francuskiego Kodeksu pracy. Dodatkowo od stycznia 2017 r. we Francji prawnie wymagane jest, aby pracodawcy negocjowali ze związkami zawodowymi umowy dotyczące prawa do odłączenia się.

Włochy

W ślad za Francją poszły Włochy, które zadecydowały, aby wprowadzić prawo do odłączenia się w 2017 r. Regulacja skupia się na osobach wykonujących pracę zdalną (ang. *smart working*,

wł. *lavoro agile*) oraz ustanawia, iż pracownicy zdalni mają prawo do odłączenia się od urządzeń technologicznych i platform internetowych bez ponoszenia jakichkolwiek konsekwencji ze strony pracodawców. We Włoszech funkcjonują również sektorowe i zakładowe układy zbiorowe, które przewidują prawo do odłączenia.

Hiszpania

Kolejnym państwem, które przyjęło prawo do odłączania się do krajowego ustawodawstwa, była Hiszpania. W 2018 r. wraz z transpozycją RODO do prawa hiszpańskiego wprowadzono nowy pakiet praw cyfrowych. Wraz z nim pracownicy zatrudnieni zarówno w sektorze prywatnym, jak i publicznym otrzymali prawo do odłączenia się, którego celem było zachowanie równowagi między życiem prywatnym i zawodowym. Zgodnie z regulacją pracodawcy powinni, po wysłuchaniu reprezentantów pracowników, ustanowić wewnętrzne zasady określające, w jaki sposób zatrudnieni mogą korzystać z prawa do odłączenia się oraz zapewnić pracownikom szkolenia na temat właściwego korzystania z nowych technologii.

Belgia

W Belgii w 2018 r. wszyscy pracodawcy zatrudniający ponad 50 pracowników zostali zobowiązani do omawiania z komisją do spraw BHP kwestii bezpiecznego korzystania z narzędzi cyfrowych oraz prawa pracowników do odłączania się. Warto zauważyć, że wraz z wprowadzeniem prawa do odłączenia się sami pracownicy nie zyskali nowych uprawnień, a jedynie większe możliwości w zakresie negocjacji z pracodawcą. W 2022 r. przyjęto jednak nową regulację, która umożliwia urzędnikom wyłączanie służbowych e-maili oraz niereagowanie na SMS-y i połączenia telefoniczne poza godzinami pracy bez obawy przed represjami. Omawiane są także plany rozszerzenia nowych przepisów na pracowników sektora prywatnego.

Irlandia

W kwietniu 2021 r. irlandzki rząd ogłosił kodeks postępowania, zgodnie z którym wszyscy pracownicy mają prawo do odłączenia się oraz nieodpowiadania natychmiast na e-maile, telefony czy inne wiadomości od pracodawcy po godzinach pracy. Kodeks ustanowił również, że pracownik, co do zasady, nie powinien być zmuszany do wykonywania pracy poza standardowym czasem pełnienia przez niego obowiązków oraz nie powinien ponosić konsekwencji za odmowę załatwiania spraw służbowych po godzinach.

2.1.3. Egzekwowanie ciągłej dostępności przez pracodawcę a mobbing

Źródło: jobs.ca.

Mobbing to działania lub zachowania wobec pracownika polegające na uporczywym i długotrwałym nękaniu lub zastraszaniu go. Występuje w przypadku, gdy dane działania mają na celu poniżenie lub ośmieszenie pracownika, ale także gdy mają wywoływać u niego zaniżoną ocenę przydatności zawodowej.

Z racji tego, iż mobbing może przybierać różne formy agresji, katalog zachowań klasyfikujących się do tego typu przemocy pozostaje otwarty. Oczekiwanie od pracownika ciągłej dostępności pod groźbą negatywnych konsekwencji może więc być uznane za rodzaj mobbingu. Świadczą o tym chociażby wyroki, w których sądy przyznawały rację pracownikom wskazującym, że uciążliwe i powtarzające się otrzymywanie wiadomości zawierających polecenia służbowe po godzinach lub w dni wolne od pracy powinno być traktowane jak mobbing.

Wyrok Sądu Okręgowego w Lublinie z 20 czerwca 2018 r. (VIII Pa 86/18)

Sąd przyznał pracownicy urzędu gminy 25 tys. zł od pracodawcy tytułem zadośćuczynienia za rozstrój zdrowia wywołany natarczywym wysyłaniem e-maili po godzinach pracy. Sprawa dotyczyła kobiety zatrudnionej na stanowisku urzędniczym na czas nieokreślony w pełnym wymiarze czasu pracy. Po zmianie wójta w gminie nowy przełożony jako podstawowy sposób komunikowania się z pracownikami przyjął wysyłanie im na adresy służbowe i prywatne poleceń w formie e-maili. Od 1 stycznia 2015 r. powódka otrzymała od wójta ok. 200 e-maili, z których

ponad 100 wysłano po godzinach pracy, w tym w porze nocnej oraz w dni wolne od pracy, w czasie urlopu wypoczynkowego czy zwolnienia lekarskiego. W wyniku postępowania zapadł wyrok Sądu Okręgowego w Lublinie, w którym Sąd uznał, że zarzucanie pracownika obowiązkami i wysyłanie e-maili z poleceniami służbowymi w dni wolne od pracy, podczas zwolnienia chorobowego i urlopu oraz nieadekwatne rozliczanie ich wykonania, może zostać uznane za **mobbing.**

Naruszanie prawa do odłączenia się – konsekwencje dla pracodawcy i mechanizmy zgłaszania skarg

Sankcje za naruszanie prawa do odłączenia się mogą różnić się w poszczególnych krajach UE. Wynika to z faktu, iż każde państwo członkowskie powinno indywidualnie ustalić wymiar kary nakładanej na pracodawcę w związku z nierespektowaniem czasu wolnego jego pracowników.

W Polsce nie wprowadzono jeszcze odrębnego prawa pracownika do odłączenia się, ale można takowe wywodzić z ogólnych przepisów o czasie pracy oraz z orzecznictwa sądowego. Przyjmuje się więc ogólnie, że pracownik nie ma obowiązku odbierania telefonu ani odpowiadania na e-maile po godzinach pracy lub w czasie urlopu. Wyjątkiem jest sytuacja, gdy jest on zobowiązany do pełnienia dyżuru, czyli pozostawania w gotowości do pracy poza standardowymi godzinami.

Najczęściej spotykanymi wykroczeniami ze strony pracodawców w zakresie stosunku pracy są nieprawidłowości związane z rozwiązywaniem umów, naruszanie przepisów dotyczących czasu pracy, niewłaściwe wypłaty wynagrodzeń oraz nieprawidłowe udzielanie urlopów. W zależności od skali oraz rodzaju wykroczenia, pracodawcy może grozić kara grzywny wynosząca od 1 000 do 30 000 zł.

Tym samym, można spodziewać się, że w Polsce nieprzestrzeganie prawa do odłączenia się sankcjonowane będzie tak, jak wszelkie inne naruszenia przepisów o czasie pracy, tj. pracodawcy będzie grozić kara grzywny w wysokości nawet do 30 000 zł. Dodatkowo, w przypadku gorszego traktowania pracownika z powodu jego ograniczonej dostępności poza wyznaczonym czasem pracy, mogą pojawić się kwestie odszkodowania za dyskryminację (w wysokości nie niższej niż obowiązujące minimalne wynagrodzenie).

Jak wynika z sondażu opinii publicznej[6], 23,9% pracowników w Polsce otrzymuje od przełożonych e-maile, SMS-y lub inne wiadomości po godzinach pracy. Choć, jak zauważają eksperci, nie jest to zabronione, takie działanie może zostać uznane za polecenie pracy

[6] Sondaż przeprowadzony przez UCE RESEARCH i ePsycholodzy.pl, https://uce-pl.com/news/blisko-24-proc-polakow-twierdzi-ze-pracodawca-kontaktuje-sie-z-nimi-w-czasie-wolnym-od-pracy.

w godzinach nadliczbowych (szczególnie wtedy, gdy kontakt wymusza na pracowniku realizację danego zadania). W przypadku konieczności udzielenia odpowiedzi na e-maila lub rozmowę telefoniczną w sprawach służbowych, zgodnie art. 151 (1) i 151 (2) Kodeksu pracy, takie działanie musi zostać zrekompensowane dodatkowym wynagrodzeniem lub czasem wolnym.

Co powinien zrobić polski pracownik, którego prawa są naruszane?

a) Rozmowa z pracodawcą

Przed podjęciem decyzji o zgłoszeniu naruszenia organom zewnętrznym zalecane jest, aby pracownik podjął próbę porozumienia się z pracodawcą. Istotne jest, aby do rozmowy włączył się dyrektor bądź właściciel firmy, gdyż może okazać się, że kadra kierownicza nie jest świadoma wykroczeń ze strony przełożonych działających na niższym szczeblu.

b) Szukanie wsparcia w związkach zawodowych

W przypadku, gdy rozmowa z pracodawcą nie przyniesie pożądanych skutków, pracownik może szukać wsparcia w związkach zawodowych, jeżeli takie działają w danym zakładzie pracy. Związek ma za zadanie reprezentować pracowników i powinien podjąć na nowo próbę porozumienia się z dyrektorem/właścicielem firmy bądź jej zarządem.

c) Zgłoszenie naruszeń Państwowej Inspekcji Pracy (PIP)

Państwowa Inspekcja Pracy (PIP) jest najważniejszą instytucją zajmującą się w Polsce kwestiami warunków pracy i praw pracowniczych. To do niej w pierwszej kolejności powinny trafiać formalne zgłoszenia łamania praw pracowniczych. Kontakt do PIP znajduje się na stronie www.pip.gov.pl, a skarga może być zgłoszona pisemnie, telegraficznie, za pomocą telefaksu,

poczty elektronicznej, formularza e-skargi, a także ustnie do protokołu. Dane pracownika wnoszącego skargę mogą pozostać anonimowe. Zgodnie z ustawą o Państwowej Inspekcji Pracy[7], inspektor pracy jest zobowiązany do nieujawniania informacji, że kontrola przeprowadzana jest w następstwie skargi, chyba że zgłaszający wyraża na to pisemną zgodę. Należy jednak pamiętać o odpowiednim uzasadnieniu stawianych zarzutów oraz przedstawieniu rzetelnych dowodów, gdyż to PIP zadecyduje, czy zgłoszenie jest wiarygodne i czy zostanie zweryfikowane.

d) Wniesienie sprawy do sądu rejonowego

Materiały przekazane do PIP mogą stanowić także materiał dowodowy, jeżeli sprawa trafi do sądu rejonowego. Występowanie na drogę sądową jest jednak ostatecznym rozwiązaniem, wykorzystywanym dopiero wtedy, kiedy poprzednie sposoby zawiodły.

2.1.4. Work-life balance – czym jest równowaga między życiem prywatnym a zawodowym?

Źródło: zapier.com.

Zgodnie z raportem OECD How's Life? Measuring Well-being, pojęcie *work-life balance* oznacza zachowywanie równowagi pomiędzy pracą (zarówno płatną, jak i nieodpłatną), życiem rodzinnym oraz czasem wolnym. Wiąże się ono z umiejętnością pracownika do takiego organizowania obowiązków, aby nie zakłócały one jego czasu wolnego. Jednak odpowiednia

[7] Artykuł 44 ust. 3 *Ustawy z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy* (Dz.U. z 2017 r. poz. 786 ze zm.).

równowaga pomiędzy poszczególnymi obszarami życia nie zależy jedynie od pracownika, lecz także od pracodawcy. To ten zwykle kreuje kulturę pracy w firmie i narzuca pewne normy.

Respektowanie czasu wolnego osób zatrudnionych zarówno stacjonarnie, jak zdalnie czy hybrydowo ma ogromne znaczenie. Od odpowiedniej równowagi pomiędzy życiem prywatnym a zawodowym zależy bowiem dobrostan każdego pracownika (samopoczucie; stan psychiczny). Jak wskazują badania, przeciążenie obowiązkami i praca przez cały czas (także ta polegająca na prowadzeniu domu czy czynnościach opiekuńczych) mogą prowadzić do wycieńczenia organizmu i problemów ze zdrowiem, chronicznego stresu, czy obniżenia produktywności.

Przed pandemią czas spędzany na wypoczynku i dbaniu o swój dobrostan przez osoby zatrudnione w pełnym wymiarze wahał się od ok. 14 do 16,5 godzin dziennie. Mężczyźni pracujący na pełen etat korzystali z wolnego czasu o 30 minut krócej w porównaniu z kobietami. Statystyki prezentują się jednak inaczej w przypadku pracy zdalnej, która upowszechniła się podczas lockdownu wywołanego pandemią COVID-19. Czas spędzany przed komputerem uległ wówczas znacznemu wydłużeniu (nawet do dwóch dodatkowych godzin dziennie), a jakość wypoczynku obniżyła się. Pracownicy wykonujący swoje obowiązki z domu częściej godzą się na nadgodziny oraz wykonywanie zadań wieczorami bądź w weekendy, rozmywając tym samym linię między życiem prywatnym a zawodowym.

Utrzymanie omawianej równowagi jest jednak niezwykle ważne. Pozwala uniknąć wypalenia zawodowego, sprzyja większej motywacji pracowników i ich zaangażowaniu w działania firmy. Przyczynia się także do samorozwoju oraz większej otwartości na nowe wyzwania. Tym samym, pomimo mniejszej liczby przepracowanych godzin, wydajność kadry pracowniczej zwiększa się, zaś potrzeba opieki medycznej i zwolnień lekarskich ulegają ograniczeniu.

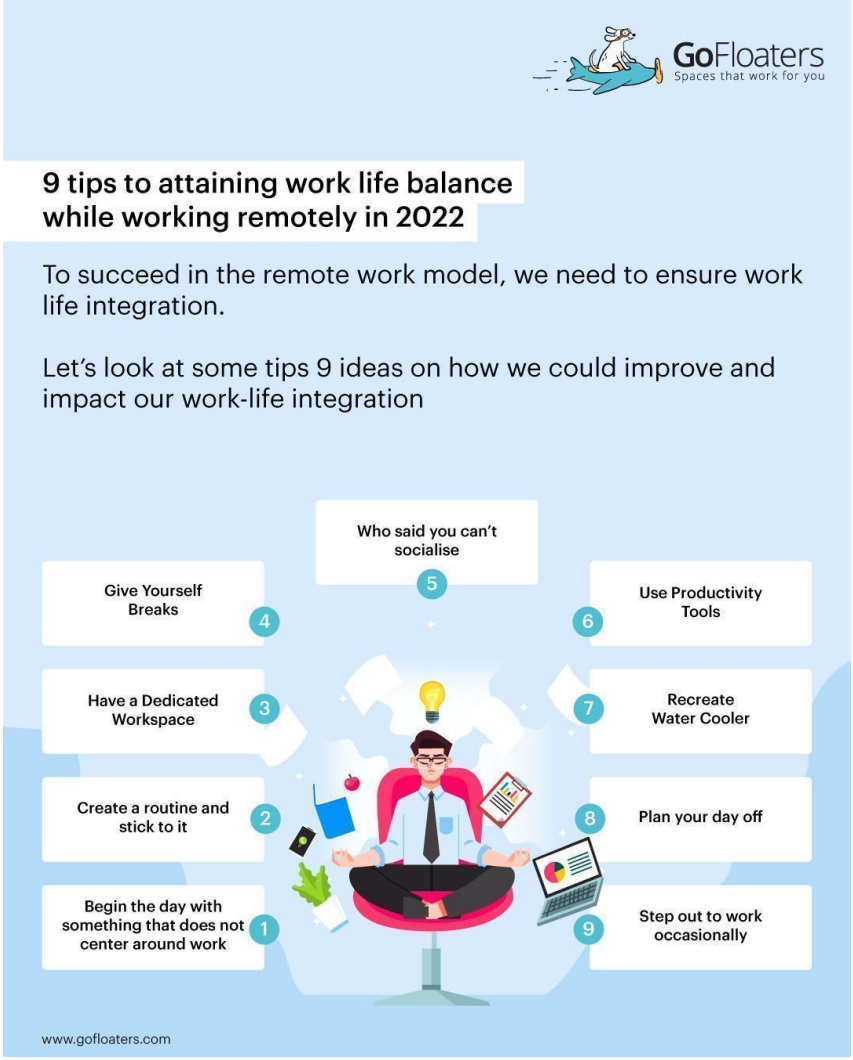
Jak pracodawca może poprawić *work-life balance* swoich pracowników?

Zachowywanie przez pracowników równowagi między życiem prywatnym a zawodowym nierzadko zależy od pracodawców i kadry kierowniczej. To oni promują konkretne zachowania i kształtują politykę pracowniczą w miejscu zatrudnienia. Dlatego tak ważnym jest, aby wspierali oni dobre nawyki pozwalające pracownikom oderwać się od codziennych obowiązków zawodowych. Przykładowo, pracodawcy mogą zachęcać swoich pracowników, by robili przerwy w pracy, pracowali w elastycznych, dogodnych dla siebie godzinach, korzystali z prawa do odłączenia się, jasno komunikowali swoje potrzeby (np. informowali o zbytnim przeciążeniu obowiązkami i konieczności zwolnienia tempa).

Istotne jest także promowanie zdrowej kultury pracy poprzez unikanie premiowania bycia ciągle dostępnym czy wprowadzenie zasady nieodpowiadania na e-maile i komunikaty po godzinach pracy. Dobrym pomysłem jest także przeprowadzenie szkolenia dla pracowników

w zakresie *work-life balance* i prawa do odłączenia się oraz przekazanie im wskazówek, jak w prosty sposób ograniczyć nadmierne korzystanie z narzędzi cyfrowych.

2.1.5. Cyfrowe BHP, czyli jak samodzielnie ograniczyć bycie ciągle podłączonym



Wskazówki dla pracownika

1. **Wyłącz powiadomienia w telefonie**

Jeżeli w prywatnym telefonie masz zainstalowane komunikatory i aplikacje wykorzystywane w miejscu pracy bądź Twoja pracownicza skrzynka e-mail jest powiązana z prywatną, wyłącz wszelkie powiadomienia, które mogą zakłócać Twój spokój w czasie wolnym. Dobrym sposobem

może być także ustawienie ograniczeń czasowych wyciszających wszelkie komunikaty po standardowych godzinach pracy.

2. **Korzystaj z firmowego komputera podczas pracy, a z prywatnego po godzinach**

Wybieranie do pracy firmowego komputera zamiast prywatnego urządzenia jest korzystniejsze nie tylko ze względu na kwestie cyberbezpieczeństwa, lecz także z uwagi na możliwość ograniczenia swojej ekspozycji na komunikaty i wiadomości otrzymywane od współpracowników po godzinach. Jeżeli w Twojej firmie stosowana jest polityka BYOD (*bring your own device*), możesz utworzyć na swoim urządzeniu dwa konta (zawodowe i prywatne) oraz przełączać się między nimi w zależności od pory dnia i potrzeb.

3. **Analogowe poranki i wieczory**

Promieniowanie telefonu czy laptopa zbliżone jest do światła słonecznego, przez co ogranicza wydzielanie melatoniny w mózgu. To z kolei utrudnia zasypianie, obniża jakość wypoczynku i prowadzi do dalszych problemów ze snem. W trosce o swój dobrostan staraj się nie korzystać z telefonu i laptopa przynajmniej godzinę przed pójściem do łóżka. Nie zaczynaj też poranka od nerwowego sprawdzania skrzynki mailowej czy mediów społecznościowych.

4. **Wprowadź ramy czasowe, w których korzystasz z narzędzi cyfrowych**

Nawet jeżeli pracujesz w elastycznych godzinach, poinformuj swoich przełożonych i osoby, z którymi współpracujesz o tym, w jakich porach można się z Tobą kontaktować, a kiedy Twoja dostępność będzie ograniczona.

5. **Wprowadź całodniowy detoks**

Choć detoks cyfrowy nie jest głównym założeniem idei *work-life balance*, całkowicie odłączenie się od sieci i mediów społecznościowych na dłużej może przynieść ogromne korzyści dla dobrostanu jednostki. Doświadczenie odstawienia elektroniki uświadamia, ile czasu rzeczywiście spędzamy w sieci. Pozwala to ustanowić zdrowe granice między życiem zawodowym a życiem prywatnym. Motywuje też to tego, aby pozbyć się złych nawyków, takich jak kompulsywne sprawdzanie skrzynki mailowej czy sięganie po telefon zaraz po przebudzeniu. Dlatego zalecane jest, aby stosować cykliczny detoks (np. całkowicie odłączać się w weekendy), a czas wolny poświęcać na odpoczynek, spotkania z rodziną i przyjaciółmi bądź aktywność fizyczną, aniżeli przeglądanie mediów społecznościowych.

2.2. Utowarowienie zasobów prywatnych – wymuszane oraz wolontaryjne

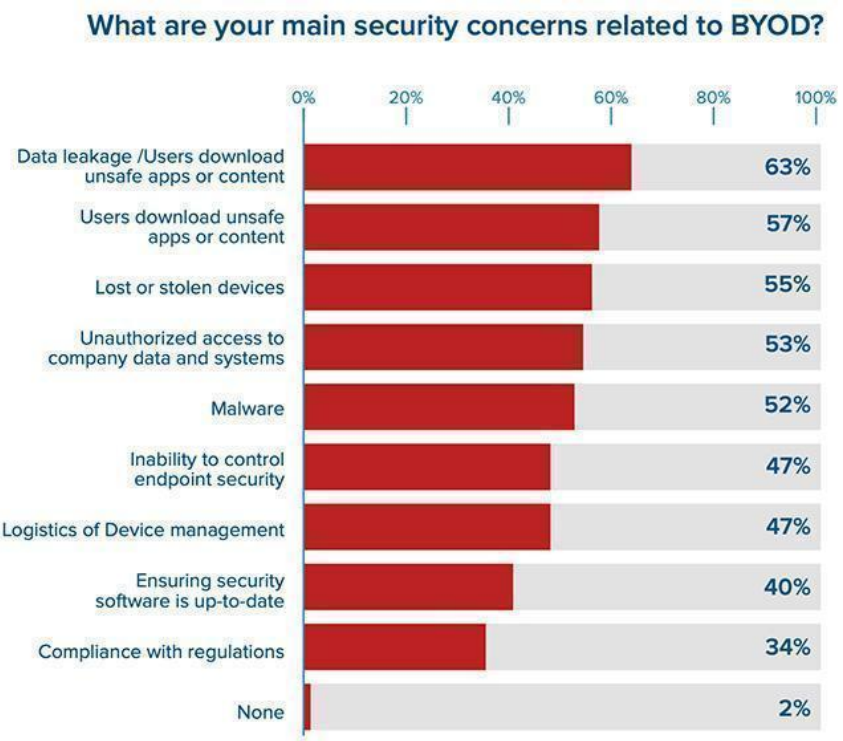
2.2.1. Czym jest polityka BYOD (bring your own device)

Sformułowanie *bring your own device* znane jest także pod skrótem BYOD. To trend polegający na wykorzystywaniu prywatnych urządzeń, takich jak laptopy, smartfony czy tablety do obowiązków zawodowych. Podążanie tym nurtem często wynika z woli samych pracowników (wolontaryjne utowarowienie zasobów prywatnych). Bywa jednak, że politykę BYOD preferują także pracodawcy (wymuszone utowarowienie zasobów prywatnych). Choć trend ten ma wiele zalet, przed wdrożeniem go w przedsiębiorstwie, należy wziąć pod uwagę potencjalne zagrożenia, takie jak chociażby kwestie bezpieczeństwa i prywatności.

Warto dodać, że BYOD jest całkowitym przeciwieństwem tradycyjnego stylu pracy określanego jako *here's your own device* (HYOD), w którym to firmy wydają swoim pracownikom wszelkie urządzenia elektroniczne potrzebne im do pracy.

Zalety polityki BYOD:

- **Elastyczność** – BYOD wiąże ze zgodą pracodawcy na dostęp do dokumentów firmowych na prywatnych urządzeniach pracownika. Tym samym, wykonywanie obowiązków zawodowych staje się możliwe w dowolnym miejscu i czasie. Dodatkowo, większa elastyczność przejawia się w możliwości testowania nowych rozwiązań, programów, narzędzi cyfrowych, gdyż pracownicy nie są ograniczeni do korzystania z urządzeń jednego typu czy marki.
- **Komfort** – jedną z zalet polityki BYOD jest to, że pracownicy mogą korzystać z urządzeń, które dobrze znają i czują się komfortowo podczas ich obsługi.
- **Większa produktywność** – korzystanie z własnego laptopa czy smartfona może ułatwiać proces wdrażania nowo zatrudnionych osób, a także zwiększać produktywność stałych pracowników.
- **Niższe koszty (korzyść pracodawcy)** – godząc się na politykę BYOD, pracodawcy często uchylają się od obowiązku zapewnienia pracownikowi sprzętu do pracy, przez co mogą uniknąć dodatkowych kosztów.
- **Decentralizacja danych (korzyść pracodawcy)** – przetrzymywanie dokumentów służbowych na prywatnym laptopie (o ile są dobrze zabezpieczone) może być korzystne dla firmy ze względu na wyższy poziom decentralizacji danych. W przypadku wycieku danych bądź zaatakowania systemu firmy przez złośliwe oprogramowanie, pliki znajdujące się na urządzeniach pracowników nie ulegną przejęciu razem z centralną bazą danych przedsiębiorcy.



Źródło: helpnetsecurity.com, *BYOD adoption is growing rapidly, but security is lagging*, https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/.

Wady polityki BYOD:

- **Cyber(nie)bezpieczeństwo** – poza korzyścią płynącą z decentralizacji danych, kwestie cyberbezpieczeństwa są największą wadą polityki BYOD. Korzystając z prywatnych urządzeń, pracownicy skłonni są przechowywać poufne dokumenty na swoich dyskach, które zwykle bywają słabiej zabezpieczone niż te firmowe. Co więcej, pracując zdalnie z miejsc publicznych (np. kawiarni, bibliotek, środków transportu), często podłączają się oni do cudzej sieci, zwiększając tym samym prawdopodobieństwo włamania się na komputery i zainstalowania w nich złośliwego oprogramowania. Dodatkowo pojawia się ryzyko kradzieży czy zgubienia urządzenia przez pracownika.
- **Niekompatybilność** – elastyczność w wyborze narzędzi pracy może przekładać się na problemy z ich kompatybilnością z systemami domyślnie wykorzystywanymi w firmie. Tym samym w przypadku BYOD mogą pojawiać się problemy związane z brakiem zgodności formatów i utrudnionym korzystaniem z dokumentów służbowych (np. ze względu na inny zapis plików w przypadku Windows, a inny w MacOS).
- **Odzyskiwanie danych** – polityka BYOD może powodować problemy związane z odzyskiwaniem danych przechowywanych na urządzeniu pracownika po wygaśnięciu stosunku pracy. Wynika to z faktu, że pracownicy posiadają pełną kontrolę nad swoimi urządzeniami i mogą samodzielnie rozporządzać plikami na nich zapisanymi.

Prawa i obowiązki związane z BYOD

W przypadku wykonywania pracy na prywatnym urządzeniu konieczne jest, aby spełniało ono wymagania związane z higieną i bezpieczeństwem pracy. Ubezpieczenie takiego sprzętu nie jest jednak obowiązkowe – pracownik i pracodawca mogą uzgodnić zakres ubezpieczenia i zasady wykorzystywania przez pracownika sprzętu niezbędnego do wykonywania pracy, a stanowiącego własność pracownika.

Przykład Polski – nowelizacja Kodeksu pracy i nowe przepisy dotyczące pracy zdalnej

Warto zaznaczyć, że pracownik zatrudniony na podstawie umowy o pracę ma prawo żądać przekazania mu służbowego komputera, a pracodawca zobowiązany jest mu go dostarczyć. Jeżeli jednak do świadczenia pracy wykorzystywany jest prywatny sprzęt, wówczas pracownikowi przysługuje ekwiwalent pieniężny. Ponadto pracodawca powinien pokrywać koszty energii elektrycznej oraz usług telekomunikacyjnych niezbędnych do wykonywania pracy zdalnej. Zwrot kosztów może nastąpić w wartości realnej lub w formie uzgodnionego między stronami ryczałtu. Przy ustalaniu wysokości ekwiwalentu oraz ryczałtu pracodawca musi wziąć pod uwagę ceny materiałów i urządzeń, a także prądu i usług telekomunikacyjnych[8].

Z zastrzeżeniem, że praca jest wykonywana w domu, pracodawca realizuje wobec pracownika obowiązki dotyczące bezpieczeństwa i higieny pracy, z wyjątkiem:

- obowiązku dbałości o bezpieczny i higieniczny stan pomieszczeń pracy,
- obowiązków dotyczących budowy lub przebudowy obiektu budowlanego, w którym znajdują się pomieszczenia pracy,
- obowiązku zapewnienia odpowiednich urządzeń higienicznosanitarnych.

Takie obowiązki pracodawcy w zakresie zapewnienia odpowiednich warunków pracy swoim pracownikom mają również wpływ na kwestie związane z zakresem pojęcia „wypadek przy pracy" i ubezpieczeniem społecznym. Pracownik, który ulegnie wypadkowi przy pracy, niezależnie od tego, gdzie wykonuje swoje obowiązki – pracując zdalnie lub w zakładzie pracy – ma prawo do **świadczenia z ubezpieczenia społecznego.**

Przed dopuszczeniem do wykonywania pracy zdalnej pracownik potwierdza w oświadczeniu (składanym w postaci papierowej lub elektronicznej) zapoznanie się z przygotowaną przez

[8] *Ustawa z dnia 1 grudnia 2022 r. o zmianie ustawy – Kodeks pracy oraz niektórych innych ustaw* (DZ.U. z 2022 r. poz. 240).

pracodawcę oceną ryzyka zawodowego i informacją zawierającą zasady bezpiecznego i higienicznego wykonywania pracy zdalnej oraz zobowiązuje siędo ich przestrzegania.

Przy ocenie ryzyka zawodowego uwzględnia się w szczególności wpływ pracy zdalnej pracy na wzrok pracownika i układ mięśniowo-szkieletowy. Pod uwagę brane są także uwarunkowania psychospołeczne danej pracy. Na podstawie wyników tej oceny pracodawca opracowuje informację zawierającą zasady i sposoby właściwej organizacji stanowiska pracy zdalnej. Powinny one uwzględniać wymagania ergonomii, bezpiecznego i higienicznego wykonywania pracy zdalnej, czynności do wykonania po zakończeniu wykonywania pracy zdalnej, a także zasady postępowania w sytuacjach awaryjnych stwarzających zagrożenie dla życia lub zdrowia ludzkiego. Pracodawca może także sporządzić uniwersalną ocenę ryzyka zawodowego dla poszczególnych grup stanowisk pracy zdalnej.

2.3. Prywatność danych osobowych i bezpieczeństwo osób pracujących w sieci

2.3.1. Praca zdalna

Ze względu na rosnącą popularność pracy hybrydowej lub pracy zdalnej w pełnym wymiarze, legislatorzy wielu państw członkowskich postanowili wprowadzić w przepisach prawa pracy odpowiednie zmiany. Dostosowania do nowych form pracy wymagały przede wszystkim obowiązki pracownika i pracodawcy. Wynikają one z konieczności zapewnienia odpowiedniej infrastruktury informatycznej czy przestrzeni do pracy w miejscu odbywania pracy zdalnej w taki sposób, by spełniały one wymogi bezpieczeństwa i higieny pracy.

Praca zdalna a prawo pracy – przykład Polski

1. **Narzędzia pracy zdalnej**

Zgodnie z proponowanym w nowelizacji Kodeksu pracy art. 67 (24) § 1, pracodawca ma obowiązek zapewnić pracownikowi wykonującemu pracę zdalną:

- **Materiały i narzędzia pracy** – dotyczy to m.in. urządzeń technicznych niezbędnych do pracy zdalnej (w zależności od specyfiki danej pracy, poza komputerem mogą to być np. odpowiednie słuchawki do odbywania spotkań online, mikrofon itd.).

- **Instalację, serwis i konserwację narzędzi pracy** – w tym urządzeń technicznych, niezbędnych pracy zdalnej. Alternatywnie pracodawca może również pokryć niezbędne koszty związane z tymi usługami.
- **Szkolenia i pomoc techniczną** niezbędne do wykonywania pracy zdalnej.
- **Pokrycie kosztów energii elektrycznej** – pracodawca ma również obowiązek pokryć koszty energii oraz usług telekomunikacyjnych niezbędnych do wykonywania pracy zdalnej.

Porozumienie zawarte między pracodawcą a zakładową organizacją związkową lub regulamin pracy mogą zobowiązać pracodawcę do pokrycia innych kosztów bezpośrednio związanych z wykonywaniem pracy zdalnej.

2. Aranżacja przestrzeni w pracy zdalnej – kontrola pracodawcy

Pracownik ma obowiązek zorganizowania sobie stanowiska pracy zdalnej uwzględniającego wymagania ergonomii. Obejmuje to m.in. wybór wygodnego krzesła, biurka o odpowiedniej wysokości, właściwego ustawienia monitora względem oczu i właściwego oświetlenia.

Z zastrzeżeniem, że praca jest wykonywana w domu pracownika, pracodawca realizuje wobec niego obowiązki dotyczące bezpieczeństwa i higieny pracy, z wyjątkiem:

- obowiązku dbałości o bezpieczny i higieniczny stan pomieszczeń pracy,
- obowiązku określonego w rozdziale III działu dziesiątego Kodeksu pracy (przepisy dotyczące obiektów budowlanych i pomieszczeń pracy),
- obowiązku zapewnienia odpowiednich urządzeń higieniczno-sanitarnych.

Takie obowiązki pracodawcy w zakresie zapewnienia odpowiednich warunków pracy swoim pracownikom mają również wpływ na kwestie związane z zakresem pojęcia „wypadek przy pracy" i ubezpieczeniem społecznym. Pracownik, który ulegnie wypadkowi przy pracy, niezależnie od tego, gdzie wykonuje swoje obowiązki (pracując zdalnie lub w zakładzie pracy), ma prawo do **świadczenia z ubezpieczenia społecznego.**

Ze względu na obowiązki pracodawcy dotyczące:

- zastosowania odpowiednich środków zapobiegających wypadkom przy pracy zdalnej,
- podjęcia niezbędnego działania eliminującego lub ograniczającego zagrożenie wystąpienia takiego wypadku,
- udzielenia pierwszej pomocy poszkodowanym oraz okoliczności i przyczyn wypadku zgodnie z porozumieniem zawartym z zakładową organizacją związkową lub w regulaminie;

pracodawca ma prawo przeprowadzić kontrolę w zakresie:

- bezpieczeństwa i higieny pracy,
- **przestrzegania bezpieczeństwa i ochrony informacji**, w tym procedur ochrony danych osobowych.

Zgodnie z nowymi regulacjami Kodeksu pracy, pracodawca będzie mógł wprowadzić kontrolę trzeźwości pracowników jedynie wtedy, gdy będzie to niezbędne do zapewnienia ochrony życia i zdrowia pracowników, innych osób lub ochrony mienia.

Każda kontrola trzeźwości powinna być:

- przeprowadzona w porozumieniu z pracownikiem,
- przeprowadzona w miejscu wykonywania pracy zdalnej i w godzinach pracy pracownika,
- dostosowana do miejsca wykonywania pracy zdalnej i jej rodzaju,
- nieutrudniająca korzystania z pomieszczeń domowych w sposób zgodny z ich przeznaczeniem,
- w przypadku okazjonalnej pracy zdalnej kontrola trzeźwości powinna odbywać się na zasadach ustalonych z pracownikiem,
- przeprowadzona z poszanowaniem prywatności pracownika i innych osób (np. innych domowników lub lokatorów).

Jeżeli pracodawca w trakcie kontroli stwierdzi uchybienia w zakresie bezpieczeństwa i higieny pracy, bezpieczeństwa i ochrony informacji, w tym ochrony danych osobowych, ma on dwie możliwości. Może wyznaczyć pracownikowi termin usunięcia uchybień albo wycofać zgodę na wykonywanie pracy zdalnej przez pracownika.

3. Ochrona danych osobowych w pracy zdalnej według nowelizacji Kodeksu pracy

Z uwagi na podwyższone ryzyko wycieku danych osobowych i wystąpienia innego rodzaju naruszeń w tym zakresie, pracodawca powinien określić procedury ochrony danych osobowych. Konieczne będzie też przeprowadzenie odpowiednich szkoleń w danej organizacji. Pracownik, który wykonuje pracę zdalną, powinien natomiast potwierdzić, że zapoznał się z wyznaczonymi przez pracodawcę normami w formie pisemnej lub elektronicznej.

Zarówno pracownik, jak i pracodawca powinni również ustalić, w jaki sposób i za pomocą jakich narzędzi będą porozumiewać się na odległość i przekazywać informacje dotyczące wykonywania pracy.

2.3.2. Jak zgodnie z RODO chronić dane osobowe, pracując zdalnie?

Wzrost popularności pracy zdalnej spowodował zwiększenie ryzyka wycieku wrażliwych informacji o firmie. Wynika to z faktu, że zarówno pracownikowi, jak i pracodawcy może być trudno dokładnie ustalić, w jakich warunkach zasady ochrony i bezpieczeństwa informacji oraz ochrony danych osobowych zostały naruszone. Ponieważ praca (przynajmniej częściowo) zdalna prawdopodobnie zostanie z nami na dłużej, trzeba przywołać najczęściej łamane zasady ochrony danych osobowych. Warto przyjrzeć się również zagrożeniom czyhającym na osoby pracujące zdalnie i sposobom na to, jak zniwelować ryzyko ich wystąpienia.

PAMIĘTAJ!

Zgodnie z art. 32 rozporządzenia o RODO, pracodawca jako administrator Twoich danych osobowych, powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający stopniowi ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

W tym celu pracodawca może podjąć następujące działania:

a) pseudonimizacja i szyfrowanie danych osobowych,

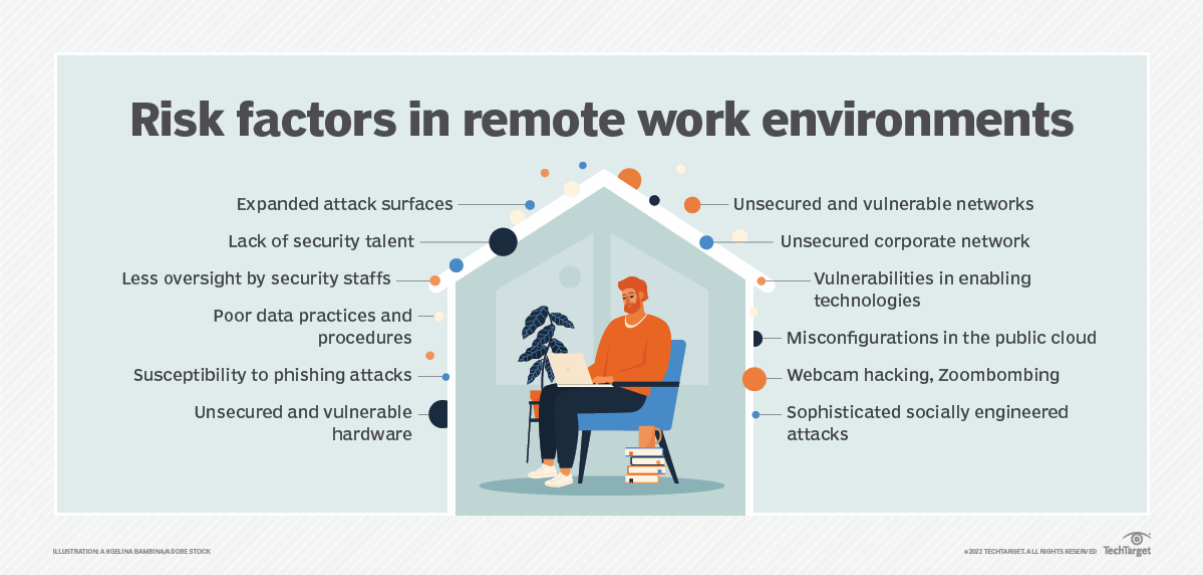
b) zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych,

c) zapewnienie możliwości szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

d) zapewnienie możliwości regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

Według wyjaśnień Komisji Europejskiej pracownicy przetwarzający dane w ramach pracy w organizacji wykonują w ten sposób zadania administratora danych. W związku z tym, oni również odpowiedzialni są za to, by zapewniać bezpieczeństwo danych osobowych.

2.3.3. Zagrożenia w sieci a praca zdalna



Chociaż bezpieczeństwo cybernetyczne jest jednym z najważniejszych wyzwań, przed którymi stoją dziś instytucje państwowe, świadomość społeczna w tym zakresie nadal pozostaje ograniczona. Prawie każdy słyszał o cyberbezpieczeństwie i jego znaczeniu, jednak zachowanie obywateli nie zawsze odzwierciedla wysoki poziom wiedzy na ten temat. Jak wynika z badań serwisu ChronPESEL.pl oraz Krajowego Rejestru Długów przeprowadzonych w 2022 r., co trzeci Polak obawia się wycieku danych osobowych, jednak mniej niż połowa badanych wiedziałaby, co w takiej sytuacji zrobić.

Mimo iż nie da się zapewnić stuprocentowej ochrony danych i bezpieczeństwa informacji, istnieje szereg środków zapobiegawczych, które mogą odpowiednio obniżyć ryzyko wystąpienia wycieku danych oraz innego rodzaju niebezpieczeństw.

Zagrożenia czyhające na pracownika w pracy zdalnej niewiele różnią się od tych, na które powinien uważać każdy użytkownik internetu. Ich celem jest najczęściej kradzież informacji chronionych lub danych o konkretnej osobie czy firmie, dzięki którym atakujący uzyska korzyść finansową, przewagę konkurencyjną lub inne cele. Według raportu Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA), najczęstsze i najgroźniejsze zagrożenia w cyberprzestrzeni to:

1. **Złośliwe oprogramowanie** (*malware*) – to szkodliwe kody lub aplikacje utrudniające lub całkowicie uniemożliwiające normalne korzystanie z urządzenia końcowego (np. komputera czy drukarki). Za sprawą zainfekowania danego sprzętu złośliwym oprogramowaniem, przestępcy mogą dostać się do danych lub uzyskać dostęp do innych

funkcji danego urządzenia. Ich celem może być również całkowite zablokowanie urządzenia pod warunkiem opłacenia okupu przez użytkownika lub inną osobę, której atak częściowo dotyczy.

2. ***Ransomware*** – rodzaj złośliwego oprogramowania, za pomocą którego przestępca blokuje użytkownikom dostęp do ich systemów lub plików osobistych, a następnie żąda uiszczenia opłaty w zamian za jego przywrócenie.
3. **Ataki przez strony internetowe** – metoda, dzięki której hakerzy zwodzą ofiary swoich ataków, wykorzystując systemy i usługi internetowe jako kanał do przygotowania i przeprowadzenia ataku. W szczególności, można wyróżnić tutaj udostępnianie lub ułatwianie dostępu do złośliwych adresów URL lub skryptów, które mają na celu skierować użytkownika na pożądaną stronę internetową czy pobranie złośliwej zawartości. Skutkiem tego jest zaimplementowanie złośliwego kodu do prawdziwie istniejącej strony internetowej w celu kradzieży informacji i uzyskania korzyści finansowych.
4. ***Phishing*** **–** podobnie, jak w przypadku innych ataków cybernetycznych, jego celem jest uzyskanie przez cyberprzestępców cennych informacji, do których należą przede wszystkim loginy, hasła, numery PESEL czy numery kart kredytowych. Nazwa pochodzi stąd, że przestępcy stosują swoistą przynętę przygotowaną odpowiednio pod konkretną osobę, której dane chcą wykraść. Wykorzystują do tego najczęściej fałszywe e-maile czy wiadomości SMS, jak również kanały komunikacyjne na portalach społecznościowych. Dla wzbudzenia zaufania cyberprzestępcy podszywają się pod firmy telekomunikacyjne, kurierskie, banki, portale aukcyjne, a nawet urzędy. Działając na emocjach ofiary, próbują ją nakłonić do kliknięcia w przygotowany przez nich link do strony internetowej, która choć podobna do autentycznej, została stworzona przez przestępcę i stanowi jego kanał do dokonania oszustwa.
5. **DDoS** - (ang. *distributed denial of service*) – rozproszona odmowa usługi to rodzaj ataku, który kierowany jest na usługi sieciowe czy systemy komputerowe. Ich zadaniem jest zajęcie wszystkich dostępnych i wolnych zasobów w celu uniemożliwienia funkcjonowania całej usługi w internecie. Atak może dotyczyć strony internetowej firmy, poczty pracownika będącej na hostingu itd. Przeprowadzany jest z różnych urządzeń komputerowych w tym samym czasie – głównie z tych, nad którymi przejęto kontrolę przy użyciu specjalnych wirusów – botów lub trojanów. Niebezpieczeństwo przy tego typu atakach polega na tym, że użytkownik danego sprzętu może nie być świadomy, że jego komputer służy do przeprowadzenia DDoS.

6. **Kradzież tożsamości** – za pomocą numeru PESEL, danych osobowych, czy dowodu osobistego przestępca podszywa się pod daną osobę, by wziąć np. kredyt lub w inny sposób wykorzystać jej tożsamość dla własnej korzyści.
7. **Naruszenie bezpieczeństwa danych** – to rodzaj incydentu związanego z bezpieczeństwem cybernetycznym, w którym następuje dostęp do informacji (lub części systemu informatycznego) bez odpowiedniego zezwolenia, zazwyczaj w złym zamiarze. Prowadzi to do potencjalnej utraty lub niewłaściwego wykorzystania tych informacji. Powodem wystąpienia tego rodzaju zagrożenia często jest tzw. błąd ludzki, który może zdarzyć się podczas konfiguracji i wdrażania niektórych usług oraz systemów, co może skutkować niezamierzonym narażeniem danych.
8. **Wyciek informacji** – częsty skutek naruszenia bezpieczeństwa danych, obejmujący szeroki zakres zagrożonych informacji – od danych osobowych umożliwiających identyfikację, poprzez dane finansowe przechowywane w infrastrukturze informatycznej aż po dane osobowe dotyczące zdrowia przechowywane w repozytoriach podmiotów świadczących usługi opieki zdrowotnej.
9. **Zagrożenie wewnętrzne** (nadużycie uprawnień) – to działanie podjęte przez osobę lub grupę osób powiązanych z ofiarą ataku w relacji zawodowej lub innej, w ramach której zarówno przeprowadzający atak, jak i ofiara pozostają w tej samej sieci czy infrastrukturze, lub mają możliwość zdobycia informacji poprzez wzajemne powiązania. Istnieje kilka wzorców związanych z tego rodzaju zagrożeniami. Mogą one wystąpić również wtedy, gdy osoby z zewnątrz współpracują z podmiotami wewnątrz firmy w celu uzyskania nieautoryzowanego dostępu do zasobów. Osoby mające dostęp do informacji wewnętrznych mogą również wyrządzić szkodę nieumyślnie przez nieuwagę lub brak wiedzy. Ponieważ osoby wtajemniczone w procesy firmy często cieszą się zaufaniem współpracowników, a także posiadają wiedzę o procesach i procedurach organizacji, trudno jest odróżnić legalny dostęp do danych i systemów od działań w złej wierze.
10. **Botnety** – sieć połączonych urządzeń zainfekowanych złośliwym oprogramowaniem typu bot. Są one zwykle wykorzystywane do przeprowadzania ataków typu DDoS. Botnety mogą być zdalnie kontrolowane przez przestępcę, aby działać w zsynchronizowany sposób w celu uzyskania określonego rezultatu.

2.3.4. Cyberhigiena – jak być bezpiecznym w sieci na co dzień?

1. **Jeśli możesz, pracuj w bezpiecznej, prywatnej przestrzeni**

Do wycieku danych może dojść nie tylko na skutek ataku hakerskiego, ale również za sprawą mniej wysublimowanych, konwencjonalnych metod – m.in. podejrzenia zawartości ekranu i zrobienia zdjęcia naszego monitora. Nie ulega wątpliwości, że poza miejscem pracy przygotowanym przez pracodawcę do jej wykonywania, najbezpieczniejszą przestrzenią do pracy zdalnej wydaje się własne, domowe miejsce do pracy. Najlepiej, aby był to zamykany na klucz pokój, w którym można spokojnie oddzielić się od reszty domowników.

Jeżeli nie istnieje możliwość pracy w odosobnionym pomieszczeniu (np. podczas podróży służbowej), kwestia zachowania bezpieczeństwa znacznie się komplikuje. W szczególności należy uważać na otwarte przestrzenie (kawiarnie, pociągi, lotniska), w których osoby pozostające w naszym otoczeniu nieustannie się zmieniają. Ponadto, w wielu miejscach tego rodzaju zainstalowany jest monitoring, który może rejestrować nie tylko działania osób znajdujących się w jego zakresie, ale również wszelkiego rodzaju inne elementy otoczenia, w tym ekrany komputerów.

Rozwiązanie: zaopatrz się w filtr/nakładkę prywatyzującą

Dzięki temu narzędziu zawartość ekranu widoczna jest tylko dla osoby korzystającej z komputera/telefonu. Technologia ta działa podobnie do mikrożaluzji – filtr składa się z mikroskopijnych kanałów skierowanych na wprost osoby korzystającej z ekranu monitora. Osoby spoglądające na ekran pod innym kątem nie zobaczą tej samej zawartości.

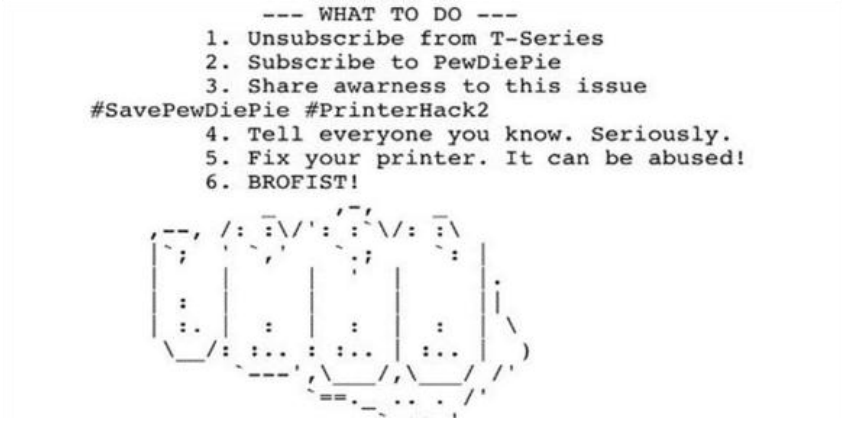
2. **Przechowuj dokumenty w bezpiecznej, zamykanej przestrzeni w miejscu odbywania pracy zdalnej**

Obowiązująca w wielu miejscach pracy tzw. polityka czystego biurka lub czystego ekranu powinna być stosowana również w miejscu odbywania pracy zdalnej. Nawet, jeżeli mamy zaufanie do domowników czy współlokatorów, nie należy pozostawiać żadnych dokumentów zawierających dane osobowe podczas naszej nieobecności. Nie należy również trzymać w widocznym miejscu haseł do urządzeń służbowych.

Rozwiązanie: wyposaż swoją przestrzeń do pracy zdalnej w zamykaną na klucz szufladę lub szafkę

Będzie to miejsce, w którym można bezpiecznie przechowywać wszystkie materiały służące do wykonywania zadań podczas pracy. W miarę możliwości, klucz należy mieć zawsze przy sobie lub schowany w tylko sobie znanym miejscu.

3. **Jeżeli nie jest to konieczne, nie drukuj dokumentów w domu lub w publicznych punktach ksero**



Eksperci do spraw cyberbezpieczeństwa już od dawna alarmują, że najbardziej lekceważonym urządzeniem pod względem konieczności wdrożenia odpowiednich zabezpieczeń jest… drukarka. Według badań InfoSecurity Magazine, ok. 66% ankietowanych osób pracujących zdalnie drukowało średnio pięć dokumentów tygodniowo. Jedna czwarta z nich nie pozbyła się jeszcze wydrukowanych dokumentów, tłumacząc, że zamierzają zabrać je z powrotem do biura. Jedynie 24% korzysta z domowej niszczarki, ale przyznaje też, że wyrzuca dokumenty do domowego kosza na śmieci. Aż 12% ankietowanych twierdzi również, że nie ma żadnej wiedzy na temat rozporządzenia o RODO.

Współczesne drukarki coraz częściej przypominają raczej komputery niż jednozadaniowe, proste urządzenia – często stanowią elementy internetu rzeczy (ang. *Internet of Things,* IoT) i są wielofunkcyjnymi narzędziami pracy. Jednym z głośniejszych ataków na domowe drukarki, który unaocznił problem braku odpowiednich zabezpieczeń tych urządzeń, był atak związany ze znanym twórcą YouTube PewDiePie. W 2018 r. haker (lub grupa wielu fanów PewDiePie) zaatakował kilkadziesiąt tysięcy drukarek na całym świecie. Bez ingerencji swoich właścicieli urządzenia zaczęły drukować broszurę propagującą treści publikowane przez PewDiePie i zachęcającą do wspierania jego działalności.

Współczesne coraz bardziej zaawansowane technologicznie drukarki posiadają pamięć podręczną, do której trafiają dokumenty do wydrukowania. Nowoczesne drukarki działają również bezprzewodowo, co oznacza, że każdy, kto posiada odpowiednie sterowniki na swoim komputerze i dostęp do sieci, w której znajduje się drukarka, może się z nią połączyć. W przypadku przejęcia kontroli nad drukarką (np. w firmie) haker może uzyskać dostęp zarówno do dokumentów, które już zostały wydrukowane, jak i innych zasobów gromadzonych w komputerze czy nawet haseł do urządzeń, które korzystały z usług drukarki.

Rozwiązanie: drukuj dokumenty jedynie w pracy, a jeśli musisz robić to w domu, zadbaj o odpowiednie zabezpieczenie swojego sprzętu

Można to zrobić poprzez ustawienie bezpiecznego hasła do wi-fi drukarki (o ile to możliwe). Jeżeli wydrukowane dokumenty nie są już potrzebne, nie wyrzucaj ich do kosza w swoim domu – zabierz je do firmy, gdzie powinna znajdować się niszczarka. Jeśli nie ma takiej możliwości, zapytaj swojego pracodawcę lub dział kadr o firmową procedurę niszczenia dokumentów.

4. Nakładka na kamerę internetową

Praca w domu oznacza zazwyczaj udział w telekonferencjach i połączeniach wideo, które wymagają użycia kamery internetowej. Niestety, hakerzy mogą łatwo uzyskać dostęp do kamery internetowej, narażając Twoją prywatność. Ponadto, jeśli w fizycznym miejscu pracy znajdują się poufne dokumenty możliwe do zarejestrowania przez kamerę internetową, przestępcy będą mogli uzyskać do nich wgląd.

Rozwiązanie: ograniczenie widoku na elementy zawierające dane osobowe

Gdy kamera internetowa jest włączona, należy ograniczyć możliwość widoku w jej otoczeniu na elementy zawierające dane osobowe. Dodatkowo, jeśli kamera internetowa jest oddzielona od urządzenia, należy ją odłączać, gdy nie jest używana. Jeśli kamera jest wbudowana, warto podjąć dodatkowe środki ochrony, np. wyposażyć się w zaślepkę na kamerę. W sklepach można łatwo znaleźć przesuwne osłony na kamery internetowe różnego typu. Zazwyczaj są one łatwe w instalacji, ponieważ większość z nich posiada warstwę kleju, która przylega do kamery. Korzystając z programów i aplikacji służących do odbywania wideokonferencji, można także używać funkcji, takich jak **rozmycie tła**.

5. **Bierz aktywny udział w firmowych szkoleniach w zakresie cyberbezpieczeństwa i zmian polityki pracodawcy dotyczących ochrony danych i informacji**

Zgodnie z RODO, w przypadku uchwalenia nowych procedur ochrony danych osobowych w firmie, przed ich wdrożeniem, pracodawca powinien pozwolić swoim pracownikom zaznajomić się z nimi.

Jeżeli pracodawca nie przeprowadził odpowiedniego szkolenia na temat używania urządzeń, korzystania z narzędzi do komunikacji wewnętrznej i zewnętrznej lub nie przedstawił podstawowych zasad związanych z ochroną danych w firmie, pracownik prawo do tego, by poprosić go o to. Jeżeli, nawet po przeprowadzonym szkoleniu, pracownik nadal nie ma pewności co do procedur postępowania w danej sytuacji, powinien zgłosić to swojemu pracodawcy lub wyznaczonej osobie w firmie odpowiedzialnej za zarządzanie infrastrukturą informatyczną, dział zasobów ludzkich itd.

Cyberhigiena podczas pracy zdalnej

Co jeszcze możesz zrobić, aby zabezpieczyć swój komputer?

Szyfruj dane osobowe

Zwłaszcza, jeżeli są to dane wrażliwe lub przesyłasz je poza organizację. Jak wspomniano już wcześniej, pracownicy przetwarzający dane w ramach zadań służbowych wykonują w ten sposób zadania administratora danych, którym jest pracodawca. Zgodnie z art. 32 RODO administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa danych odpowiadający zakresowi, kontekstowi i celom przetwarzania danych oraz ryzyku naruszenia praw lub wolności osób fizycznych. Jako środki zabezpieczeń rozporządzenie o RODO wymienia m.in. pseudonimizację i szyfrowanie danych osobowych.

Chociaż nie ma wyraźnych wymogów RODO co do najskuteczniejszej metody zabezpieczenia, w rozporządzeniu wielokrotnie podkreślono, że **szyfrowanie i pseudonimizacja** to odpowiednie środki techniczne i organizacyjne dla zachowania bezpieczeństwa danych osobowych.

Szyfrowanie ma na celu takie zakodowanie danej treści, że zrozumie je tylko odbiorca, który ma do niej odpowiedni klucz. Najprościej ujmując, chodzi o to, by np. ciąg liter zamienić w ciąg innych liter lub cyfr, dodać dodatkowe ciągi liter lub cyfr itd.

Pseudonimizacja to natomiast przetwarzanie danych osobowych w taki sposób, aby nie było możliwe zidentyfikowanie, do kogo one należą bez dostępu do informacji, przechowywanych bezpiecznie w innym miejscu. Polega więc na maskowaniu danych poprzez zastąpienie informacji o danej osobie wymyślonymi identyfikatorami.

Jaka jest różnica między tymi dwoma metodami?

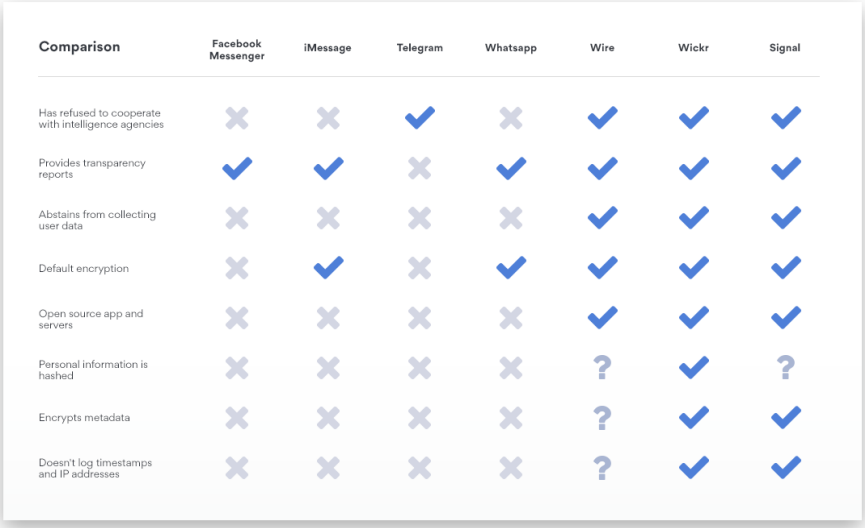
Podobnie jak pseudonimizacja, szyfrowanie ukrywa informacje poprzez zastąpienie identyfikatorów czymś innym. O ile jednak pseudonimizacja umożliwia każdemu, kto ma dostęp do danych, wgląd w część zbioru danych, o tyle szyfrowanie pozwala na dostęp do pełnego zbioru danych tylko zatwierdzonym użytkownikom. Pseudonimizacja i szyfrowanie mogą być stosowane jednocześnie lub oddzielnie.

Metody zabezpieczania/szyfrowania danych w komunikacji wewnętrznej, a także w komunikacji z zewnętrznymi podmiotami

a. Komunikacja wewnętrzna – używanie szyfrowanych komunikatorów i bezpiecznych platform

Chociaż e-mail wciąż pozostaje jedną z najpopularniejszych metod komunikacji służbowej (w 2021 r. każdego dnia wysyłano i odbierano 316,9 mld e-maili, a do 2025 r. liczba ta ma wzrosnąć do 376,4 mld), nie jest jednocześnie najbezpieczniejszym systemem wymiany poufnych informacji. W związku z dużą popularnością, poczta elektroniczna jest też głównym kanałem ataków hakerskich. Firma Deloitte stwierdziła, że 91% wszystkich cyberataków pochodzi z wiadomości e-mail typu *phishing*. Koszty ponoszone przez organizacje na skutek takiego ataku mogą być bardzo wysokie.

W przypadku komunikacji wewnętrznej, w ramach której często wymienia się poufne informacje o firmie, jej pracownikach czy klientach można korzystać z innych, bezpieczniejszych narzędzi.



Whatsapp i Messenger – najczęściej wybierane komunikatory i ich właściwości

1. **WhatsApp:**
   - wykorzystuje szyfrowanie Signala,
   - większość osób w Europie prawdopodobnie korzysta z tej aplikacji,
   - przyjazna dla użytkownika aplikacja, która oferuje dodatkowe funkcje,
   - jest własnością Facebooka,
   - w aplikacji doszło wcześniej do poważnych naruszeń w zakresie ochrony danych osobowych.
2. **Messenger:**
   - szeroki zasięg – ze względu na powiązanie z Facebookiem większość osób posiada ten komunikator,
   - można z niego korzystać nawet po dezaktywacji konta na Facebooku,
   - szyfrowanie nie jest domyślne,
   - komunikator nie szyfruje przeszłych rozm,
   - aplikacja śledzi zachowanie użytkownika.

Najlepsze aplikacje pod względem bezpieczeństwa danych:

1. **Signal:**
   - obsługuje czaty grupowe, wiadomości SMS, głosowe i wideo, umożliwia przekazywanie dokumentów i zdjęć,
   - oferuje znikające wiadomości (z czasomierzem),
   - wykorzystuje protokół sygnałowy – niesfederowany protokół kryptograficzny, który może być używany do szyfrowania połączeń głosowych i rozmów przez komunikatory internetowe, w którym wiadomości w formie jawnej mogą odczytać wyłącznie osoby komunikujące się,
   - oprogramowanie typu *open source* (tj. którego kod źródłowy jest udostępniany bezpłatnie i może być rozpowszechniany i modyfikowany bez uiszczania opłat),
   - nie przechowuje danych użytkownika ani metadanych,
   - propagowany przez Edwarda Snowdena,
   - wymaga podania numeru telefonu do rejestracji.

Bezpieczne oprogramowania i platformy przestrzeni roboczej:

1. Microsoft Teams.
2. Google Workspace.
3. Slack.
4. Asana.
5. Trello.

b. Komunikacja zewnętrzna – szyfrowanie plików zawierających dane osobowe i listy adresatów e-mail

Zaleca się, by w miarę możliwości w każdym przypadku przekazywania danych z jednej lokalizacji do drugiej, pseudonimizować je lub szyfrować, aby zabezpieczyć przed wyciekiem.

Przekazywanie danych osobowych w liście mailingowej

Używaj pola UDW (ukryte do wiadomości, ang. BCC). Pole UDW pozwala na wysyłkę wiadomości w taki sposób, że odbiorcy nie widzą wzajemnie swoich adresów. Opcję tę można znaleźć w każdej poczcie elektronicznej.

Przekazywanie danych osobowych w plikach przesyłanych drogą mailową

W dokumentach wysyłanych za pośrednictwem poczty elektronicznej może kryć się wiele danych osobowych lub innych informacji prawnie chronionych, dlatego należy je dodatkowo zabezpieczyć. Metody szyfrowania plików mogą różnić się w zależności od formatu, w którym zostały zapisane. Wszystkie jednak łączy jedna, podstawowa zasada: przekazywania hasła do zaszyfrowanego dokumentu za pośrednictwem innego środka komunikacji niż drogą mailową.

W celu odpowiedniego szyfrowania pliku, najczęściej wybieranymi programami są **WinRAR** oraz **7-zip**. Przy każdym z nich, po wybraniu opcji „dodaj do archiwum”, otworzy się okno pozwalające m.in. ustawić hasło dostępu do dokumentu.

Regularnie twórz kopie zapasowe swoich danych i przechowuj je na zewnętrznych dyskach

W przypadku zainfekowania sprzętu wirusem lub innych zdarzeń, które mogą doprowadzić do usunięcia danych z komputera i braku możliwości przywrócenia ich, najlepszym rozwiązaniem jest regularne wykonywanie **kopii zapasowych.**

Kopie zapasowe, zwane także backupem, to kopie informacji, które są przechowywane gdzie indziej niż ich oryginał. Pierwszym krokiem powinno być podjęcie decyzji, czy chce się zrobić kopię zapasową:

1. Konkretnych danych, które są z jakiegoś powodu ważne.
2. Całego systemu operacyjnego.

Większość narzędzi do wykonywania kopii zapasowych jest domyślnie skonfigurowana dla pierwszego celu i wykonuje kopię danych w oparciu o to, których dokumentów najczęściej używasz. Jeżeli nie masz pewności co do tego, które pliki kopiować, zaleca się archiwizować wszystkie.

Jak często robić kopie zapasowe?

Odpowiedź zależy od indywidualnych preferencji i częstotliwości wprowadzanych zmian. Niektórzy robią to co godzinę, inni raz dziennie, a jeszcze inni raz w tygodniu. Zalecane jest jednak robienie kopii zapasowej dokumentów codziennie.

Jak tworzyć kopie zapasowe dokumentów?

W zależności od posiadanego systemu operacyjnego komputera polecane są programy, dzięki którym będzie można ustawić okres, co który automatycznie utworzona zostanie kopia zapasowa. Należą do nich m.in. Microsoft Windows Backup and Restore czy Time Machine firmy Apple. Programy te działają zarówno w trakcie używania urządzenia, jak i wtedy, kiedy jest ono w stanie spoczynku.

Dane na zewnętrznym nośniku czy dane w chmurze?

Najlepiej jedno i drugie. Nośnikiem zewnętrznym może być m.in. pendrive, przenośny dysk zewnętrzny czy inne urządzenia, z którymi można połączyć się za pomocą sieci wi-fi. Plusem ich wykorzystywania jest z pewnością to, że można na nich zapisywać duże zbiory danych w dość krótkim czasie. Niestety, ponieważ jest to fizyczna metoda tworzenia kopii zapasowych, może ona ulec takim samym awariom czy zniszczeniom, jak komputer. Kopia zapasowa na zewnętrznym nośniku może zostać skradziona, zgubiona, ulec zalaniu, przegrzaniu itd. Co więcej, jeżeli urządzenie, z którego pochodzą dane, zostało wcześniej zarażone złośliwym oprogramowaniem, to niestety istnieje ryzyko zainfekowania również nośnika, a w konsekwencji samej kopii zapasowej.

Tworzenie kopii zapasowej w chmurze polega natomiast na umieszczaniu kopii dokumentów lub innych plików w internecie. Dokładniej są to zbiory rozproszonych na całym świecie serwerów i centrów danych, na których przechowywane są dane. Dzieje się to automatycznie, zazwyczaj

za pośrednictwem domyślnie działającego narzędzia na platformie służącej do edycji tekstów (np. Google Docs), które co pewien oznaczony czas lub po każdej zmianie w pliku tworzy kopię zapasową. Zdecydowaną zaletą przechowywania kopii plików w chmurze jest ich trwałość i możliwość dostępu do kopii zapasowej z każdego innego urządzenia (o ile oczywiście posiadamy hasło do konta, w ramach którego chmura istnieje). Nie jest to jednak rozwiązanie całkowicie pozbawione wad – jeżeli zależy nam na szybkim tworzeniu kopii dużej ilości danych, rozwiązanie to może być dużo wolniejsze niż w przypadku fizycznej kopii zapasowej na dysku zewnętrznym. Może się też okazać, że zabraknie nam miejsca w chmurze na gromadzenie nowych danych i będziemy zmuszeni część z nich usunąć lub wykupić u dostawcy chmury dostęp do dodatkowych zasobów.

Zabezpiecz dostęp do komputera, telefonu, a nawet spotkań online

Tak jak szyfrowanie samych danych jest konieczne dla zapewnienia bezpieczeństwa danych osobowych, tak niezwykle istotne jest, by odpowiednio zabezpieczyć również sprzęt, którego używamy. Używanie haseł czy innego rodzaju szyfrowania gwarantuje, że dostęp do określonych zasobów posiadają jedynie osoby do tego uprawnione.

Istnieje kilka metod zabezpieczania sprzętu:

- **Silne hasło, czyli hasło:**
    - **długie** – zawierające co najmniej osiem znaków (im dłuższe, tym lepsze),
    - **złożone –** zawierające przynajmniej jeden znak z każdej z kategorii: duże litery, małe litery, znaki specjalne (np. !, ?), liczby,
    - **trudne do odgadnięcia** – jeżeli chcesz wybrać frazę, cytat czy powiedzenie, upewnij się, że nie jest ono związane bezpośrednio z Tobą, Twoją pracą lub otoczeniem; jeżeli jednak wiesz, że bez łatwych skojarzeń nie zapamiętasz hasła – zastąp słowa odpowiednimi symbolami lub cyframi z klawiatury, np. „Ala ma kota” **można** zapisać jako „4LaM@k0T@”,
    - i**nne niż wcześniejsze hasło do danego urządzenia** – w przypadku zmiany hasła do istniejącego konta, nie powinno ono być takie samo jak wcześniejsze; nie należy też zmieniać hasła tylko w nieznaczny sposób, dodając np. cyfrę na końcu lub początku.

Wskazówka: użyj narzędzia do zarządzania hasłami do przechowywania zaszyfrowanych haseł online – pozwoli ono na tworzenie skomplikowanych haseł zawierających małe i wielkie litery, cyfry, różne znaki specjalne itd. Dzięki temu powstanie pozbawiony sensu ciąg znaków, który będzie trudny do złamania.

PAMIĘTAJ!

- nie używaj hasła, które jest jednocześnie nazwą lub jest podobne do nazwy użytkownika, firmy itd.,
- nie używaj sekwencji liter lub cyfr z klawiatury lub alfabetu,
- nie używaj więcej niż dwóch liter lub cyfr powtarzających się (np. abba),
- nie używaj niczyich danych osobowych do tworzenia hasła,
- nie używaj wersji słów pisanych wspak (np. janek1 jako 1kenaj),
- nie wpisuj hasła w obecności innych osób,
- nie zapisuj hasła na papierze – jeżeli musisz je zapisać, użyj narzędzia służącego do zarządzania hasłami na nośniku USB i noś je ze sobą,
- nie używaj tego samego hasła do wszystkich urządzeń czy witryn,
- nie loguj się na nie swoim urządzeniu,
- nie wysyłaj hasła w wiadomości mailowej,
- nie udostępniaj haseł online – jeśli musisz udostępnić informacje o loginie współpracownikowi, zadzwoń do niego ze szczegółami, zamiast wysyłać hasło e-mailem, SMS-em lub innym komunikatorem,
- jeżeli wykryto włamanie do Twojego komputera/witryny, natychmiast zmień hasło.

Antyporadnik – lista najmniej bezpiecznych haseł dostępu[9]:

1. password
2. 123456
3. 123456789

[9] Według badania przeprowadzonego przez firmę NordPass, Top 200 most common passwords, https://nordpass.com/most-common-passwords-list/.

4. guest
5. qwerty
6. 12345678
7. 111111
8. 12345
9. col123456
10. 123123
11. 1234567
12. 1234
13. 1234567890
14. 000000
15. 555555
16. 666666
17. 123321
18. 654321
19. 7777777
20. 123

Uwierzytelnianie wieloskładniowe

Uwierzytelnianie wieloskładnikowe (MFA lub 2FA) to metoda zabezpieczenia, która wymaga użycia co najmniej dwóch niezależnych elementów składowych, aby uwierzytelnić dane działanie (np. wpisanie hasła do konta, a następnie wpisanie kodu SMS). Metoda ta zapobiega większości ataków opartych na poświadczeniu tożsamości.

Wiele aplikacji czy platform już teraz oferuje możliwość włączenia tego rodzaju zabezpieczenia (np. Apple ID, Microsoft, Google, Twitter czy Facebook). Drugim składnikiem uwierzytelniającym mogą być: kod SMS, jednorazowy kod z aplikacji (Google Authenticator lub Microsoft Authenticator) lub stały kod zaproponowany przez dostawcę danego narzędzia i wybrany przez użytkownika.

Klucze U2F

Według specjalistów z zakresu cyberbezpieczeństwa, klucz U2F to jedyna metoda dwuetapowego uwierzytelnienia, która w 100% chroni przed atakami typu *phishing* (ale nie przed innymi atakami, np. *malware*). W przypadku bowiem oszukania osoby posiadającej klucz U2F przez cyberprzestępców i wprowadzenia loginu oraz hasła na fałszywą stronę, atakującemu nie uda się przejąć danych do konta użytkownika.

Dzieje się tak za sprawą *secure element* (tzw. małego komputera) wbudowanego w klucz U2F. Działa on w ten sposób, że po włożeniu klucza do portu USB (lub zbliżenia go do czytnika w smartfonie), klucz uruchamia się i może przeprowadzić operacje kryptograficzne w swoim wewnętrznym systemie, a nie na urządzeniu użytkownika.

Dodatkowo warto zaopatrzyć się w dwa klucze – choć ten sam klucz można podpiąć różne serwisy, warto mieć jeden zapasowy. Po zakupie klucz należy skonfigurować. Wiele serwisów oferuje możliwość dodania klucza jako formy uwierzytelniania wielopoziomowego. Rozwiązanie to zalecają również różnego rodzaju media społecznościowe, konta Amazon, GitHub czy poczty e-mail. Jeżeli zdecydujesz się stosowanie klucza U2F, należy usunąć z danego serwisu pozostałe metody dwupoziomowego uwierzytelniania.

Zabezpieczanie spotkań online

Zabezpieczenia wymagają nie tylko sprzęty, ale też spotkania i wideokonferencje w sieci. Praca zdalna często oznacza poleganie na oprogramowaniu do wideokonferencji, co z kolei stwarza potencjalne zagrożenia dla bezpieczeństwa urządzenia. Po serii ataków na platformie Zoom, polegających na włamywaniu się nieproszonych osób na wideokonferencje po to, by zastraszyć bądź nękać jej uczestników (*zoom bombing*), firma została zmuszona do usunięcia błędów w zabezpieczeniach. Pomimo swojej nazwy, *zoom bombing* może mieć miejsce również

na innych platformach. Na skutek tego rodzaju ataku może dojść do wycieku poufnych informacji na temat firmy, klientów, innych pracowników czy samego użytkownika.

W odpowiedzi na ataki bombowe Zoom, FBI opublikowało porady, które mają pomóc użytkownikom chronić się podczas korzystania z oprogramowania do wideokonferencji:

1. Sprawdź, czy spotkanie jest prywatne, wymagając hasła do dołączenia do spotkania lub kontrolując dostęp gości z poczekalni.
2. Uwzględnij wymagania dotyczące bezpieczeństwa przy wyborze dostawców. Szyfrowanie *end-to-end* (polegające na ukryciu wiadomości u nadawcy i odszyfrowaniu jej dopiero u odbiorcy) zapewnia prywatność i bezpieczeństwo – sprawdź więc, czy używane oprogramowanie do wideokonferencji ma tę funkcję.
3. Upewnij się, że oprogramowanie jest aktualne, instalując najnowsze poprawki i aktualizacje.

Najbezpieczniejszą platformą do wideokonferencji jest obecnie Microsoft Teams. Płynna integracja wszystkich aplikacji Office pozwala również na dodatkowe ustawienia bezpieczeństwa, dzięki czemu wszyscy w organizacji mogą pracować razem, zachowując bezpieczeństwo nawet w domowym biurze.

Zainstaluj i aktualizuj programy antywirusowe, a także ochronę przed złośliwym oprogramowaniem

Aktualizowanie systemów, aplikacji i przeglądarek często jest lekceważone i odkładane na później. W rzeczywistości, zrobienie tego we właściwym czasie może zapobiec dużej części ataków. Upewnij się więc, że korzystasz z aktualnego i nowoczesnego oprogramowania antywirusowego. Aktualizacje zawierają ważne zmiany, które poprawiają wydajność i bezpieczeństwo urządzeń. Obecnie aktualizacje wydawane są nawet co miesiąc, ale warto aktywować tryb dobowej kopii bezpieczeństwa. Znacznie zwiększa to bezpieczeństwo, ponieważ programiści mogą szybko niwelować zauważone luki bezpieczeństwa, jeszcze lepiej chroniąc urządzenia przed złośliwym oprogramowaniem.

Prostym krokiem, który należy wykonać, jest także upewnienie się, że oprogramowanie chroniące przed *malware* jest zainstalowane i używane oprócz standardowego oprogramowania antywirusowego. Narzędzie to może nie tylko zapewnić ochronę przed atakami, ale także ostrzegać użytkownika, gdy dochodzi do próby ataku.

Unikaj podłączania swoich urządzeń do sieci publicznych

Korzystanie z sieci publicznej, a więc takiej, do której każdy może się podłączyć, przez sam fakt pełnej otwartości może być kanałem licznych ataków i wiąże się z zagrożeniem wycieku danych. Jeżeli musisz pracować w przestrzeni publicznej, pamiętaj o tym, by łączyć się tylko z zaufanymi sieciami i zawsze przy pomocy VPN lub połączeniem z telefonu (poprzez tzw. hotspot).

Czym więc jest VPN?

To wirtualne sieci prywatne, które zapewniają bezpieczne, bezpośrednie połączenia z siecią komputerową organizacji. Mogą być niezbędne podczas uzyskiwania dostępu do plików, pracy z poufnymi informacjami lub korzystania z niektórych witryn internetowych.

VPN szyfruje połączenia użytkowników z jej serwerami, pozwalając na bezpieczny i pewny dostęp do sieci organizacji. Szyfrowany tunel korporacyjnej sieci VPN pomoże także zapewnić bezpieczeństwo danych w trakcie ich przesyłania. Uniemożliwi również atakującym, którzy nie mają korporacyjnej sieci VPN, dostęp do serwerów.

Bezpieczeństwo VPN można zwiększyć poprzez zastosowanie solidnej metody uwierzytelniania. Wiele sieci VPN używa nazwy użytkownika i hasła, ale można pomyśleć też o uaktualnieniu i wykorzystaniu kart inteligentnych (*smart cards*) pozwalających na ochronę procesu logowania użytkowników i lepszą kontrolę dostępu do konta.

Oczywiście nie ma znaczenia, jak silna jest sieć VPN. Jeśli hasło zostanie złamane, hakerzy będą mogli łatwo się do niej dostać. Należy więc regularnie je aktualizować. Korzystanie z VPN warto ograniczyć tylko do sytuacji, gdy jest to konieczne. Jeśli urządzenia służbowe do użytku osobistego są używane wieczorami lub w weekendy (jeśli jest to zgodne z polityką firmy), VPN najlepiej wyłączyć.

Co poza VPN?

Inną możliwością jest wykorzystanie sieci 5G. Oferuje ona lepszą łączność i obiecuje większe bezpieczeństwo niż w przypadku korzystania z połączeń wi-fi czy nawet VPN. Zapowiadane rzadsze opóźnienia w przypadku 5G mogą sprawić, że stanie się ona realną alternatywą dla wi-fi. Technologia ta ma wbudowane szyfrowanie poprzez narzędzia uniemożliwiające śledzenie czy *spoofing*.

Podczas pracy w domu, należy koniecznie zabezpieczyć także router domowy. Powinien on być zaktualizowany i zabezpieczony długim, unikalnym hasłem – innym niż hasło automatyczne, w które wyposażony jest każdy router. Można w tym celu wejść na stronę ustawień routera, wpisując odpowiednią frazę w przeglądarce i zmienić tam hasło. Na tej samej stronie można najczęściej również zmienić SSID, czyli nazwę sieci bezprzewodowej, aby utrudnić osobom

trzecim identyfikację i dostęp do domowej sieci wi-fi. Nie należy używać swojego nazwiska, adresu zamieszkania ani niczego, co mogłoby posłużyć do identyfikacji.

Należy upewnić się też, że włączone jest szyfrowanie sieci, co zwykle można zrobić w ustawieniach bezpieczeństwa na stronie konfiguracji sieci bezprzewodowej. Do wyboru jest kilka metod zabezpieczeń, takich jak WEP, WPA i WPA2. Najsilniejszą z nich jest WPA2, która wymaga sprzętu nowszego niż z 2006 r.

3. Wpływ cyfryzacji na rynek pracy

3.1. Dyskryminacyjne traktowanie w procesach rekrutacji

W świecie przed zaawansowaną technologią wszelkie decyzje dotyczące zatrudnienia i ewaluacji pracownika podejmowane były przez ludzi. Decyzje te zwykle uwzględniały kontekst lokalny, kwestie etyczne, aspekty prawne w zakresie transparentności procesu i słuszności wyborów kadry zarządczej. Obecnie jednak wiele firm korzysta z systemów informatycznych, które oferują większą wydajność i pozwalają ograniczyć żmudne analizowanie dokumentów w poszukiwaniu konkretnych informacji.

Systemy te, znane jako ADS (algorytmiczne systemy decyzyjne, ang. *algorithmic decision systems*), opierają się na analizie dużych ilości danych przetwarzanych w celu uzyskania wyników, które stanowią następnie podstawę do podejmowania decyzji. Ludzka interwencja w ten proces zwykle jest znikoma, a w niektórych przypadkach może być całkowicie wyeliminowania. Wpływ danej decyzji na konkretną osobę może mieć jednak ogromne znaczenie, ponieważ kształtować będzie jej sytuację życiową.

Całkowite poleganie na ADS w procesie decyzyjnym wiąże się więc z wieloma wątpliwościami natury etycznej, politycznej czy prawnej. Ze względu na ryzyko przenoszenia przez algorytmiczne systemy uprzedzeń ich twórców, nieograniczone zawierzanie technologii budzi kontrowersje w szczególności w odniesieniu do takich obszarów, jak zatrudnienie czy dostęp do usług prywatnych i publicznych (np. służby zdrowia, systemów oceny zdolności kredytowej).

3.1.1. Co może zrobić osoba dotknięta algorytmiczną dyskryminacją

Przyjmuje się, że w procesie rekrutacyjnym powinny być stosowane przepisy dotyczące równego traktowania w zatrudnieniu (w Polsce tę kwestię ujęto art. 18 [3a] i nast. Kodeksu pracy) oraz zakazu dyskryminacji (art. 11 [3] Kodeksu pracy). Oznacza to, że jakakolwiek dyskryminacja w zatrudnieniu (w szczególności ze względu na płeć, wiek, niepełnosprawność, rasę, religię, narodowość, przekonania polityczne, przynależność związkową, pochodzenie etniczne, wyznanie, orientację seksualną) jest niedopuszczalna.

Zdarzają się jednak przypadki dyskryminującego zachowania w procesie rekrutacji. Chodzi m.in. o preferowanie kandydatów płci męskiej, odmawianie przyjmowania do pracy młodych mężatek bądź kobiet posiadających dzieci czy umieszczania w ofertach klauzul dyskryminujących osoby z zagranicy. Wykluczające kryteria mogą być tym częściej obecne, im większy jest stopień wykorzystywania przez firmę e-rekrutacji opartej na systemach zautomatyzowanego

podejmowania decyzji. Może wówczas dochodzić nie tylko do niecelowego dyskryminowania kandydatów poprzez stronnicze AI – zarząd firmy może celowo wprowadzać do systemu dyskwalifikujące kryteria.

W przypadku dyskryminacji w procesie rekrutacyjnym, objawiającej się wykluczającą treścią ogłoszenia bądź niedyskretnymi pytaniami o życie prywatne i rodzinne, osoba poszkodowana może dochodzić ochrony swojego interesu na drodze sądowej. Ciężar dowodu w takim postępowaniu spoczywa na pracodawcy, a potencjalny kandydat musi jedynie uprawdopodobnić, że dyskryminacja miała miejsce (art. 18 [3b] k.p.). W przypadku, gdy sąd potwierdzi naruszenie, pracodawca zobowiązany będzie wypłacić dyskryminowanej osobie odszkodowanie w wysokości nie niższej niż minimalne wynagrodzenie za pracę.

Przy algorytmicznym podejmowaniu decyzji wykazanie nieuzasadnionego odrzucenia w procesie rekrutacyjnym oraz dochodzenie roszczeń z tego tytułu jest jednak znacznie trudniejsze. Jest to związane z tzw. problemem czarnej skrzynki (*black box problem*), czyli brakiem transparentności w działaniu narzędzi sztucznej inteligencji. Sprawia on, że często nawet sami twórcy, a więc także pracodawcy wdrażający dane narzędzie AI, nie są świadomi jego niepożądanego działania. Jednak nie oznacza to, że są oni zwolnieni z odpowiedzialności za naruszenia. Osoba podejrzewająca, że została nieuczciwie odrzucona przez algorytm, może podjąć konkretne kroki celem ochrony jej interesu i zmiany decyzji podjętej przez system.

Kluczowy w tej kwestii pozostaje art. 22 rozporządzenia o RODO. Przepis ten nakłada na administratora danych obowiązek wdrożenia odpowiednich środków ochrony praw, wolności i uzasadnionych interesów osób, których dane (a więc i decyzje) dotyczą, a także mechanizmów umożliwiających konkretnej osobie zakwestionowanie decyzji opartej jedynie na zautomatyzowanym przetwarzaniu.

Jeżeli, Twoim zdaniem, w procesie e-rekrutacji niesłusznie odrzucono Twoją kandydaturę:

1. Zweryfikuj, czy decyzja była całkowicie zautomatyzowana. W tym celu przeczytaj dokładnie warunki prowadzenia rekrutacji bądź skontaktuj się z działem HR firmy i ustal, jak działa algorytm w kontekście procesu aplikowania o pracę.
2. Poproś firmę (administratora danych) o możliwość przedstawienia Twojej perspektywy i tego, z jakiego powodu uważasz odrzucenie za niesłuszne.
3. Zawnioskuj o wyjaśnienie decyzji przez firmę i poproś o ponowne przeanalizowanie Twojej aplikacji, ale tym razem przez człowieka. Administrator ma obowiązek, najszybciej jak to możliwe, odpowiedzieć na takie żądanie (maksymalnie w terminie miesiąca). W ciągu miesiąca administrator powinien także poinformować o niespełnieniu żądania i jego przyczynach.

4. Jeżeli jednak administrator zignoruje żądanie albo odpowiedź nie będzie satysfakcjonująca, można szukać wsparcia u organów ochrony danych osobowych i złożyć skargę.
5. Dodatkowo, niezależnie od postępowania przed organem ochrony danych osobowych, masz prawo do ochrony swoich praw przed sądem cywilnym. Jeżeli uznasz, że przetwarzanie Twoich danych narusza przepisy prawa, możesz pozwać administratora danych lub podmiot przetwarzający. Przed sądem możesz żądać odszkodowania za naruszenie przepisów o ochronie danych osobowych, a także podnosić kwestie dyskryminacji, które spowodowały szkodę majątkową lub niemajątkową.

3.1.2. Unijne regulacje dotyczące AI a proces rekrutacyjny

Jak już wspomniano, w projekcie rozporządzenia w sprawie sztucznej inteligencji (AI Act) kwestie związane z zatrudnieniem i zarządzaniem zasobami ludzkimi zostały umieszczone na liście systemów o wysokim poziomie ryzyka. Oznacza to, że narzędzia służące chociażby do zautomatyzowanej oceny kandydata na dane stanowisko, będą musiały przejść specjalną ścieżkę, aby być dopuszczone do obrotu.

Wiele obowiązków spoczywać będzie na dostawcach systemów AI, którzy podlegać będą restrykcyjnym wymogom w zakresie projektowania, testowania, audytowania i certyfikowania systemów AI. Co więcej, podmioty wykorzystujące systemy AI proponowane przez dostawców (np. firmy) będą zobowiązane wykorzystywać je zgodnie z prawem i instrukcją obsługi oraz zapewniać adekwatność danych wprowadzanych do systemów, ich monitorowanie i przechowywanie rejestrów zdarzeń na wypadek incydentów.

Oczekuje się, że nowe obostrzenia zapewnią dodatkowe zabezpieczenie przed nacechowanymi dyskryminacyjnie, pozbawionymi czynnika ludzkiego decyzjami. Równocześnie AI Act nie przyznaje dodatkowych uprawnień samym podmiotom dotkniętym przez takie decyzje. Unijne ramy uzupełni jednak planowana dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję (*AI Liability Directive*, AILD), która po raz pierwszy wprowadzi przepisy dotyczące szkód wyrządzonych przez systemy sztucznej inteligencji. Jej celem jest ustanowienie szerszej ochrony osób poszkodowanych przez stosowane AI oraz ułatwienie im dochodzenia roszczeń. Projektowane przepisy stanowią więc krok naprzód w zapewnieniu skutecznego dostępu do środków zaradczych także w przypadku dyskryminacji w zakresie stosowania systemów zatrudniania. Zakładają one bowiem, że to pracodawca nie dopełnił obowiązku dochowania należytej staranności, wykorzystując system zatrudniania, który dyskryminuje określone kategorie osób.

Prace zarówno nad projektem rozporządzenia dotyczącego sztucznej inteligencji (AI Act), jak i dyrektywą w sprawie odpowiedzialności za sztuczną inteligencję są już na zaawansowanym

etapie. Jednak zgodnie z aktualnym brzmieniem nowych regulacji, ich przepisy będą stosowane we wszystkich państwach członkowskich UE dopiero po upływie dwóch lat od ich przyjęcia.

3.2. Przyszłość pracy

3.2.1. Ginące zawody, kompetencje przyszłości i odpowiedzialność pracodawcy za dostosowanie umiejętności pracowników do automatyzacji

Jak pokazują najnowsze badania Centrum Badań nad Polityką Gospodarczą (CEPR), nawet 40% respondentów twierdzi, że prawdopodobieństwo, że w najbliższym dziesięcioleciu zostaną zastąpieni przez maszynę, robota lub algorytm wynosi więcej niż 50%. Obawy przed bezrobociem technologicznym nie są całkowicie nieuzasadnione. Jak wynika z raportu *Future Jobs*, znacznie zwiększa się udział nowych technologii w wykonywanych zadaniach. W 2018 r. średnio 71% czasu pracy stanowiły czynności wykonywane przez ludzi, a 29% te wykonywane maszynowo. Prognozuje się, że do 2025 r. proporcje te ulegają istotnej zmianie. Ludzie będą odpowiedzialni za ok. 48% działań, podczas gdy pozostałe 52% zadań będzie w pełni zautomatyzowane.

Jeżeli chodzi o skutki automatyzacji, to można zakładać, że najbardziej odczują ją osoby wykonujące pracę fizyczną, która może być łatwo zastąpiona przez roboty (tj. opartą na przewidywalnych sekwencjach). Digitalizacja może jednak wpłynąć także na sytuację niektórych specjalistów. Według raportu *Future of Jobs* pośród zbędnych zawodów, takich jak mechanik, magazynier i kierownik produkcji, znajdziemy także analityka finansowego czy urzędnika. Eksperci McKinsey Global Institute studzą jednak te obawy – szacuje się bowiem, że globalnie jedynie 5% zawodów zostanie całkowicie zlikwidowanych.

Niewątpliwie zmienią się natomiast sposób wykonywania obowiązków służbowych (większy udział systemów IT i maszyn w wykonywanych obowiązkach) oraz pożądane kompetencje pracowników. Mając na uwadze, że wiele zadań będzie wykonywanych przez maszyny, wzrośnie popyt na umiejętności, których komputery nie są w stanie precyzyjnie odtworzyć. Mowa tutaj o kompetencjach miękkich, czyli tych, które wymagają kreatywności, inteligencji emocjonalnej, krytycznego myślenia. Digitalizacja zwiększy także zapotrzebowanie na umiejętności techniczne i stworzy miejsca pracy dla dobrze wykwalifikowanych pracowników umysłowych, zdolnych obsługiwać nowe systemy. To natomiast może rodzić obawy o rosnącą polaryzację rynku (gorsze położenie pracowników fizycznych przy rosnącym znaczeniu na tych najlepiej wykształconych). Niepokoje te zdają się potwierdzać wyniki badania Europejskiego Centrum Rozwoju Kształcenia Zawodowego (Cedefop), które wykazały, że ponad 70% zatrudnionych potrzebuje co najmniej podstawowych umiejętności informatycznych w celu odnalezienia się na dzisiejszym rynku pracy,

ale aż 30% z nich jest zagrożonych trwałą niezdolnością nabycia pożądanych kompetencji (a więc także utratą pracy).

3.2.2. Kompetencje przyszłości i zawody zbędne w dobie digitalizacji

Coraz to powszechniejsze stosowanie technologii będzie oznaczać, że w ciągu najbliższych lat znacznie zmienią się pożądane na rynku pracy kompetencje. Przewiduje się, że wraz z automatyzacją i algorytmizacją zmniejszy się popyt na umiejętności łatwo zastępowalne przez maszyny. Mowa tutaj zarówno o zdolnościach manualnych (w przypadku pracowników fizycznych, produkcyjnych), jak również tych dotyczących pracy umysłowej (np. liczenia czy twórczego pisania). Zwiększy się natomiast zapotrzebowanie na **kompetencje przyszłości** definiowane w raporcie DELab (*Kompetnecje przyszłości. Jak je kształtować w elastycznym ekosystemie edukacyjnym*?) jako: *konkretne umiejętności umożliwiające podejmowanie i realizowanie zadań w środowisku pracy, które jest z gruntu elastyczne, rozproszone geograficznie, podatne na częste i szybkie zmiany, zakłada konieczność operowania technologiami cyfrowymi i współpracę ze zautomatyzowanymi systemami i maszynami wykorzystującymi sztuczną inteligencję*.

Kompetencje te firma McKinsey podzieliła na trzy grupy: techniczne i cyfrowe, społeczne oraz poznawcze.

Kompetencje przyszłości	
Techniczne i cyfrowe	• Wskazuje się, że popyt na **podstawowe** umiejętności cyfrowe wzrośnie o 65%. Mowa tutaj o zdolnościach posługiwania się technologią w codziennej pracy, zwłaszcza w dziedzinie rozwiązywania problemów i wyszukiwania informacji. • Do 2030 r. pracownicy w Europie będą przeznaczać ponad 40% czasu więcej na czynności wykorzystujące zaawansowane kompetencje cyfrowe. Co więcej, popyt na umiejętności programistyczne i informatyczne wzrośnie o 90%
Społeczne	• Do 2030 r. na europejskim rynku pracy popyt na kompetencje społeczne, przede wszystkim przedsiębiorczość i zdolność do podejmowania inicjatyw, wzrośnie o 22%
Poznawcze (wyższe): krytyczne myślenie,	• Zapotrzebowanie na wyższe kompetencje poznawcze

kreatywność, umiejętność zarządzania ludźmi	wzrośnie o 14% do 2030 r. Równocześnie o 23% spadnie znaczenie podstawowych umiejętności poznawczych, takich jak czytanie, pisanie, a także podstawowe przetwarzanie danych

Kompetencje przyszłości w podziale na trzy grupy umiejętności: poznawcze, społeczne i techniczne

Światowe Forum Ekonomiczne (ŚFE) wskazuje, że w najbliższych latach najważniejsze będą umiejętności, takie jak:

- **zarządzanie ludźmi (HR)** – budowanie kadry pracowniczej poprzez wyszukiwanie najlepszych osób do wykonywania konkretnych zadań; motywowanie oraz zarządzanie ludźmi podczas pracy,
- **umiejętność negocjowania** – zdolność rozwiązywania konfliktów i pokonywania różnic zdań; wykazywanie się siłą perswazji,
- **inteligencja emocjonalna** – umiejętność identyfikowania i nazywania emocji własnych i innych osób; zdolność radzenia sobie z emocjami i wykorzystywania ich przy dokonywaniu oceny i podejmowaniu decyzji; zrozumienie potrzeb innych (pracowników i klientów),
- **współpraca z innymi** – umiejętność pracy w grupie,
- **elastyczność poznawcza** – zdolność „przełączania się" pomiędzy wykonywanymi zadaniami,
- **rozwiązywanie złożonych problemów** – umiejętność wypracowywania nieoczywistych rozwiązań w różnych kontekstach,

- **krytyczne myślenie** – wykorzystanie logiki i rozumowania do zidentyfikowania mocnych i słabych stron alternatywnych rozwiązań, wniosków lub podejść do problemów,
- **kreatywność** – zdolność do nieszablonowego myślenia, wychodzenia z innowacyjnymi pomysłami, rozwiązywania problemów w nieoczywisty sposób.

Co więcej, ŚFE w swoim raporcie wymienia także **zawody, które stracą na znaczeniu w dobie digitalizacji**. Zaliczono do nich profesje, takie jak: pracownik wprowadzający dane, pracownik księgowości i listy płac, sekretarz administracyjny i wykonawczy, pracownik montażu i produkcji, pracownik działu informacji i obsługi klienta, menedżer administracji i usług biznesowych, księgowy i rewident, magazynier, główny menadżer i kierownik operacyjny, urzędnik pocztowy, analityk finansowy, kasjer i kontroler biletów, mechanik, telemarketer, elektronik i instalator telekomunikacyjny, bankier, kierowca, broker i agent sprzedaży, obwoźny sprzedawca i akwizytor, pracownik ubezpieczeń, działu statystycznego i finansowego, prawnik.

Zawody – prognoza na 2020 r.

Stabilne zawody	Nowe zawody	Zbędne zawody
Dyrektor zarządzający i prezes	Analityk danych i data scientist*	Pracownik wprowadzający dane
Główny menadżer i kierownik operacyjny*	Specjalista AI i ML	Pracownik księgowości i listy płac
Programista i analityk oprogramowania*	Główny menadżer i kierownik operacyjny*	Sekretarz administracyjny i wykonawczy
Specjalista działu sprzedaży i marketingu*	Specjalista Big Data	Pracownik montażu i produkcji
Przedstawiciel handlowy	Specjalista ds. transformacji technologicznej	Pracownik działu informacji i obsługi klienta*
Specjalista ds. zarządzania zasobami ludzkimi	Specjalista działu sprzedaży i marketingu*	Menadżer administracji i usług biznesowych
Doradca finansowy i inwestycyjny	Specjalista ds. nowych technologii	Księgowy i rewident
Specjalista ds. baz danych i sieci	Specjalista ds. rozwoju organizacji*	Magazynier
Specjalista ds. logistyki i łańcucha dostaw	Programista i analityk oprogramowania*	Główny menadżer i kierownik operacyjny*
Specjalista ds. zarządzania ryzykiem	Specjalista ds. automatyzacji procesów	Urzędnik pocztowy
Analityk bezpieczeństwa danych*	Specjalista ds. innowacji	Analityk finansowy
Analityk zarządzania i organizacji	Analityk bezpieczeństwa danych*	Kasjer i kontroler biletów
Inżynier elektrotechniki	Specjalista działu e-commerce i mediów społecznościowych	Mechanik
Specjalista ds. rozwoju organizacji*	Projektant UX i interakcji maszyna-człowiek	Telemarketer
Operator zakładu przetwórstwa chemicznego	Specjalista ds. szkoleń i rozwoju	Elektronik i instalator telekomunikacyjny
Nauczyciel uniwersytecki i szkolnictwa wyższego	Specjalista i inżynier robotyki	Bankier
Urzędnik ds. zgodności	Specjalista ds. ludzi i kultury	Kierowca
Inżynier energetyki i naftowy	Pracownik działu informacji i obsługi klienta*	Broker i agent sprzedaży
Specjalista i inżynier robotyki	Projektant usług i rozwiązań	Obwoźny sprzedawca i akwizytor
Operator i pracownik rafinerii ropy naftowej i gazu ziemnego	Specjalista ds. marketingu i strategii online	Pracownik ubezpieczeń, działu statystycznego i finansowego
		Prawnik

Źródło: World Economic Forum (2018) The Future of Jobs Report 2018, s. 9. Zawody oznaczone * występują w więcej niż jednej kolumnie tabeli, co spowodowane jest różnicami między poszczególnymi sektorami.

3.2.3. Digitalizacja a trendy w obszarze zarządzania przedsiębiorstwem – rola pracodawców

Aby w pełni wykorzystać digitalizację oraz korzyści płynące z wdrażania nowych technologii, firmy będą musiały przeorganizować swoje struktury i zmienić dotychczasowe podejście do pracy. Wymagać to będzie przeprojektowania formalnej organizacji firmy, uzupełniania kadry o pracowników posiadających nowe kompetencje, przekwalifikowywania bądź rozwijania posiadanych talentów. Według McKinsey, ze względu na zmianę pożądanych zawodów i najbardziej cenionych umiejętności, organizacje będą zobowiązane wprowadzić **aktualizację w pięciu kluczowych obszarach** — sposobie myślenia, strukturze organizacyjnej, alokacji pracy, składzie kadry pracowniczej oraz obowiązkach kadry zarządzającej i HR.

Jeżeli chodzi o sposób myślenia w firmie, kluczem do przyszłego sukcesu organizacji będzie promowanie trendu tzw. uczenia się przez całe życie (*lifelong learning*), a więc oferowanie pracownikom możliwości zdobywania nowych umiejętności i wiedzy podczas całej ścieżki kariery, nie zaś jedynie na jej początku. W zakresie struktury organizacyjnej wskazuje się, że priorytetem w nadchodzących latach będzie wprowadzenie bardziej dynamicznych i innowacyjnych sposobów zarządzania, a także częstsza współpraca pomiędzy zespołami i wymienianie się wiedzą oraz funkcjami przez pracowników.

Firmy wdrażające automatyzację na szeroką skalę spodziewają się także przekazywania zadań wykonywanych obecnie przez pracowników o wysokich kwalifikacjach, pracownikom o niższych kwalifikacjach (wspieranym przez maszyny i komputery). Jeśli chodzi o kadrę pracowniczą, to przewidywane jest częstsze sięganie po pomoc różnego rodzaju freelancerów i pracowników tymczasowych. Wynikać to będzie z rozrastania się tzw. gospodarki współdzielenia/na żądanie (*sharing economy; on-demand economy*), czyli modeli biznesowych opartych na pośrednictwie platform współpracy, tworzących ogólnodostępny rynek czasowego korzystania z dóbr lub usług, często dostarczanych przez osoby prywatne.

Zachowanie konkurencyjności firmy przy równoczesnym wsparciu pracowników w procesie digitalizacji

W raporcie *Poza zatrudnieniem. Jak firmy zmieniają kwalifikacje, aby rozwiązać problem niedoboru talentów* McKinsey przedstawiło różne taktyki pozwalające na zachowanie konkurencyjności przedsiębiorstw i zniwelowanie luki pomiędzy pożądanymi a dostępnymi umiejętnościami pracowników sektora prywatnego. Pośród praktyk, które powinni rozważyć pracodawcy dążący do rozwoju swojej firmy i budowania kompetentnej kadry pracowniczej, znalazły się:

- **Przekwalifikowywanie** – zachęcanie do zdobywania nowych kompetencji i podnoszenia dotychczasowych umiejętności przez zatrudnionych pracowników, a także wdrażanie i kształcenie nowozatrudnionych osób w zakresie pożądanych zdolności. Kluczową kwestią dla firm będzie zdecydowanie o sposobie przeprowadzania szkoleń: wewnętrznie (z wykorzystaniem dostępnych zasobów i programów) bądź zewnętrznie (w ramach współpracy z instytucją edukacyjną bądź ośrodkiem szkoleniowym). Jeżeli chodzi o obszary, w które przedsiębiorcy planują inwestować, to najczęściej dotyczą one budowania umiejętności strategicznych dla ich firmy, tj. zaawansowanych kompetencji IT, umiejętności twórczego pisania, krytycznego myślenia, zdolności rozwiązywania problemów. Natomiast w przypadku mniej złożonych umiejętności, pracodawcy deklarują możliwość zatrudniania osób spoza organizacji.

- **Przenoszenie w ramach przedsiębiorstwa** – przenoszenie pracowników o określonych umiejętnościach do działów/zespołów, w których lepiej mogą wykorzystywać swoje umiejętności. W ankiecie McKinsey przeprowadzonej wśród zarządców firm w lutym 2018 r. 55% respondentów stwierdziło, że wolałoby relokować część pracowników na inne lub zupełnie nowe stanowiska niż całkowicie ich zwolnić.

- **Zatrudnianie** – pozyskiwanie pojedynczych osób lub całych zespołów o wymaganych, specyficznych umiejętnościach (choć podaż ekspertów na rynku może być niewystarczająca, aby wszystkie firmy mogły realizować tę strategię). Z jednej strony koszty zatrudniania mogą być niższe niż przekwalifikowania, jednak z drugiej – pozyskiwanie nowych członków zespołu wiąże się z ryzykiem, jak dana osoba będzie wykonywać swoją pracę. Aby z sukcesem pozyskiwać nowe, kluczowe talenty, firmy powinny więc wprowadzać innowacje w sposobie rekrutowania kandydatów, a także oferować atrakcyjną kulturę pracy i benefity pozapłacowe.

- **Tworzenie nowych form współpracy** – firmy mogą korzystać z umiejętności wnoszonych przez osoby spoza organizacji (freelancerów, ekspertów, agentów tymczasowych z agencji pośrednictwa pracy). Minusem tego modelu jest jednak ryzyko przekazywania osobom postronnym tajemnic handlowych (np. know-how, utworów objętych prawem własności intelektualnej), a także trudności w dopasowaniu się do kultury i trybu pracy firmy. Z tego względu pracodawcy deklarują obsadzenie niezależnymi kontraktorami stanowisk niezwiązanych z kluczowymi działaniami firmy lub wymagających niskich kwalifikacji.

- **Ewentualne zwolnienia** – zwalnianie pracowników może być konieczne w niektórych firmach, a zwłaszcza w branżach, które nie rozwijają się dość dynamicznie i gdzie automatyzacja w znaczący sposób zastąpi siłę roboczą. Strategię zwolnień można

zrealizować poprzez ograniczenie lub wstrzymanie zatrudniania nowych pracowników, przy jednoczesnym umożliwieniu kontynuowania normalnego procesu wycofywania się i przechodzenia na emeryturę zatrudnionych już osób.

Choć zwolnienia pracowników spowodowane szerszym wykorzystywaniem maszyn są możliwe, trudno spodziewać się, aby pracownicy wszystkich sektorów musieli obawiać się o swoje stanowiska. Niewątpliwie jednak pojawią się nowe technologie, systemy i programy, które będą wymagać zdobycia dodatkowych umiejętności w obszarze IT.

Jak pracodawcy mogą wspierać swoich pracowników w procesie digitalizacji przedsiębiorstwa? Przede wszystkim mogą oni:

- zapoznać pracowników z nowymi narzędziami – wyeliminować strach i zachowawczość względem nowych technologii oraz pokazać, jak można wykorzystywać narzędzia cyfrowe w codziennej pracy,
- podnosić świadomość pracowników – wyjaśniać, dlaczego i w jaki sposób firma korzysta z danej technologii; mając informacje w tym zakresie, pracownicy lepiej zrozumieją nowe narzędzia pracy i będą zmotywowani do korzystania z nich,
- dobrze przygotować kadrę kierowniczą na nadchodzące zmiany – kierownictwo powinno znać odpowiedzi na podstawowe pytania dotyczące nowych narzędzi pracy oraz pokazywać pozostałym członkom zespołu, w jaki sposób korzystać z wdrażanych technologii,
- przeprowadzić szkolenia z nowych systemów – nawet pracownicy biegle posługujący się technologią potrzebują czasu, aby zapoznać się z nowymi programami i narzędziami cyfrowymi, z których dotychczas nie korzystali; firma powinna zapewnić profesjonalne szkolenia dla wszystkich pracowników.

3.2.4. Inne podmioty odgrywające ważną rolę w procesach cyfryzacji pracy i przekwalifikowywania pracowników

Instytucje edukacyjne

Rolę szkolnictwa w procesie digitalizacji zauważają już organy Unii Europejskiej. W konkluzjach Rady Europejskiej podkreślono, że dostęp do wysokiej jakości kształcenia wspieranego technologiami cyfrowymi jest warunkiem koniecznym do transformacji poszczególnych sektorów i dalszego wzrostu gospodarczego.

Także Komisja Europejska uwzględniła stworzenie planu działania w zakresie edukacji cyfrowej na lata 2021–2027 określającego wizję edukacji cyfrowej w Europie. Celem obu inicjatyw było zachęcanie uniwersytetów, szkół i kadry nauczycielskiej do odgrywania aktywniejszej roli w budowaniu kompetencji cyfrowych oraz zaspokajaniu potrzeb rynku pracy. Rolę tych instytucji w transformacji cyfrowej zdają się potwierdzać także publikacje ekonomiczne, takie jak chociażby raport PwC i ŚFE *Podnoszenie kwalifikacji dla wspólnego dobrobytu* (2021), w którym podkreślono, że instytucje szkolnictwa wyższego mają potencjał, by napędzać zmiany – podnosić ogólny poziom wiedzy, umiejętności oraz kompetencje studentów i społeczeństwa.

Władza publiczna

Rolą państwa jest wspieranie zarówno przedsiębiorców, jak i pracowników w procesie digitalizacji. Istotnym jest więc, aby decydenci wdrażali polityki sprzyjające zdobywaniu umiejętności cyfrowych bądź przekwalifikowywaniu się pracowników (np. w ramach programów dofinansowywania szkoleń dla małych i średnich przedsiębiorstw). Co więcej, ważne jest, aby pobudzać rynek pracy i unikać bezrobocia poprzez stosowanie aktywnej polityki w zakresie zatrudnienia – zamiast polegać na zasiłkach dla bezrobotnych, państwo powinno inwestować w agencje zatrudnienia, które staną się centrami pośrednictwa pracy i ułatwią przekwalifikowanie osób bezrobotnych.

Organizacje pozarządowe

Organizacje pozarządowe i think tanki często występują jako inkubatory rozwiązań korzystnych społecznie. Mają zwykle większą swobodę w działaniu niż instytucje państwowe i mogą wychodzić z propozycjami różnych rozwiązań problemów. Z tego względu niektóre firmy podejmują inicjatywy filantropijne lub współpracują z fundacjami w obszarach związanych z nabywaniem nowych umiejętności przez pracowników. Przykładem jest inicjatywa Generation działająca na rzecz walki z bezrobociem poprzez likwidowanie luki w kompetencjach wśród młodych ludzi, a także wspieranie osób dorosłych w poszukiwaniu odpowiednich dla nich stanowisk poprzez rekrutowanie, szkolenie i mentoring.

Związki zawodowe i organizacje branżowe

Działając jako partnerzy społeczni, stowarzyszenia branżowe i związki zawodowe odgrywają ważną rolę w procesie digitalizacji rynku pracy. Przykładowo w Szwecji tworzone są rady ochrony pracy finansowane przez firmy i związki zawodowe. Podmioty te szkolą osoby, które straciły pracę – zapewniają im tymczasowe wsparcie finansowe i ułatwiają proces przekwalifikowywania, aby bezrobotni szybciej wrócili na rynek pracy.

3.3. Nowe modele biznesowe i ich wpływ na rynek pracy

3.3.1. Erozja siły przetargowej pracowników – jak nowe technologie utrudniają zrzeszanie się pracowników

Nowe technologie ułatwiają komunikację i łączą ze sobą użytkowników, pomimo dzielącej ich odległości. Równocześnie jednak prowadzą do większego wyobcowania i coraz rzadszych interakcji międzyludzkich. Zjawisko to nie dotyczy jedynie sfery życia prywatnego, ale także zawodowego. Cyfryzacja i przeniesienie się pracy do świata online spowodowały, że pracownicy sporadycznie nawiązują trwałe relacje oraz rzadziej spotykają się i dyskutują o problemach w miejscu pracy.

Nowe technologie sprzyjają izolacji nie tylko w przypadku pracy zdalnej. Narzędzia AI wykorzystywane przez przedsiębiorców do kontrolowania pracowników oraz mierzenia ich wydajności często stosowane są także do inwigilowania i utrudniania pracownikom zrzeszania się.

Bywa, że modele biznesowe dużych firm opierają się na szeroko zakrojonej kontroli pracowników i ciągłym podnoszeniu tempa pracy. Zrzeszanie się pracowników w celu reprezentowania ich zbiorowych i indywidualnych praw oraz interesów stanowi więc realne ryzyko dla systemu, w którym liczy się jedynie maksymalizacja zysków przedsiębiorcy. Z tego względu koncerny stosują środki zmierzające do tego, by uniemożliwić pracownikom uzwiązkowienie się. Praktyka ta nasiliła się podczas pandemii COVID-19, kiedy to zaczęto wykorzystywać wprowadzone w tym okresie zalecenia BHP do tego, by wdrożyć w zakładach pracy narzędzia do pomiaru dystansu pomiędzy osobami w magazynach, zakazując im równocześnie przebywania zbyt blisko siebie. Firmy zaczęły nabywać oprogramowania umożliwiające analizowanie i wizualizowanie danych dotyczące związków powstających wewnątrz zakładów pracy (np. geoSPatial Operating Console lub SPOC). Co więcej, działy kadr monitorowały listy mailingowe pracowników wykorzystywane do celów aktywistycznych czy grupy pracowników w mediach społecznościowych.

W przypadku pracy platformowej wpływ nowych technologii na zrzeszanie się pracowników nie jest jednoznacznie pozytywny bądź negatywny. Aplikacje wykorzystywane do świadczenia usług mogą ułatwiać mobilizowanie się kurierów i kierowców – dostępne w ich systemach czaty wewnętrzne oferują pracownikom platformowym (ang. *gig-worker*) przestrzeń do wymiany informacji, a masowe sieci komunikacyjne mogą łączyć pojedynczych kurierów na poziomie miast, regionów, a nawet krajów.

Równocześnie skuteczność związków zawodowych pracowników platformowych często zależy od poparcia władz publicznych dla różnych form samoorganizacji. Przykładowo w Bolonii we współpracy ze związkowcami utworzono *Kartę praw podstawowych pracy cyfrowej*

w kontekście miejskim (wł. *Carta dei diritti fondamentali del lavoro digitale nel Contesto Urbano*) ustanawiającą ramy minimalnych norm dotyczących wynagrodzenia, czasu pracy i ochrony ubezpieczeniowej pracowników platformowych. Co jednak istotne, sam burmistrz Bolonii okazywał wiele wsparcia dla inicjatywy i wezwał klientów do bojkotu platform, które nie podpisały karty.

W krajach, w których państwo nie roztacza opieki nad pracownikami platformowymi, poziom ich uzwiązkowienia jest znacznie niższy, a siła przetargowa słabsza. Bywa to nadużywane przez platformy, które wykorzystują mechanizmy w aplikacjach do tego, by lepiej kontrolować kurierów czy kierowców oraz udaremniać próby sprzeciwiania się polityce firmy.

Przykładem tego, jak za pomocą technologii giganci gospodarki współdzielenia ograniczają inicjatywy pracowników walczących o swoje prawa, jest szybko uciszony strajk polskich kurierów dowożących posiłki w kwietniu 2021 r. Powodem strajku był nieuczciwy sposób rozdzielania zleceń i wynagradzania przez algorytm, a metodą sprzeciwu zaprzestanie realizowania zamówień przez kurierów, mimo deklarowanej w aplikacji gotowości do pracy. Kierowcy liczyli, że wywrą presję na przedsiębiorcy i skłonią go do rozmów z reprezentantami społeczności. Jednak firma za pomocą aplikacji, bez jakiejkolwiek próby porozumienia się z kurierami, zablokowała strajkujących i przekazała ich zamówienia osobom, które gotowe były wykonać pracę pomimo krzywdzących warunków.

3.3.2. Wpływ cyfryzacji na rynek pracy – praca platformowa

Praca platformowa jest formą zatrudnienia, w ramach której pracownik korzysta z platformy cyfrowej, aby uzyskać dostęp do innych organizacji lub osób w celu świadczenia określonych usług w zamian za dane wynagrodzenie. Do zadań wykonywanych odpłatnie za pośrednictwem platform cyfrowych należą m.in. przewozy taksówkarskie i kurierskie, dostawy, serwis napraw domowych, jak i prace umysłowe, np. copywriting czy księgowość. Choć aplikacje, takie jak Uber czy Bolt rozwijają się w europejskiej przestrzeni dopiero od dekady, to pracownicy świadczący usługi w ramach platform tego typu stanowią dziś znaczną część siły roboczej (28,3 mln pracowników w 2022 r. w Unii Europejskiej). Jest to liczba porównywalna do liczby osób zatrudnionych w sektorach produkcji przemysłowej (29 mln pracowników). Co więcej, według Komisji Europejskiej, do 2025 r. na platformach ma przybyć kolejne 15 milionów zatrudnionych. Do najbardziej popularnych platform w UE należą Uber, Deliveroo, Amazon Mechanical Turk, Fiverr, Upwork, Appjobs, Glovo czy JustEat (w Polsce znane jako Pyszne.pl).

Model biznesowy platform pracy opiera się na technologiach wykorzystujących algorytmy do tego, aby skutecznie dopasować podaż i popyt na pracowników i świadczone przez nich usługi. Dodatkowo, wykorzystanie odpowiednio zaprojektowanych aplikacji pozwala na bezkontaktowe,

zautomatyzowane podejmowanie decyzji oraz monitorowanie wykonywanych zadań. Dzięki opartemu na algorytmach systemowi zarządzania możliwe jest zrezygnowanie z tradycyjnej kadry menadżerskiej. To natomiast sprawia, że platformy podtrzymują, iż występują w roli jedynie pośrednika, który oferuje usługi łączenia osób samozatrudnionych z potencjalnym klientem, nie zaś w roli pracodawcy.

Kto najczęściej szuka zatrudnienia za pośrednictwem platform pracy?

- osoby młode,
- mężczyźni,
- imigranci (zwłaszcza w zakresie pracy fizycznej),
- osoby z wykształceniem pomaturalnym, dla których praca ta stanowi dodatkowe źródło dochodów.

Ponadto pracowników platformowych podzielić można na dwie skrajne grupy na rynku pracy. Do pierwszej z nich należą pracownicy umysłowi, uprzywilejowani pod względem swoich kompetencji, np. programiści mogący wpływać na warunki współpracy ze zleceniodawcami (freelancing, świadczenie usług IT). W drugiej grupie znajdują się natomiast osoby o niskich, łatwo zastępowalnych kompetencjach, których siła negocjacyjna na rynku pracy jest niska (np. imigranci świadczący usługi przewozu taksówkarskiego).

Zalety i wady pracy platformowej

Do zalet pracy platformowej należą:

- elastyczne godziny pracy i możliwość samodzielnego planowania grafiku w pracy,
- bezpośredni kontakt ze zleceniodawcami,
- większa niezależność.

W obecnym kształcie platform cyfrowych, widoczne są jednak liczne wady tego typu zatrudnienia:

- Problemy z zakresu bezpieczeństwa i higieny pracy:
    - brak uregulowanych zasad BHP,
    - ryzyka fizyczne,
    - stres spowodowany niepewnością zatrudnienia;

- warunki zatrudnienia:
    - 5,5 mln osób pracujących za pośrednictwem platform pracy w UE jest niewłaściwie sklasyfikowanych jako samozatrudnione,
    - osobom błędnie sklasyfikowanym jako samozatrudnione nie przysługują te same prawa i świadczenia, co osobom zatrudnionym;
- problemy wynikające z algorytmizacji pracy,
- ograniczone możliwości zrzeszania się,
- nieprzewidywalne zarobki i godziny pracy (według Komisji Europejskiej 41% czasu pracy pracowników platformowych obejmują nieodpłatne zadania, takie jak np. przeglądanie ogłoszeń czy oczekiwanie na zlecenia).

Prawo unijne a praca platformowa

Niektóre państwa członkowskie wprowadziły już regulacje w zakresie pracy platformowej w ustawodawstwie krajowym. Dyskusje o tym szczególnym rodzaju zatrudnienia prowadzone są także na poziomie wspólnotowym. Pojęcie pracowników platformowych zostało już wprowadzone do przepisów unijnych, np. poprzez dyrektywę w sprawie przejrzystych i przewidywalnych warunków pracy w Unii Europejskiej. Przełomowa w tym zakresie ma być jednak **dyrektywa o poprawie warunków pracy platformowej**, której projekt pod koniec 2021 r. przedstawiła Komisja Europejska.

Najważniejsze przepisy zawarte w projekcie dyrektywy w sprawie poprawy warunków pracy platformowej:

- Osoby pracujące za pośrednictwem platform cyfrowych zyskają status zatrudnienia odpowiadający ich rzeczywistym warunkom pracy, co sprawdzane będzie poprzez ustalenie kryteriów potrzebnych do uznania platformy za pracodawcę.
- Platforma uznana będzie za pracodawcę, jeśli spełni co najmniej dwa z następujących kryteriów:
    - określa poziom wynagrodzenia lub ustala jego pułap,
    - nadzoruje środkami elektronicznymi wykonanie pracy,
    - ogranicza swobodę wyboru godzin pracy lub okresów nieobecności, swobodę przyjmowania lub odrzucania zadań lub swobodę korzystania z podwykonawców lub zastępstw,

- ustala konkretne wiążące reguły wyglądu i zachowania wobec odbiorcy usługi lub zleceniodawcy pracy,
- ogranicza możliwości rozbudowy bazy klientów lub wykonywania pracy na rzecz osób trzecich.

- Pracownikom platformy powinny przysługiwać prawa pracownicze i socjalne wynikające ze statusu osoby zatrudnionej:
  - gwarantowany czas odpoczynku i płatne urlopy,
  - płaca minimalna,
  - możliwość prowadzenia zbiorowych negocjacji,
  - bezpieczeństwo i ochrona zdrowia,
  - świadczenia dla bezrobotnych i chorobowe,
  - emerytury oparte na składkach.
- Platforma może zakwestionować klasyfikację, ale musi udowodnić, że stosunek pracy nie istnieje.
- Platformy zobowiązane zostaną do zwiększenia przejrzystości stosowania algorytmów oraz zapewnienia monitorowania warunków pracy przez człowieka.
- Pracownicy zyskają prawo do kwestionowania zautomatyzowanych decyzji.

Notatki

Notatki

Notatki

Notatki

Notatki

Notatki

Notatki

Notatki

Notatki

Komisja Krajowa NSZZ „Solidarność”
ul. Wały Piastowskie 24, 80-855 Gdansk

Biuro Programów Europejskich
www.solidarnosc.org.pl

DARBO RINKOS SKAITMENINIMAS

Mokymo modulis, sukurtas vykdant projektą
„Veiklų inicijavimas įgyvendinant Europos socialinių partnerių pagrindų susitarimą dėl skaitmeninimo"
bendrai finansuojamas Europos Sąjungos lėšomis

LT

Co-funded by the European Union

NSZZ Solidarność Komisja Krajowa

NSZZ Solidarność Komisja Krajowa

Darbo rinkos skaitmeninimas

Mokymo modulis, sukurtas vykdant projektą

Veiklų inicijavimas įgyvendinant Europos socialinių partnerių pagrindų susitarimą dėl skaitmeninimo,

bendrai finansuojamas Europos Sąjungos lėšomis

Co-funded by the European Union

2023 m. birželio mėn.

Autorės:

Blanka Wawrzyniak

Marta Musidłowska

Esminė parama:

Hanna Sakowicz-Daszczyńska

Redagavimas:

Julia Zaleska

Grafinis dizainas, spausdinimas

PP WiB Piotr Winczewski

ph. +48 58 341 99 89, e-mail: wib1@wp.pl

Šaltiniai:

robot hand finger /rawpixel.com/freepik.com

Tesla Robot Dance / wikimedia.org

factory worker portrait / aleksandarlittlewolf/ freepik.com

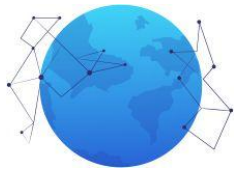
AI used in this publication: freepik.com

Nemokamas leidinys, finansuojamas Europos Sąjungos lėšomis, išleistas vykdant projektą Nr. 101051759 **Veiklų inicijavimas įgyvendinant Europos socialinių partnerių pagrindų susitarimą dėl skaitmeninimo (EFAD)** Originalus pavadinimas: "Initiating activities to implementation the European Social Partners Framework Agreement on Digitalisation (EFAD)".

Įžanginė pastaba

Šis leidinys sukurtas įgyvendinant projektą „Veiklų inicijavimas įgyvendinant Europos socialinių partnerių pagrindų susitarimą dėl skaitmeninimo” Tai vadovas, kuris bus naudojamas tiek projekto mokymų metu, tiek po jų. Mokymo moduliu siekiama parengti socialinius partnerius dinamiškiems pokyčiams, vykstantiems darbo rinkoje dėl skaitmeninės transformacijos. Tai pokyčiai, susiję, be kita ko, su gamybos automatizavimu, naujais verslo modeliais, nuotoliniu darbu ir novatoriškais valdymo metodais įmonėse. Leidinyje taip pat aptariamos darbuotojų teisės skaitmeniniame amžiuje. Juo siekiama suteikti darbuotojams priemonių, kad jie galėtų atsijungti ir išlaikyti darbo ir asmeninio gyvenimo pusiausvyrą.

Turinys



Įvadas

Nors dirbtinis intelektas (DI) yra plati sąvoka, apimanti grupę algoritmų, kurie gali keisti savo parametrus ir kurti naujus rezultatus, paprasčiausiai jį galima apibūdinti kaip mašinų gebėjimą suprasti, mokytis, planuoti ir demonstruoti kūrybiškumą.

Daugeliui ekspertų dirbtinio intelekto vystymosi tempas ir jo poveikis mus supančiam pasauliui kelia nerimą. Tam, be kita ko, įtakos turi tai, kad dirbtinio intelekto sistemas kuria didžiausios JAV ir Kinijos technologijų bendrovės, kurioms svarbiausia - komercinis pelnas. Apie nevaržomos dirbtinio intelekto plėtros pavojus įspėja ir pati technologijų pramonė. Atvirą laišką, kuriame raginama sustabdyti eksperimentus su dirbtinio intelekto sistemomis ir sistemomis, galingesnėmis už „Chat GPT-4“, pasirašė, be kita ko, tokie asmenys kaip Elonas Muskas (bendrovių „SpaceX“, „Tesla“ ir „Twitter“ generalinis direktorius), Steve'as Wozniakas (vienas iš „Apple“ įkūrėjų), Yuvalas Noah Harari (futuristas, Jeruzalės hebrajų universiteto profesorius) ir kt.

Siekiant užtikrinti, kad dirbtinio intelekto sistemos būtų saugios ir kad jose būtų atsižvelgiama į poveikį žmonių gerovei, būtina kontroliuoti dirbtinio intelekto kūrimą. Tačiau plačiai paplitusioje informacijoje apie dirbtinį intelektą išryškėja labiausiai nerimą keliančios vizijos, nebūtinai pagrįstos realybe. Tai, savo ruožtu, lemia skeptišką nuomonę apie naujas technologijas, masinio nedarbo baimę ir nenorą naudotis skaitmeninėmis priemonėmis. Tačiau svarbu nepamiršti, kad technologijos dabar yra neatsiejama kasdienio gyvenimo dalis. Jos - ne tik pramogų šaltiniai, bet ir priemonės, palengvinančios buitinių ir profesinių pareigų atlikimą. Todėl priimant novatoriškus sprendimus ir šviečiant visuomenę, kaip tinkamai jomis naudotis, yra nepaprastai svarbu.

Informuotumo didinimo veikla taip pat (arba ypač) turėtų būti skiriama darbo vietoje naudojamoms skaitmeninėms priemonėms. Kaip bus nurodyta toliau vadove, naujosios technologijos naudojamos daugelyje sektorių ir įvairiuose įdarbinimo etapuose (nuo įdarbinimo iki darbuotojų vertinimo). Jos palengvina ir verslo valdymo procesus, ir kasdienį daugelio žmonių (tiek fizinių, tiek kitų darbuotojų) darbą. Geriausias to pavyzdys - plačiai naudojami mašininiai kalbos vertėjai, pavyzdžiui, „Google Translator“ arba „Deepl“, kurie pagerina tarpvalstybinį įmonių bendravimą arba suteikia galimybę versti profesinius tekstus be profesionalaus vertėjo.

Taip pat vis daugiau vilčių, kad darbą supaprastins generatyvinis dirbtinis intelektas. Tokios programos, kaip „GPT Chat“ ar „DALL-E“, jau naudojamos kūrybinėms užduotims atlikti, pavyzdžiui, elektroniniams laiškams rašyti ar duomenų analizei atlikti. Pavyzdžiui, pasitelkus generatyvinį dirbtinį intelektą, galima greičiau išanalizuoti straipsnio turinį arba įrašyti susitikimo eigą. vos per vieną akimirką. Pateikus atitinkamą komandą (pvz., „nurodykite pagrindines diskusijos išvadas“) ir į sistemą įvedus pagrindinius parametrus, galima tikėtis, kad bus sugeneruoti laukiami rezultatai (išvados).

Kartu svarbu nepamiršti, kad dideli kalbos modeliai (LLM, angl. *Large Language Model*), tokie kaip „Chat GPT“, nors ir sukuria natūraliai skambantį turinį, tačiau sukuria jį automatiškai ir nereflektuotai. Tai savo ruožtu gali lemti, kad algoritmų sukurti tekstai, nors ir labai patikimi, turi daug klaidų. Todėl taip svarbu ugdyti naudotojų kritinio mąstymo įgūdžius, gebėjimą analizuoti realią aplinką ir atsijoti tai, kas neteisinga (pvz., *netikras naujienas, angl. fake news)*. Be to, dirbant skaitmeniniame amžiuje būtina ne tik rengti įvairių sektorių darbuotojus automatizavimui ir suteikti jiems naujų kompetencijų, bet ir išmokyti darbuotojus sugyventi su technologijomis ir gebėti „atsijungti“. Tai yra būtinos tinkamos darbo ir asmeninio gyvenimo pusiausvyros sąlygos.

Šis darbas buvo sukurtas 2022/2023 metais. Atsižvelgdamos į dinamišką inovacijų, ypač dirbtinio intelekto (DI) priemonių, raidą, vadovo autorės norėtų atkreipti dėmesį į tai, kad dėl technologinės pažangos dalis turinio artimiausiais mėnesiais ir metais gali pasenti.

Žodynėlis

Dirbtinio intelekto aktas / dirbtinio intelekto įstatymas

– ES reglamentas, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės.

Algoritmas

– instrukcijų rinkinys (skaičiavimo formulės), kuris savarankiškai priima sprendimus pagal statistinius modelius arba sprendimų priėmimo taisykles be aiškaus žmogaus įsikišimo.

Anonimizavimas

– asmens duomenų keitimo procesas, kai asmens duomenys pakeičiami taip, kad jų nebūtų galima priskirti identifikuotam ar identifikuojamam fiziniam asmeniui.

Automatizavimas

– technologijų naudojimas gamybai kontroliuoti ir produktams bei paslaugoms kurti naudojant skaitmenines priemones.

Blockchain

– vadinamoji blokų grandinė – technologija, skirta informacijai apie internetinius sandorius perduoti ir saugoti; decentralizuotų duomenų, kuriais saugiai dalijamasi, registras. Blokų grandinės technologija leidžia grupei pasirinktų dalyvių dalytis duomenimis.

Atsineškite savo įrenginį (BYOD)

– tendencija naudoti asmeninius prietaisus, pavyzdžiui, nešiojamuosius kompiuterius, išmaniuosius telefonus ir planšetinius kompiuterius, profesinėms pareigoms atlikti.

GPT pokalbiai

– dirbtinio intelekto įrankis (pokalbių robotas), kuris dialogo forma leidžia atsakyti į naudotojo klausimus natūralia kalba.

Asmens duomenys

– bet kokia informacija, susijusi su identifikuotu ar identifikuojamu gyvu fiziniu asmeniu (individuali informacija, kurią surinkus galima nustatyti asmens tapatybę, taip pat sudaro asmens duomenis).

Deep fake

– iš dviejų angliškų frazių: *deep learning (gilus mokymas)* ir *fake (klastotė, padirbtas)*. Tai garso ir vaizdų apdorojimas siekiant sukurti netikrą pranešimą, naudojant dirbtinio intelekto metodus. Tai leidžia sukurti medžiagą, kurią sunku arba neįmanoma atskirti nuo filmų ar nuotraukų, sukurtų tradicinėmis priemonėmis ir su tikrais žmonėmis.

Dideli kalbos modeliai (LLM, *Large Language Models*)

– mašininio mokymosi modeliai, galintys atlikti įvairias natūralios kalbos apdorojimo užduotis. Mokant tokią sistemą, jai pateikiami dideli duomenų kiekiai (pvz. knygos, straipsniai, interneto svetainės), kad ji galėtų išmokti dėsningumų ir ryšių tarp žodžių ir ateityje kurti naują turinį. LLM pavyzdys yra GPT Chat, kurią sukūrė OpenAI ir kuri 2022 m. lapkričio mėn. buvo paskelbta viešai. Šis modelis, reaguodamas į naudotojo užklausas, geba apdoroti informaciją ir generuoti tekstą, panašų į parašytą žmogaus.

Melagingos naujienos (Fake news)

– melaginga arba iš dalies melaginga sensacingo pobūdžio informacija, kuri sąmoningai klaidina gavėją.

Dalijimosi ekonomika / užsakomoji ekonomika (*sharing economy*; *on-demand economy)*

– verslo modelių, pagrįstų bendradarbiavimo platformų tarpininkavimu, rinkinys, sukuriantis atviros prieigos rinką laikinam naudojimuisi prekėmis ar paslaugomis, kurias dažnai teikia privatūs asmenys

Ateities kompetencijos

– specifiniai įgūdžiai, padedantys imtis užduočių ir jas atlikti darbo aplinkoje, kuri iš esmės yra lanksti, geografiškai išsklaidyta, linkusi dažnai ir sparčiai keistis ir kurioje reikia naudotis

skaitmeninėmis technologijomis bei bendradarbiauti su automatinėmis sistemomis ir mašinomis, naudojančiomis dirbtinį intelektą.

Mobingas

– į darbuotoją nukreipti veiksmai ar elgesys, pasireiškiantys nuolatiniu ir ilgalaikiu priekabiavimu ar bauginimu.

Darbas su platforma

– įdarbinimo forma, kai darbuotojas naudojasi skaitmenine platforma, kad galėtų prisijungti prie kitų organizacijų ar asmenų ir teikti konkrečias paslaugas, o už tai gauna atlyginimą. Skaitmeninėse platformose už atlygį atliekamos tokios užduotys kaip taksi ir kurjerių paslaugos, prekių pristatymas, namų remonto paslaugos, taip pat protinis darbas, pavyzdžiui, tekstų rašymas ir buhalterinės apskaitos tvarkymas.

Remiamas darbas

– darbas, kada kai kurias veiklas gali pakeisti robotai, o kitoms reikia žmogaus indėlio.

Atsijungimo teisė

– Teisė nedalyvauti atliekant su darbu susijusias užduotis ne darbo valandomis ir nedalyvauti bendraujant skaitmeninėmis priemonėmis.

Profiliavimas

– bet koks automatizuotas asmens duomenų tvarkymas, susijęs su jų naudojimu tam tikriems asmeniniams asmens veiksniams įvertinti. Visų pirma profiliavimas naudojamas siekiant analizuoti arba prognozuoti to asmens veiklą, jo ekonominę padėtį, sveikatą, asmeninius pasirinkimus, interesus, susidomėjimus, patikimumą, elgesį, buvimo vietą ar judėjimą.

Pseudonimiškumas

– tvarkyti asmens duomenis taip, kad nebūtų įmanoma nustatyti, kam jie priklauso, neturint prieigos prie kitos informacijos, saugiai saugomos kitoje vietoje.

BDAR

– 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679. dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB *(toliau: BDAR – bendrasis duomenų apsaugos reglamentas).*

Bendradarbiaujantys robotai *(collaborative robots; co-botai)*

– įranga, skirta sumažinti gamyklos darbuotojų darbo krūvį, nes atlieka dalį jų užduočių.

Savarankiškas mokymasis (ML, *machine learning*)

– dirbtinio intelekto sritis, skirta algoritmams, kurie nuolat tobulina savo veikimą dėl patirties arba duomenų poveikio. Mašininio mokymosi algoritmai iš pavyzdinių duomenų (vadinamų mokymosi rinkiniu) sukuria matematinį modelį, kuris leidžia prognozuoti ar priimti sprendimus, o žmogui nereikia to daryti.

Spoofing

– atakos, kai nusikaltėliai apsimeta bankais, valstybinėmis institucijomis ir įstaigomis, įmonėmis ar net privačiais asmenimis, kad išviliotų iš aukų duomenis ar pinigus.

Startuolis *(Start-up)*

– naujai įsteigta įmonė arba laikina organizacija, ieškanti verslo modelio pelningam augimui.

Dirbtinis intelektas *(DI, AI)*

– mašinų gebėjimas suprasti, mokytis, planuoti ir demonstruoti kūrybiškumą. Pagal dirbtinio intelekto įstatymo projekte siūlomą apibrėžtį, dirbtinio intelekto sistema – tai programinė įranga, sukurta naudojant vieną ar daugiau reglamente išsamiai aprašytų metodų ir būdų, kuri tam tikrais žmogaus apibrėžtais tikslais gali generuoti rezultatus, pavyzdžiui, turinį, prognozes, rekomendacijas ar sprendimus, darančius poveikį aplinkai, su kuria ji sąveikauja. Ši apibrėžtis yra labai plati ir nelabai tiksli, tačiau tai suprantama tokios sparčiai besivystančios technologijos kaip dirbtinis intelektas kontekste.

Duomenų šifravimas

– neskelbtinos ar asmeninės informacijos kodavimo būdų rinkinys, skirtas jos konfidencialumui užtikrinti.

Wearables

– „dėvimieji" elektroniniai prietaisai, t. y. dėvimi prie odos. Jie gali stebėti ir analizuoti naudotojo sveikatos parametrus ar elgesį. Šiuo metu populiariausi tokio tipo prietaisai yra išmanieji laikrodžiai *(smartwatch),* sporto apyrankės (*vadinamosios išmaniosios apyrankės - smartband*) ir sportiniai laikrodžiai.

Darbo ir asmeninio gyvenimo pusiausvyra

– išlaikyti pusiausvyrą tarp darbo (tiek apmokamo, tiek neapmokamo), šeimos gyvenimo ir laisvalaikio.

Automatinis sprendimų priėmimas

– Veikla, pagrįsta pažangiais skaičiavimais ir išskirtinai techninėmis informacijos apdorojimo priemonėmis. Sprendimų priėmimas kompiuteriu, nedalyvaujant žmogiškajam veiksniui.

1. Skaitmeninimo poveikis darbo procesams

1.1 Europos socialinių partnerių pagrindų susitarimas dėl skaitmeninimo - bendros pastabos

Skaitmeninė ekonomikos transformacija daro didžiulį poveikį darbdaviams, darbuotojams ir pačiai darbo eigai. Siekiant palengvinti skaitmeninių technologijų integravimą darbo vietose, 2020 m. birželio mėn. buvo sudarytas Europos socialinių partnerių autonominis bendrasis susitarimas (EFAD). Juo siekiama užkirsti kelią rizikoms, su kuriomis gali susidurti darbuotojai ir darbdaviai, ir jas sumažinti. Susitarimas taikomas visiems viešajame ir privačiajame sektoriuose ir visų rūšių ekonominėje veikloje dirbantiems ar darbuotojus samdantiems asmenims.

EFAD susitarimas yra savarankiška iniciatyva ir Europos socialinių partnerių derybų pagal 2019-2021 m. šeštąją daugiametę darbo programą rezultatas. Atsižvelgiant į Europos socialinio dialogo ir darbo santykių įstatymo (angl. Sutarties dėl Europos Sąjungos veikimo (SESV) 155 straipsnį, šiuo autonominiu Europos pagrindų susitarimu BusinessEurope, SMEunited, CEEP ir ETUC nariai (ir EUROCADRES/CEC ryšių palaikymo komitetas) įsipareigojo skatinti ir įgyvendinti priemones ir įrankius (prireikus nacionaliniu, sektoriaus ar įmonės lygmeniu) pagal valstybių narių ir Europos ekonominės erdvės šalių socialiniams partneriams būdingas procedūras ir praktiką.

Kiti pastaraisiais metais sudaryti autonominiai susitarimai – tai Europos socialinių partnerių autonominis pagrindų susitarimas dėl aktyvaus senėjimo ir kartų kaitos arba Europos pagrindų susitarimas dėl su darbu susijusio streso.

I. Pagrindiniai EFAD susitarimo tikslai:

1. didinti darbdavių, darbuotojų ir jų atstovų informuotumą ir geresnį supratimą apie galimybes ir iššūkius darbe, kylančius dėl skaitmeninės transformacijos,
2. teikti pagalbą darbuotojams, jų atstovams ir darbdaviams rengiant priemones ir veiksmus, kad būtų galima pasinaudoti naujomis skaitmeninėmis galimybėmis ir spręsti iškilusius sunkumus, atsižvelgiant į esamas iniciatyvas, praktiką ir kolektyvines sutartis.
3. Skatinti darbdavių ir profesinių sąjungų partnerystę.

II. Partnerystės kūrimo žingsniai siekiant palengvinti skaitmeninės transformacijos procesą įmonėje

Darbuotojų atstovams bus suteiktos tokios priemonės ir informacija, kurių reikia veiksmingam dalyvavimui įvairiuose proceso etapuose.

1 etapas.

„Bendras tyrinėjimas, rengimas ir parama“, kurie susiję su informuotumo didinimu. sąlygų ir paramos bei pasitikėjimo atmosferos kūrimas. Šia veikla siekiama sudaryti sąlygas atvirai diskutuoti apie skaitmeninimo galimybes ir iššūkius / grėsmes, taip pat jų poveikį darbo vietai ir aptarti galimus veiksmus bei sprendimus.

2 etapas.

„Bendras žemėlapių sudarymas / reguliarus vertinimas / analizė“ - tai teminių sričių žemėlapių sudarymas siekiant nustatyti naudą ir galimybes, taip pat iššūkius ir riziką, kurią darbuotojams ir įmonei gali sukelti veiksminga skaitmeninių technologijų integracija.

3 etapas.

„Bendra situacijos apžvalga ir skaitmeninės transformacijos strategijos priėmimas“, kuri yra pirmųjų dviejų etapų rezultatas. Tai yra pagrindinis supratimas apie galimybes ir iššūkius/rizikas, skirtingus įmonės skaitmeninimą sudarančius elementus ir jų tarpusavio sąsajas bei susitarimas dėl skaitmeninės strategijos, kurioje nustatomi įmonės tikslai ateičiai.

4 etapas.

„Priimti tinkamas priemones ir (arba) veiksmus“, remiantis bendra padėties apžvalga. Tai apima: galimybę išbandyti numatytus sprendimus, prioritetų nustatymą, veiksmų įgyvendinimą vėlesniais laiko etapais, vadovybės ir darbuotojų bei jų atstovų vaidmenų ir atsakomybės išaiškinimą ir apibrėžimą, taip pat išteklius ir papildomas priemones (pvz., ekspertų paramą, stebėseną).

5 etapas.

„Reguliari bendra stebėsena ir (arba) tolesni veiksmai, mokymasis, vertinimas“ - tai bendras veiksmų efektyvumo vertinimas ir diskusija, ar reikia tolesnės analizės, informuotumo didinimo, paramos ar kitų veiksmų.

III. Į susitarimo taikymo sritį įeina:

1. Skaitmeniniai įgūdžiai ir įsidarbinimas

Socialiniai partneriai turėtų būti suinteresuoti sudaryti palankesnes sąlygas darbuotojams gauti kokybišką mokymą ir kelti kvalifikaciją. Pagrindinis iššūkis šiuo atveju bus nustatyti, kokius skaitmeninius įgūdžius ir procesų pokyčius reikia įgyvendinti konkrečioje įmonėje.

Priemonės, kurias reikia apsvarstyti:

- Šalių įsipareigojimas persikvalifikuoti.
- Galimybė dalyvauti mokymuose ir jų organizavimas, aukšta mokymų kokybė ir veiksmingumas, ne viso darbo laiko galimybių diegimas ir konkretaus darbo laiko skyrimas mokymui.
- Aiškiai apibrėžtos dalyvavimo sąlygos, įskaitant: trukmę, finansinius aspektus, darbuotojų dalyvavimą ir kompensaciją, jei mokymai vyksta ne darbo metu.

2. Prisijungimo ir atsijungimo būdai

Darbdavio pareiga yra užtikrinti darbuotojų saugą ir sveikatą visais su darbu susijusiais aspektais. Todėl teisė atsijungti yra vienas iš pagrindinių šio vadovo aspektų. Raginame profesinių sąjungų narius, kad visiško ir pagrįsto aiškumo nustatymas dėl darbdavio lūkesčių darbuotojui naudojantis skaitmeniniais prietaisais turėtų būti remiamas atitinkamo lygio kolektyvinėse derybose.

Įdiegus naujus skaitmeninius prietaisus galima sudaryti lanksčias darbo sąlygas, naudingas darbuotojams ir darbdaviams. Kartu tai gali kelti rimtą riziką, susijusią su sudėtingu darbo ir asmeninio gyvenimo atskyrimu. Todėl daugiausia dėmesio reikėtų skirti neigiamų reiškinių, turinčių įtakos darbuotojų sveikatai ir saugai, prevencijai. Tam reikia aiškiai apibrėžti teises, atsakomybę ir užduotis, kuriose prevencijos principas yra svarbiausias prioritetas.

Priemonės, į kurias reikia atsižvelgti:

- Mokyti darbuotojus ir kitaip didinti jų informuotumą
- Sukurti naują darbo kultūrą tarp vadovų, kurie vengia bendrauti su darbuotojais ne darbo metu.
- Pateikti aiškias gaires dėl galiojančių teisės aktų, susijusių su darbo laiku, nuotoliniu ir mobiliuoju darbu.
- Efektyviai organizuoti darbą, įskaitant užtikrinimą, kad dėl darbuotojų skaičiaus darbuotojai nebūtų priversti dirbti po darbo valandų.
- Tinkamai atlyginti už papildomai dirbtą laiką.
- Įspėti ir palaikyti procedūras, skirtas atsijungti ir apsaugoti nuo sankcijų už nesusisiekimą su darbuotoju po darbo valandų.
- Vykdyti Izoliacijos darbe prevenciją.

3. Dirbtinis intelektas ir žmogaus kontrolės principų užtikrinimas

Neabejotina, kad dirbtinis intelektas darys vis didesnį poveikį žmonių darbui. Todėl Europos autonomijos susitarime nustatyti tam tikri jo diegimo į darbo rinką principai ir kryptys. Svarbus elementas, kuris turėtų būti užtikrintas kiekvienoje darbo vietoje, yra žmogaus vykdoma dirbtinio intelekto kontrolė, kuri yra robotikos ir dirbtiniu intelektu grindžiamų taikomųjų programų naudojimo pagrindas. Sistema turėtų būti teisėta ir sąžininga, joje turėtų būti laikomasi etinių standartų, atitinkančių žmogaus teises. Tuo tarpu techniniu ir socialiniu požiūriu ji turėtų būti saugi ir skaidri.

4. Pagarba žmogaus orumui ir sekimas

Dėl didelio šiuolaikinių technologijų įsiskverbimo į darbo procesą kyla pavojus pažeisti pagrindines dirbančio asmens vertybes (pavyzdžiui, renkant slaptus duomenis – prieigą prie patalpų ar dokumentų pagal pirštų atspaudus, vyzdžio ar implantuotos mikroschemos skenavimą). Tokios technologijos didina žmogaus orumo pažeidimo riziką, ypač asmens stebėjimo atveju. Dėl to gali pablogėti darbo sąlygos.

Asmens duomenų kiekio mažinimas ir skaidrumas, taip pat aiškios jų tvarkymo taisyklės mažina įkyraus stebėjimo ir netinkamo duomenų naudojimo riziką. Įdarbinimo kontekste darbuotojų asmens duomenų tvarkymo taisyklės nustatytos BDAR reglamente. Be to, EFAD

susitarimo socialiniai partneriai primena, kad BDAR 88 straipsnyje nurodoma galimybė kolektyvinėse sutartyse nustatyti išsamesnes darbuotojų asmens duomenų saugojimo taisykles. Taip siekiama užtikrinti darbuotojų teisių ir laisvių, susijusių su jų asmens duomenų tvarkymu, apsaugą darbo santykių kontekste.

Priemonės, į kurias reikia atsižvelgti:

- Įgalinti darbuotojų atstovus spręsti duomenų, sutikimo, privatumo ir stebėjimo klausimus.
- Duomenis rinkti konkrečiu ir skaidriu tikslu. Duomenys neturėtų būti renkami ar saugomi tik todėl, kad tai įmanoma, arba neapibrėžtu tikslu.
- Informuoti darbuotojus, kad jie gali nesutikti tvarkyti tam tikros grupės asmens duomenų arba kad jie gali bet kada atšaukti anksčiau duotą sutikimą.
- Suteikti personalo atstovams priemones ir (skaitmenines) priemones, pvz., skaitmenines skelbimų lentas, kad jie galėtų atlikti savo pareigas.

5. Įgyvendinimas ir tolesni veiksmai

Organizacijos narės socialinio dialogo komitetui teiks ataskaitas apie susitarimo įgyvendinimą. Per pirmuosius trejus metus nuo šio susitarimo pasirašymo socialinio dialogo komitetas buvo įpareigotas parengti ir patvirtinti metinį paketą, kuriame būtų apibendrinta, kaip įgyvendinamas susitarimas. Išsamią ataskaitą apie vykdomą įgyvendinimo veiklą komitetas parengs ir Europos socialiniai partneriai ją patvirtins kitais metais. Susitarimas nepažeidžia socialinių partnerių teisės sudaryti pritaikomuosius ir (arba) papildomus susitarimus, atsižvelgiant į konkrečius atitinkamų socialinių partnerių poreikius.

1.2 Naujosios technologijos darbo vietoje – technologijomis paremtas (bendradarbiaujantis) ir visiškai automatizuotas darbas

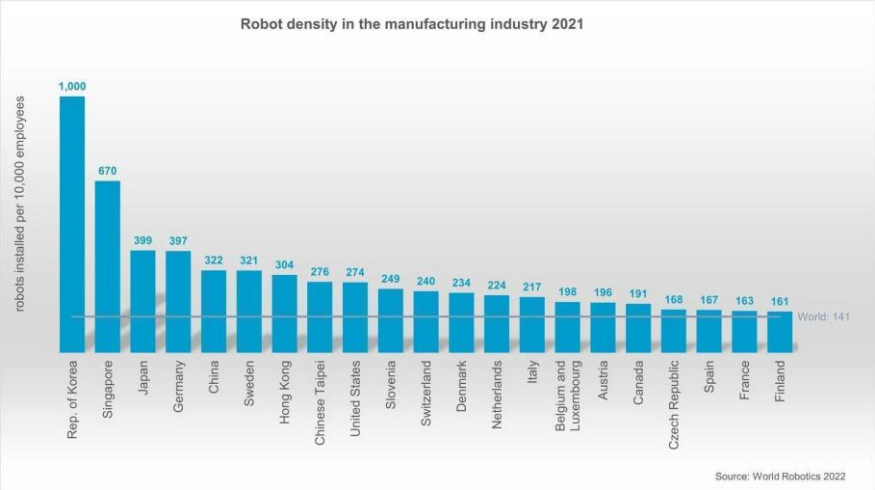
Požiūris į robotizaciją keičiasi tiek iš įmonių, tiek iš pačių darbuotojų perspektyvos. Robotas nebėra vien tik vaizduotės sritis, jis tampa gamybos priemone, galinčia palengvinti žmonėms tenkančią naštą ir padėti jiems spręsti konkrečias problemas. Tačiau, priklausomai nuo sektoriaus ir gamybos etapo, automatizavimas gali būti diegiamas skirtingu mastu. Pagal įsitraukimo į užduotis lygį robotai gali būti skirstomi ne tik į tuos, kurie atlieka daugiausia intelektinį darbą (pvz., visos dirbtinio intelekto priemonės), bet ir į tuos, kurie palengvina žmonėms pasikartojančias užduotis (pvz., produktų pakavimas).

Kas yra automatizuota gamybos sistema?

Gamybos automatizavimu vadinama tokia įmonių plėtros kryptis, kai žmonių fizinis ir protinis darbas gerokai sumažinamas arba visiškai pakeičiamas mašinų darbu. Šio reiškinio ištakos siekia XX a., kai 1913 m. Henris Fordas visiems laikams pakeitė pasaulį, įdiegęs judančią surinkimo liniją, kurią valdė specializuoti darbininkai. Tokio darbo prielaida buvo padidinti gamybos mastą ir kartu sumažinti galutinio produkto kainą.

Dabar mūsų laukia kitas gamybos evoliucijos etapas – automatizavimo racionalizavimas pasitelkiant skaitmeninimą. Naudojant tokias technologijas kaip intuityvaus programavimo moduliai, tampa lengviau kurti išsamias instrukcijas robotams. Pažangūs jutikliai leidžia mašinoms suprasti jas supančią aplinką ir geriau reaguoti. Tarptautinės robotikos federacijos duomenimis, nuo 2015 m. iki 2020 m. robotų[1] tankis pasaulyje beveik padvigubės - nuo 66 vienetų 2015 m. iki 126 vienetų 2020 m.

Daugiausiai automatizuotos gamybos turinčios šalys (2021 m.)



Šaltinis: Tarptautinė robotikos federacija (*The Robot Report,* 2021 m.).

Remiamasis darbas

Pagalbinis darbas – tai toks atvejis, kai tam tikrus gamybos veiksmus gali pakeisti robotai, o kitiems reikia žmogaus indėlio. Bendradarbiaujantys robotai (*collaborative robots*; *vadinamieji*

[1] Tarptautinės robotikos federacijos naudojamas rodiklis, kuriuo matuojamas robotų skaičius, tenkantis 10 000 darbuotojų pramonėje.

„ko-botai“) dažniausiai naudojami gamybos procesams palaikyti, o jų užduotis - išlaisvinti gamyklos darbuotojus nuo dalies darbo krūvio. Svarbus bruožas, skiriantis vadinamuosius ko-botus nuo standartinių pramoninių sistemų (kurios paprastai yra atskirtos nuo žmonių), yra tai, kad kolaboratyvinės robotikos atveju valdomos robotų sistemos dalijasi ta pačia darbo erdve su žmonėmis.

Robotų bendravimo su žmonėmis būdai:

1. **Ribota žmogaus sąveika –** robotas visiškai sustoja, kai paskirtoje zonoje pasirodo žmogus, ir tęsia darbą savarankiškai darbuotojui palikus erdvę.
2. **Bendradarbiavimas su žmonėmis –** dėl įmontuotų jutiklių „co-bot“ sulėtina darbą arba nutraukia darbą, kai kas nors yra šalia, taip užtikrindamas saugią žmogaus ir mašinos sąveiką.
3. **Rankinis valdymas –** ko-botą visą laiką valdo operatorius. Pavyzdžiui, įrenginys laiko krovinį, o žmogus valdo jo ranką.

Visiškai automatizuotas veikimas

Automatizavimas pramonėje suprantamas kaip technologijų naudojimas gamybai valdyti ir produktams bei paslaugoms kurti naudojant skaitmenines priemones. Visiško automatizavimo atveju žmonės ir mašinos nebeatlieka viena kitą papildančių užduočių ir pradeda veikti tais pačiais diapazonais. Dėl robotizacijos darbuotojų dalyvavimas gamybos procesuose gerokai sumažėja arba visai išnyksta. Visi gamybos procesai tampa visiškai automatizuoti ir žmogaus įsikišimas nereikalingas jokiame produkto kūrimo etape.

Nepaisant plačiai paplitusios baimės dėl didėjančio pramoninių procesų automatizavimo, šios rūšies technologijų diegimas gali būti naudingas įvairiais su gamybos procesais susijusiais lygmenimis, taip pat ir tais atvejais, kai darbas yra pavojingas žmogaus gyvybei ir sveikatai.

Diskusija – ar reikėtų apmokestinti robotų darbą?

Mažėjant gamybos procesų automatizavimo sąnaudoms, didėja pramoninio robotizavimo mastas. Numatomos ir teigiamos pasekmės, pavyzdžiui, ekonomikos augimas ar didesnis našumas, ir neigiamos pasekmės, pavyzdžiui, užimtumo mažėjimas įvairiose gamybos sektoriaus šakose.

Seno verslo modelių transformacija kelia daug diskusijų, o šalyse, kuriose automatizavimas jau dabar vystosi stulbinamai sparčiai, teisės aktų leidėjai susiduria su naujais iššūkiais.

Kadangi dėl robotų naudojimo pramonėje gerokai sumažėjo darbo sąnaudos ir pelnas, **robotų darbo jėgos apmokestinimo klausimas** tapo vienu iš sunkiai išsprendžiamų klausimų. Tačiau kai kalbama apie naujų mašinų ir įrangos įsigijimą, atskirų šalių vyriausybės, siekdamos paskatinti skaitmeninę transformaciją ir pramonės sektoriaus modernizavimą, taiko mokesčių lengvatas. Pavyzdžiui, Lenkijoje nuo 2022 m. verslininkams leidžiama atskaityti iki 150 proc. išlaidų, patirtų įsigyjant funkciškai susijusias mašinas ir įrangą, skirtą darbo vietų, kuriose vyksta žmogaus ir roboto sąveika, saugai užtikrinti.

Teigiami ir neigiami robotizacijos padariniai

1. **Valdymas**

a) **Teigiami aspektai:**

- Gebėjimas tobulinti produktus ir greičiau juos pateikti rinkai
- Spartesnis naujų technologijų kūrimas
- Įmonių konkurencingumo didinimas

b) **Neigiami:**

- Didėjantis nedarbas - remiantis 2023 m. *Darbo vietų ateities* ataskaitos (Pasaulio ekonomikos forumas) autorių skaičiavimais, netolimoje ateityje mašinos atliks daugiau procentų užduočių nei žmonės. Nors 2018 m. vidutiniškai 71 proc. darbo laiko sudarė užduotys, kuriose dalyvauja žmogiškasis veiksnys, 2025 m. ši proporcija gerokai pasikeis. Žmonės bus atsakingi už maždaug 48 proc. veiklos, o likusieji 52 proc. bus visiškai automatizuoti.
- Energijos suvartojimo ir aplinkos taršos didėjimas.

2. **Darbdavys**

a) **Teigiami aspektai:**

- Gamybos sąnaudų mažinimas
- Klaidų rizikos mažinimas
- Galimybė geriau fiksuoti veiklos rezultatus
- Greičiau nustatomos kliūtys, todėl lengviau optimizuoti darbą
- Galimybė kai kuriose šalyse (pvz., Lenkijoje) atskaityti konkrečios paskirties pramoninių robotų įsigijimo išlaidas

b) **Neigiami:**

- Didelės pradinės įrangos montavimo išlaidos
- Būtinybė inventorizuoti ir didelės remonto išlaidos
- Esant labai automatizuotiems procesams, įrangos gedimai sukelia gamybos prastovas
- Mažesnis reagavimo į netikėtas problemas ar klaidas lankstumas, palyginti su darbuotojų reagavimu
- Būtinybė laikytis griežtų taisyklių
- Didelės energijos sąnaudos

3. **Darbuotojas**

a) **Teigiami aspektai:**

- Gamybos proceso tvarkymo supaprastinimas
- Pagalba atliekant sudėtingesnę ar pasikartojančią veiklą
- Didesnis gamybos efektyvumas, mažiau įtraukiant darbuotojus
- Galimybė skirti daugiau laiko tobulinimuisi, nes pasikartojanti veikla perduodama automatizuotoms priemonėms
- Naujų darbo vietų, susijusių su mašinų kūrimu, eksploatavimu ar remontu, atsiradimas.

b) **Neigiami:**

- Galimas darbo vietų praradimas dėl proceso automatizavimo.
- Didesnė perdegimo darbe tikimybė, kurią lemia baimė prarasti darbą.
- Grėsmė sveikatai ir (arba) gyvybei mašinoms sugedus arba netinkamai naudojant

1.3. Neproporcingo ir perteklinio stebėjimo darbo vietoje prevencija

Kontroliavimas darbo vietoje – galimybės ir rizika

Technologijų bendrovės noriai reaguoja į darbdaviams kylantį naujų technologijų poreikį. Tuo tarpu dirbtinio intelekto įrankiai kuriami taip, kad sudaro galimybę taikyti darbuotojams visišką kontrolę – nepriklausomai nuo to, ar jie apie tai žino ir sutinka. Taip pat pastebimos stiprios tendencijos priimti naująją padėtį kaip „natūralią“ įmonių raidos pasekmę.

Galimybės:

- stebėsena, naudojama esant pavojingoms situacijoms ir įvykus nelaimingam atsitikimui darbe, gali būti naudinga darbuotojui (pvz., kai reikia įrodyti, kad darbo vieta nebuvo pakankamai saugi),
- kai kuriuose sektoriuose stebėsena būtina siekiant užtikrinti taisyklių atitiktį (pvz., bankininkystėje ji gali padėti užkirsti kelią naudojimuisi viešai neatskleista informacija),
- darbuotojų mokymo metu naudojama priežiūra gali pagreitinti įvadinius procesus (pvz., statybų pramonėje naudojami *dėvimi įrenginiai* - išmanieji šalmai su vibracijos jutikliais, kurie įspėja darbuotojus apie potencialiai pavojingus aplinkoje esančius objektus).

Stellate pavyzdys

„Stellate“, San Franciske įsikūręs duomenų analizės startuolis, turi darbuotojų komandą, išsibarsčiusią po visą pasaulį. Įmonė ne tik naudojasi nuotolinio darbo įrankiais, bet ir stebi savo darbuotojų tobulėjimą per mokymo ir mentorystės programas. Pagrindinis tokių iniciatyvų tikslas - ne bausti už netinkamą darbuotojų darbą ar kitą netinkamą elgesį, o skatinti įmonės darbuotojus naudotis priemonėmis, kurios padėtų didinti jų darbo efektyvumą.

Grėsmės:

- dėl pernelyg didelio ar netinkamo skaitmeninių technologijų naudojimo gali būti pažeistos darbuotojų teisės į privatumą ir duomenų apsaugą,
- pavojus darbuotojų psichinei ir fizinei sveikatai dėl streso, kurį kelia pernelyg griežta priežiūra ir nustatyti darbo standartai,
- apsunkintas darbuotojų vienijimasis – darbuotojų stebėjimas ir įmonės nuotaikų pažinimas leidžia užfiksuoti susivienijimui palankius judesius (pavyzdžiui, didelėse darbovietėse pasitaiko, kad darbuotojų duomenys naudojami siekiant išsiaiškinti darbuotojų požiūrį į darbdavį ir nustatyti, kur darbuotojai labiausiai linkę prieštarauti įmonės politikai).

Pagrindiniai darbo vietos stebėsenos principai

Pripažįstama, kad darbdaviai turėtų turėti galimybę prižiūrėti darbo vietas ir vertinti savo darbuotojų darbą, kad užtikrintų geresnį įmonės valdymą, apsaugotų įmonės paslaptis, užtikrintų įstatymų laikymąsi ir užkirstų kelią darbuotojų nusikalstamumui. Tuo pat metu Europos Sąjunga ir atskiros valstybės narės daug dėmesio skiria darbuotojų privatumui ir pagarbai jų asmeniniam gyvenimui.

Darbo vietos stebėjimas yra teisėtas, tačiau...[2]

- prieš pradedant naudoti vaizdo stebėjimą, turi būti išsamiai nurodyti informacijos tvarkymo tikslai (pvz., siekiant užtikrinti darbuotojų saugumą),
- darbdavys privalo informuoti asmenis, kuriems gali būti taikoma stebėsena, apie tai, kad stebėsena vykdoma, ir apie tai, kokia sritis yra stebima.

Taip pat svarbu, kad stebėsenos tikslai, taikymo sritis ir būdas būtų nustatyti kolektyvinėje sutartyje arba darbo tvarkos taisyklėse, pvz., kaip kolektyvinių derybų dalis. Tais atvejais, kai darbdaviui netaikoma kolektyvinė sutartis arba jis neprivalo nustatyti darbo tvarkos taisyklių, taisyklės surašomos pranešime.

[2] Bendrijos teisėje numatytos darbo vietų stebėsenos taisyklės (Europos žmogaus teisių konvencijos 8 straipsnis, BDAR reglamentas), teismų ir tribunolų sprendimai, atskirų valstybių narių darbo kodeksai.

Slaptas vaizdo stebėjimas leidžiamas tik ribotai, jei yra pagrįstas įtarimas, kad padarytas sunkus nusižengimas ar nusikalstama veika, dėl kurios darbdaviui padaryta didelė žala.

Be to, darbdavys gali naudoti ir kitų rūšių stebėseną. Pavyzdžiui, tai gali būti:

- tarnybiniame automobilyje įrengtas GPS,
- interneto ir greitųjų žinučių, naudojamų įmonės įrangoje, stebėjimas,
- įmonės mobiliojo telefono arba nešiojamojo kompiuterio geolokacija.

Nuostatos dėl vaizdo stebėjimo atitinkamai taikomos visoms stebėjimo formoms (pvz., darbdavys gali stebėti darbuotojo elektroninį paštą tik iš anksto pranešęs darbuotojui).

Stebėsena darbe ir teisė – šalių partnerių pavyzdžiai

Lenkija

Pagal Lenkijos darbo kodeksą stebėjimas – tai specifinis darbo vietos patalpų arba teritorijos aplink darbo vietą stebėjimas techninėmis priemonėmis, leidžiančiomis fiksuoti vaizdą.

Stebėti Lenkijoje leidžiama, jei tai būtina:

- užtikrinant darbuotojų saugą,
- nuosavybės apsaugai arba gamybos kontrolei,
- saugojant konfidencialią informaciją, kurią atskleidus darbdavys gali patirti žalą,
- elektroninio pašto stebėjimui (Darbo kodekso 223 straipsnis), kuris leidžiamas tiek, kiek tai būtina siekiant užtikrinti darbo organizavimą, leidžiantį visapusiškai išnaudoti darbo laiką ir tinkamai naudotis darbuotojui suteiktomis darbo priemonėmis; elektroninio pašto stebėjimas neturi pažeisti susirašinėjimo slaptumo ir kitų darbuotojo asmeninių teisių.

Vaizdo įrašus darbdavys gali naudoti tik tam tikslui, kuriam jie buvo surinkti, ir saugoti ne ilgiau kaip tris mėnesius nuo įrašymo dienos.

Kaip teisėtai vykdyti stebėseną? Šešių etapų procedūra

Vykdydamas teisėtą stebėseną, darbdavys turi įvertinti, kokį poveikį jo veiksmai gali turėti darbuotojams. Toliau pateikiamuose žingsniuose nurodoma, kokiais klausimais turėtų būti grindžiama tokia analizė.

Žingsniai	Klausimas	Veiksmas
2 žingsnis	Kodėl vykdoma arba turėtų būti vykdoma stebėsena?	• Darbuotojų stebėsenos tikslo supratimas. • Tikslus stebėsenos funkcijos apibrėžimas (duomenys, surinkti vykdant konkrečią stebėseną, gali būti naudojami tik tam tikslui, kuriam jie buvo surinkti). **Išimtis**: jei vykdydama stebėseną įmonė gauna informacijos apie veiklą, kurios negalima ignoruoti (pvz., galimą nusikalstamą veiklą, patyčias), surinkti duomenys gali būti naudojami siekiant patraukti atsakingus asmenis atsakomybėn.
3 žingsnis	Ar tai galima pasiekti be stebėsenos?	• Nustačius priežastį, dėl kurios reikia įdiegti stebėseną, svarbu nustatyti, ar tą patį tikslą galima pasiekti be darbuotojų stebėsenos. **Pavyzdys:** darbuotojų lankomų svetainių stebėseną galima pakeisti netinkamų svetainių blokavimu arba leidimu darbuotojams įkelti failus tik iš tam tikrų paskyrų ir tik tam tikro dydžio.
4 žingsnis	Jei tam tikro tikslo neįmanoma pasiekti be stebėsenos, ar yra mažiau invazinių kontrolės priemonių nei šiuo metu svarstomos?	**Pavyzdžiui,** tikrinti, ar darbuotojai nepažeidžia įmonės konfidencialumo politikos, galima tiek kontroliuojant darbuotojų siunčiamų el. laiškų turinį, tiek atliekant automatinę stebėseną, pavyzdžiui, tikrinant el. pašto adresus ir el. laiško temos eilutes arba blokuojant el. laiškus su tam tikro dydžio priedais.
5 žingsnis	Kaip stebėsena paveiks darbuotojus?	• Reikia atsakyti į šiuos klausimus: ○ Ar stebėsena gali būti laikoma menkinančia arba nesąžininga? ○ Ar stebėsena turės įtakos darbdavio

		ir darbuotojų tarpusavio pasitikėjimui? ○ Ar galima bet kokią konfidencialią ar neskelbtiną informaciją perduoti žmonėms, kuriems nėra jokio reikalo jos žinoti? **Pavyzdys:** buhalterijai gali būti pranešta, kad asmuo nedirbo dėl ligos (kad būtų galima išmokėti ligos pašalpą), tačiau medicininės neatvykimo priežastis turi žinoti tik personalo vadovas.
6 žingsnis	Ar stebėsenos įvedimas yra pagrįstas?	• Sprendimą, ar stebėsenos įvedimas yra pagrįstas (lengviau pateisinti mažiau įkyrią stebėseną, apie kurį darbuotojai yra informuojami). • Prieš pradedant stebėseną, galima konsultuotis su darbuotojais, kad kartu būtų sukurtas stebėsenos pagrindimas.

Darbuotojų kontroliavimas ir nuotolinis darbas

Dirbančius asmenis galima stebėti į darbuotojų kompiuterius įdiegiant kontrolės programas, apie kurias darbuotojai dažnai neinformuojami. Vadinamoji „bossware“[3] gali įrašinėti klavišų paspaudimus, daryti ekrano nuotraukas ir net įjungti nuotoliniu būdu dirbančių darbuotojų interneto kameras.

Verta pažymėti, kad nuolatinė baimė būti darbdavio stebimam gali pabloginti darbuotojų psichinę būklę. Tyrimo duomenimis, net 56 % respondentų jaučia stresą ir nerimą dėl to, kad darbdavys stebi jų elektroninį bendravimą, 41 % nuolat svarsto, ar nėra stebimi, o 32 % dėl to rečiau daro pertraukas darbe.

Kaip efektyviai kontroliuoti darbą nepakenkiant darbuotojų gerovei?

Patarimai darbdaviui:

- informuokite darbuotoją apie naudojamas priežiūros priemones,
- paaiškinkite stebėsenos naudojimo taisykles ir nustatykite jos ribas (pvz., tvarkomų duomenų rūšį),

[3] Pavadinimas kilęs iš angliškų žodžių *boss* ir *software* ir reiškia darbdavio programinę įrangą.

- vietoj pernelyg didelės priežiūros ir įsigilinimo į kasdienę darbuotojo veiklą, įveskite atskaitomybės už rezultatus sistemą (pvz., kassavaitinę užduočių peržiūrą ir įvertinimą),
- naudokitės stebėsenos ir užduočių valdymo programomis (pvz., Connecteam) ir pagerinkite nuotolinį komandų bendravimą bei bendrą planavimą.

1.4 Nuotolinio ir „teledarbo“ skirtumas – poveikis darbuotojų santykiams

Europos Komisijos atlikto tyrimo duomenimis, metais prieš prasidedant COVID-19 pandemijai tik 5,4 proc. dirbančių 27 ES valstybių narių gyventojų dirbo iš namų – ši dalis nepakito nuo 2009 m. Dėl pandemijos ši dalis išaugo daugiau nei dvigubai – iki 12,3 %. Kai kuriose valstybėse narėse šis skaičius viršijo net ketvirtadalį visų dirbančių žmonių, nepriklausomai nuo pramonės ar ekonomikos sektoriaus.

Nepaisant pradinių sunkumų prisitaikant prie naujos realybės (pirmiausia dėl tinkamos IRT infrastruktūros ar mokymų apie darbo procesų skaitmeninimą trūkumo), šiandien darbuotojai neįsivaizduoja grįžimo į ankstesnius laikus. į tai, kaip jie dirbo iki pandemijos. Jie vertina didesnį darbo lankstumą, galimybę leisti laiką su šeima ir didesnį darbo našumą.

Tačiau, nepaisant hibridinio darbo populiarumo, vis dar daug darbdavių ir darbuotojų renkasi grįžti į biurą. Šį sprendimą jie argumentuoja geresniais darbo santykiais ir bendradarbiavimu, taip pat galimybe sukurti kolektyvinėms naujovėms ir geresniam produktyvumui palankią aplinką, aiškiai atskiriant asmeninį ir profesinį gyvenimą.

Nuotolinis darbas - pagrindinės sąvokos

Populiarėjant darbui su skaitmeninėmis priemonėmis ir daugybei jų teikiamų galimybių, atsirado būtinybė vartoti įvairius naujus terminus. Kad būtų lengviau orientuotis apibrėžimų labirinte, buvo sukurta lentelė, kurioje pateikiami įvairių darbo būdų skirtumai.

Darbo naudojant skaitmeninius įrankius tipas	Apibrėžimas
Nuotolinis darbas	Nuotolinis darbas - tai bet koks darbas, atliekamas ne darbdavio patalpose, neatsižvelgiant į naudojamą technologiją. Pagal Lenkijos darbo kodekso pakeitimus tai yra: visiškai arba iš dalies atliekamas darbas darbuotojo nurodytoje ir su darbdaviu kiekvieną kartą suderintoje vietoje
„Teledarbas“	Teledarbas – tai bet kokia darbo organizavimo ir (arba) atlikimo forma, naudojant informacines technologijas, pagal darbo sutartį ir (arba) darbo santykius, kai darbas, kuris taip pat gali būti atliekamas darbdavio patalpose, reguliariai atliekamas ne tose patalpose
Nuotolinis darbas („teledarbas“) ne visą darbo dieną	Šią darbo tvarką, pagal kurią nuotolinio darbo dienos derinamos su darbo dienomis biure, pirmą kartą 20 amžiaus 8 dešimtmečio pradžioje pradėjo taikyti Jackas Nillesas JAV
IRT grindžiamas nuotolinis („teledarbas“) ir mobilusis darbas *(TICTM)*	TICTM – tai informacinių ir ryšių technologijų, pavyzdžiui, išmaniųjų telefonų, planšetinių kompiuterių, nešiojamųjų kompiuterių ir stalinių kompiuterių, naudojimas darbui ne darbdavio patalpose. Jis apima visas nuotolinio (tele) darbo formas, tačiau siekiama atskirti darbą iš namų ar nuolatinės vietos (teledarbas) ir IRT grindžiamą mobilųjį darbą. Pastarasis terminas Vokietijoje vartojamas siekiant atskirti nuotolinį (tele) darbą namuose nuo mobilesnės darbo formos.
Pažangus ir (arba) judrus darbas	Pažangus darbas – tai lanksti darbo sistema, leidžianti darbuotojams patogiai ir efektyviai dirbti neribojant laiko ir vietos (bet kada ir bet kur), naudojant tinklines IRT. Panašus terminas („judrus darbas“) vartojamas Italijoje
Lanksčios darbo sąlygos	Lankstus darbo grafikas – tai alternatyvios darbo galimybės, leidžiančios atlikti darbą už tradicinių standartinės darbo dienos laiko ir (arba) erdvės ribų.
Virtualus darbas	Virtualus darbas – tai apmokamas arba neapmokamas darbas, atliekamas naudojant skaitmenines ir telekomunikacijų technologijas arba kuriantis skaitmeninės

	žiniasklaidos turinį.
Hibridinis darbas	Tai susitarimas, pagal kurį darbas gali būti atliekamas iš dalies darbdavio patalpose ir iš dalies namuose ar kitose vietose.

Nuotolinis darbas ir „teledarbas“ - ką apie tai sako įstatymai?

ES lygmens reguliavimas

Šiuo metu trūksta privalomų teisės aktų, skirtų nuotoliniam darbui, nors keliose direktyvose ir reglamentuose nagrinėjami klausimai, kuriais siekiama užtikrinti geras nuotolinio darbo sąlygas. Tačiau yra Europos *pagrindų susitarimas dėl nuotolinio darbo (*2002 m.). Šis dokumentas yra savarankiškas Europos socialinių partnerių (ETUC, UNICE, UEAPME ir CEEP) susitarimas ir įpareigoja asocijuotas nacionalines organizacijas jį įgyvendinti pagal kiekvienai valstybei narei būdingą „tvarką ir praktiką“.

Nuotolinis darbas ir teisė – Lenkijos pavyzdys

2022 m. gruodžio 1 d. įstatymu, kuriuo iš dalies keičiamas Darbo kodekso įstatymas ir tam tikri kiti įstatymai, į Lenkijos darbo teisę buvo įtraukta nuotolinio darbo sąvoka, kartu panaikinant nuostatas dėl teledarbo. Pagal šį pakeitimą nuotolinis darbas – **tai darbas, visiškai arba iš dalies atliekamas darbuotojo nurodytoje ir kiekvienu atveju su darbdaviu suderintoje vietoje,** įskaitant darbuotojo namų adresą, inter alia, naudojant tiesioginio ryšio per atstumą priemones.

Teledarbas – tai bet kokia darbo organizavimo ir (arba) atlikimo naudojant informacines technologijas forma, susijusi su darbo sutartimi ir (arba) darbo santykiais, kai darbas, **kuris taip pat galėtų būti atliekamas darbdavio patalpose, reguliariai atliekamas ne tose patalpose**. Todėl nuotolinis darbas gali būti laikinas, o teledarbas iš esmės grindžiamas nuolatiniu pareigų atlikimu iš namų.

Nuotolinio darbo taisyklės turėtų būti nustatytos susitarus su profesinėmis sąjungomis darbo tvarkos taisyklėse arba individualiame susitarime su darbuotoju. Be to, darbdavys negali neleisti dirbti nuotoliniu būdu tėvams, auginantiems vaiką iki ketverių metų, neįgaliųjų tėvams ar globėjams arba nėščioms moterims (išskyrus atvejus, kai tai neįmanoma dėl atliekamų pareigų

pobūdžio). Darbdavys taip pat privalo aprūpinti darbuotoją reikiama įranga ir įrankiais nuotoliniam darbui atlikti ir, be kita ko, kompensuoti elektros energijos ar interneto vartojimo išlaidas.

Nuotolinis darbas gali būti atliekamas darbuotojo prašymu arba darbdavio nurodymu. Darbdavys taip pat gali įsakyti dirbti nuotoliniu būdu esant nepaprastosios padėties, ekstremaliosios situacijos ar ekstremaliosios situacijos epidemijos atveju ir dėl nenugalimos jėgos aplinkybių, pavyzdžiui, sunaikinus darbo vietą dėl gaisro ar potvynio.

Į Darbo kodekso pataisas taip pat įtrauktas pasiūlymas dėl vadinamojo proginio nuotolinio darbo, pagal kurį darbuotojo prašymu jis galės dirbti nuotoliniu būdu iki 24 dienų per kalendorinius metus. Darbuotojo prašymas dėl proginio nuotolinio darbo vis dėlto nėra privalomas ir darbdavys gali atsisakyti jį tenkinti.

Svarbu tai, kad darbdaviui draudžiama diskriminuoti darbuotoją dėl to, kad jis dirba nuotoliniu būdu, taip pat dėl to, kad jis atsisako dirbti tokį darbą. Be to, darbdavys privalo leisti nuotolinį darbą dirbančiam darbuotojui būti darbo vietos patalpose, bendrauti su kitais darbuotojais, naudotis darbdavio patalpomis ir įrenginiais, įmonės socialinėmis patalpomis ir visuomenine veikla - tokiomis pačiomis sąlygomis, kaip ir kitiems darbuotojams.

1.5 Algoritmai ir diskriminacija darbo vietoje

Informacijos valdomame pasaulyje vis dažniau girdime apie dirbtinį intelektą (*artificial intelligence* – AI), kurio taikymo sritis galima rasti beveik visur. Galima tikėtis, kad jis vis dažniau bus naudojamas ir darbo srityje. Remiantis „Forbes“ tyrimu, maždaug keturios iš penkių įmonių mano, kad dirbtinis intelektas yra svarbiausias jų verslo strategijos prioritetas. Tačiau viltis optimizuoti išlaidas ir padidinti gamybos efektyvumą lydi darbuotojų baimė prarasti darbo vietas - remiantis „Forrester Future of Jobs Forecast“ ataskaita, dėl automatizacijos prarastų darbo vietų skaičius sieks 12 milijonų vien Europoje iki 2040 m.

Nepaisant to, kad viešos diskusijos kelia daug emocijų, vis dar trūksta tvirto paaiškinimo, kaip veikia dirbtinis intelektas ir ar bet kokio tipo automatizavimas tikrai gali būti priskiriamas dirbtiniam intelektui. Norint visapusiškai suprasti problemą, taip pat būtina apsvarstyti, kuo skiriasi dirbtinio intelekto sistema nuo algoritmų, nes šios sąvokos dažnai vartojamos pakaitomis.

Dirbtinis intelektas yra labai plati sąvoka, apimanti grupę algoritmų, kurie gali keisti savo parametrus ir kurti naujus algoritmus, reaguodami į išmoktus įvesties duomenis. Šis gebėjimas keistis, prisitaikyti ir augti remiantis naujais duomenimis vadinamas „intelektu“.

Paprasčiausiai dirbtinį intelektą galima apibrėžti kaip **mašinų gebėjimą suprasti, mokytis, planuoti ir demonstruoti kūrybiškumą.** Tuo tarpu pagal dirbtinio intelekto reglamento (Dirbtinio intelekto akto) projekte siūlomą apibrėžtį dirbtinio intelekto sistema – tai programinė įranga, sukurta naudojant vieną ar daugiau reglamente išvardytų metodų[4], kuri tam tikrais žmogaus nustatytais tikslais gali generuoti rezultatus, pavyzdžiui, turinį, prognozes, rekomendacijas ar sprendimus, darančius poveikį aplinkai, su kuria ji sąveikauja.

Algoritmas - tai instrukcijų rinkinys, tiksliau, skaičiavimo formulė, kuri savarankiškai priima sprendimus, pagrįstus statistiniais modeliais arba sprendimų priėmimo taisyklėmis, be aiškaus žmogaus įsikišimo. Tai yra instrukcijų seka, nurodanti kompiuteriui, ką daryti pagal tiksliai apibrėžtus veiksmus ir taisykles, skirtas užduočiai atlikti. Taigi tai iš anksto nustatyta, griežta, užkoduota veiksmų eiga, kuri paleidžiama susidūrus su konkrečiu elementu.

Dirbtinio intelekto sričiai priskiriama problema yra **savaiminis mokymasis** (angl. *machine learning*, ML). Pagrindinis jos tikslas – sukurti automatiškai veikiančią sistemą, kuri gebėtų tobulėti remdamasi duomenų patirtimi ir tuo pagrindu įgyti naujų žinių. Procesas grindžiamas modelio radimu pateiktuose duomenyse, siekiant atsakyti į klausimą apie nežinomą rinkinį. Todėl tai yra tam tikras ateities prognozavimas naudojant tikimybę ir statistiką.

Ne visi dirbtiniai intelektai pasižymi saviauklos gebėjimais. Kartais algoritmas gali būti parašytas taip, kad programa, į kurią jis įterptas, vykdytų komandas nesimokydama iš naujų duomenų (kaip ML atveju).

Tinkamai suprogramuoto algoritmo pavyzdys – garsiojo IBM superkompiuterio „Deep Blue“ algoritmas. Ši mašina išgarsėjo po to, kai prieš 25 metus jai pavyko laimėti šachmatais prieš meistrą Garį Kasparovą. Taip atsitiko todėl, kad „Deep Blue“ turėjo įrašytus visus galimus ėjimus, priklausomai nuo figūrų išsidėstymo šachmatų lentoje ir priešininko strategijos. Dėl to ir dėl didelės skaičiavimo galios jis galėjo veiksmingai veikti bet kokioje situacijoje.

IBM „Deep Blue“ įdiegto algoritmo priešingybė – „DeepMind“ sukurta programa „AlphaGo“. Naudodama savaiminio mokymosi mechanizmus, ši sistema išmoko žaisti GO (senovinį kinų stalo

[4] Reglamente išvardyti dirbtinio intelekto metodai ir būdai:

(a) mašininio mokymosi mechanizmai, įskaitant prižiūrimąjį mokymąsi, neprižiūrimąjį mašininį mokymąsi ir mokymąsi naudojant pastiprinimą, taikant įvairius metodus, įskaitant gilųjį mokymąsi,

(b) logika ir žiniomis pagrįsti metodai, įskaitant žinių atvaizdavimą, indukcinį (loginį) programavimą, žinių bazes, išvedimo ir dedukcijos mechanizmus, (simbolinį) samprotavimą ir ekspertines sistemas,

(c) statistiniai metodai, Bajeso įverčiai, paieškos ir optimizavimo metodai.

žaidimą, kurio tikslas – iš pradžių tuščioje lentoje savo akmenimis apsupti kuo didesnę teritoriją) ir netgi įveikė geriausiu pasaulyje laikomą žaidėją.

Kita vertus, **bendrasis dirbtinis intelektas** – tai sistema, kuri pati save suvokia, turi išsamių žinių arba pažintinių įgūdžių ir gali savarankiškai mąstyti bei atlikti užduotis. Technologinio singuliarumo sukūrimas jau daugelį metų kelia daug diskusijų – visų pirma dėl to, ar jis apskritai įmanomas. Pasak vieno pagrindinių bendrojo dirbtinio intelekto atsiradimo kritikų, filosofo Huberto Dreifuso (Hubert Dreyfus), kompiuteriai, kurie neturi kūno, nepraeina vaikystės ir paauglystės, nedalyvauja kultūrinėje patirtyje, apskritai negali įgyti intelekto žmogiškąja prasme. Vienas iš pagrindinių Dreyfuso argumentų buvo tas, kad žmogaus intelekto vystymasis iš dalies vyksta nesąmoningai, todėl negali būti išreikštas ir įtrauktas į kompiuterio programą.

Algoritmai darbe

1. **Kandidato gyvenimo aprašymo analizė naudojant algoritmą prieš užmezgant darbo santykius.**

Algoritminis įdarbinimas apima dirbtinio intelekto ir mašininio mokymosi sistemų naudojimą kandidatų paieškai, atrankai, pokalbiams ir įdarbinimui. Taikant šį metodą kandidatui įvertinti naudojami keli kriterijai, įskaitant jo patirtį ir išsilavinimą, o gauti gyvenimo aprašymai dažnai filtruojami pagal raktinius žodžius. Algoritmai taip pat gali padėti įvertinti socialinius emocinius įgūdžius, pavyzdžiui, kandidato polinkį greitai mokytis ir dirbti komandoje.

Naudodamos įvairias dirbtinio intelekto priemones įdarbinimo metu įmonės nori užtikrinti, kad procesas vyktų sąžiningai. Taip yra todėl, kad teoriškai pirmojo automatinio vertinimo metu nelieka vietos žmogiškajam veiksniui ir galimai diskriminacijai. Tačiau šios sistemos dažnai kritikuojamos dėl to, kad atspindi jas užprogramavusių žmonių šališkumą.

Svarbu tai, kad algoritmai nepriima galutinio sprendimo dėl įdarbinimo. Jais visų pirma siekiama susiaurinti didelį kandidatų ratą.

CV analizės metodai pagal algoritmą:

- **CV vertinimas balais** – algoritmas skiria taškus pagal įdarbintojo iš anksto nustatytus kriterijus
- **reitingavimas** – gyvenimo aprašymų išdėstymas pagal raktažodžių paplitimą

- **atitikimas** – raktinių žodžių, atitinkančių darbo skelbime nurodytus raktažodžius, nustatymas
- **analizė** – algoritmas analizuoja gyvenimo aprašymo semantiką, išskiria pagrindinę informaciją ir suskirsto ją į įvairias kategorijas: patirtis, įgūdžiai, kontaktinė informacija

2. Algoritmų savybės ir naudojimo sritys darbo vietoje

Algoritmų tipai:

- **aprašomasis** – naudojamas praeities įvykiams fiksuoti ir jų poveikiui dabartiniams įvykiams analizuoti, pavyzdžiui, veiklos vertinimo algoritmai, skirti įvairių rūšių duomenims, susijusiems su darbuotojo veikla, rinkti ir bendram įvertinimui pateikti
- **prognostiniai** – jais siekiama numatyti būsimą elgesį arba įvertinti įvykio tikimybę (pvz., numatyti naujų darbuotojų paklausos padidėjimą)
- **įsakomojo / rekomendacinio pobūdžio** – jų užduotis yra iš įvairių galimybių pasirinkti geriausią scenarijų ir rekomenduoti konkretų veiksmą arba tiesiog jį įgyvendinti (pvz., nuspręsti dėl žmogiškųjų išteklių, užduočių paskirstymo ar tvarkaraščio).

Algoritmų naudojimas darbe susijęs su vadinamuoju **algoritminiu valdymu**. Tai reiškia „valdymo sistemą, kurioje algoritmams suteikiama atsakomybė už darbui įtakos turinčių sprendimų priėmimą ir vykdymą, taip sumažinant žmogaus dalyvavimą ir darbo proceso priežiūrą“.

Šešios pagrindinės darbo eigos valdymo funkcijos, kurioms buvo naudojami algoritmai:

1. darbuotojų stebėjimas ir (arba) kontrolė
2. tikslų nustatymas
3. rezultatų valdymas
4. tvarkaraščių sudarymas
5. atlyginimas
6. darbo santykių nutraukimas

Didesnė galimybė darbdaviui kontroliuoti darbuotojus naudojant algoritmus

- **Algoritminis rekomendavimas** – darbdaviai naudoja algoritmus, kad įvertintų tam tikrą situaciją ir pateiktų pasiūlymus, kuriais siekiama, kad darbuotojas imtųsi algoritme nurodytų veiksmų.
- **Algoritminis apribojimas** – algoritmų naudojimas siekiant rodyti tik tam tikrą informaciją ir leisti tam tikrus veiksmus, o kitų neleisti.

Toks algoritmų naudojimas gali padidinti darbuotojų nusivylimą, kurie, turėdami laikytis nesuprantamų rekomendacijų, gali jausti, kad jų balso svarba yra menkesnė.

Darbui vertinti naudojami algoritmai

- **Algoritminė apskaita** – skaičiavimo procedūrų naudojimas siekiant stebėti, apibendrinti ir pateikti, dažnai realiuoju laiku, įvairius tiksliai atrinktus duomenis iš vidaus ir išorės šaltinių.
- **Kompiuterinės technologijos** – naudojamos vertinimams ir reitingams rinkti, kad būtų galima apskaičiuoti tam tikrą darbuotojo veiklos rodiklį; taip pat prognostinei analizei, kad būtų galima numatyti būsimus rezultatus.

Vertinant darbą pagal algoritmus gali kilti specifinių problemų, susijusių ne tik su diskriminacija, bet ir su darbuotojų privatumo jausmo praradimu, informacijos saugumu ir pan.

Atlyginimui naudojami algoritmai

Algoritminis atlygis gali realiuoju laiku atlyginti už elgesį, kuris atitinka iš anksto nustatytas gaires. Taip pat galima taikyti žaidybinimo principus, kad darbuotojams darbo patirtis taptų pozityvesnė ir įdomesnė.

Drausmė darbo vietoje

Algoritminis pakeitimas (*algorithmic replacing*) – tai greitas ar net automatinis prastai dirbančių darbuotojų atleidimas ir jų pakeitimas efektyvesniais darbuotojais.

Automatinis sprendimų priėmimas ir profiliavimas

BDAR reglamento 22 straipsnyje nustatyta, kad duomenų subjektas turi teisę į tai, kad jam nebūtų taikomas sprendimas, kuris grindžiamas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, ir kuris sukelia teisines pasekmes arba daro panašų didelį poveikį

atitinkamam asmeniui. Asmens teisė ginčyti automatizuotą sprendimą dėl jo asmens grindžiama dviem kvalifikuoto profiliavimo pagrindais: automatizuotu duomenų tvarkymu ir teisiniu poveikiu arba veiksniais, darančiais didelį poveikį asmeniui.

Kas yra automatizuotas sprendimų priėmimas?

Dėl užkoduotų žinių ir tikslios aplinkos sąlygų analizės kompiuteris gali duoti nurodymus be žmogiškojo faktoriaus. Šis veiksmas grindžiamas pažangiais skaičiavimais ir išskirtinai techninėmis apdorojimo priemonėmis. Taigi, žmogaus dalyvavimas sprendimų priėmimo procesuose yra minimalus, o rezultatai pateikiami automatizuotai.

Tačiau tam, kad duomenų tvarkymas būtų laikomas visiškai automatizuotu, į sprendimų priėmimo procesą neturi kištis žmogus. Reikėtų pažymėti, kad akivaizdus žmogaus dalyvavimas priimant sprendimus, pavyzdžiui, tik patvirtinant algoritmo nurodytą sprendimą, nebus laikomas pagrindu netaikyti BDAR 22 straipsnyje nustatyto draudimo. Tačiau jei asmuo, turintis įgaliojimus ir teisę pakeisti sprendimą, imtųsi veiksmų jam pakeisti, automatizuotas sprendimų priėmimas nebūtų vykdomas.

Situacijų, kurioms taikomas BDAR 22 straipsnis, katalogas yra platus ir apima tiek situacijas, kai sprendimas sukelia teisines pasekmes (t. y. daro poveikį asmens teisėms pagal įstatymą; pvz., teisei į bedarbio pašalpą), tiek ir „panašiai reikšmingą poveikį“ (pvz., susijusį su subjekto finansine padėtimi ar sveikata).

Kas yra profiliavimas?

BDAR 22 straipsnis taip pat apima specialią automatizuoto sprendimų priėmimo kategoriją, t. y. sprendimų priėmimą remiantis profiliavimu. Terminas „profiliavimas“ (BDAR 4 straipsnis) reiškia bet kokios formos automatizuotą asmens duomenų tvarkymą, susijusį su asmens duomenų naudojimu tam tikriems fizinio asmens veiksniams įvertinti. Visų pirma tai taikoma analizuojant ar prognozuojant aspektus, susijusius su **to fizinio asmens darbo rezultatais**, ekonomine padėtimi, sveikata, asmeniniais pageidavimais, interesais, patikimumu, elgesiu, buvimo vieta arba judėjimu[5].

[5] Pažymėtina, kad, nepaisant panašumų, profiliavimas ir automatizuotas sprendimų priėmimas yra du skirtingi veiksmai, kurie gali būti susiję arba nesusiję.

Praktiniai profiliavimo pavyzdžiai:

- **rinkodara** – vartotojų profilių kūrimas, renkant informaciją apie pirkiniams teikiamą pirmenybę ir sistemai siūlant individualiai klientui pritaikytus produktus
- **paskolos ir kreditai** – kandidatų profiliavimas ir teigiamo sprendimo dėl kredito priėmimas remiantis algoritmui pateiktų asmens duomenų analize
- **socialinės paramos išmokos** – profiliavimo naudojimas siekiant teisingai paskirstyti valstybės paramos išteklius
- **įdarbinimas ir žmogiškieji ištekliai** – masiniai įdarbinimo procesai dažnai vykdomi naudojant sistemas, kurios pačios analizuoja kandidato gyvenimo aprašymą ir kitus duomenis ir, remdamosi tokia analize, nusprendžia, ar kandidatą atmesti, ar priimti (pvz., atlikus CV analizę pagal raktinius žodžius). Žmogiškųjų išteklių srityje profiliavimas taip pat naudojamas darbo vietoms vertinti

Su profiliavimu susijusi rizika

- **Privatumo pažeidimas ir skaidrumo trūkumas** – nors daugelis žmonių žino, kad tam tikros rūšies duomenys (pvz., medicininiai) yra ypač jautrūs ir turėtų būti saugomi, dalis visuomenės nežino, kiek informacijos apie juos galima gauti iš elgsenos duomenų, naudojamų nepageidaujamam profiliavimui. Be to, pats profiliavimo procesas dažnai gali būti neskaidrus ir nesuprantamas tiems, kuriems jis taikomas.
- **Diskriminacija** – žmonių sukurti algoritmai gali turėti savo kūrėjų šališkumo. Todėl sistema gali mažiau palankiai vertinti, pavyzdžiui, kitokių religinių pažiūrų, seksualinės orientacijos ar odos spalvos žmones.
- **Įvairovės mažinimas** – profiliavimas skirtas tam tikro turinio gavėjų suskirstymui į grupes, jų įvertinimui, apibūdinimui, siekiant pritaikyti medžiagą pagal atitinkamų asmenų interesus ar įsitikinimus (pvz., politinius). Taip supaprastinamas naudotojui pateikiamos informacijos katalogas, apribojant turinio įvairovę ir sukuria vadinamuosius informacinius burbulus bei susiaurina virtualų gavėjo akiratį.

Profiliavimas darbo procese – atvejo analizė

Nuo 2020 m. Austrijos valstybinė užimtumo tarnyba (AMS) naudoja algoritminį darbo ieškančių asmenų profiliavimą, kad padidintų konsultavimo proceso veiksmingumą ir suderintų

dabartines programas su darbo rinkos poreikiais. Sistema siekiama suskirstyti darbo ieškančius asmenis į tris kategorijas:

– A grupė. Geros galimybės susirasti darbą artimiausiu laikotarpiu.

– B grupė. Vidutinės perspektyvos.

– C grupė. Menkos ilgalaikės perspektyvos.

Tada, atsižvelgiant į suteiktą kategoriją, algoritmas pritaiko pagalbos programą prie asmens poreikių.

Klausimas diskusijai: Ar pagrįstas algoritminis bedarbių profiliavimas, siekiant pritaikyti paramos programas prie jų poreikių?

Pavyzdys: Niujorke pasiūlytas įstatymas, kuriuo ribojamas dirbtinio intelekto priemonių naudojimas įdarbinimo procesuose. Kaip nurodyta, pagrindinė problema, su kuria susiduriama, susijusi su dirbtinio intelekto vertinimais, nes buvo grupių, kurios neatitiko iš anksto užprogramuoto rakto ir buvo pašalintos iš proceso. Kaip pavyzdį galima paminėti žmonių, turinčių kalbos sutrikimų, diskvalifikavimą per vaizdo pokalbį, kurį vertino kompiuteris, arba kandidatų, sergančių artritu ar kitomis ligomis, ribojančiomis jų fizinį pasirengimą, atmetimas (kai vertinamas testų atlikimo laikas).

Klausimas diskusijai: Ar reikėtų uždrausti bet kokį algoritminį vertinimą įdarbinimo procese?

Pavyzdys: verslininkas kūrė ir diegė dirbtinio intelekto įrankį savo įmonėje, kad padėtų įdarbinti konkrečiam darbui tinkamus žmones. Darbas buvo sustabdytas, kai įmonė suprato, kad sistema diskriminuoja moteris. Moterų profiliai dažniau buvo atmetami dėl to, kad dirbtinis intelektas rėmėsi per pastaruosius 10 metų įmonėje dirbusių žmonių (daugiausia vyrų) gyvenimo aprašymų duomenimis. Dėl to kompiuteris nusprendė teikti pirmenybę vyrams, o tai automatiškai sumažino tikimybę, kad bus priimtos paraiškos, turinčios moteriškų bruožų.

Diskusijos klausimas: Ar galite įvardyti kitus diskriminacijos pavyzdžius, kurie galėtų pasireikšti, kai įdarbinant naudojama profiliavimo algoritmus?

Algoritmų naudojimo darbuotojų atžvilgiu rizika ir nauda

Grėsmės:

- didesnė darbdavio kontrolė darbuotojo privatumo sąskaita (nėra tinkamo darbuotojo sutikimo)
- žmogaus savarankiškumo mažinimas, pakeičiant tiesioginį vadovų ir jų pavaldinių kontaktą, t. y. valdymo sistemų "dehumanizavimas"
- algoritminis šališkumas ir diskriminacija

Nauda:

- didesnis produktyvumas dėl sutaupyto laiko ir efektyvesnio sprendimų priėmimo
- efektyvesnis pamainų planavimas ir pareigų paskirstymas
- galimybė greičiau įdarbinti darbuotojus
- galimybė geriau suprasti darbo vietoje kylančias problemas, geriau pažinti darbo aplinką
- retesnis darbuotojų favorizavimas ir šališkumo, galinčio egzistuoti tiesioginiuose santykiuose, pašalinimas
- automatinis sprendimų priėmimas riboja galimybę kištis į vadovybės sprendimus dėl darbo užmokesčio, atostogų patvirtinimo ar pamainų paskirstymo

Darbuotojo ir darbdavio santykių algoritmizavimas

Darbo procesų algoritmizavimas jau tapo daugelio įmonių realybe. Tačiau jis dažnai veikia darbuotojų nenaudai tokiais klausimais kaip:

- **Automatinis darbuotojų atleidimas iš darbo** (klausimas bus aptartas seminaro metu)
- **Algoritminis atsiskaitymas už darbą:**
    - Kurjerių programėlės algoritmas nurodė pristatantiems vairuotojams vykdyti užsakymus, neatsižvelgiant į atstumą iki užsakymo atsiėmimo vietos. Vairuotojams nebuvo mokama už atstumą iki užsakymo atsiėmimo vietos. Verslininkas padengdavo tik trumpesnio atstumo nuvažiavimo išlaidas, todėl, atėmus degalų sąnaudas ir automobilio nusidėvėjimą, vairuotojai negaudavo jokio pelno.
    - Bendrovė tvirtino, kad uždarbis priklauso nuo nuvažiuotų kilometrų skaičiaus ir kad už kiekvieną užsakymą yra nustatytas fiksuotas tarifas, vadinamas „baziniu tarifu“, kuris įvairiuose miestuose gali skirtis.

- Tačiau problema taip pat buvo darbuotojų netikrumas dėl valandinio įkainio - pandemijos laikotarpiu kurjeriams per vieną dieną būdavo pranešama, kad įkainis pasikeitė, todėl jie dažnai ne užsidirbdavo, o būdavo priversti „primokėti“ už atliktą darbą.
- Po streiko kurjeriams buvo pažadėta keletas pakeitimų, įskaitant galimybę atsisakyti užsakymo ne vieną, o tris kartus per dieną. Taigi, nepalankiai pasikeitus baziniam tarifui, kurjeriai turi galimybę atsisakyti užsakymo. Tačiau didesnio tarifų stabilizavimo nepažadėta.

- **Algoritminis darbuotojų identifikavimas**
  - Taksi programėlėse naudojama programinė įranga, kuria remiantis įkeltomis asmenukėmis tikrinama vairuotojų tapatybė. 2018 m. buvo nustatyta, kad vienos bendrovės naudojama tokio tipo programinė įranga yra linkusi klysti dirbant su tamsiaodžiais asmenimis (verta paminėti, kad didžioji dauguma taksi programėlėmis besinaudojančių vairuotojų yra vyrai ir daugelis jų yra iš BAME *(juodaodžiai, azijiečiai ir etninių mažumų atstovai)* aplinkos).
  - Dėl tapatybės tikrinimo keliolika kurjerių pranešė, kad dėl problemų su algoritmu jiems buvo grasinama nutraukti darbo sutartį, įšaldytos jų sąskaitos arba jie buvo visam laikui atleisti iš darbo po to, kai jų daryta asmenukė neatitiko realaus laiko tapatybės patikrinimo *(Real Time ID Check)*. Kai kurie žmonės buvo atleisti iš darbo po to, kai asmenukės funkcija apskritai atsisakė veikti. Šiame procese nebuvo numatyta teisė pateikti apeliaciją.
- **Algoritminis darbuotojų (našumo ir ne tik) vertinimas** (tema bus aptarta seminaro diskusijoje)

Algoritmavimas ir duomenų apsauga

Kaip jau minėta, algoritmas - tai instrukcijų, kaip faktų apie pasaulį rinkinį paversti naudinga informacija, rinkinys. Dar paprasčiau tariant, faktai laikomi duomenimis, o informacija - žiniomis, kuriomis toliau gali naudotis žmonės arba kitos mašinos.

Duomenys darbo vietoje ir jų apsauga

Siekdami išvengti privatumo konfliktų, darbdaviai turėtų įgyvendinti tinkamas asmens duomenų apsaugos priemones, ypač kai tokie duomenys naudojami automatizuotam sprendimų priėmimui, turinčiam tiesioginį poveikį darbuotojui. Todėl būtina tinkamai subalansuoti darbdavio interesą diegti duomenimis grindžiamas technologijas bei duomenų subjekto gerovę ir veikti pagal pagrindinius duomenų apsaugos principus.

- **Darbdaviai turėtų rinkti duomenis apie darbuotojus tik tada, kai tai būtina darbovietės valdymui ir darbuotojų darbo rezultatams.**

Laikydamiesi duomenų kiekio mažinimo principo, darbdaviai turėtų apriboti darbuotojų duomenų rinkimą, t. y. bet kokios informacijos, susijusios su jų tapatybe, sveikata ir biometriniais duomenimis, duomenimis, susijusiais su veikla darbo vietoje (pvz., apie produktyvumą), taip pat informacija, gauta iš darbuotojų veiklos socialiniuose tinkluose. Neribotai renkant duomenis darbuotojams be reikalo kyla rizika – darbdaviai gali, pavyzdžiui, piktnaudžiauti asmens duomenimis arba nekontroliuojamai juos nutekinti.

- **Darbuotojai turėtų turėti teisę tikrinti, taisyti ir gauti savo duomenis.**

Darbuotojai turėtų turėti galimybę gauti visą svarbią informaciją apie savo duomenis, įskaitant informaciją apie tai, kodėl ir kaip buvo renkami jų duomenys, kokios išvados apie darbuotoją buvo padarytos iš duomenų ir ar duomenys buvo panaudoti priimant su jų įdarbinimu susijusį sprendimą. Darbdaviai turėtų būti atsakingi už netikslių duomenų ištaisymą.

- **Darbuotojų duomenys turėtų būti apsaugoti nuo netinkamo naudojimo**

Darbdavys jokiomis aplinkybėmis neturėtų leisti parduoti ar licencijuoti darbuotojų duomenų trečiosioms šalims. Jei ne ši išlyga, pažadas gauti pelno iš darbuotojų duomenų panaudojimo sukeltų pernelyg didelę riziką, kad darbdaviai duomenis panaudos netinkamai, siekdami papildomai užsidirbti.

- **Sutikimas tvarkyti asmens duomenis**

Darbo santykiuose sutikimas tvarkyti asmens duomenis yra labai prieštaringas, nes dėl šalių disbalanso lengva suabejoti darbuotojo savanoriškumu duodant tokį sutikimą. Pažymėtina, kad darbdavys, grasindamas neigiamomis pasekmėmis darbo santykių srityje, galėtų lengvai priversti darbuotoją taikstytis su jo lūkesčiais. Tačiau pagal BDAR 155 straipsnį valstybės narės gali nustatyti konkrečias taisykles dėl darbuotojų asmens duomenų tvarkymo įdarbinant ir ypač dėl sąlygų, kuriomis asmens duomenys gali būti tvarkomi su darbuotojo sutikimu.

Pavyzdžiui, Lenkijoje darbdavys gali rinkti Darbo kodekse išvardytus asmens duomenis, jei darbuotojas sutinka. Tačiau reikėtų pažymėti, kad sutikimas turi būti duotas savanoriškai, todėl jis nebus veiksmingas, jei darbuotojas neturės galimybės jo atsisakyti, bijodamas neigiamų pasekmių. Be to, sutikimą galima bet kada atšaukti.

Skirtinguose darbo etapuose naudojamų duomenų tipai

I etapas. Darbo paieška

Ko gali tikėtis darbdavys?

Darbdavys gali tikėtis, kad kandidatas jam pateiks pagrindinius duomenis, reikalingus siekiant sudaryti sutartį. Šiuos duomenis gali sudaryti:

- identifikaciniai duomenys (vardas, pavardė, tėvų vardai, pavardės, gimimo data),
- tokio asmens nurodyti kontaktiniai duomenys;
- išsilavinimas, įgūdžiai, darbo patirtis (mokyklos ir universiteto diplomai, išklausyti mokymai ir kursai, ankstesni darbdaviai, užimamos pareigos ir profesinės pareigos).

Svarbu tai, kad, nepaisant duomenų pateikimo, dalyvaujant įdarbinimo procese, sutartis galiausiai nebūtinai turi būti sudaryta.

Ko gali tikėtis kandidatas?

Potencialus darbdavys, kuris renka kandidatų duomenis, jau pirmajame įdarbinimo proceso etape privalo informuoti šiuos asmenis apie:

- visą bendrovės pavadinimą ir registruotąjį adresą,
- duomenų apsaugos pareigūno (jei yra jį paskyręs) kontaktinius duomenis,
- duomenų tvarkymo tikslą ir duomenų tvarkymo teisinį pagrindą, duomenų rinkimo metu jam žinomus gavėjus (suprantama plačiąja prasme) arba gavėjų kategorijas,
- ketinimą tvarkyti duomenis tarpvalstybiniu mastu (jei toks ketinimas yra),
- laikotarpį, kurį duomenys bus tvarkomi, arba šio laikotarpio nustatymo kriterijus,
- kandidato teisę reikalauti susipažinti su duomenimis, įskaitant duomenų kopiją, taip pat ištaisyti, ištrinti arba apriboti duomenų tvarkymą,
- teisę bet kada atšaukti sutikimą, nedarant poveikio duomenų tvarkymo, atlikto remiantis sutikimu iki jo atšaukimo, teisėtumui (jei duomenys renkami remiantis sutikimu),
- teisę pateikti skundą Duomenų apsaugos tarnybos pirmininkui,
- savanoriškumą ar pareigą pateikti duomenis ir jų nepateikimo pasekmes.

II etapas. Įdarbinimo procesas

Per pokalbį įdarbintojas gali užduoti daug išsamių klausimų apie jūsų gyvenimo aprašyme pateiktą informaciją. Tačiau svarbu, kad jie būtų tik apie tai, kas susiję su pareigybe, į kurią kandidatuojama. Klausimai, kurie gali sugėdinti kandidatą, pažeisti jo teisę į privatumą ar asmeninius interesus (pavyzdžiui, susiję su privačiu gyvenimu, religija, seksualine orientacija, politinėmis pažiūromis ir t. t.), yra nepriimtini.

Duomenų saugojimo laikas

Kandidato duomenų saugojimo laikotarpis turėtų atitikti duomenų valdytojo iš anksto nustatytas duomenų tvarkymo taisykles. Todėl paprastai darbdavys turėtų visam laikui ištrinti kandidato, su kuriuo nusprendė nesudaryti darbo sutarties, asmens duomenis iš karto po įdarbinimo proceso pabaigos, t. y. po to, kai su naujai įdarbintu darbuotoju pasirašoma darbo sutartis (pvz., ištrindamas arba grąžindamas duomenis).

III etapas. Įdarbinimo laikotarpis

Atsiradus darbo santykiams, darbdaviui ir darbuotojui atsiranda tam tikros teisės ir pareigos. Jų įgyvendinimas akivaizdžiai susijęs su darbuotojo asmens duomenų tvarkymu. Nors asmens duomenų administravimas iš esmės reglamentuojamas BDAR reglamentu, tačiau darbo atveju nacionaliniuose teisės aktuose jis dar labiau patikslintas.

Pavyzdžiui, Lenkijoje pagal Darbo kodekso 221 straipsnio 2 ir 4 dalis darbdavys turi teisę reikalauti, kad darbuotojas, kurį jis nusprendė įdarbinti, pateiktų (be asmens duomenų, kuriuos jis galėjo gauti iš jo įdarbinimo metu) taip pat:

- gyvenamosios vietos adresą,
- asmens kodą,
- kitus asmens duomenis, įskaitant, inter alia, jo vaikų vardus, pavardes ir gimimo datas, jei tokių duomenų pateikimas yra būtinas siekiant pasinaudoti jo specialiomis teisėmis pagal darbo teisę,
- išsilavinimą ir ankstesnę darbo istoriją, jei nebuvo pagrindo jų reikalauti iš pretendento į darbą,
- mokėjimo sąskaitos numerį, jei darbuotojas neprašė išmokėti atlyginimo į rankas.

Darbdavio informacinės pareigos darbuotojui

Kadangi darbdavys darbuotojo duomenis tvarkys kitu tikslu nei kandidato, darbuotojas turėtų būti apie tai informuotas. Šį tikslą galima pasiekti įtraukiant tokią informaciją į kandidatams

įdarbinimo proceso metu teikiamą informacinę sąlygą, papildant ją informacija apie duomenų tvarkymo tikslą ir nurodant duomenų gavėjus, jei kandidatas įdarbinamas, arba papildant šią informaciją netrukus po to, kai darbuotojas įdarbinamas.

Darbe naudojamų algoritmų kontrolė (algoritmų skaidrumas)

Toliau pateikti dirbtinio intelekto naudojimo darbo vietoje pavyzdžiai rodo, kad nekontroliuojamas dirbtinio intelekto įrankių naudojimas įmonėse gali padidinti darbo vietos nesaugumą ir taip neigiamai paveikti darbuotojų gyvenimą. Tuo pat metu, remiantis McKinsey pasaulinio instituto skaičiavimais, iki 2030 m. net 70 proc. įmonių bus įdiegusios vienokias ar kitokias dirbtinio intelekto sistemas. Štai kodėl taip svarbu kritiškai vertinti naujas technologijas ir leisti reguliavimo institucijoms bei nepriklausomoms organizacijoms atlikti dirbtinio intelekto auditą.

- Jungtinėje Karalystėje „Horizon“ programinė įranga, kurią naudojo Nacionalinis paštas, klaidingai įtarė atskirus darbuotojus pavogus iki keliasdešimt tūkstančių Didžiosios Britanijos svarų sterlingų. Dėl dirbtinio intelekto klaidos net 736 pašto darbuotojai buvo patraukti baudžiamojon atsakomybėn, o kai kuriems iš jų buvo pateikti kaltinimai ir jie buvo nuteisti.
- Nyderlanduose vienos taksi programėlės vairuotojai padavė įmonę į teismą po to, kai algoritmas užblokavo jų sąskaitas dėl tariamo sukčiavimo. Teismas atmetė jų ieškinius, nes nustatė, kad pažeidimai neatitiko visiškai automatizuoto sprendimų priėmimo apibrėžties pagal BDAR. Dėl to darbuotojai liko be jokios teisinės apsaugos.
- Italijoje teismas įpareigojo vieną iš maisto pristatymo įmonių atskleisti programėlės algoritmą ir pašalinti elementus, kurie dėl to, kad neatsižvelgia į darbo teisės reglamentuojamus klausimus (pvz., nedarbingumo atostogas ar teisę streikuoti), yra diskriminacinio pobūdžio.

Algoritmas ir įmonės slaptumas

Pagal ES teisę informacija apie technologijas ar bet kurį kitą įmonės aspektą gali būti saugoma kaip komercinė paslaptis. Tačiau ji turi atitikti šias sąlygas:

- informacija apie algoritmą nėra žinoma nei plačiajai visuomenei, nei šio sektoriaus ekspertams,
- algoritmo informacija turi komercinę vertę,
- informacija saugoma saugioje vietoje, o visi, kurie turi prieigą prie jos arba kuriems ji perduodama, yra pasirašę konfidencialumo susitarimą.

Darbo procesuose naudojamų naujų technologijų atveju šias sąlygas įvykdyti nėra sunku. Įmonės dažnai remiasi komercinėmis paslaptimis, pabrėždamos savo susirūpinimą dėl konkurencingumo praradimo, jei bus atskleistos jų vidaus sistemos. Todėl algoritmų įžvalga ir dirbtinio intelekto priemonių tikrinimas privačiajame sektoriuje yra ypač problemiški. Be to, papildomos teisinių apsaugos priemonių formos – konfidencialumo išlygos - neleidžia vidiniams asmenims (esamiems ar buvusiems darbuotojams) dalytis informacija apie jų darbą koordinuojančius mechanizmus.

Dirbtinio intelekto įstatymas (*DI įstatymas* – *AI Act*)

Pasikartojantys kaltinimai, kad dirbtinio intelekto algoritmai sukelia šališkumą, netikslumą ar diskriminaciją, paskatino Europos Komisiją imtis reguliavimo, kuriuo siekiama kontroliuoti dirbtinio intelekto priemones ir užkirsti kelią neigiamam jų naudojimo poveikiui.

2021 m. balandžio 12 d. EK pateikė ES reglamento dėl dirbtinio intelekto projektą - pirmąjį tokį išsamų teisės aktą dėl dirbtinio intelekto priemonių. Reglamento tikslas - sukurti tinkamą aplinką dirbtinio intelekto plėtrai Europos Sąjungoje, kartu atsižvelgiant į riziką, susijusią su naujausių technologijų kūrimu. Visų pirma AI aktu siekiama, kad ES diegiami algoritmai būtų saugūs, skaidrūs, etiški, nešališki ir kontroliuojami žmonių.

Rizika pagrįstas požiūris

Pagrindinė šio teisės akto esmė – nustatyti konkrečios dirbtinio intelekto sistemos keliamą riziką ir numatyti, kokios reguliavimo prievolės ir reikalavimai bus taikomi dirbtinio intelekto kūrėjams ir diegėjams.

- **Nepriimtina rizika** – dirbtinio intelekto uždraudimas

Draudimas taikyti ES vertybėms prieštaraujantį ypač žalingą dirbtinio intelekto (DI) taikymą, dėl kurio kyla pavojus, kad bus pažeistos pagrindinės asmens teisės, pavyzdžiui, atliekant piliečių vertinimą (vadinamąjį *socialinį vertinimą* – *social scoring*), pasinaudojant tam tikros žmonių grupės pažeidžiamumu dėl amžiaus, judėjimo sutrikimų ar psichikos sutrikimų, naudojant pasąmonės metodus, naudojant biometrinius identifikavimo duomenis viešosiose erdvėse ir teisėsaugos tikslais (su keliomis išimtimis).

- **Didelė rizika** – dirbtinis intelektas priimtinas, bet tam tikromis sąlygomis

Priemonės, darančios neigiamą poveikį žmonių saugumui ar pagrindinėms teisėms, t. y. toliau išvardytų sričių sistemos, buvo priskirtos didelės rizikos kategorijai:

  - biometrinis asmenų identifikavimas ir skirstymas į kategorijas,

- ypatingos svarbos infrastruktūros valdymas,
- profesinis švietimas ar mokymas – galimybė nuspręsti dėl asmens galimybės įgyti profesinį išsilavinimą ir mokymą (pvz., egzaminų vertinimas),
- gaminių sauga (pvz., dirbtinio intelekto panaudojimas robotais paremtoje chirurgijoje),
- įdarbinimo, darbuotojų valdymo ir galimybės dirbti savarankiškai (pvz., CV analizės) programinė įranga, skirta įdarbinimo procedūroms,
- pagrindinės privačios ir viešosios paslaugos (pvz., kreditingumo įvertinimas, kredito vertinimas – *scoring*),
- teisėsauga – kišimasis į pagrindines asmenų teises (pvz., dokumentų autentiškumo tikrinimas),
- migracijos, prieglobsčio ir sienų kontrolės valdymas (pvz., prieglobsčio prašymų vertinimas),
- teisingumo vykdymas ir demokratiniai procesai (pvz., siūlyti bausmės rūšį ir dydį asmeniui, nuteistam už nusikaltimą).

Konkrečių reikalavimų, taikomų didelės rizikos sistemoms, pavyzdžiai:

- **Skaidrumo reikalavimai** – didelės rizikos DI sistemų veikimas turėtų būti pakankamai skaidrus, kad naudotojai galėtų interpretuoti su jomis susijusius rezultatus. Didelės rizikos dirbtinio intelekto sistemoms turėtų būti parengtos naudojimo instrukcijos.
- **Privaloma didelės rizikos sistemų priežiūra** – būtina, kad žmonės galėtų veiksmingai prižiūrėti didelės rizikos dirbtinio intelekto sistemas, įskaitant konkrečios dirbtinio intelekto sistemos galimybių ir apribojimų supratimą. Tinkamos priežiūros priemonės gali būti sprendimas nenaudoti DI sistemos tam tikroje situacijoje, DI sistemos priimto sprendimo ignoravimas arba sistemos nutraukimas naudojant STOP mygtuką.

Dirbtinio intelekto įstatyme dėl dirbtinio intelekto keliami darbo klausimai

Didelės rizikos sistemos, darančios poveikį darbo rinkai ir kurioms taikoma speciali priežiūra, išvardytos *AI akto* projekto III priede. Tai yra DI sistemos:

1. naudojamos įdarbinant ar atrenkant konkrečius asmenis, ypač tos, kurios naudojamos laisvoms darbo vietoms skelbti, iš anksto atrinkti ar filtruoti paraiškas, vertinti kandidatus per pokalbius ar testus,
2. priimančios sprendimus dėl paaukštinimo ar atleidimo, nustatyti užduočių paskirstymą, stebėti darbuotojų veiklą ir elgesį,

3. priimančios sprendimą dėl galimybės dalyvauti profesiniame mokyme arba vertinti besimokančiuosius.

Minėtos dirbtinio intelekto sistemos gali turėti didelį poveikį asmenų, kurių duomenis jos tvarko, darbo perspektyvoms, taigi gali turėti įtakos jų pragyvenimo šaltiniui ir pajamoms. Europos Komisija taip pat nurodė, kad netinkamai sukurtos ir naudojamos sistemos gali įtvirtinti diskriminacinius modelius (pavyzdžiui, moterų, pagyvenusių žmonių, neįgaliųjų, rasinės, etninės ar kitokios seksualinės orientacijos asmenų atžvilgiu). Be to, dirbtinio intelekto sistemos, naudojamos produktyvumui tikrinti (ypač pagrįstos biometriniais duomenimis), gali daryti poveikį asmens duomenų apsaugai ir teisei į privatumą. Todėl joms turėtų būti taikomi ypač griežti reikalavimai, o darbuotojai visada turėtų turėti galimybę apskųsti algoritmų sprendimus.

Dirbtinio intelekto įstatymo kritika

Daug kritikos sulaukta ir dėl DI įstatymo taikymo užimtumo klausimams. Pasak ekspertų, reglamente per mažai dėmesio skiriama darbo klausimams, o algoritmų skaidrumo kontrolė susiaurinama iki bendrųjų skaidrumo reikalavimų, išvardytų reglamento projekto 52 straipsnyje. Be to, abejojama, ar reglamentas vis dėlto įsigalios iki 2025 m.

Baimė prarasti darbą dėl algoritmizavimo ir (arba) robotizavimo

„McKinsey“ skaičiavimais, iki 2030 m. dėl automatizavimo įvairiose pramonės šakose reikės perkvalifikuoti net 375 mln. darbuotojų. Šiek tiek kitokią prognozę, nors ir ne mažiau nerimą keliančią, savo ataskaitoje pateikė Pasaulio ekonomikos forumas, kuris leidinyje „*Darbo vietų ateitis*“ nurodė, kad dėl pažangos algoritmizavimo ir skaičiavimo technikos srityse artimiausiais metais visame pasaulyje mašinos gali pakeisti 75 mln. darbo vietų.

Kalbant apie robotizacijos poveikį, galima daryti prielaidą, kad labiausiai nukentės tie, kurie dirba fizinį darbą, ypač darbą, pagrįstą nuspėjamomis sekomis. Tačiau automatizavimas gali neigiamai paveikti ir kai kuriuos specialistus. Minėtoje „*Darbo vietų ateities*“ ataskaitoje teigiama, kad tarp dirbtinio intelekto išstumiamų profesijų, pavyzdžiui, mechaniko, sandėlininko ir gamybos vadovo, taip pat yra teisininkų ir finansų analitikų profesijos. Dar daugiau, automatizavimo poveikį pajus tie, kurių profesijos susijusios su duomenų rinkimu ir apdorojimu, t. y. užduotimis, kurias mašinos atlieka daug greičiau ir tiksliau.

Net 60 proc. darbuotojų žino, kad trečdalis jų dabartiniame darbe atliekamų užduočių yra automatizuotos. Todėl nenuostabu, kad dirbantieji nerimauja dėl savo darbo vietų. Pagal bendrovės „Procontent Communication“ ataskaitą „*Pandemija automatizuoja Lenkiją? “,* beveik kas penktas respondentas (18,7 %) baiminasi, kad jo darbas bus automatizuotas, o po to jis neteks darbo. Tačiau ekspertai nuogąstavimus švelnina - žvelgiant pasauliniu mastu, tikėtina, kad visiškai išnyks tik 5 proc. darbo vietų. Be to, nors daugelį darbo vietų užims mašinos, galima

tikėtis, kad vietoj jų atsiras naujų profesijų, nes padidės minkštųjų įgūdžių, kuriems reikia kūrybiškumo, emocinio intelekto ir kritinio mąstymo, paklausa.

Be to, technologijų plėtra prisidės prie nuolatinio naujų gerai apmokamų darbo vietų kūrimo IT sektoriuje - iki dešimtmečio pabaigos pasaulyje gali būti sukurta iki 50 mln. darbo vietų. Atrodo, kad tokį optimistinį požiūrį patvirtina ir minėtas Pasaulio ekonomikos forumo tyrimas, kuriame nurodoma, kad didėjant automatizacijai bus sukurta iki 133 mln. darbo vietų. Nors dėl skaitmeninimo sukeltų pokyčių dinamiškumo sunku tiksliai nustatyti būsimo užimtumo lygio formą, ekspertų vertinimu, abejotina, kad artimiausiu metu atsiras technologinis struktūrinis nedarbas.

Technologijos įtraukties labui

Darbo vietų skaitmeninimas padeda veiksmingiau integruoti į darbo rinką tas socialines grupes, kurios anksčiau buvo laikinai ar visam laikui iš jos išstumtos.

Neįgalieji gali naudotis šiais privalumais:

- nėra sunkumų nuvykti į darbo vietą, su kuriais anksčiau susidurdavo tam tikrų fizinių apribojimų turintys asmenys,
- mažesnis dirgiklių poveikis ir ramesnis nuotolinio darbo režimas padeda efektyviau dirbti žmonėms, turintiems intelekto sutrikimų, hiperaktyvumo, koncentracijos ir mokymosi sunkumų,
- naudojant elektronines telekomunikacijų priemones (elektroninį paštą, greitąsias žinutes), kalbos sutrikimų turintys asmenys gali aktyviai dalyvauti diskusijose.

Naudos **tėvams** pavyzdžiai:

- galimybė daugiau laiko praleisti su vaikais,
- mažesnė rizika visai šeimai užsikrėsti populiariomis infekcinėmis ligomis (gripu, peršalimo ligomis, COVID-19),
- galimybė jauniems tėvams veiksmingai derinti asmeninį ir profesinį gyvenimą.

Nuotolinis darbas taip pat daro didelį poveikį jaunų motinų pasilikimui darbo rinkoje (net 49 proc. dirbančių motinų prisipažįsta pažįstančios bent vieną asmenį, kuris išėjo iš darbo arba ketina tai padaryti dėl reikalavimo grįžti į biurą).

Taksi programėlių naudojimo privalumų pavyzdžiai:

- lyčių lygybės siekimas (daugumoje Amerikos miestų moterys iki šiol sudarė mažiau nei 5 proc. taksi vairuotojų, o dalijimosi ekonomikos programų atveju šis skaičius jau yra apie 20-30%),
- lengvesnis imigrantų (pvz., iš Ukrainos) patekimas į darbo rinką,
- pigesnių važiavimo kainų siūlymas – pavyzdžiui, „Uber“ programėlė Los Andžele veikia 21 mažas pajamas gaunančiame rajone, kur galima važiuoti gerokai pigiau nei tradicinėse taksi bendrovėse.

1.6 Naujųjų technologijų poveikis sutartiniams santykiams – diskusija apie išmaniąsias sutartis ir jų būsimą taikymą darbuotojo ir darbdavio santykiuose

Skaitmeninimas jau išplito beveik visose mūsų kasdienio ir asmeninio gyvenimo srityse. Tai pasakytina ir apie sutartinius santykius, anksčiau sudarytus žodžiu ar raštu, kurie dabar dažnai sustiprinami ar papildomi naudojant skaitmenines priemones. Atsižvelgiant į didžiulį informacijos kiekį internete ir vis dažniau sudaromus tarpusavio įsipareigojimus su skaitmeniniais elementais, artimiausioje ateityje didžiausią poveikį sutartiniams santykiams neabejotinai turės blokų grandine pagrįstos priemonės, pavyzdžiui, išmaniosios sutartys (*smart contracts*).

Kas yra blokų grandinė?

Blokų grandinė (angl. *blockchain*) – tai technologija, skirta informacijai apie internetu sudarytus sandorius perduoti ir saugoti. Atskira informacija išdėstoma nuosekliais duomenų blokais. Kai blokas užpildomas tam tikru sandorių skaičiumi, tolesnė sandorių informacija saugoma kitame bloke. Dėl nuorodos į ankstesnį bloką ir juose esančios informacijos grandininio sujungimo tampa neįmanoma pakeisti ar ištrinti vieno sandorio įrašą, kad toks pakeitimas nebūtų užfiksuotas visuose kituose blokuose. Šis sprendimas skatina atliktų operacijų skaidrumą ir užkerta kelią nesąžiningam manipuliavimui informacija.

Kas yra išmaniosios sutartys?

Išmanioji sutartis yra „savaime besivykdanti” programa, pagrįsta logika *„jei-tai*”. Ji parašyta tik programavimo kalba ir gali būti vykdoma naudojant paskirstytosios knygos technologiją (*DLT*) arba blokų grandinę. Pastaruoju atveju programa saugoma blokų grandinėje ir paleidžiama, kai tam tikros sąlygos sukelia kitą veiksmą - pavyzdžiui, ji gali sukelti mokėjimą arba suteikti tam tikrą

paslaugą. Taigi, tai yra **tam tikros sutarties sukurtos realybės sujungimas su realiuoju pasauliu pasitelkiant technologijas.** Dėl to sutartis tampa skaidresnė ir patikimesnė, o šalims suteikia pasitikėjimo dėl jos sąlygų vykdymo, kai susiklosto tam tikra situacija.

Išmaniųjų sutarčių naudojimo pavyzdžiai

- Nekilnojamojo turto įsigijimas – dėl išmaniųjų sutarčių šis procesas, kuris paprastai yra labai sudėtingas ir reikalauja daugelio tarpininkų (notaro, nekilnojamojo turto agento, teisininko patarėjo, kredito įstaigos) dalyvavimo, yra labai supaprastintas ir nereikalauja minėtų dalyvių dalyvavimo, todėl nuosavybės teisę galima įgyti elektroniniu būdu.
- Pirkimas internetu – šiuo atveju išmaniosios sutartys užtikrina, kad mokėjimas būtų atliktas nedelsiant, todėl produktas pirkėjui išsiunčiamas greičiau.
- Asmens duomenų tvarkymas – kadangi asmens duomenys ir skaitmeniniai ID saugomi blokų grandinėje, tapatybės vagystės rizika gerokai sumažėja.
- Rinkimų ar referendumų rezultatų registravimas – balsavimo rezultatų klastojimo rizikos mažinimas. Išmaniųjų sutarčių naudojimą šiam tikslui, be kita ko, galima pastebėti Estijoje.
- Draudimo išmokų ir įmokų mokėjimas – automatinis žalos atlyginimas, įmokų apskaičiavimas.

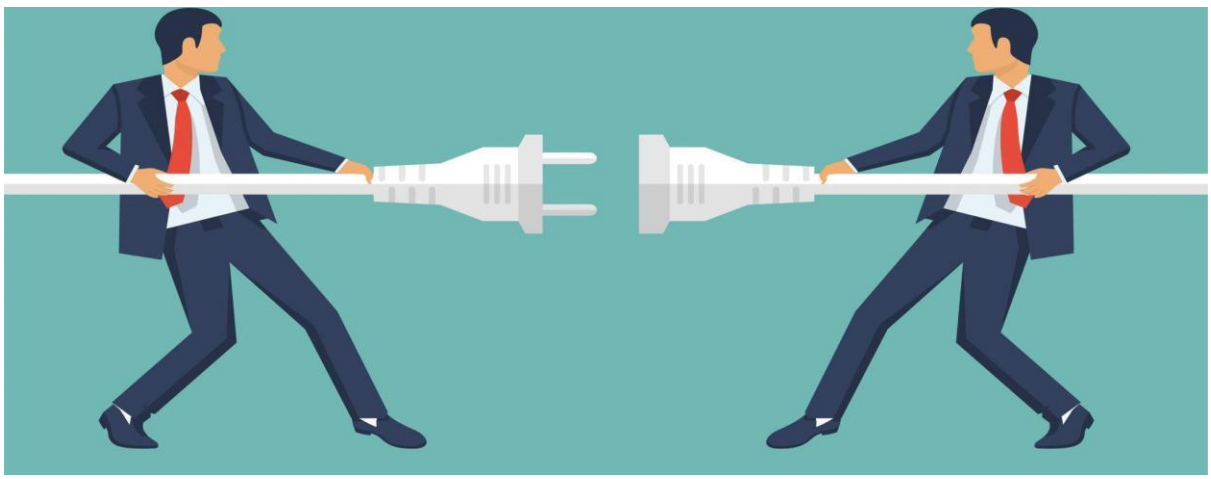
2. Skaitmeninimo poveikis darbuotojų asmeniniam gyvenimui

2.1. Darbuotojų darbo laiko apsauga dirbant nuotoliniu būdu. Nuotolinis darbas ir darbo bei asmeninio gyvenimo pusiausvyra

„Eurofound“ atlikto tyrimo duomenimis, trečdalis darbuotojų Europos Sąjungoje pandemijos metu pradėjo dirbti iš namų, o dėl perėjimo prie nuotolinio darbo net 27 proc. respondentų teigė, kad darbo pareigas atlieka laisvu laiku. Lokdauno metu riba tarp asmeninio ir profesinio gyvenimo ėmė nykti. Darbuotojai įgijo galimybę patys organizuoti savo laiką, tačiau taip pat susidūrė su rizika, kad bus nuolat pasiekiami ir negalės visiškai atsijungti nuo elektroninės žiniasklaidos ne darbo metu.

Svarbu tai, kad dirbant užduotimis grindžiamu režimu (nesiremiančiame griežtomis darbo valandomis) galioja tos pačios taisyklės kaip ir tradicinėje sistemoje, t. y. darbuotojas turėtų dirbti 8 valandas per dieną per penkių dienų darbo savaitę. Užduotys, atliekamos už šios sistemos ribų, turėtų būti laikomos viršvalandžiais. Tačiau nors lankstus darbo grafikas neabejotinai naudingas darbuotojams, jie dažnai klaidingai mano, kad kadangi nebūna biure nustatytomis valandomis, tai turėtų parodyti, kad yra pasiekiami bet kuriuo paros metu.

2.1.1. Teisė atsijungti



Šaltinis: Shutterstock.

Kaip numatyta Visuotinės žmogaus teisių deklaracijos 24 straipsnyje, kiekvienas žmogus turi teisę į poilsį ir laisvalaikį, įskaitant protingą darbo laiko apribojimą ir periodines mokamas atostogas. Be to, pagal Pagrindinių teisių chartijos 31 straipsnį kiekvienas darbuotojas turi teisę į sveikatą, saugą ir orumą gerbiančias darbo sąlygas ir teisę į kasdienio bei kassavaitinio poilsio laikotarpius, kasmetines mokamas atostogas ir, svarbiausia, į maksimalaus darbo laiko apribojimą.

Naujoji popandeminė tikrovė, kurioje riba tarp asmeninio ir profesinio gyvenimo dažnai būna neryški, parodė, kad reikia įgyvendinti reglamentą, kuris užtikrintų darbuotojams galimybę atsijungti nuo darbo ir neatsakinėti į savo vadovų el. laiškus po darbo valandų be neigiamų pasekmių. Dėl šios priežasties 2021 m. Europos Parlamentas priėmė rezoliuciją, kurioje pasisakė už teisę atsijungti, taip ragindamas Europos Komisiją apsvarstyti galimybę parengti direktyvos dėl teisės būti neprisijungus projektą.

Verta pažymėti, kad Europos Parlamento rezoliucijos neturi privalomosios galios. Todėl Europos Komisija neprivalo imtis veiksmų dėl Parlamento pasiūlytos direktyvos įgyvendinimo. Tačiau, atsižvelgiant į klausimo esmę, galima tikėtis, kad Komisija sieks reglamentuoti teisę atsijungti nuo darbo ir užtikrinti vienodą darbuotojų apsaugos lygį visoje Europos Sąjungoje.

Europos Parlamento pasiūlyta direktyva dėl teisės būti neprisijungus prie interneto siekiama užtikrinti:

1) būtiniausias taisykles, užtikrinančias darbuotojams, kurie kasdieniame darbe naudojasi nuotolinio ryšio priemonėmis, teisę būti neprisijungusiems prie interneto,
2) draudimą diskriminuoti atsijungimo teise besinaudojančius darbuotojus ar taikyti jiems mažiau palankias sąlygas (įskaitant darbo sutarčių nutraukimą),
3) vienodą požiūrį į visus darbuotojus - tiek viešojo, tiek privataus sektoriaus, tiek į žemesnio lygio darbuotojus ar vadovus (nors pastaruoju atveju tai gali būti sudėtinga dėl vadovams taikomų specialių nuostatų),
4) veiksmingą teisminę procedūrą ir galimybę kreiptis į teismą dėl suteiktų teisių pažeidimų (galimybę pasinaudoti teismine apsauga nuo neigiamų pasekmių).

Darbdavių pareigos, susijusios su darbuotojų teise būti neprisijungusiems prie interneto

Naujos darbuotojų teisės taip pat reiškia papildomas darbdavių pareigas. Tarp jų - būtinybė sukurti vidinę sistemą, kuri leistų tiksliai įvertinti darbuotojo kiekvieną dieną dirbtą laiką (laikantis teisės į privatumą ir asmens duomenų apsaugą). Be to, taip pat svarbu padėti darbuotojams būti neprisijungusiems prie interneto – aiškiai informuoti apie naująjį įstatymą įmonės politikoje, rengti mokymus ir informacines kampanijas šioje srityje. Vis dėlto, kalbant apie informuotumo

didinimą, tinkamiausia ir perspektyviausia atrodo pareiga raštu informuoti kiekvieną darbuotoją apie jo teises.

Be to, darbdaviai neturėtų skatinti nuolatinio pasiekiamumo kultūros apdovanodami darbuotojus, kurie nesinaudoja savo teise atsijungti. Sveikatos ir saugos vertinimas, susijęs su teise atsijungti (pvz., psichosocialinės rizikos požiūriu), taip pat turėtų būti svarbus aspektas.

2.1.2. Darbo ir asmeninio gyvenimo pusiausvyra – valstybės vaidmuo

Šaltinis: Technologijų antraštės.

Valstybė ir jos darbo politika atlieka svarbų vaidmenį formuojant darbuotojo ir darbdavio santykius. Kalbant apie darbo ir asmeninio gyvenimo pusiausvyrą, kai kurios šalys imasi iniciatyvų, skatinančių gerąją įdarbinimo praktiką. Viena vertus, tai susiję su nacionalinių teisės aktų įgyvendinimu, kita vertus, su priemonėmis, kurios neturi teisiškai privalomos galios, tačiau jomis siekiama formuoti tam tikrą elgesį.

Tokios „švelnios“ priemonės galėtų būti, pavyzdžiui, geros elgsenos kodeksų įgyvendinimas arba gero pavyzdžio kitiems darbdaviams rodymas skatinant darbuotojams palankų požiūrį valdžios struktūrose. Tokį kelią pasirinko Malta, kuri 2020 m. paskelbė *Priemonių, kuriomis siekiama darbo ir asmeninio gyvenimo pusiausvyros, vadovą*. Šiame leidinyje surinktos ir išsamiai aprašytos darbuotojų teisės, pateikti nurodymai, kaip tinkamai dirbti skaitmeninimo laikais (pavyzdžiui, kaip organizuoti savo darbą atliekant pareigas nuotoliniu būdu). Tačiau vadovo

naudingumas pasireiškia ne tik geresniu darbuotojų privilegijų išmanymu ar papildomomis žiniomis skaitmeninimo srityje. Tokie gerosios praktikos kodeksai, taikomi darbo vietoje (arba tam tikrame sektoriuje), taip pat gali būti savotišku derybų su darbdaviu koziriu.

Maltos vadovo atveju projekto iniciatoriai nurodė, kad svarbiausias jų tikslas buvo užtikrinti viešajame sektoriuje dirbančių asmenų profesinio ir asmeninio gyvenimo pusiausvyrą didinant darbuotojų informuotumą. Vis dėlto verta pažymėti, kad žinyne niekaip neišplečiamas darbuotojų teisių katalogas, o tik atkreipiamas dėmesys į tinkamą įdarbinimo praktiką ir darbuotojai supažindinami su galimybe derėtis dėl darbo sąlygų, atitinkančių dokumento nuostatas.

Teisės į atsijungimą propagavimo pavyzdžiai ES šalyse

Nors šiuo metu dar nėra visos Europos teisinės sistemos, reglamentuojančios teisę atsijungti, ES jau yra keletas teisėkūros veiksmų pavyzdžių. Kartu teisė atsijungti skatinama kolektyvinėmis darbo sutartimis. Be to, kai kurios valstybės narės jau įgyvendino savo teisės aktus dėl teisės atsijungti.

Prancūzija

Prancūzija laikoma teisės atsijungti pradininke. Dar 2013 m. ten buvo priimtas tarpsektorinis susitarimas dėl gyvenimo kokybės darbe. Susitarime įmonės skatinamos nesikišti į darbuotojų asmeninį gyvenimą ir apibrėžiamas laikas, kada darbuotojų kontaktiniai įrenginiai turi būti išjungti. Vėliau, 2016 m. rugpjūčio 8 d., šios nuostatos buvo priimtos ir įtrauktos į Prancūzijos darbo kodeksą. Be to, nuo 2017 m. sausio Prancūzijoje teisiškai reikalaujama, kad darbdaviai derėtųsi su profesinėmis sąjungomis dėl susitarimų, susijusių su teise atsijungti.

Italija

Po Prancūzijos sekė Italija, kuri 2017 m. nusprendė įvesti teisę atsijungti. Reglamente daugiausia dėmesio skiriama nuotolinį darbą dirbantiems žmonėms (*išmanusis darbas,* itališkai - *lavoro agile*) ir jame nustatyta, kad nuotoliniai darbuotojai turi teisę atsijungti nuo technologinių prietaisų ir interneto platformų be jokių pasekmių iš savo darbdavių. Italijoje taip pat galioja sektorių ir įmonių kolektyvinės sutartys, kuriose numatyta teisė atsijungti.

Ispanija

Dar viena šalis, kuri į nacionalinius teisės aktus įtraukė teisę atsijungti, buvo Ispanija. 2018 m. į Ispanijos nacionalinę teisę perkėlus BDAR, įvestas naujas skaitmeninių teisių paketas. Juo tiek privačiajame, tiek viešajame sektoriuje dirbantiems darbuotojams buvo suteikta teisė atsijungti, siekiant išlaikyti darbo ir asmeninio gyvenimo pusiausvyrą. Pagal reglamentą darbdaviai, išklausę

darbuotojų atstovų nuomonę, turėtų nustatyti vidaus politiką, kaip darbuotojai gali pasinaudoti teise atsijungti, ir rengti darbuotojams mokymus apie tinkamą naujų technologijų naudojimą.

Belgija

2018 m. Belgijoje visi darbdaviai, turintys daugiau kaip 50 darbuotojų, privalėjo su sveikatos ir saugos komitetu aptarti saugų skaitmeninių priemonių naudojimą ir darbuotojų teisę atsijungti. Verta pažymėti, kad įvedus teisę atsijungti, patys darbuotojai neįgijo naujų teisių, o tik daugiau galimybių derėtis su darbdaviu. Tačiau 2022 m. buvo priimtas naujas reglamentas, pagal kurį valstybės tarnautojai gali išjungti darbinį el. paštą ir neatsakinėti į trumpąsias žinutes bei telefono skambučius ne darbo metu, nebijodami represijų. Taip pat svarstomi planai naująjį reglamentavimą taikyti ir privačiojo sektoriaus darbuotojams.

Airija

2021 m. balandį Airijos vyriausybė paskelbė elgesio kodeksą, pagal kurį visi darbuotojai turi teisę po darbo valandų atsijungti ir iš karto neatsakyti į darbdavio elektroninius laiškus, telefono skambučius ar kitus pranešimus. Kodekse taip pat nustatyta, kad darbuotojas paprastai neturėtų būti verčiamas dirbti ne standartinėmis darbo valandomis ir neturėtų patirti pasekmių už atsisakymą spręsti darbo reikalus po darbo valandų.

2.1.3 Darbdavio reikalavimas būti nuolat pasiekiamam ir mobingas

Šaltinis: jobs.ca.

Mobingas – tai veiksmai ar elgesys su darbuotoju, pasireiškiantis nuolatiniu ir ilgalaikiu priekabiavimu ar bauginimu. Taip yra tada, kai tokiais veiksmais siekiama pažeminti ar išjuokti darbuotoją, taip pat kai jais siekiama, kad darbuotojas turėtų prastą nuomonę apie savo profesinį tinkamumą.

Kadangi mobingas gali pasireikšti įvairiomis agresijos formomis, elgesio, kuris laikomas šios rūšies smurtu, sąrašas lieka atviras. Todėl reikalavimas, kad darbuotojas, visą laiką būtų pasiekiamas, nes kitaip jam grėstų neigiamos pasekmės, gali būti laikomas mobingo rūšimi. Tai rodo, pavyzdžiui, sprendimai, kuriais teismai gynė darbuotojus, nurodžiusius, kad varginantis ir įkyrus žinučių su darbo nurodymais gavimas po darbo valandų arba poilsio dienomis turėtų būti traktuojamas kaip mobingas.

Liublino apygardos teismo 2018 m. birželio 20 d. sprendimas. (VIII Pa 86/18)

Teismas priteisė iš darbdavio 25 000 zlotų kompensacijos savivaldybės įstaigos darbuotojai už jos sveikatos sutrikdymą, kurį sukėlė įkyrus elektroninių laiškų siuntimas po darbo valandų. Byla buvo susijusi su moterimi, dirbančia nuolatine valstybės tarnautoja visą darbo dieną. Pasikeitus savivaldybės merui, naujasis vadovas kaip pagrindinį bendravimo su darbuotojais būdą patvirtino nurodymų siuntimą elektroniniais laiškais jų darbo ir asmeniniais adresais. Nuo 2015 m. sausio 1 d. ieškovė iš mero gavo apie 200 elektroninių laiškų, iš kurių daugiau nei 100 buvo išsiųsti po darbo valandų, įskaitant naktį ir švenčių dienas, atostogas ar nedarbingumo laikotarpį. Bylos nagrinėjimas baigėsi Liublino apygardos teismo sprendimu, kuriame teismas nusprendė, kad darbuotojo įpareigojimas eiti pareigas ir elektroninių laiškų su darbo užduotimis siuntimas ne darbo dienomis, nedarbingumo atostogų ir švenčių dienomis bei netinkamas atsiskaitymas už jų vykdymą gali būti laikomas **mobingu.**

Teisės nutraukti darbo santykius pažeidimas – pasekmės darbdaviui ir skundų nagrinėjimo mechanizmai

Baudos už teisės atsijungti pažeidimus ES šalyse gali skirtis. Taip yra dėl to, kad kiekviena valstybė narė turėtų individualiai nustatyti sankcijų, taikomų darbdaviui už tai, kad jis nesilaiko savo darbuotojų laisvo laiko, dydį.

Lenkijoje atskira darbuotojo teisė atsijungti dar neįvesta, tačiau ją galima numanyti iš bendrųjų darbo laiko nuostatų ir teismų praktikos. Todėl visuotinai pripažįstama, kad darbuotojas neprivalo atsiliepti į telefono skambučius ar atsakyti į elektroninius laiškus po darbo valandų ar atostogų metu. Išimtis yra tada, kai darbuotojas privalo budėti, t. y. būti pasirengęs darbui ne standartinėmis valandomis.

Dažniausiai pasitaikantys darbdavių nusižengimai darbo santykių srityje yra susiję su darbo sutarčių nutraukimu, darbo laiko taisyklių pažeidimais, netinkamu darbo užmokesčio mokėjimu ir netinkamu atostogų suteikimu. Priklausomai nuo nusižengimo masto ir rūšies, darbdaviui gali būti skiriama bauda nuo 1 000 PLN iki 30 000 PLN.

Todėl galima tikėtis, kad Lenkijoje už teisės atsijungti nesilaikymą bus taikomos sankcijos kaip ir už bet kurį kitą darbo laiko taisyklių pažeidimą, t. y. darbdaviui grės iki 30 000 zlotų bauda. Be to, jei su darbuotoju elgiamasi blogiau dėl jo ribotų galimybių dirbti ne jam nustatytu darbo laiku, gali kilti problemų dėl kompensacijos už diskriminaciją (ne mažesnės nei taikomas minimalus darbo užmokestis).

Remiantis nuomonių apklausos[6] duomenimis, 23,9 proc. darbuotojų Lenkijoje gauna elektroninių laiškų, trumpųjų žinučių ar kitų pranešimų iš vadovų po darbo valandų. Nors, kaip pažymi ekspertai, tai nėra draudžiama, tokie veiksmai gali būti vertinami kaip nurodymas dirbti viršvalandžius (ypač kai kontaktas verčia darbuotoją atlikti tam tikrą užduotį). Jei būtina atsakyti į elektroninį laišką ar telefono skambutį darbo reikalais, pagal Darbo kodekso 151 straipsnio 1 ir 2 dalis už tokį veiksmą turi būti kompensuojama papildomu darbo užmokesčiu arba laisvu laiku.

Ką turėtų daryti Lenkijos darbuotojas, kurio teisės pažeidžiamos?

a) Pasikalbėti su darbdaviu

Prieš nusprendžiant pranešti apie pažeidimą išorės institucijoms, darbuotojui patartina pabandyti susisiekti su darbdaviu. Svarbu, kad pokalbyje dalyvautų įmonės direktorius arba savininkas, nes gali būti, kad vadovai nežino apie žemesnio lygmens viršininkų padarytus pažeidimus.

b) Ieškoti profesinių sąjungų paramos

Jei pokalbis su darbdaviu nepadeda, darbuotojas gali kreiptis pagalbos į profesinę sąjungą, jei tokia yra darbovietėje. Profesinė sąjunga yra tam, kad atstovautų darbuotojams, ir turėtų dar kartą pabandyti susitarti su įmonės direktoriumi (savininku) arba jos valdyba.

[6] UCE RESEARCH ir ePsycholodzy.co.uk atlikta apklausa, https://uce-pl.com/news/blisko-24-proc-polakow-twierdzi-ze-pracodawca-kontaktuje-sie-z-nimi-w-czasie-wolnym-od-pracy.

c) Pranešti apie pažeidimus Valstybinei darbo inspekcijai (VDI, *lenk. PIP*)

Valstybinė darbo inspekcija (VDI) yra svarbiausia institucija, sprendžianti darbo sąlygų ir darbuotojų teisių klausimus Lenkijoje. Būtent jai pirmiausia turėtų būti teikiami oficialūs pranešimai apie darbo teisių pažeidimus. Susisiekti su VDI galima adresu: *www.pip.gov.pl*, o skundą galima pateikti raštu, telegrafu, faksu, elektroniniu paštu, el. skundo forma arba žodžiu į protokolą. Skundą pateikusio darbuotojo duomenys gali likti anonimiški. Pagal Valstybinės darbo inspekcijos įstatymą[7] , darbo inspektorius privalo neatskleisti, kad patikrinimas atliekamas dėl skundo, išskyrus atvejus, kai skundo pateikėjas su tuo sutinka raštu. Tačiau svarbu nepamiršti tinkamai pagrįsti pateiktus kaltinimus ir pateikti patikimų įrodymų, nes VDI spręs, ar pranešimas yra patikimas ir ar jis bus tikrinamas.

d) Iškelti bylą apygardos teisme

VDI pateikta medžiaga taip pat gali tapti įrodymu, jei byla nagrinėjama apylinkės teisme. Tačiau kreipimasis į teismą yra kraštutinė priemonė, naudojama tik tada, kai ankstesni būdai nepadeda.

[7] *2007 m. balandžio 13 d. Valstybinės darbo inspekcijos įstatymo* 44 straipsnio 3 dalis (OL 2017, p. 786 su pakeitimais).

2.1.4. Work-life balance – kas yra darbo ir asmeninio gyvenimo pusiausvyra?

Šaltinis: zapier.com.

EBPO ataskaitoje „Kaip sekasi gyventi? Gerovės vertinimas“ *darbo ir asmeninio gyvenimo pusiausvyros* sąvoka reiškia darbo (tiek apmokamo, tiek neapmokamo), šeimyninio gyvenimo ir laisvalaikio pusiausvyros išlaikymą. Ji reiškia darbuotojo gebėjimą organizuoti savo pareigas taip, kad jos netrukdytų jo laisvalaikiui. Tačiau tinkama pusiausvyra tarp skirtingų gyvenimo sričių priklauso ne tik nuo darbuotojo, bet ir nuo darbdavio. Būtent darbdavys paprastai kuria darbo kultūrą įmonėje ir nustato tam tikras normas.

Labai svarbu atsižvelgti į darbuotojų laisvalaikį, nesvarbu, ar jie dirba stacionariai, nuotoliniu būdu, ar mišriai. Juk kiekvieno darbuotojo gerovė (savijauta; psichinė būsena) priklauso nuo geros darbo ir asmeninio gyvenimo pusiausvyros. Tyrimų duomenimis, pareigų perteklius ir nuolatinis darbas (įskaitant namų ruošos ir priežiūros darbus) gali lemti išsekimą ir sveikatos sutrikimus, lėtinį stresą ir sumažėjusį produktyvumą.

Prieš pandemiją visą darbo dieną dirbančių asmenų laisvalaikiui ir rūpinimuisi savo gerove skirtas laikas svyravo nuo 14 iki 16,5 valandos per dieną. Visą darbo dieną dirbantys vyrai laisvalaikiui skyrė 30 minučių mažiau laiko nei moterys. Tačiau statistika atrodo kitaip, kai dirbama nuotoliniu būdu, kuris plačiai paplito dėl COVID-19 pandemijos sukelto lokdauno metu. Tuomet prie kompiuterio praleidžiamas laikas gerokai pailgėjo (iki dviejų papildomų valandų per dieną), o poilsio kokybė suprastėjo. Darbuotojai, atliekantys savo pareigas iš namų, dažniau sutinka

dirbti viršvalandžius ir atlikti užduotis vakarais ar savaitgaliais, taip nutrindami ribą tarp asmeninio ir profesinio gyvenimo.

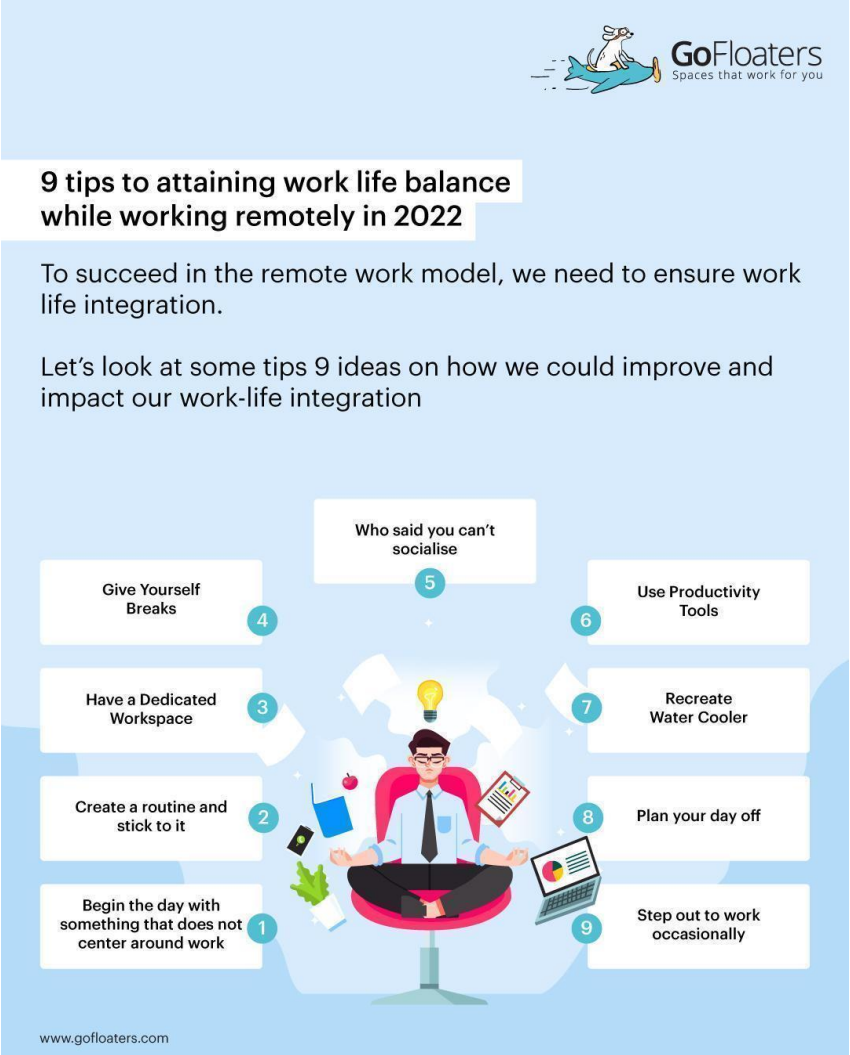
Tačiau labai svarbu išlaikyti šią pusiausvyrą. Ji padeda išvengti profesinio perdegimo, skatina didesnę darbuotojų motyvaciją ir atsidavimą įmonei. Ji taip pat prisideda prie saviugdos ir didesnio atvirumo naujiems iššūkiams. Taigi, nepaisant mažesnio darbo valandų skaičiaus, didėja darbuotojų produktyvumas, mažėja medicininės priežiūros ir nedarbingumo atostogų poreikis.

Kaip darbdaviai gali pagerinti darbuotojų *darbo ir asmeninio gyvenimo pusiausvyrą?*

Darbuotojų darbo ir asmeninio gyvenimo pusiausvyra neretai priklauso nuo darbdavių ir vadovų. Būtent jie skatina tam tikrą elgesį ir formuoja darbovietės politiką. Todėl svarbu, kad jie remtų gerus įpročius, leidžiančius darbuotojams pailsėti nuo kasdienių darbo pareigų. Pavyzdžiui, darbdaviai gali skatinti darbuotojus daryti pertraukas darbe, dirbti lanksčiu, jiems patogiu grafiku, naudotis teise atsijungti, aiškiai informuoti apie savo poreikius (pavyzdžiui, pranešti, kad yra perkrauti pareigomis ir jiems reikia sulėtinti tempą).

Taip pat svarbu skatinti sveiką darbo kultūrą, vengiant nuolatinio buvimo pasiekiamu arba įvedant neatsakinėjimo į el. laiškus ir žinutes politiką. po darbo valandų. Taip pat pravartu surengti darbuotojams mokymus apie *darbo ir asmeninio gyvenimo pusiausvyrą* bei teisę atsijungti ir pateikti patarimų, kaip lengvai gali sumažinti perteklinį skaitmeninių priemonių naudojimą.

2.1.5. Skaitmeninė sveikata ir sauga, arba kaip pačiam sumažinti nuolatinį prisijungimą.



Patarimai darbuotojui

1. **Išjunkite pranešimus telefone**

Jei jūsų asmeniniame telefone yra greitųjų žinučių ir programų, naudojamų darbe arba jūsų darbinė el. pašto dėžutė susieta su privačia, išjunkite visus pranešimus, kurie gali trukdyti jums laisvalaikiu. Taip pat gali būti gera idėja nustatyti laiko ribas, kad po standartinių darbo valandų būtų išjungti bet kokie pranešimai.

2. **Darbo metu naudokitės įmonės kompiuteriu, o po darbo valandų – asmeniniu.**

Pasirinkti įmonės kompiuterį darbui, o ne asmeninį įrenginį yra geriau ne tik dėl kibernetinio saugumo problemų, bet ir dėl galimybės atsiriboti nuo gaunamų pranešimų ir kolegų žinučių po

darbo valandų. Jei jūsų įmonėje galioja BYOD (*atsinešk savo prietaisą, angl. bring your own device*) politika, savo prietaise galite susikurti dvi paskyras (profesinę ir privačią) ir perjunginėti jas priklausomai nuo paros laiko ir poreikių.

3. Analoginiai rytai ir vakarai

Telefono ar nešiojamojo kompiuterio skleidžiama spinduliuotė yra panaši į saulės šviesą, todėl mažina melatonino išsiskyrimą smegenyse. Tai savo ruožtu apsunkina užmigimą, blogina poilsio kokybę ir sukelia papildomų miego problemų. Dėl geros savijautos stenkitės nesinaudoti telefonu ir nešiojamuoju kompiuteriu bent valandą prieš miegą. Taip pat nepradėkite ryto nervingai tikrindami elektroninio pašto dėžutę ar socialinę žiniasklaidą.

4. Nusistatykite laiką, per kurį naudojatės skaitmeninėmis priemonėmis

Net jei dirbate lanksčiu grafiku, informuokite savo vadovus ir žmones, su kuriais dirbate, apie tai, kokiu laiku su jumis galima susisiekti ir kada jūsų pasiekiamumas bus ribotas.

5. Įveskite visos dienos detoksikaciją

Nors skaitmeninė detoksikacija nėra pagrindinis *darbo ir asmeninio gyvenimo pusiausvyros* idėjos principas, visiškas atsijungimas nuo interneto ir socialinės žiniasklaidos ilgesnį laiką gali būti labai naudingas žmogaus savijautai. Atsijungę nuo elektronikos geriau suvokiame, kiek laiko iš tikrųjų praleidžiame internete. Tai padeda nustatyti sveikas darbo ir asmeninio gyvenimo ribas. Tai taip pat motyvuoja mus atsikratyti blogų įpročių, pavyzdžiui, įkyriai tikrinti elektroninio pašto dėžutę arba vos pabudus griebtis telefono. Todėl rekomenduojama taikyti ciklinę detoksikaciją (pvz., visiškai atsijungti savaitgaliais) ir laisvalaikį leisti ne naršant socialinę žiniasklaidą, o ilsintis, susitinkant su šeima ir draugais arba užsiimant fizine veikla.

2.2. Priverstinis ir savanoriškas privačių išteklių komercializavimas

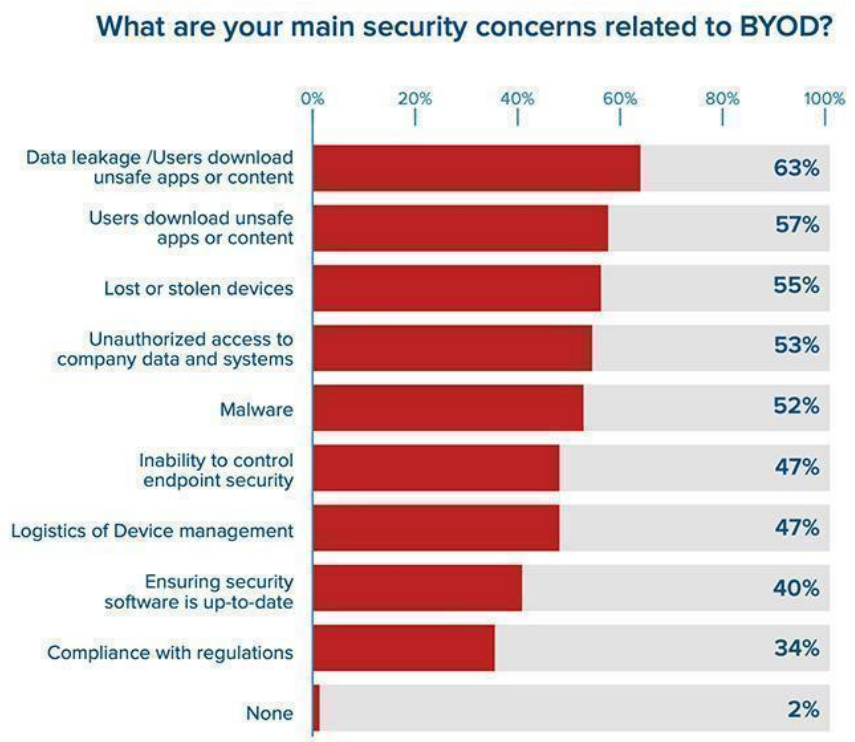
2.2.1. Kas yra BYOD (angl. bring your own device) politika?

Frazė "*atsineškite savo įrenginį*" taip pat žinoma akronimu BYOD. Tai tendencija naudoti darbe asmeninius įrenginius, pavyzdžiui, nešiojamuosius kompiuterius, išmaniuosius telefonus ar planšetinius kompiuterius. Ši tendencija dažnai palaikoma pačių darbuotojų valia (savanoriškas privačių išteklių komercializavimas). Tačiau kartais BYOD politikai pirmenybę teikia ir darbdaviai (priverstinis privačių išteklių komercializavimas). Nors ši tendencija turi daug privalumų, prieš ją diegiant įmonėje reikėtų apsvarstyti galimą riziką, pavyzdžiui, saugumo ir privatumo klausimus.

Verta paminėti, kad BYOD yra visiška priešingybė tradiciniam darbo stiliui, vadinamam HYOD (angl. *here's your own device)*, kai įmonės savo darbuotojams išduoda bet kokius darbui reikalingus elektroninius prietaisus.

BYOD politikos privalumai:

- **Lankstumas** – BYOD apima darbdavio sutikimą naudotis įmonės dokumentais darbuotojo privačiuose įrenginiuose. Taip profesines pareigas galima atlikti bet kur ir bet kada. Be to, didesnis lankstumas pasireiškia galimybe išbandyti naujus sprendimus, programinę įrangą, skaitmeninius įrankius, nes darbuotojai neapsiriboja vieno tipo ar modelio prietaisų naudojimu.
- **Patogumas** – vienas iš BYOD politikos privalumų yra tas, kad darbuotojai gali naudotis jiems gerai pažįstamais ir patogiais įrenginiais.
- **Didesnis produktyvumas** – naudojimasis nuosavu nešiojamuoju kompiuteriu ar išmaniuoju telefonu gali palengvinti naujų darbuotojų įvedimo į darbą procesą, taip pat padidinti nuolatinių darbuotojų produktyvumą.
- **Mažesnės išlaidos (darbdavio nauda)** – sutikdami su BYOD politika, darbdaviai dažnai atsisako savo pareigos aprūpinti darbuotoją darbo įranga ir taip išvengia papildomų išlaidų.
- **Duomenų decentralizacija (darbdavio nauda)** - verslo dokumentų laikymas asmeniniame nešiojamajame kompiuteryje (jei jie yra gerai apsaugoti) gali būti naudingas įmonei dėl didesnio duomenų decentralizavimo lygio. Duomenų nutekėjimo arba kenkėjiškos programinės įrangos atakos prieš įmonės sistemą atveju darbuotojų įrenginiuose esantys failai nebus perimti kartu su įmonės centrine duomenų baze.



Šaltinis: helpnetsecurity.com, *BYOD diegimas sparčiai auga, tačiau saugumas atsilieka,* https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/.

BYOD politikos trūkumai:

- **Kibernetinis (ne)saugumas** – be duomenų decentralizavimo naudos, kibernetinio saugumo klausimai yra didžiausias BYOD politikos trūkumas. Naudodamiesi asmeniniais įrenginiais darbuotojai linkę laikyti konfidencialius dokumentus savo įrenginiuose, kurie paprastai yra mažiau saugūs nei įmonės įrenginiai. Be to, dirbdami nuotoliniu būdu viešose vietose (pvz., kavinėse, bibliotekose, transporto priemonėse), jie dažnai jungiasi prie svetimo tinklo, todėl didėja tikimybė, kad į kompiuterius bus įsilaužta ir juose bus įdiegta kenkėjiška programinė įranga. Be to, kyla rizika, kad darbuotojo įrenginys gali būti pavogtas arba pamestas.
- **Nesuderinamumas** – darbo priemonių pasirinkimo lankstumas gali sukelti suderinamumo su įmonėje standartiškai naudojamomis sistemomis problemų. Taigi BYOD atveju gali kilti problemų, susijusių su formatų nesuderinamumu ir apsunkintu verslo dokumentų naudojimu (pvz., dėl to, kad failai vienaip išsaugomi „Windows“, o kitaip „MacOS“ sistemoje).
- **Duomenų atkūrimas** – dėl BYOD politikos gali kilti problemų, susijusių su darbuotojo įrenginyje saugomų duomenų atkūrimu pasibaigus darbo santykiams. Taip yra todėl, kad darbuotojai visiškai kontroliuoja savo įrenginius ir gali savarankiškai disponuoti juose saugomais failais.

BYOD teisės ir pareigos

Jei darbai atliekami su privačia įranga, būtina, kad ji atitiktų sveikatos ir saugos reikalavimus. Tačiau tokios įrangos apdraudimas nėra privalomas – darbuotojas ir darbdavys gali susitarti dėl draudimo apimties ir taisyklių, kuriomis vadovausis darbuotojas, naudodamasis jam priklausančia darbui būtina įranga.

Lenkijos pavyzdys - Darbo kodekso pakeitimas ir naujos nuotolinio darbo taisyklės

Pažymėtina, kad darbuotojas, dirbantis pagal darbo sutartį, turi teisę reikalauti įmonės kompiuterio, o darbdavys privalo jį darbuotojui suteikti. Tačiau jei darbui atlikti naudojama privati įranga, darbuotojas turi teisę gauti piniginę išmoką. Be to, darbdavys turėtų padengti nuotoliniam darbui būtinos elektros energijos ir telekomunikacijų paslaugų išlaidas. Kompensacija gali būti realios vertės arba šalių sutarta vienkartinė suma. Nustatydamas pašalpos ir vienkartinės sumos dydį, darbdavys turi atsižvelgti į medžiagų ir įrangos, taip pat elektros energijos ir telekomunikacijų paslaugų kainas[8] .

Jei darbas atliekamas namuose, darbdavys privalo vykdyti sveikatos ir saugos įsipareigojimus darbuotojui, išskyrus:

- pareigą rūpintis saugia ir higieniška darbo patalpų būkle,
- prievoles, susijusias su pastato, kuriame yra darbo patalpos, statyba ar pertvarkymu,
- pareigą užtikrinti tinkamas higienos ir sanitarines sąlygas.

Tokie darbdavio įsipareigojimai sudaryti tinkamas darbo sąlygas darbuotojams taip pat turi įtakos klausimams, susijusiems su sąvokos „nelaimingas atsitikimas darbe“ taikymo sritimi ir socialiniu draudimu. Nelaimingą atsitikimą darbe patyręs darbuotojas, nepriklausomai nuo to, kur jis atlieka savo pareigas - dirbdamas nuotoliniu būdu ar darbo vietoje - turi teisę į **socialinio draudimo išmokas.**

Prieš gaudamas leidimą dirbti nuotoliniu būdu, darbuotojas pareiškimu (pateikiamu popieriuje arba elektroniniu būdu) patvirtina, kad susipažino su darbdavio rizikos vertinimu ir informacija, kurioje išdėstyti saugaus ir sveiko nuotolinio darbo principai, ir įsipareigoja jų laikytis.

Atliekant profesinės rizikos vertinimą visų pirma atsižvelgiama į nuotolinio darbo poveikį darbuotojo regėjimui ir raumenų bei kaulų sistemai. Taip pat atsižvelgiama į psichosocialines

[8] *2022 m. gruodžio 1 d. Įstatymas, kuriuo iš dalies keičiamas Įstatymas - Darbo kodeksas ir kai kurie kiti įstatymai* (DZ.U., 2022 m., 240 punktas).

atitinkamo darbo sąlygas. Remdamasis vertinimo rezultatais, darbdavys parengia informaciją, kurioje pateikiami tinkamo nuotolinės darbo vietos organizavimo principai ir būdai. Juose turėtų būti atsižvelgta į ergonomikos reikalavimus, saugų ir higieniška nuotolinio darbo atlikimą, veiksmus, kuriuos reikia atlikti baigus nuotolinį darbą, taip pat į avarinių situacijų, keliančių pavojų žmogaus gyvybei ar sveikatai, sprendimo taisykles. Darbdavys taip pat gali parengti universalų rizikos vertinimą konkrečioms nuotolinio darbo pareigybių grupėms.

2.3. Asmens duomenų privatumas ir tinkle dirbančių asmenų saugumas

2.3.1. Nuotolinis darbas

Dėl populiarėjančio mišraus arba nuotolinio darbo, trunkančio visą darbo dieną, daugelyje valstybių narių įstatymų leidėjai nusprendė atitinkamai pakeisti savo darbo įstatymus. Visų pirma reikėjo pritaikyti darbuotojo ir darbdavio pareigas prie naujų darbo formų. Jos kyla dėl būtinybės užtikrinti, kad nuotolinio darbo vietoje esanti IT infrastruktūra ar darbo vieta atitiktų sveikatos ir saugos reikalavimus.

Nuotolinis darbas ir darbo teisė - Lenkijos pavyzdys

1. **Nuotolinio darbo įrankiai**

Pagal siūlomą Darbo kodekso 67 straipsnio 24 dalies 1 pastraipos pakeitimą darbdavys privalo nuotoliniu būdu dirbančiam darbuotoju užtikrinti:

- **Darbo medžiagas ir įrankius** – techninę įrangą, reikalingą darbui nuotoliniu būdu (priklausomai nuo darbo specifikos, be kompiuterio, tai gali būti tinkamos ausinės internetiniams susitikimams, mikrofonas ir t. t.).
- **Darbo priemonių,** įskaitant techninę įrangą, reikalingą darbui nuotoliniu būdu, **įrengimą, priežiūrą ir aptarnavimą.** Darbdavys taip pat gali padengti su šiomis paslaugomis susijusias būtinas išlaidas.
- Nuotoliniam darbui atlikti reikalingus **mokymus ir techninę pagalba.**
- **Elektros energijos išlaidų padengimą** – darbdavys taip pat privalo padengti nuotoliniam darbui reikalingos energijos ir telekomunikacijų paslaugų išlaidas.

Darbdavio ir įmonės profesinės organizacijos susitarimu arba vadovaujantis darbo tvarkos taisyklėmis darbdavys gali būti įpareigotas padengti kitas išlaidas, tiesiogiai susijusias su nuotolinio darbo atlikimu.

2. Nuotolinio darbo erdvės įrengimas – darbdavio kontrolė

Darbuotojas privalo įsirengti savo nuotolinę darbo vietą atsižvelgdamas į ergonominius reikalavimus. Tai, be kita ko, apima patogios kėdės pasirinkimą, tinkamo aukščio stalą, tinkamą monitoriaus padėtį akių atžvilgiu ir tinkamą apšvietimą.

Jei darbas atliekamas darbuotojo namuose, darbdavys privalo vykdyti darbuotojo sveikatos ir saugos pareigas, išskyrus:

- pareigą rūpintis saugia ir higieniška darbo patalpų būkle,
- Darbo kodekso III skyriaus dešimtajame skirsnyje (Statybos objektų ir darbo patalpų taisyklės) nustatytą pareigą,
- pareigą užtikrinti tinkamas higienos ir sanitarines sąlygas.

Tokie darbdavio įsipareigojimai sudaryti tinkamas darbo sąlygas darbuotojams taip pat turi įtakos klausimams, susijusiems su sąvokos „nelaimingas atsitikimas darbe“ taikymo sritimi ir socialiniu draudimu. Darbuotojas, patyręs nelaimingą atsitikimą darbe, nepriklausomai nuo to, kur jis atlieka savo pareigas (dirbdamas nuotoliniu būdu ar darbovietėje), turi teisę į **socialinio draudimo išmokas.**

Dėl darbdavio įsipareigojimų, susijusių su:

- tinkamų priemonių taikymu, kad būtų išvengta nelaimingų atsitikimų dirbant nuotoliniu būdu,
- būtinais veiksmais, siekiančiais pašalinti arba sumažinti tokio nelaimingo atsitikimo riziką,
- pirmosios pagalbos suteikimu nukentėjusiems asmenims ir nelaimingo atsitikimo aplinkybėmis bei priežastimis - pagal susitarimą, sudarytą su įmonės profesine arba nuostatus

darbdavys turi teisę atlikti patikrinimą dėl:

- sveikatos ir saugos darbe,
- **informacijos saugumo ir apsaugos reikalavimų laikymosi,** įskaitant asmens duomenų apsaugos procedūras.

Pagal naująsias Darbo kodekso nuostatas darbdavys galės pradėti tikrinti darbuotojų blaivumą tik tuo atveju, kai tai bus būtina siekiant užtikrinti darbuotojų, kitų asmenų gyvybės ir sveikatos apsaugą arba turto apsaugą.

Kiekvienas blaivumo patikrinimas turėtų būti toks:

- atliekamas susitarus su darbuotoju,
- atliekamas nuotolinėje darbo vietoje ir darbuotojo darbo valandomis,
- pritaikytas prie nuotolinio darbo vietos ir tipo,
- netrukdantis naudoti vidaus patalpų pagal paskirtį,
- jei nuotoliniu būdu dirbama retai, blaivumas turėtų būti tikrinamas taip, kaip buvo susitarta su darbuotoju,
- atliekamas gerbiant darbuotojo ir kitų asmenų (pvz., kitų namiškių ar nuomininkų) privatumą.

Jei patikrinimo metu darbdavys nustato trūkumus sveikatos ir saugos, saugumo ir informacijos apsaugos srityje, įskaitant duomenų apsaugą, jis turi dvi galimybes. Gali arba nustatyti darbuotojui terminą trūkumams pašalinti, arba atšaukti darbuotojui duotą sutikimą dirbti nuotoliniu būdu.

3. Asmens duomenų apsauga dirbant nuotoliniu būdu pagal Darbo kodekso pakeitimus

Atsižvelgdamas į padidėjusią asmens duomenų nutekėjimo ir kitų pažeidimų šioje srityje riziką, darbdavys turėtų nustatyti asmens duomenų apsaugos procedūras. Organizacijoje taip pat turės būti rengiami atitinkami mokymai. Kita vertus, nuotolinį darbą dirbantis darbuotojas turėtų raštu arba elektronine forma patvirtinti, kad susipažino su darbdavio nustatytais standartais.

Tiek darbuotojas, tiek darbdavys taip pat turėtų nustatyti, kaip ir kokiomis priemonėmis jie bendraus nuotoliniu būdu ir perduos su darbo atlikimu susijusią informaciją.

2.3.2. Kaip laikantis BDAR apsaugoti asmens duomenis dirbant nuotoliniu būdu?

Populiarėjant darbui nuotoliniu būdu padidėjo rizika, kad gali būti nutekinta konfidenciali įmonės informacija. Taip yra todėl, kad tiek darbuotojui, tiek darbdaviui gali būti sunku tiksliai nustatyti, kokiomis sąlygomis buvo pažeistos informacijos apsaugos, saugumo ir duomenų apsaugos taisyklės. Kadangi (bent iš dalies) nuotolinis darbas greičiausiai dar ilgai mus lydės, būtina prisiminti dažniausiai pažeidžiamas duomenų apsaugos taisykles. Taip pat verta

panagrinėti, kokie pavojai tyko nuotoliniu būdu dirbančių asmenų ir kaip sumažinti jų atsiradimo riziką.

ATMINKITE!

Pagal BDAR reglamento 32 straipsnį darbdavys, kaip jūsų asmens duomenų valdytojas, turėtų įgyvendinti tinkamas technines ir organizacines priemones, kad užtikrintų saugumo lygį, atitinkantį įvairios tikimybės ir svarbos fizinių asmenų teisių ar laisvių pažeidimo rizikos laipsnį.

Šiuo tikslu darbdavys gali imtis šių veiksmų:

a) asmens duomenų pseudonimų suteikimas ir šifravimas,

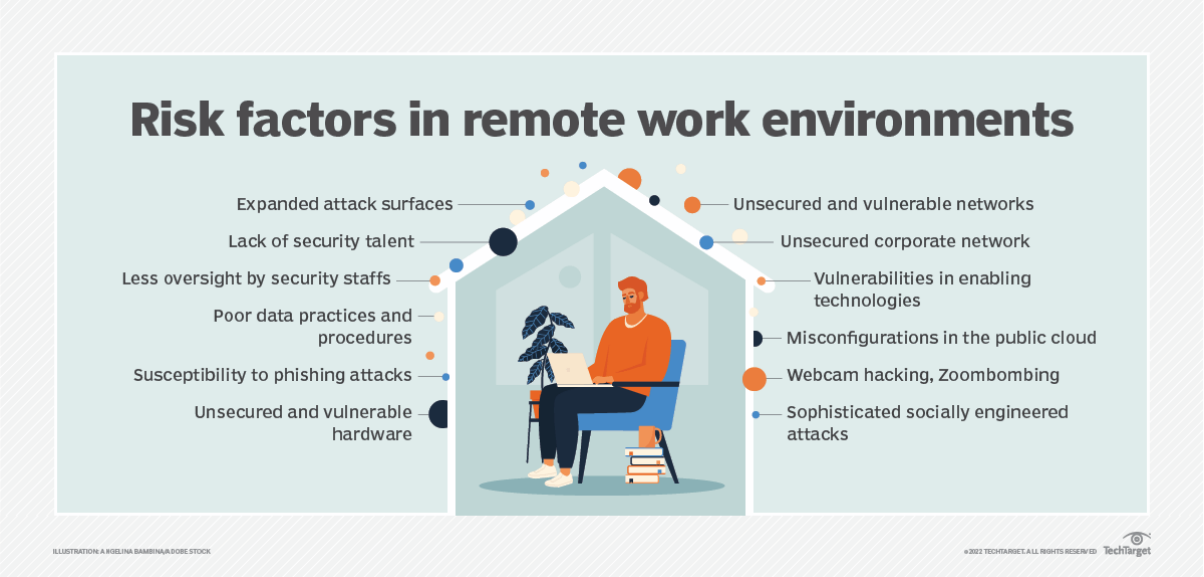
b) duomenų tvarkymo sistemų ir paslaugų konfidencialumo, vientisumo, prieinamumo ir atsparumo užtikrinimas,

c) užtikrinti, kad fizinio ar techninio incidento atveju būtų galima greitai atkurti asmens duomenų prieinamumą ir prieigą prie jų,

d) užtikrinti, kad techninių ir organizacinių priemonių, skirtų asmens duomenų tvarkymo saugumui užtikrinti, veiksmingumą būtų galima reguliariai išbandyti, išmatuoti ir įvertinti.

Kaip paaiškino Europos Komisija, darbuotojai, tvarkantys duomenis kaip savo darbo dalį įmonėje, atlieka duomenų valdytojo užduotis. Todėl jie taip pat yra atsakingi už asmens duomenų saugumo užtikrinimą.

2.3.3. Tinklo grėsmės ir nuotolinis darbas



Nors kibernetinis saugumas yra vienas svarbiausių iššūkių, su kuriais šiandien susiduria valstybės institucijos, visuomenės informuotumas apie jį vis dar yra ribotas. Beveik visi yra girdėję apie kibernetinį saugumą ir jo svarbą, tačiau piliečių elgesys ne visada atspindi aukštą šios srities žinių lygį. Remiantis interneto svetainės ChronPESEL.pl ir Nacionalinio skolų registro 2022 m. atliktos apklausos duomenimis, kas trečias lenkas bijo asmens duomenų nutekėjimo, tačiau mažiau nei pusė apklaustųjų žinotų, ką daryti esant tokiai situacijai.

Nors neįmanoma užtikrinti 100 proc. duomenų apsaugos ir informacijos saugumo, yra keletas prevencinių priemonių, kuriomis galima tinkamai sumažinti duomenų nutekėjimo ir kitų pavojų riziką.

Nuotolinio darbo aplinkoje tykantys pavojai mažai kuo skiriasi nuo tų, kurių turėtų saugotis bet kuris interneto naudotojas. Jų tikslas dažniausiai yra pavogti saugomą informaciją arba duomenis apie konkretų asmenį ar įmonę, kad nusikaltėlis galėtų įgyti finansinį pranašumą, konkurencinį pranašumą ar siekti kitų tikslų. Remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) ataskaita, dažniausios ir pavojingiausios kibernetinės grėsmės yra šios:

1. **Kenkėjiška programinė įranga** (*malware*) – tai kenkėjiškas kodas arba programos, kurios trukdo arba visiškai užkerta kelią įprastam galutinio įrenginio (pvz., kompiuterio ar spausdintuvo) naudojimui. Užkrėtę atitinkamą įrangą kenkėjiška programine įranga, nusikaltėliai gali gauti prieigą prie duomenų ar kitų įrenginio funkcijų. Jie taip pat gali siekti visiškai užblokuoti įrenginį, jei naudotojas ar kitas asmuo, iš dalies paveiktas atakos, sumoka išpirką.

2. **Išpirkos reikalaujanti programinė įranga** (*ransomware*) – kenkėjiškos programinės įrangos rūšis, kai nusikaltėlis užblokuoja naudotojų prieigą prie jų sistemų ar asmeninių failų ir reikalauja sumokėti mokestį už jų atkūrimą.
3. **Atakos per svetaines** – tai metodas, kai programišiai apgauna savo atakų aukas, naudodamiesi interneto sistemomis ir paslaugomis kaip kanalu pasirengti atakai ir ją vykdyti. Visų pirma čia galima išskirti kenkėjiškų URL adresų ar skriptų pateikimą ar palengvinimą, siekiant nukreipti naudotoją į norimą svetainę arba atsisiųsti kenkėjišką turinį. Rezultatas – kenkėjiško kodo įdiegimas į tikrą egzistuojančią svetainę, siekiant pavogti informaciją ir gauti finansinės naudos.
4. ***Phishing*** – kaip ir kitų kibernetinių atakų atveju, kibernetiniai nusikaltėliai siekia gauti vertingos informacijos, daugiausia prisijungimo vardų, slaptažodžių, PESEL numerių arba kredito kortelių numerių. Pavadinimas kilo iš to, kad nusikaltėliai naudoja masalą, pritaikytą konkrečiam asmeniui, kurio duomenis jie nori pavogti. Tam jie paprastai naudoja suklastotus el. laiškus arba SMS žinutes, taip pat bendravimo kanalus socialiniuose tinkluose. Siekdami įgyti pasitikėjimą, kibernetiniai nusikaltėliai apsimeta telekomunikacijų bendrovėmis, kurjerių tarnybomis, bankais, aukcionų svetainėmis ir net valstybinėmis institucijomis. Veikiami aukos emocijų, jie stengiasi priversti ją spustelėti jų paruoštą nuorodą į svetainę, kuri, nors ir panaši į tikrąją, yra sukurta nusikaltėlio ir yra jo sukčiavimo kanalas.
5. **DDoS** (angl. *distributed denial of service*) - tai atakos, nukreiptos prieš tinklo paslaugas arba kompiuterių sistemas, rūšis. Jų užduotis - užgrobti visus turimus ir laisvus išteklius, kad visa paslauga negalėtų veikti internete. Ši ataka gali paveikti įmonės interneto svetainę, darbuotojo prieglobos paštą ir t. t. Ji vykdoma iš skirtingų kompiuterinių įrenginių vienu metu - dažniausiai iš tų, kurių kontrolė perimta naudojant specialius virusus - botus arba Trojos arklius. Tokio tipo atakos pavojus yra tas, kad atitinkamos įrangos naudotojas gali nežinoti, jog jo kompiuteris naudojamas DDoS vykdyti.
6. **Tapatybės vagystė** – nusikaltėlis, pasinaudodamas kieno nors asmens kodu, asmens duomenimis arba asmens tapatybės kortele, apsimeta tuo asmeniu, norėdamas paimti, pavyzdžiui, kreditą arba kitaip pasinaudoti jo tapatybe savo naudai.
7. **Duomenų saugumo pažeidimas** – kibernetinio saugumo incidentas, kai prie informacijos (arba informacinės sistemos dalies) prieita be tinkamo leidimo, paprastai turint piktavališkų ketinimų. Dėl to ta informacija gali būti prarasta arba netinkamai panaudota. Šios rūšies grėsmės atsiradimo priežastis dažnai yra vadinamoji žmogiškoji klaida, kuri gali įvykti konfigūruojant ir diegiant tam tikras paslaugas ir sistemas, dėl kurios netyčia atskleidžiami duomenys.

8. **Informacijos nutekėjimas** – dažna duomenų saugumo pažeidimų pasekmė, apimanti įvairią informaciją, kuriai kyla pavojus – nuo asmenį identifikuojančios informacijos (PII) iki finansinių duomenų, saugomų IT infrastruktūroje, ir asmens sveikatos duomenų, saugomų sveikatos priežiūros paslaugų teikėjų saugyklose.
9. **Grėsmė iš vidaus** (piktnaudžiavimas įgaliojimais) – kai asmuo ar asmenų grupė yra susiję su atakos auka profesiniais ar kitokiais santykiais, kai ir užpuolikas, ir auka yra tame pačiame tinkle ar infrastruktūroje arba turi galimybę gauti informacijos dėl tarpusavio ryšio. Su šių tipų grėsmėmis siejami keli dėsningumai. Jos taip pat gali kilti, kai pašaliniai asmenys bendradarbiauja su įmonės vidaus subjektais, siekdami gauti neteisėtą prieigą prie išteklių. Asmenys, turintys prieigą prie vidinės informacijos, taip pat gali sukelti žalą netyčia dėl neatidumo ar žinių stokos. Kadangi asmenimis, žinančiais neviešą informaciją, dažnai pasitiki kolegos, o be to tie asmenys išmano organizacijos procesus ir procedūras, gali būti sunku atskirti teisėtą prieigą prie duomenų ir sistemų nuo nesąžiningų veiksmų.
10. **Botnetai** – tarpusavyje sujungtų įrenginių, užkrėstų botų kenkėjiškomis programomis, tinklas. Paprastai jie naudojami DDoS atakoms vykdyti. Nusikaltėlis gali nuotoliniu būdu valdyti botnetus, kad jie veiktų sinchroniškai ir pasiektų tam tikrą rezultatą.

2.3.4. Kibernetinė higiena – kaip kasdien būti saugiam internete?

1. **Jei galite, dirbkite saugioje, privačioje erdvėje.**

Duomenys gali nutekėti ne tik dėl įsilaužimo, bet ir ne tokiais sudėtingais, įprastais būdais, pavyzdžiui, pamačius ekrano turinį ir nufotografavus monitorių. Savaime suprantama, kad, be darbdavio paruoštos darbo vietos, saugiausia erdvė dirbti nuotoliniu būdu yra namų darbo vieta. Geriausia, jei tai būtų rakinamas kambarys, kuriame galėtumėte tyliai atsiskirti nuo likusių namų gyventojų.

Jei neįmanoma dirbti izoliuotame kambaryje (pvz., komandiruotės metu), saugaus darbo klausimas tampa gerokai sudėtingesnis. Ypač saugokitės atvirų erdvių (kavinių, traukinių, oro uostų), kuriose aplinkiniai žmonės nuolat keičiasi. Be to, daugelyje tokių vietų yra įrengtos vaizdo stebėjimo kameros, kurios gali fiksuoti ne tik jų veikimo zonoje esančių asmenų veiksmus, bet ir įvairius kitus aplinkos elementus, įskaitant kompiuterių ekranus.

Sprendimas: Įsigykite privatumo filtrą

Naudojant šį įrankį, ekrano turinį mato tik kompiuterį ir (arba) telefoną naudojantis asmuo. Ši technologija veikia panašiai kaip ir mikrožaliuzės - filtrą sudaro mikroskopiniai kanalai, nukreipti į monitoriaus ekranu besinaudojantį asmenį. Žmonės, žiūrintys į ekraną kitu kampu, nematys to paties turinio.

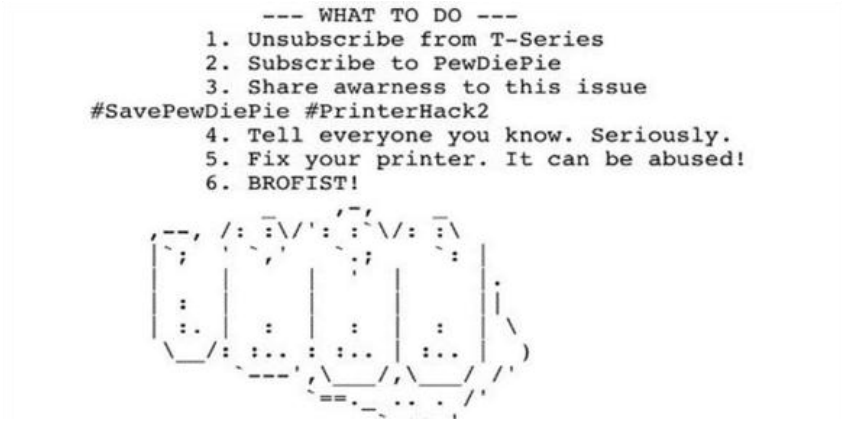
2. **Dirbdami nuotoliu dokumentus laikykite saugioje, rakinamoje vietoje**

Daugelyje darbo vietų galiojanti vadinamoji „švaraus stalo“ arba „švaraus ekrano“ politika turėtų būti taikoma ir nuotolinio darbo vietoje. Net jei pasitikime namiškiais ar kambario draugais, nesant mūsų neturėtų būti paliekami jokie dokumentai, kuriuose yra asmeninės informacijos. Taip pat neturėtumėte laikyti darbo įrenginių slaptažodžių matomoje vietoje.

Sprendimas: nuotolinio darbo vietoje įsirenkite rakinamą stalčių arba spintelę.

Tai bus vieta, kurioje darbo metu galėsite saugiai laikyti visas užduočių medžiagas. Jei įmanoma, raktą visada turėkite su savimi arba paslėpkite tik jums žinomoje vietoje.

3. **Jei nebūtina, nespausdinkite dokumentų namuose arba viešose kopijavimo vietose.**



Kibernetinio saugumo ekspertai jau seniai perspėja, kad labiausiai ignoruojamas įrenginys, kuriame reikia įdiegti tinkamą apsaugą, yra... spausdintuvas. Žurnalo "InfoSecurity Magazine" atlikto tyrimo duomenimis, maždaug 66 % apklaustų nuotolinių darbuotojų spausdino vidutiniškai

penkis dokumentus per savaitę. Ketvirtadalis jų dar neišmetė atspausdintų dokumentų, aiškindami, kad ketina juos nunešti atgal į biurą. Tik 24 proc. naudoja namų smulkintuvą, tačiau taip pat pripažįsta, kad išmeta dokumentus į namų šiukšlių dėžę. Net 12 % apklaustųjų taip pat teigia, kad nežino apie BDAR reglamentą.

Šiuolaikiniai spausdintuvai vis labiau panašėja į kompiuterius, o ne į vienkartinius paprastus įrenginius. Tai daugiafunkciniai darbo įrankiai ir jie dažnai yra daiktų interneto (angl. *Internet of Things,* IoT) dalis. Viena iš labiau žinomų atakų prieš buitinius spausdintuvus, išryškinusi netinkamo šių prietaisų saugumo problemą, buvo susijusi su gerai žinomu „YouTube“ kūrėju PewDiePie. 2018 m. programišius (arba daugybės PewDiePie gerbėjų grupė) atakavo dešimtis tūkstančių spausdintuvų visame pasaulyje. Nesikišant jų savininkams, įrenginiai pradėjo spausdinti brošiūrą, kurioje reklamuojamas PewDiePie skelbiamas turinys ir skatino remti jo veiklą.

Šiuolaikiniuose vis pažangesniuose spausdintuvuose yra talpykla, kurioje spausdinami dokumentai. Šiuolaikiniai spausdintuvai taip pat veikia belaidžiu ryšiu, o tai reiškia, kad prie jų gali prisijungti bet kas, turintis kompiuteryje tinkamas tvarkykles ir prieigą prie tinklo, kuriame yra spausdintuvas. Jei programišius perima spausdintuvo kontrolę (pvz., įmonėje), jis gali gauti prieigą ir prie jau išspausdintų dokumentų, ir prie kitų kompiuteryje saugomų išteklių ar net prie įrenginių, kurie naudojosi spausdintuvo paslaugomis, slaptažodžių.

Sprendimas: dokumentus spausdinkite tik darbe, o jei turite tai daryti namuose, įsitikinkite, kad jūsų įranga tinkamai apsaugota.

Tai galima padaryti nustačius saugų spausdintuvo „Wi-Fi“ slaptažodį (jei įmanoma). Jei atspausdintų dokumentų jums nebereikia, neišmeskite jų į šiukšliadėžę namuose - nuneškite juos į įmonę, kur turėtų būti smulkintuvas. Jei tokios galimybės nėra, pasiteiraukite savo darbdavio arba personalo skyriaus apie įmonės dokumentų naikinimo tvarką.

4. Internetinės kameros dangtelis

Darbas namuose paprastai reiškia dalyvavimą telekonferencijose ir vaizdo skambučiuose, kuriuose reikia naudoti interneto kamerą. Deja, programišiai gali lengvai pasiekti jūsų interneto kamerą ir taip pažeisti jūsų privatumą. Be to, jei fizinėje darbo vietoje yra konfidencialių dokumentų, kuriuos galima užfiksuoti internetine vaizdo kamera, nusikaltėliai galės prie jų prieiti.

Sprendimas: apriboti vaizdą, kad nesimatytų elementų, kuriuose yra asmeninių duomenų.

Įjungus internetinę vaizdo kamerą, turėtų būti apribota galimybė matyti jos aplinkoje esančius daiktus, kuriuose yra asmeninės informacijos. Be to, jei internetinė vaizdo kamera yra atskirta nuo prietaiso, nenaudojama ji turėtų būti atjungta. Jei internetinė vaizdo kamera yra įmontuota, verta imtis papildomų apsaugos priemonių, pavyzdžiui, įsigyti kameros dangtelį. Parduotuvėse nesunkiai galima rasti įvairių tipų stumdomų internetinės vaizdo kameros dangtelių. Paprastai juos lengva sumontuoti, nes dauguma jų turi lipnų sluoksnį, kuris prilimpa prie kameros. Naudodamiesi vaizdo konferencijoms skirta programine įranga ir programomis, taip pat galite naudoti tokias funkcijas kaip **fono neryškumas**.

5. **Aktyviai dalyvaukite įmonės mokymuose apie kibernetinį saugumą ir darbdavio politikos pokyčius, susijusius su duomenų ir informacijos apsauga.**

Pagal BDAR, jei bus priimtos naujos duomenų apsaugos procedūros įmonėje, darbdavys turėtų leisti darbuotojams su jomis susipažinti prieš jas įgyvendindamas.

Jei darbdavys nepravedė tinkamų mokymų apie prietaisų naudojimą, vidinių ir išorinių komunikacijos priemonių naudojimą arba apie pagrindinius principus, susijusius su duomenų apsauga įmonėje, darbuotojas turi teisę paprašyti, kad jis tai padarytų. Jei net ir po mokymų darbuotojas vis dar nėra tikras dėl procedūrų, kurių reikia laikytis tam tikroje situacijoje, jis turėtų apie tai pranešti darbdaviui arba paskirtam įmonės asmeniui, atsakingam už IT valdymą, žmogiškųjų išteklių skyriui ir pan.

Kibernetinė higiena dirbant nuotoliniu būdu

Ką dar galite padaryti, kad apsaugotumėte savo kompiuterį?

Užšifruoti asmens duomenis

Ypač jei tai neskelbtini duomenys arba jei juos siunčiate už įmonės ribų. Kaip minėta pirmiau, darbuotojai, tvarkantys duomenis vykdydami savo darbo užduotis, atlieka duomenų valdytojo, t. y. darbdavio, užduotis. Pagal BDAR 32 straipsnį duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų tokį duomenų saugumo lygį, kuris atitiktų duomenų tvarkymo apimtį, kontekstą ir tikslus bei kišimosi į fizinių asmenų teises ar laisves pavojų. Kaip saugumo priemonės BDAR reglamente, be kita ko, minimas pseudonimų suteikimas ir asmens duomenų šifravimas.

Nors BDAR nėra aiškių reikalavimų dėl veiksmingiausio saugumo būdo, reglamente ne kartą pabrėžiama, kad **šifravimas ir pseudonimų suteikimas** yra tinkamos techninės ir organizacinės priemonės asmens duomenų saugumui užtikrinti.

Šifravimo tikslas – užkoduoti tam tikrą turinį taip, kad jį suprastų tik gavėjas, turintis tinkamą raktą. Paprasčiausiai siekiama, pavyzdžiui, raidžių eilutę paversti kitų raidžių ar skaičių eilute, pridėti papildomų raidžių ar skaičių eilučių ir pan.

Kita vertus, pseudonimizavimas – tai asmens duomenų tvarkymas taip, kad neįmanoma nustatyti, kam jie priklauso, neturint prieigos prie informacijos, saugomos kitoje vietoje. Taigi, tai yra duomenų maskavimas pakeičiant informaciją apie asmenį išgalvotais identifikatoriais.

Kuo skiriasi šie du metodai?

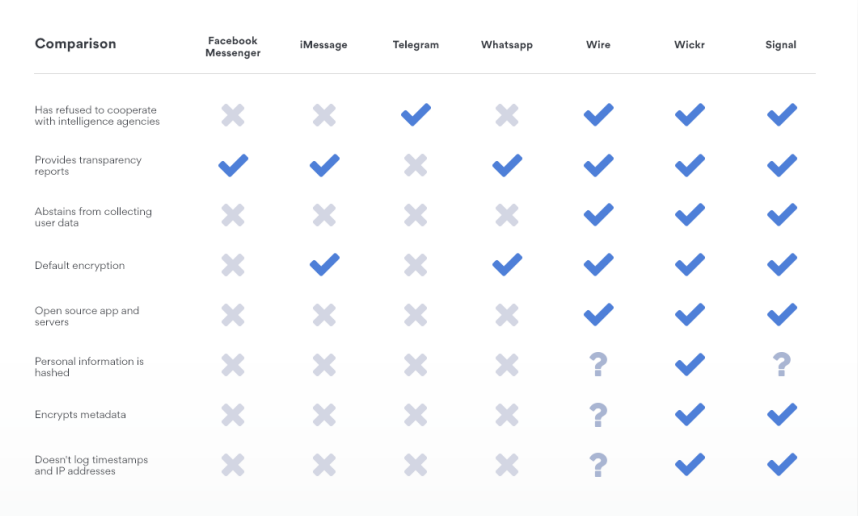
Kaip ir pseudonimizavimas, šifravimas slepia informaciją, pakeisdamas identifikatorius kažkuo kitu. Tačiau pseudonimizavimas leidžia bet kuriam asmeniui, turinčiam prieigą prie duomenų, matyti dalį duomenų rinkinio, o šifravimas leidžia tik patvirtintiems naudotojams pasiekti visą duomenų rinkinį. Pseudonimizavimas ir šifravimas gali būti naudojami vienu metu arba atskirai.

Duomenų apsaugos ir (arba) šifravimo metodai, taikomi vidiniam bendravimui ir bendravimui su išorės subjektais.

a. Vidaus komunikacija – šifruotų pranešimų ir saugių platformų naudojimas

Nors el. paštas vis dar išlieka vienas populiariausių verslo komunikacijos būdų (2021 m. kasdien buvo išsiųsta ir gauta 316,9 mlrd. el. laiškų, o iki 2025 m. šis skaičius turėtų išaugti iki 376,4 mlrd.), jis taip pat nėra saugiausia sistema keistis konfidencialia informacija. Dėl savo didelio populiarumo el. paštas taip pat yra pagrindinis programišių kanalas. Bendrovė „Deloitte“ nustatė, kad 91 proc. visų kibernetinių atakų įvyksta iš *apgaulingų* elektroninių laiškų. Tokių atakų kaina įmonėms gali būti labai didelė.

Vidiniams ryšiams, kai dažnai keičiamasi konfidencialia informacija apie įmonę, jos darbuotojus ar klientus, galima naudoti kitas, saugesnes priemones.



Comparison	Facebook Messenger	iMessage	Telegram	Whatsapp	Wire	Wickr	Signal
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓
Open source app and servers	✗	✗	✗	✗	✓	✓	✓
Personal information is hashed	✗	✗	✗	✗	?	✓	?
Encrypts metadata	✗	✗	✗	✗	?	✓	✓
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	?	✓	✓

"Whatsapp" ir "Messenger" - populiariausios žinutės ir jų funkcijos

1. **"WhatsApp":**
   - naudoja Signalo šifravimą,
   - dauguma žmonių Europoje tikriausiai naudojasi šia programa,
   - patogią programą, kuri suteikia papildomų funkcijų,
   - priklauso „Facebook“,
   - anksčiau taikant programą buvo padaryta rimtų duomenų apsaugos pažeidimų.
2. ***Messenger:***
   - platus pasiekiamumas – dėl sąsajos su "Facebook" šią žinutę turi dauguma žmonių,
   - Ją galima naudoti net ir išjungus "Facebook" paskyrą,
   - šifravimas nėra numatomasis,
   - komunikatorius nešifruoja ankstesnių pokalbių,
   - programa stebi naudotojo elgesį.

Geriausios programos duomenų saugumo požiūriu:

1. **Signal:**
    - palaiko grupinius pokalbius, SMS, balso ir vaizdo pranešimus, leidžia perduoti dokumentus ir nuotraukas,
    - siūlo dingstančius pranešimus (su laikmačiu),
    - naudojamas signalizavimo protokolas - nefederuotas kriptografinis protokolas, kuris gali būti naudojamas balso skambučiams ir tiesioginių žinučių siuntimo pokalbiams šifruoti, kai atviru tekstu parašytus pranešimus gali perskaityti tik bendraujantys asmenys,
    - atvirojo kodo (*open source*) programinė įranga (t. y. programinė įranga, kurios pirminis kodas pateikiamas nemokamai ir gali būti platinamas bei keičiamas nemokamai),
    - nesaugo naudotojo duomenų ar metaduomenų,
    - propaguojamas Edwardo Snowdeno,
    - registracijai reikia nurodyti telefono numerį.

Saugios programinės įrangos ir darbo vietos platformos:

1. „Microsoft Teams“
2. „Google Workspace“
3. „Slack“
4. „Asana“
5. „Trello“

b. Išorinis bendravimas – failų su asmens duomenimis ir el. pašto gavėjų sąrašų šifravimas.

Rekomenduojama, kai tik įmanoma, duomenis perduodant iš vienos vietos į kitą, juos pseudonimizuoti arba užšifruoti, kad būtų apsisaugota nuo nutekėjimo.

Asmens duomenų pateikimas adresatų sąraše

Naudokite lauką UDW (paslėptas į pranešimą, BCC). UDW laukas leidžia siųsti pranešimus taip, kad gavėjai nematytų vienas kito adresų. Šią parinktį galima rasti kiekviename el. pašte.

Asmens duomenų perdavimas elektroniniu paštu siunčiamose bylose

Elektroniniu paštu siunčiamuose dokumentuose gali būti paslėpta daug asmeninių duomenų ar kitos teisiškai saugomos informacijos, todėl juos reikia papildomai apsaugoti. Failų šifravimo metodai gali skirtis priklausomai nuo formato, kuriuo jie saugomi. Tačiau visus juos sieja vienas bendras principas: užšifruoto dokumento slaptažodžio perdavimas ne el. paštu, o kitomis ryšio priemonėmis.

Norint tinkamai užšifruoti failą, dažniausiai pasirenkamos šios programos: **„WinRAR“** ir **„7-zip**“. Kiekvienoje iš jų, pasirinkus parinktį „įtraukti į archyvą“, atidaromas langas, kuriame, be kita ko, galima nustatyti prieigos prie dokumento slaptažodį.

Reguliariai kurkite atsargines duomenų kopijas ir saugokite jas išoriniuose diskuose

Jūsų įrenginys gali būti užkrėstas virusu arba gali įvykti kas nors kito, dėl ko duomenys dings iš kompiuterio ir negalėsite jų atkurti. Tokiam atvejui geriausia išeitis – reguliariai daryti **atsargines kopijas.**

Atsarginės kopijos *(backup)* – tai informacijos kopijos, saugomos kitoje vietoje nei originalas. Pirmiausia reikėtų nuspręsti, ar norite daryti atsarginę kopiją:

1. konkrečių duomenų, kurie dėl tam tikrų priežasčių yra svarbūs,
2. visos operacinės sistemos.

Dauguma atsarginių kopijų darymo įrankių pagal numatytuosius nustatymus yra sukonfigūruoti pirmajam tikslui ir kopijuoja duomenis pagal tai, kokius dokumentus naudojate dažniausiai. Jei nesate tikri, kuriuos failus kopijuoti, rekomenduojama juos visus archyvuoti.

Kaip dažnai daryti atsargines kopijas?

Atsakymas priklauso nuo asmeninių pageidavimų ir pokyčių dažnumo. Vieni žmonės tai daro kas valandą, kiti – kartą per dieną, treti – kartą per savaitę. Tačiau rekomenduojama kasdien daryti atsargines dokumentų kopijas.

Kaip sukurti atsarginę dokumentų kopiją?

Priklausomai nuo kompiuterio operacinės sistemos, yra rekomenduojamų programų, kuriose galima nustatyti laikotarpį, per kurį kaskart automatiškai atliekama atsarginė kopija. Tai „Microsoft Windows Backup and Restore“ arba „Apple“ programa „Time Machine“. Šios programos veikia ir tada, kai įrenginys naudojamas, ir tada, kai jis neveikia.

Duomenys išorinėje laikmenoje, ar duomenys debesyje?

Pageidautina ir vienur ir kitur. Išorinė laikmena, be kita ko, gali būti atmintinė (pendrive), nešiojamasis išorinis diskas arba kiti įrenginiai, prie kurių galima prisijungti per „Wi-Fi“. Jų naudojimo privalumas neabejotinai yra tas, kad per gana trumpą laiką į jas galima įrašyti didelius duomenų rinkinius. Deja, kadangi tai yra fizinis atsarginių kopijų darymo būdas, jis gali patirti tokius pačius gedimus ar pažeidimus kaip ir kompiuteris. Atsarginė kopija išorinėje laikmenoje gali būti pavogta, pamesta, užlieta vandeniu, perkaitinta ir pan. Be to, jei įrenginys, iš kurio duomenys buvo gauti, anksčiau buvo užkrėstas kenkėjiškomis programomis, deja, yra rizika, kad bus užkrėsta ir laikmena, taigi ir pati atsarginė kopija.

Kita vertus, atsarginės kopijos debesyje – tai dokumentų ar kitų failų kopijų laikymas internete. Tiksliau, tai yra visame pasaulyje išsibarsčiusių serverių ir duomenų centrų, kuriuose saugomi duomenys, rinkiniai. Tai vyksta automatiškai, paprastai naudojant numatytuosius tekstų tvarkymo platformos įrankius (pvz., „Google Docs“), kurie sukuria atsarginę kopiją kas nustatytą laiką arba po kiekvieno failo pakeitimo. Neabejotinas failų kopijų saugojimo debesyje privalumas yra jų pastovumas ir galimybė pasiekti atsarginę kopiją iš bet kurio kito įrenginio (žinoma, su sąlyga, kad turite paskyros, kurioje yra debesis, slaptažodį). Tačiau tai nėra visiškai be trūkumų – jei norite greitai sukurti didelės apimties duomenų atsarginę kopiją, šis sprendimas gali būti daug lėtesnis nei fizinė atsarginė kopija išoriniame diske. Be to, debesyje gali pritrūkti vietos naujiems duomenims saugoti ir gali tekti dalį jų ištrinti arba iš debesijos paslaugų teikėjo nusipirkti papildomų išteklių.

Saugi prieiga prie kompiuterio, telefono ir net internetinių susitikimų

Asmens duomenų saugumui užtikrinti būtina šifruoti pačius duomenis, todėl labai svarbu, kad mūsų naudojama įranga taip pat būtų tinkamai apsaugota. Naudojant slaptažodžius ar kitų rūšių šifravimą užtikrinama, kad prieigą prie tam tikrų išteklių turėtų tik įgalioti asmenys.

Yra keli įrangos apsaugos būdai:

- **Tai yra stiprus slaptažodis:**
    - **ilgas** – jį sudaro ne mažiau kaip aštuoni simboliai (kuo ilgesnis, tuo geriau),
    - **sudėtingas** – **jame** yra bent po vieną kiekvienos kategorijos simbolį: didžiosios raidės, mažosios raidės, specialieji simboliai (pvz., !, ?), skaičiai,
    - **sunku atspėti** – jei norite pasirinkti frazę, citatą ar posakį, įsitikinkite, kad jis nėra tiesiogiai susijęs su jumis, jūsų darbu ar aplinka; tačiau jei žinote, kad slaptažodžio be lengvų asociacijų neįsiminsite, pakeiskite žodžius atitinkamais

klaviatūros simboliais ar skaičiais, pavyzdžiui, „Ala turi katę“ (*lenkiškai „Ala ma kota*“) **galima** užrašyti kaip "4LaM@k0T@",

- **skiriasi nuo ankstesnio atitinkamo įrenginio slaptažodžio** – jei keičiate esamos paskyros slaptažodį, jis neturėtų būti toks pat kaip ankstesnis; taip pat nereikėtų slaptažodžio keisti tik nežymiai, pavyzdžiui, pridedant vieną skaitmenį. pabaigoje arba pradžioje.

Patarimas: naudokite slaptažodžių valdymo įrankį, kad užšifruotus slaptažodžius galėtumėte saugoti internete - taip galėsite sukurti sudėtingus slaptažodžius, kuriuose būtų didžiosios ir mažosios raidės, skaičiai, įvairūs specialieji simboliai ir pan. Taip sukursite beprasmišką simbolių eilutę, kurią bus sunku nulaužti.

ATMINKITE!

- nenaudokite slaptažodžio, kuris taip pat yra vardas arba panašus į vartotojo vardą, įmonės pavadinimą ir t. t,
- nenaudokite raidžių ar skaičių sekos iš klaviatūros ar abėcėlės,
- nenaudokite daugiau nei dviejų pasikartojančių raidžių ar skaičių (pvz., abba),
- nenaudokite niekieno asmeninių duomenų slaptažodžiui sukurti,
- nenaudokite atvirkščiai rašomų žodžių variantų (pvz., janek1 kaip 1kenaj),
- neįveskite slaptažodžio kitiems matant,
- nerašykite slaptažodžio ant popieriaus – jei turite jį užrašyti, naudokite slaptažodžių valdymo įrankį USB atmintinėje ir nešiokitės jį su savimi.
- nenaudokite to paties slaptažodžio visuose įrenginiuose ar svetainėse,
- neprisijunkite prie ne savo įrenginio,
- nesiųskite slaptažodžio el. paštu,
- nesidalykite slaptažodžiais internete – jei reikia pasidalyti prisijungimo informacija su kolega, paskambinkite jam ir praneškite duomenis, o ne siųskite slaptažodį. el. paštu, SMS žinute ar kita žinute,
- jei buvo įsilaužta į jūsų kompiuterį / svetainę, nedelsdami pakeiskite slaptažodį.

Antipavyzdys - mažiausiai saugių slaptažodžių sąrašas:[9] **,**

1. slaptažodis
2. 123456
3. 123456789
4. svečias
5. qwerty
6. 12345678
7. 111111
8. 12345
9. col123456
10. 123123
11. 1234567
12. 1234
13. 1234567890
14. 000000
15. 555555
16. 666666
17. 123321
18. 654321
19. 7777777
20. 123

[9] Remiantis "NordPass" atliktu tyrimu "Top 200 dažniausiai naudojamų slaptažodžių", https://nordpass.com/most-common-passwords-list/.

Daugiakomponentis autentiškumo nustatymas

Daugiakomponentis autentiškumo patvirtinimas (MFA arba 2FA) - tai apsaugos metodas, pagal kurį veiksmui patvirtinti (pvz., įvedant paskyros slaptažodį ir SMS kodą) reikia naudoti bent du nepriklausomus komponentus. Šis metodas užkerta kelią daugumai atakų, pagrįstų tapatybės duomenimis.

Daugelis programų ar platformų jau suteikia galimybę įjungti tokio tipo apsaugą (pvz., „Apple ID“, „Microsoft“, „Google“, „Twitter“ ar „Facebook“). Antrasis autentiškumo patvirtinimo komponentas gali būti SMS kodas, vienkartinis kodas iš programos („Google Authenticator“ arba „Microsoft Authenticator“) arba nuolatinis kodas, kurį pasiūlo atitinkamos priemonės teikėjas ir pasirenka naudotojas.

U2F raktai

Kibernetinio saugumo ekspertų teigimu, U2F raktas yra vienintelis dviejų žingsnių autentifikavimo metodas, kuris 100 % apsaugo nuo sukčiavimo (*phishing)* atakų, bet ne nuo kitų, pvz., kenkėjiškų programų *(malware)*. Taip yra todėl, kad jei U2F raktą turintį asmenį apgauna kibernetiniai nusikaltėliai ir įveda prisijungimo vardą ir slaptažodį suklastotoje interneto svetainėje, užpuolikui nepavyks perimti naudotojo paskyros duomenų.

Taip yra dėl saugaus elemento *(secure element)* – vadinamojo mažojo kompiuterio, įtaisyto U2F rakte. Jis veikia taip, kad raktą įkišus į USB jungtį (arba priartinus jį prie išmaniojo telefono skaitytuvo), raktas įsijungia ir gali atlikti kriptografines operacijas savo vidinėje sistemoje, o ne naudotojo įrenginyje.

Be to, verta įsigyti du raktus – nors tą patį raktą galima prijungti prie skirtingų paslaugų, verta turėti vieną atsarginį. Įsigijus raktą, jį reikia sukonfigūruoti. Daugelyje paslaugų siūloma galimybė pridėti raktą kaip daugiapakopio autentiškumo patvirtinimo formą. Šį sprendimą taip pat rekomenduoja įvairios socialinės žiniasklaidos, „Amazon“, „GitHub“ ar el. pašto paskyros. Jei nuspręsite naudoti U2F raktą, kitus dviejų pakopų autentifikavimo būdus reikia pašalinti iš atitinkamos paslaugos.

Susitikimų internetu užtikrinimas

Apsaugoti reikia ne tik techninę įrangą, bet ir tinkle vykstančius susitikimus bei vaizdo konferencijas. Dirbant nuotoliniu būdu dažnai tenka naudotis vaizdo konferencijų programine įranga, o tai savo ruožtu kelia galimą pavojų įrenginio saugumui. Po kelių atakų prieš „Zoom“ platformą, kai į vaizdo konferencijas įsilaužtavo nekviesti asmenys, kad įbaugintų ar persekiotų jos dalyvius (*zoom bombardavimas),* bendrovė buvo priversta ištaisyti saugumo spragas. Nepaisant pavadinimo, „zoom *bombing*“ gali būti vykdomas ir kitose platformose. Dėl tokio tipo atakų gali nutekėti konfidenciali informacija apie įmonę, klientus, kitus darbuotojus ar patį naudotoją.

Reaguodamas į „Zoom“ bombardavimus, FBI paskelbė patarimų, kaip padėti naudotojams apsisaugoti naudojant vaizdo konferencijų programinę įrangą:

1. Patikrinkite, ar susitikimas yra privatus, reikalaudami slaptažodžio, kad galėtumėte prisijungti prie susitikimo, arba kontroliuodami svečių patekimą iš laukiamojo kambario.
2. Rinkdamiesi tiekėjus atsižvelkite į saugumo reikalavimus. Šifravimas nuo galo iki galo (*end-to-end)* – kai pranešimas paslepiamas siuntėjo pusėje ir iššifruojamas tik gavėjo pusėje, užtikrina privatumą ir saugumą, todėl patikrinkite, ar jūsų naudojama vaizdo konferencijų programinė įranga turi šią funkciją.
3. Įsitikinkite, kad programinė įranga yra atnaujinta, ir įdiekite naujausius pataisymus ir atnaujinimus.

Šiuo metu saugiausia vaizdo konferencijų platforma yra „Microsoft Teams“. Dėl sklandžios visų „Office“ programų integracijos taip pat galima nustatyti papildomus saugumo nustatymus, todėl visi organizacijos nariai gali dirbti kartu, išlikdami saugūs net ir namų biure.

Įdiekite ir nuolat atnaujinkite antivirusinę programinę įrangą ir apsaugą nuo kenkėjiškų programų

Sistemų, programų ir naršyklių atnaujinimas dažnai apleidžiamas ir atidedamas. vėlesniam laikui. Iš tikrųjų, jei tai atliekama tinkamu laiku, galima išvengti didelės dalies atakų. Taigi įsitikinkite, kad naudojate atnaujintą ir modernią antivirusinę programinę įrangą. Atnaujinimuose yra svarbių pakeitimų, kurie pagerina prietaisų veikimą ir saugumą. Šiuo metu atnaujinimai išleidžiami net kas mėnesį, tačiau verta įjungti kasdienį atsarginių kopijų režimą. Tai gerokai padidina saugumą, nes kūrėjai gali greitai ištaisyti pastebėtas saugumo spragas ir taip dar labiau apsaugoti įrenginius nuo kenkėjiškų programų.

Be standartinės antivirusinės programinės įrangos, taip pat reikia įsitikinti, kad įdiegta ir naudojama ne tik standartinė antivirusinė programinė įranga, bet ir apsaugos nuo kenkėjiškų programų programinė įranga. Ši priemonė gali ne tik apsaugoti nuo atakų, bet ir įspėti naudotoją, kai bandoma atakuoti.

Venkite jungti įrenginius prie viešųjų tinklų

Naudojantis viešuoju tinklu, t. y. tinklu, prie kurio gali prisijungti bet kas, dėl to, kad jis yra visiškai atviras, galima vykdyti daugybę atakų ir kyla duomenų nutekėjimo rizika. Jei tenka dirbti viešoje erdvėje, būtinai junkitės tik prie patikimų tinklų ir visada naudodami VPN arba ryšį iš telefono (per vadinamąjį karštąjį tašką, *hotspot*).

Kas yra VPN?

Tai virtualūs privatūs tinklai, kurie užtikrina saugų tiesioginį prisijungimą prie įmonės kompiuterių tinklo. Jie gali būti labai svarbūs, kai reikia pasiekti failus, dirbti su konfidencialia informacija arba naudojantis tam tikromis interneto svetainėmis.

VPN šifruoja naudotojų prisijungimus prie savo serverių, todėl suteikiama saugi ir patikima prieiga prie įmonės tinklo. Užšifruotas įmonės VPN tunelis taip pat padės užtikrinti, kad perduodami duomenys būtų saugūs. Jis taip pat užkirs užpuolikams, kurie neturi korporatyvinio VPN, prieigą prie serverių.

VPN saugumą galima padidinti naudojant patikimą autentifikavimo metodą. Daugelis VPN naudoja vartotojo vardą ir slaptažodį, bet taip pat galite pagalvoti apie atnaujinimą ir išmaniųjų kortelių (*smart cards*) naudojimą, kad apsaugotumėte naudotojo prisijungimo procesą ir geriau kontroliuotumėte prieigą prie paskyros.

Žinoma, nesvarbu, koks stiprus yra VPN. Jei slaptažodis bus nulaužtas, įsilaužėliai galės lengvai į jį patekti. Todėl jį reikėtų reguliariai atnaujinti. Naudojantis VPN verta apsiriboti tik tais atvejais,

kai tai būtina. Jei verslo įrenginiai asmeniniam naudojimui naudojami vakarais arba savaitgaliais (jei tai atitinka įmonės politiką), VPN geriausia išjungti.

Kas kita, jei ne VPN?

Kita galimybė - naudoti 5G tinklą. Jis užtikrina geresnį ryšį ir žada didesnį saugumą nei naudojant Wi-fi ar net VPN ryšį. Skelbiama, kad 5G tinkle rečiau pasitaiko vėlavimo atvejų, todėl jis gali tapti realia alternatyva Wi-fi. Šioje technologijoje įdiegtas šifravimas naudojant priemones, kurios neleidžia sekimo ar suklastojimo *(spoofing)*.

Dirbant namuose, būtina apsaugoti ir namų maršrutizatorių. Jis turėtų būti atnaujintas ir apsaugotas ilgu unikaliu slaptažodžiu, kuris skirtųsi nuo automatinio slaptažodžio, kurį turi kiekvienas maršrutizatorius. Norėdami tai padaryti, galite nueiti į maršrutizatoriaus nustatymų puslapį, naršyklėje įvesdami atitinkamą frazę, ir ten pakeisti slaptažodį. Tame pačiame puslapyje paprastai galite pakeisti ir SSID, t. y. belaidžio tinklo pavadinimą, kad tretiesiems asmenims būtų sunkiau nustatyti ir pasiekti jūsų namų Wi-fi tinklą. Nenaudokite savo vardo, pavardės, namų adreso ar bet ko, kas galėtų būti panaudota identifikavimui.

Taip pat turėtumėte įsitikinti, kad įjungtas tinklo šifravimas, o tai paprastai galima padaryti belaidžio ryšio konfigūracijos puslapio saugumo nustatymuose. Galima rinktis iš kelių saugumo metodų, pavyzdžiui, WEP, WPA ir WPA2. Stipriausias iš jų yra WPA2, kuriam reikalinga naujesnė nei 2006 m. techninė įranga.

3. skaitmeninimo poveikis darbo rinkai

3.1. Diskriminacinis elgesys įdarbinimo procesuose

Iki technologijų atsiradimo pasaulyje visus sprendimus, susijusius su įdarbinimu ir darbuotojo vertinimu, priimdavo žmonės. Priimant šiuos sprendimus paprastai būdavo atsižvelgiama į vietos kontekstą, etinius aspektus, teisinius aspektus, susijusius su proceso skaidrumu ir vadovybės sprendimų pagrįstumu. Tačiau šiandien daugelis įmonių naudoja IT sistemas, kurios užtikrina didesnį efektyvumą ir sumažina varginantį dokumentų nagrinėjimą ieškant konkrečios informacijos.

Šios sistemos, vadinamos ADS (algoritminėmis sprendimų priėmimo sistemomis*, angl. algorithmic decision systems),* grindžiamos didelių duomenų kiekių analize, o gautų rezultatų pagrindu vėliau yra priimami sprendimai. Žmogaus įsikišimas į šį procesą paprastai būna nereikšmingas, o kai kuriais atvejais jo galima visiškai atsisakyti. Tačiau konkretaus sprendimo poveikis konkrečiam asmeniui gali būti labai svarbus, nes jis nulems jo gyvenimo situaciją.

Todėl visiškai pasikliaujant ADS priimant sprendimus kyla nemažai etinių, politinių ir teisinių problemų. Dėl pavojaus, kad algoritminės sistemos perduos savo kūrėjų šališkumą, neribotas pasikliovimas technologijomis yra prieštaringai vertinamas, ypač tokiose srityse kaip užimtumas ar galimybė naudotis privačiomis ir viešosiomis paslaugomis (pvz., sveikatos priežiūra, kreditingumo vertinimo sistemos).

3.1.1. Ką gali padaryti asmuo, nukentėjęs nuo algoritminės diskriminacijos

Daroma prielaida, kad atrankos procese turėtų būti taikomos nuostatos dėl vienodo požiūrio įdarbinimo srityje (Lenkijoje šis klausimas reglamentuojamas Darbo kodekso 18 [3a] ir tolesniuose straipsniuose) ir diskriminacijos draudimo (Darbo kodekso 11 [3] straipsnis). Tai reiškia, kad bet kokia diskriminacija įdarbinant (ypač dėl lyties, amžiaus, negalios, rasės, religijos, pilietybės, politinių įsitikinimų, narystės profesinėse sąjungose, etninės kilmės, religijos, seksualinės orientacijos) yra nepriimtina.

Tačiau įdarbinimo procese pasitaiko diskriminavimo atvejų. Pavyzdžiui, pirmenybė teikiama kandidatams vyrams, atsisakoma įdarbinti jaunas ištekėjusias moteris ar moteris su vaikais arba įtraukiamos užsieniečius diskriminuojančios nuostatos. Išskirtiniai kriterijai gali būti tuo dažnesni, kuo daugiau įmonė naudoja el. atranką, pagrįstą automatizuotomis sprendimų priėmimo sistemomis. Tokiu atveju gali būti ne tik netyčia diskriminuojami kandidatai dėl šališko dirbtinio intelekto – įmonės vadovybė gali sąmoningai į sistemą įtraukti diskvalifikacinius kriterijus.

Jei įdarbinimo procese buvo diskriminacijos, pasireiškiančios draudžiamuoju skelbimo turiniu arba nediskretiškais klausimais apie privatų ir šeimyninį gyvenimą, nukentėjęs asmuo gali siekti savo interesų apsaugos teisme. Įrodinėjimo našta tokioje byloje tenka darbdaviui, o potencialus kandidatas turi tik įtikinamai įrodyti diskriminacijos faktą (Darbo kodekso 18 [3b] straipsnis). Jei teismas patvirtins pažeidimą, darbdavys privalės sumokėti diskriminuojamam asmeniui ne mažesnę kaip minimalaus darbo užmokesčio kompensaciją.

Tačiau, kai sprendimai priimami algoritmiškai, įrodyti ir pareikalauti nepagrįsto atmetimo atrankos procese yra daug sunkiau. Taip yra dėl vadinamosios juodosios dėžės problemos, t. y. dirbtinio intelekto priemonių veikimo skaidrumo trūkumo. Tai reiškia, kad dažnai net patys kūrėjai, taigi ir darbdaviai, diegiantys dirbtinio intelekto priemonę, nežino apie nepageidaujamą jos veikimą. Tačiau tai nereiškia, kad jie atleidžiami nuo atsakomybės už pažeidimus. Asmuo, kuris įtaria, kad algoritmas jį nepagrįstai atmetė, gali imtis konkrečių veiksmų, kad apgintų savo interesus ir pakeistų sistemos priimtą sprendimą.

Šiuo atžvilgiu svarbiausias išlieka BDAR reglamento 22 straipsnis. Šiuo straipsniu nustatoma, kad duomenų valdytojas privalo įdiegti tinkamas priemones, skirtas apsaugoti duomenų (taigi ir sprendimų) subjektų teises, laisves ir teisėtus interesus, taip pat mechanizmus, leidžiančius konkrečiam asmeniui užginčyti sprendimą, pagrįstą tik automatizuotu duomenų tvarkymu.

Jei, jūsų manymu, jūsų paraiška el. atrankos metu buvo atmesta nepagrįstai:

1. Patikrinkite, ar sprendimas buvo visiškai automatizuotas. Šiuo tikslu atidžiai perskaitykite įdarbinimo sąlygas arba kreipkitės į įmonės personalo skyrių ir išsiaiškinkite, kaip algoritmas veikia darbo paraiškos teikimo procese.
2. Paprašykite įmonės (duomenų valdytojo) suteikti jums galimybę pateikti savo požiūrį ir paaiškinti, kodėl, jūsų nuomone, atmetimas buvo neteisingas.
3. Paprašykite, kad bendrovė paaiškintų savo sprendimą ir kad jūsų paraišką dar kartą peržiūrėtų žmogus. Administratorius privalo kuo greičiau (ne vėliau kaip per vieną mėnesį) atsakyti į tokį prašymą. Per vieną mėnesį administratorius taip pat turėtų jus informuoti, kad prašymas nebuvo patenkintas, ir nurodyti to priežastis.
4. Tačiau jei duomenų valdytojas ignoruoja prašymą arba atsakymas netenkina, galite kreiptis pagalbos į duomenų apsaugos institucijas ir pateikti skundą.
5. Be to, nepriklausomai nuo to, kaip vyksta procesas duomenų apsaugos institucijoje, turite teisę ginti savo teises civiliniame teisme. Jei manote, kad tvarkant jūsų duomenis pažeidžiamas įstatymas, galite pateikti ieškinį duomenų valdytojui arba duomenų tvarkytojui. Teisme galite reikalauti atlyginti žalą dėl duomenų apsaugos teisės aktų

pažeidimų, taip pat kelti diskriminacijos, dėl kurios padaryta turtinė ar neturtinė žala, klausimus.

3.1.2. Europos Sąjungos AI reglamentai ir įdarbinimo procesas

Kaip jau minėta, Dirbtinio intelekto reglamento projekte užimtumo ir žmogiškųjų išteklių valdymo klausimai įtraukti į didelės rizikos sistemų sąrašą. Tai reiškia, kad priemonės, skirtos bent jau automatiniam kandidato į darbo vietą vertinimui, turės pereiti specialų kelią, kad būtų suteiktas leidimas.

Daug įpareigojimų teks dirbtinio intelekto sistemų tiekėjams, kuriems bus taikomi griežti dirbtinio intelekto sistemų projektavimo, testavimo, audito ir sertifikavimo reikalavimai. Be to, tie, kurie naudoja tiekėjų pasiūlytas dirbtinio intelekto sistemas (pvz., įmonės), privalės jas naudoti pagal teisės aktus ir naudojimo instrukcijas, užtikrinti į sistemas įvestų duomenų adekvatumą, jų stebėseną ir įvykių žurnalų saugojimą incidentų atveju.

Tikimasi, kad naujieji reikalavimai suteiks papildomų apsaugos priemonių nuo diskriminacinių sprendimų, kuriems trūksta žmogiškojo veiksnio. Tuo pat metu DI įstatymu nesuteikiama papildomų įgaliojimų patiems subjektams, kuriems tokie sprendimai daro poveikį. Vis dėlto ES sistemą papildys planuojama DI atsakomybės direktyva (*AI Liability Directive*, AILD), kurioje pirmą kartą bus įtvirtintos nuostatos dėl dirbtinio intelekto sistemų padarytos žalos atlyginimo. Ja siekiama nustatyti platesnę asmenų, kuriems žalą padarė taikomas dirbtinis intelektas, apsaugą ir palengvinti jų teisių gynimą. Taigi siūlomos taisyklės yra žingsnis į priekį siekiant užtikrinti veiksmingą galimybę pasinaudoti teisių gynimo priemonėmis ir diskriminacijos naudojant dirbtinio intelekto sistemas atvejais. Taip yra todėl, kad juose daroma prielaida, jog būtent darbdavys neįvykdė savo pareigos elgtis rūpestingai, nes naudojo įdarbinimo sistemą, kuri diskriminuoja tam tikrų kategorijų asmenis.

Darbas tiek su dirbtinio intelekto reglamento projektu (Dirbtinio intelekto įstatymas), ir Direktyvos dėl atsakomybės už dirbtinį intelektą rengimo darbai jau yra pažengę į priekį. Tačiau pagal dabartinę naujųjų reglamentų formuluotę jų nuostatos visose ES valstybėse narėse bus taikomos tik po dvejų metų nuo jų priėmimo.

3.2. Darbo ateitis

3.2.1. Nykstančios profesijos, ateities kompetencijos ir darbdavių atsakomybė už darbuotojų įgūdžių pritaikymą automatizavimui

Remiantis naujausiais Ekonominės politikos tyrimų centro (CEPR) atliktais tyrimais, net 40 proc. respondentų teigia, kad per ateinantį dešimtmetį juos daugiau nei 50 proc. pakeis mašinos, robotai ar algoritmai. Baimė dėl technologinio nedarbo nėra visiškai nepagrįsta. *Darbo vietų ateities (Future Jobs)* ataskaitos duomenimis, naujų technologijų dalis atliekamose užduotyse gerokai didėja. 2018 m. vidutiniškai 71 proc. darbo laiko sudarė žmogaus atliekama veikla ir 29 proc. mašinų atliekama veikla. Prognozuojama, kad iki 2025 m. šios proporcijos gerokai pasikeis. Žmonės bus atsakingi už maždaug 48 % veiklos, o likusieji 52 % užduočių bus visiškai automatizuoti.

Kalbant apie automatizavimo poveikį, galima daryti prielaidą, kad labiausiai nukentės dirbantys fizinį darbą, kurį lengvai gali pakeisti robotai (t. y. darbą, pagrįstą nuspėjama seka). Tačiau skaitmeninimas gali paveikti ir kai kuriuos specialistus. Remiantis *Darbo vietų ateities* ataskaita, tarp atleidžiamų profesijų, pavyzdžiui, mechaniko, sandėlininko ir gamybos vadovo, taip pat rasime finansų analitiką ar tarnautoją. Tačiau McKinsey pasaulinio instituto ekspertai šiuos nuogąstavimus sušvelnina, nes manoma, kad pasaulyje bus visiškai panaikinta tik 5 proc. profesijų.

Neabejotinai keisis darbo pareigų atlikimo būdas (vis didesnė IT sistemų ir mašinų dalis atliekamose pareigose) ir pageidaujamos darbuotojų kompetencijos. Atsižvelgiant į tai, kad daugelį užduočių atliks mašinos, didės įgūdžių, kurių kompiuteriai negali tiksliai atkurti, poreikis. Kalbame apie minkštąsias kompetencijas, t. y. tas, kurioms reikia kūrybiškumo, emocinio intelekto, kritinio mąstymo. Skaitmeninimas taip pat padidins techninių įgūdžių paklausą ir sukurs darbo vietų gerai kvalifikuotiems darbuotojams, gebantiems valdyti naujas sistemas. Kita vertus, tai gali kelti susirūpinimą dėl didėjančios rinkos poliarizacijos (žemesnio rango darbininkų menkavertiškumo, didėjant geriausiai išsilavinusių darbuotojų svarbai). Atrodo, kad šiuos nuogąstavimus patvirtina Europos profesinio mokymo plėtros centro (Cedefop) atlikto tyrimo rezultatai, kurie parodė, kad daugiau nei 70 % dirbančiųjų reikia bent pagrindinių IT įgūdžių, kad jie rastų savo vietą šiuolaikinėje darbo rinkoje, tačiau net 30 % gresia pavojus, kad jie visam laikui negalės įgyti reikiamų kompetencijų (ir dėl to praras darbą).

3.2.2. Būsimų ir nereikalingų profesijų kompetencijos skaitmeninimo amžiuje

Dėl didėjančio technologijų naudojimo artimiausiais metais labai keisis darbo rinkoje pageidaujamos kompetencijos. Prognozuojama, kad didėjant automatizavimui ir algoritmizavimui, mažės įgūdžių, kuriuos lengvai pakeis mašinos, paklausa. Šiuo atveju kalbame tiek apie fizinius įgūdžius (fizinių, gamybos darbuotojų atveju), tiek apie įgūdžius, susijusius su protiniu darbu (pvz., skaičiavimo ar kūrybinio rašymo įgūdžius). Kita vertus, didės **ateities kompetencijų,** kurios DELab ataskaitoje („*Ateities kompetencijos. Kaip jas formuoti lanksčioje švietimo ekosistemoje*?“), apibrėžtos kaip: *specifiniai gebėjimai imtis ir atlikti užduotis darbo aplinkoje, kuri iš esmės yra lanksti, geografiškai išsklaidyta, linkusi dažnai ir greitai keistis, apimanti poreikį naudotis skaitmeninėmis technologijomis ir bendradarbiauti su automatizuotomis sistemomis ir mašinomis, naudojančiomis dirbtinį intelektą*.

„McKinsey“ šias kompetencijas suskirstė į tris grupes: technines ir skaitmenines, socialines ir kognityvines.

Ateities kompetencijos	
Techninės ir skaitmeninės	• Manoma, kad **pagrindinių** skaitmeninių įgūdžių paklausa padidės 65 proc. Kalbame apie gebėjimą naudotis technologijomis kasdieniame darbe, ypač problemų sprendimo ir informacijos paieškos srityse. • Iki 2030 m. darbuotojai Europoje daugiau nei 40 proc. daugiau laiko skirs veiklai, kurioje naudojami pažangūs skaitmeniniai įgūdžiai. Be to, programavimo ir IT įgūdžių paklausa padidės 90 proc.
Socialinės	• Iki 2030 m. Europos darbo rinkoje socialinių kompetencijų, ypač verslumo ir gebėjimo imtis iniciatyvos, poreikis padidės 22 proc.
Kognityvinės (aukštesniosios): kritinis mąstymas, kūrybiškumas, gebėjimas valdyti žmones.	• Iki 2030 m. aukštesnių pažintinių gebėjimų poreikis padidės 14 proc. Tuo pat metu pagrindinių pažinimo įgūdžių, tokių kaip skaitymas, rašymas ir pagrindinis duomenų apdorojimas, svarba sumažės 23 proc.

Kompetencje przyszłości w podziale na trzy grupy umiejętności: poznawcze, społeczne i techniczne

Pasaulio ekonomikos forumas (WFE) nurodo, kad tokie įgūdžiai, kaip:

- **personalo valdymas (ŽI)** – darbo jėgos formavimas ieškant geriausių žmonių konkrečioms užduotims atlikti; žmonių motyvavimas ir valdymas jiems dirbant,
- **derybų įgūdžiai** – gebėjimas spręsti konfliktus ir įveikti nuomonių skirtumus; gebėjimas įtikinti,
- **emocinis intelektas** – gebėjimas atpažinti ir įvardinti savo emocijas, kitų žmonių emocijas; gebėjimas valdyti ir naudoti emocijas priimant vertinimus ir sprendimus; kitų žmonių (darbuotojų ir klientų) poreikių supratimas,
- **bendradarbiavimas su kitais** – gebėjimas dirbti grupėje,
- **kognityvinis lankstumas** – gebėjimas „persijungti“ iš vienos užduoties į kitą,
- **sudėtingų problemų sprendimas** – gebėjimas rasti neakivaizdžius sprendimus įvairiomis aplinkybėmis,
- **kritinis mąstymas** – logikos ir argumentacijos naudojimas siekiant nustatyti alternatyvių sprendimų, išvadų ar požiūrių į problemas privalumus ir trūkumus,
- **kūrybiškumas – gebėjimas** mąstyti nestandartiškai, siūlyti novatoriškas idėjas, spręsti problemas neakivaizdžiais būdais.

Be to, WFE savo ataskaitoje taip pat išvardijo **profesijas, kurios skaitmeninimo amžiuje praras svarbą**. Tai tokios profesijos kaip: duomenų įvesties tarnautojas, apskaitos ir darbo užmokesčio apskaitos tarnautojas, administracijos ir vykdomasis sekretorius, surinkimo ir gamybos tarnautojas, informacijos ir klientų aptarnavimo tarnautojas, administracinių ir verslo paslaugų vadybininkas, buhalteris ir auditorius, sandėlininkas, vyriausiasis vadybininkas ir operacijų vadovas, pašto tarnautojas, finansų analitikas, kasininkas ir bilietų kontrolierius, mechanikas, telemarketingo specialistas, elektronikos ir telekomunikacijų montuotojas, bankininkas, vairuotojas, brokeris ir prekybos agentas, išvežiojantysis pardavėjas ir agitatorius, draudimo, statistikos ir finansų tarnautojas, teisininkas.

3.2.3. Skaitmeninimas ir verslo valdymo tendencijos - darbdavių vaidmuo

Norėdamos visapusiškai pasinaudoti skaitmeninimo ir naujų technologijų diegimo teikiamais privalumais, įmonės turės pertvarkyti savo struktūras ir pakeisti dabartinį požiūrį į darbą. Tam reikės pertvarkyti formalią įmonės organizaciją, papildyti darbuotojų, turinčių naujų kompetencijų, perkvalifikuoti arba ugdyti esamus talentus. Pasak McKinsey, dėl pageidaujamų profesijų kaitos ir labiausiai vertinamų įgūdžių, organizacijoms teks įvesti **atnaujinimus penkiose pagrindinėse srityse** – mąstysenos, organizacinės struktūros, darbo paskirstymo, darbo jėgos sudėties ir valdymo bei personalo atsakomybės.

Kalbant apie įmonių mąstyseną, ateityje organizacijos sėkmę lems vadinamojo mokymosi visą gyvenimą (*lifelong learning*) tendencijos skatinimas, t. y. galimybė darbuotojams įgyti naujų įgūdžių ir žinių ne tik karjeros pradžioje, bet ir jos metu. Kalbant apie organizacinę struktūrą, kaip artimiausių metų prioritetai nurodomi dinamiškesnių ir inovatyvesnių valdymo būdų diegimas, taip pat dažnesnis komandų bendradarbiavimas ir dalijimasis žiniomis bei funkcijomis tarp darbuotojų.

Įmonės, plačiai diegiančios automatizavimą, taip pat tikisi, kad šiuo metu aukštos kvalifikacijos darbuotojų atliekamos užduotys bus perduotos žemesnės kvalifikacijos darbuotojams (padedamiems mašinų ir kompiuterių). Kalbant apie žmogiškuosius išteklius, tikimasi, kad bus dažniau pasitelkiami įvairūs laisvai samdomi ir laikini darbuotojai. Tai lems augsianti vadinamoji dalijimosi ekonomika ir (arba) ekonomika pagal pareikalavimą (*sharing economy; on-demand economy*), t. y. verslo modeliai, pagrįsti bendradarbiavimo platformomis, sukūrusiomis atviros prieigos rinką laikinam naudojimuisi prekėmis ar paslaugomis, kurias dažnai teikia privatūs asmenys.

Įmonės konkurencingumo išsaugojimas remiant darbuotojus skaitmeninimo procese

Ataskaitoje *Beyond Hiring. Kaip įmonės persikvalifikuoja, kad išspręstų talentų trūkumo problemą, „*McKinsey“ nurodė įvairias taktikas, kaip išlaikyti įmonių konkurencingumą ir sumažinti atotrūkį tarp pageidaujamų ir turimų privataus sektoriaus darbuotojų įgūdžių. Tarp praktikų, kurias turėtų apsvarstyti darbdaviai, siekiantys plėtoti verslą ir kurti kompetentingą darbo jėgą, buvo šios:

- **Perkvalifikavimas** – esamų darbuotojų naujų kompetencijų įgijimo ir esamų įgūdžių tobulinimo skatinimas, taip pat naujų darbuotojų pageidaujamų gebėjimų diegimas ir mokymas. Svarbiausias klausimas įmonėms bus apsispręsti, kokiu būdu bus vykdomas mokymas: įmonės viduje (naudojant turimus išteklius ir programas) ar išorėje (bendradarbiaujant su švietimo įstaiga ar mokymo centru). Kalbant apie sritis, į kurias verslininkai planuoja investuoti, jos dažniausiai susijusios su strategiškai svarbių įmonei gebėjimų ugdymu, t. y. pažangios IT kompetencijos, kūrybinio rašymo įgūdžiai, kritinis mąstymas, problemų sprendimo įgūdžiai. Kita vertus, kalbant apie mažiau sudėtingus įgūdžius, darbdaviai deklaruoja galimybę įdarbinti žmones ne iš įmonės.

- **Perkėlimas įmonės viduje** – specifinių įgūdžių turinčių darbuotojų perkėlimas į skyrius ir (arba) komandas, kuriose jie gali geriau panaudoti savo įgūdžius. 2018 m. vasario mėn. atliktos „McKinsey“ įmonių vadovų apklausos duomenimis. 55 proc. respondentų teigė, kad jie mieliau rinktųsi kai kurių darbuotojų perkėlimą į kitas ar visiškai naujas pareigas, nei visišką jų atleidimą.

- **Įdarbinimas** – asmenų ar ištisų komandų, turinčių reikiamų specifinių įgūdžių, paieška (nors ekspertų pasiūla rinkoje gali būti nepakankama, kad visos įmonės galėtų taikyti šią strategiją). Viena vertus, samdymo sąnaudos gali būti mažesnės nei perkvalifikavimo, tačiau, kita vertus, ieškant naujų komandos narių tenka rizikuoti, kaip asmuo dirbs. Todėl, norėdamos sėkmingai pritraukti naujų pagrindinių talentų, įmonės turėtų diegti naujoves kandidatų atrankoje, taip pat siūlyti patrauklią darbo kultūrą ir su darbo užmokesčiu nesusijusias lengvatas.

- **Naujų bendradarbiavimo formų kūrimas** – įmonės gali pasinaudoti įgūdžiais, kuriuos įgyja žmonės iš išorės (laisvai samdomi darbuotojai, ekspertai, laikini įdarbinimo agentūrų darbuotojai). Tačiau šio modelio trūkumas – rizika perduoti komercines paslaptis (pvz., praktinę patirtį, darbus, kuriems taikomos intelektinės nuosavybės teisės) pašaliniams asmenims, taip pat sunkumai prisitaikant prie įmonės kultūros ir darbo režimo. Dėl šios priežasties darbdaviai deklaruoja, kad su pagrindine įmonės veikla nesusijusias arba žemos kvalifikacijos reikalaujančias darbo vietas užima nepriklausomi rangovai.

- **Galimas atleidimas iš darbo** – kai kuriose įmonėse gali tekti atleisti darbuotojus, ypač tose pramonės šakose, kurios neauga pakankamai sparčiai ir kuriose automatizavimas iš esmės pakeis darbo jėgą. Atleidimų strategija gali būti įgyvendinama mažinant arba sustabdant naujų darbuotojų priėmimą, kartu leidžiant tęsti įprastą jau dirbančių darbuotojų išėjimo į pensiją procesą.

Nors atleidimai dėl didesnio mašinų naudojimo yra galimi, sunku tikėtis, kad visų sektorių darbuotojai turės baimintis dėl savo darbo vietų. Tačiau neabejotinai atsiras naujų technologijų, sistemų ir programų, dėl kurių reikės įgyti papildomų IT įgūdžių.

Kaip darbdaviai gali padėti savo darbuotojams skaitmeninti įmonę? Visų pirma, jie gali:

- supažindinti darbuotojus su naujais įrankiais – pašalinti baimę ir konservatyvumą naujų technologijų atžvilgiu ir parodyti, kaip skaitmeniniai įrankiai gali būti naudojami kasdieniame darbe,
- didinti darbuotojų informuotumą – paaiškinti, kodėl ir kaip įmonė naudoja technologijas; turėdami informacijos šioje srityje, darbuotojai geriau supras naujas darbo priemones ir bus motyvuoti jomis naudotis,
- gerai parengti vadovus būsimiems pokyčiams – vadovai turėtų žinoti atsakymus į pagrindinius klausimus apie naujas darbo priemones ir parodyti kitiems komandos nariams, kaip naudotis diegiamomis technologijomis,
- net ir gerai technologijas išmanantiems darbuotojams reikia laiko susipažinti su nauja programine įranga ir skaitmeniniais įrankiais, kuriais jie anksčiau nesinaudojo; įmonė turėtų rengti profesionalius mokymus visiems darbuotojams.

3.2.4. Kiti subjektai, atliekantys svarbų vaidmenį skaitmeninant darbą ir perkvalifikuojant darbuotojus

Švietimo įstaigos

Švietimo vaidmenį skaitmeninimo procese jau pripažino Europos Sąjungos institucijos. Europos Vadovų Tarybos išvadose pabrėžiama, kad galimybė įgyti aukštos kokybės skaitmeninėmis technologijomis paremtą išsilavinimą yra būtina atskirų sektorių pertvarkos ir tolesnio ekonomikos augimo sąlyga.

Be to, Europos Komisija numatė parengti 2021-2027 m. skaitmeninio švietimo veiksmų planą, kuriame būtų išdėstyta skaitmeninio švietimo Europoje vizija. Abiejų iniciatyvų tikslas – paskatinti universitetus, mokyklas ir dėstytojus aktyviau dalyvauti ugdant skaitmeninius gebėjimus ir tenkinant darbo rinkos poreikius. Šių institucijų vaidmenį skaitmeninės transformacijos procese, regis, patvirtina ir ekonominiai leidiniai, pavyzdžiui, PwC ir WFE ataskaita *„Kvalifikacijų kėlimas bendram labui“* (*„Raising Skills for Shared Prosperity“,* 2021 m.), kurioje pabrėžiama, kad aukštojo mokslo institucijos turi potencialą skatinti pokyčius - didinti bendrą studentų ir visuomenės žinių, įgūdžių ir kompetencijų lygį.

Viešosios valdžios institucija

Valstybės vaidmuo – remti verslininkus ir darbuotojus skaitmeninimo procese. Todėl svarbu, kad valdantieji įgyvendintų politiką, skatinančią įgyti skaitmeninių įgūdžių arba perkvalifikuoti darbuotojus (pavyzdžiui, įgyvendinant mokymo subsidijų programas mažosioms ir vidutinėms įmonėms). Be to, svarbu skatinti darbo rinką ir išvengti nedarbo vykdant aktyvią užimtumo politiką – užuot pasikliovus bedarbio pašalpomis, valstybė turėtų investuoti į įdarbinimo agentūras, kurios taptų įdarbinimo centrais ir palengvintų bedarbių perkvalifikavimą.

Nevyriausybinės organizacijos

Nevyriausybinės organizacijos ir analitiniai centrai dažnai veikia kaip socialiai naudingų sprendimų inkubatoriai. Jos paprastai turi didesnę veiksmų laisvę nei valstybinės institucijos ir gali siūlyti kitokius problemų sprendimus. Dėl šios priežasties kai kurios įmonės imasi filantropinių iniciatyvų arba bendradarbiauja su fondais tose srityse, kurios susijusios su darbuotojų naujų įgūdžių įgijimu. Kaip pavyzdį galima paminėti iniciatyvą „Generation“, kuria siekiama kovoti su nedarbu mažinant jaunimo įgūdžių trūkumą, taip pat padėti suaugusiesiems rasti tinkamą darbą juos įdarbinant, mokant ir konsultuojant.

Profesinės sąjungos ir sektorių organizacijos

Profesinės sąjungos ir sektorių asociacijos, veikdamos kaip socialiniai partneriai, atlieka svarbų vaidmenį skaitmeninant darbo rinką. Pavyzdžiui, Švedijoje steigiamos įmonių ir profesinių sąjungų finansuojamos darbo apsaugos tarybos. Šie subjektai moko darbo netekusius asmenis - teikia jiems laikiną finansinę paramą ir palengvina perkvalifikavimo procesą, kad bedarbiai greičiau grįžtų į darbo rinką.

3.3. Nauji verslo modeliai ir jų poveikis darbo rinkai

3.3.1. Darbuotojų derybinių galių mažėjimas - kaip dėl naujų technologijų darbuotojams sunkiau jungtis į profesines sąjungas

Naujosios technologijos palengvina bendravimą ir sujungia vartotojus, nepaisant juos skiriančio atstumo. Tačiau tuo pat metu jos didina susvetimėjimą ir mažina žmonių bendravimą. Šis reiškinys būdingas ne tik asmeninio, bet ir profesinio gyvenimo sričiai. Skaitmeninimas ir darbo perkėlimas į internetinį pasaulį lėmė, kad darbuotojai epizodiškai užmezga ilgalaikius santykius, rečiau susitinka ir aptaria problemas darbovietėje.

Naujosios technologijos skatina izoliaciją ne tik dirbant nuotoliniu būdu. Įmonių naudojamos dirbtinio intelekto priemonės, skirtos darbuotojų kontrolei ir jų produktyvumui matuoti, taip pat dažnai naudojamos darbuotojų asociacijoms slopinti ir trukdyti.

Kartais pasitaiko atvejų, kai didelių įmonių verslo modeliai grindžiami plataus masto darbuotojų kontrole ir nuolatiniu darbo tempo didinimu. Todėl darbuotojų susivienijimas į profesines sąjungas, siekiant atstovauti jų kolektyvinėms ir individualioms teisėms ir interesams, kelia realų pavojų sistemai, kuri rūpinasi tik įmonių pelno didinimu. Dėl šios priežasties korporacijos imasi priemonių, kad neleistų darbuotojams jungtis į profesines sąjungas. Ši praktika suintensyvėjo per COVID-19 pandemiją, kai per tą laikotarpį įvestos sveikatos ir saugos rekomendacijos pradėtos taikyti darbovietėse, siekiant įdiegti priemones, kuriomis matuojamas atstumas tarp žmonių sandėliuose, kartu draudžiant jiems būti per arti vienas kito. Įmonės pradėjo įsigyti programinę įrangą, kuri suteikė galimybę analizuoti ir vizualizuoti duomenis apie santykius darbo vietose (pvz., geoSPatial Operating Console arba SPOC). Be to, žmogiškųjų išteklių skyriai stebėjo aktyvistiniais tikslais naudojamus darbuotojų pašto sąrašus arba darbuotojų grupes socialinėje žiniasklaidoje.

Kalbant apie platforminį darbą, naujų technologijų poveikis darbuotojų asociacijoms nėra vienareikšmiškai teigiamas ar neigiamas. Paslaugoms teikti naudojamos programėlės gali palengvinti kurjerių ir vairuotojų darbą – jų sistemose esantys vidiniai pokalbių kambariai suteikia platformų darbuotojams (angl. *gig-workers*) erdvę keistis informacija, o masinės komunikacijos tinklai gali sujungti atskirus kurjerius miestų, regionų ir net šalių lygmeniu.

Kartu platformų darbuotojų profesinių sąjungų veiksmingumas dažnai priklauso nuo valdžios institucijų paramos įvairioms saviorganizacijos formoms. Pavyzdžiui, Bolonijoje bendradarbiaujant su profesinių sąjungų atstovais buvo sukurta *Skaitmeninio darbo miesto sąlygomis pagrindinių teisių chartija* (it. *Carta dei diritti fondamentali del lavoro digitale nel Contesto Urbano),* nustatanti minimalių platformų darbuotojų darbo užmokesčio, darbo laiko ir

draudimo apsaugos standartų sistemą. Reikšminga tai, kad pats Bolonijos meras išreiškė didelę paramą šiai iniciatyvai ir paragino klientus boikotuoti platformas, kurios nepasirašė chartijos.

Šalyse, kuriose valstybė nesirūpina platformų darbuotojais, jų profsąjungų lygis yra daug žemesnis, o jų derybinė galia mažesnė. Tuo kartais piktnaudžiauja platformos, kurios naudoja programėlėse esančius mechanizmus, kad geriau kontroliuotų kurjerius ar vairuotojus ir užkirstų kelią bandymams pasipriešinti įmonės politikai.

Pavyzdys, kaip dalijimosi ekonomikos milžinai naudojasi technologijomis, kad apribotų už savo teises kovojančių darbuotojų iniciatyvas, yra 2021 m. balandžio mėn. greitai nutildytas Lenkijos maisto pristatymo kurjerių streikas. Streiko priežastis buvo nesąžiningas užsakymų paskirstymo ir apmokėjimo algoritmas, o protesto būdas – kurjeriai nustojo vykdyti užsakymus, nors deklaravo norą dirbti programėlėje. Vairuotojai tikėjosi daryti spaudimą bendrovei ir priversti ją kalbėtis su bendruomenės atstovais. Tačiau įmonė, naudodamasi programėle, nesistengdama bendrauti su kurjeriais, užblokavo streikuotojus ir perdavė jų užsakymus žmonėms, kurie, nepaisant skaudžių sąlygų, buvo pasirengę dirbti.

3.3.2. Skaitmeninimo poveikis darbo rinkai – darbas platformoje

Darbas per platformą – tai įdarbinimo forma, kai darbuotojas naudojasi skaitmenine platforma, kad už tam tikrą atlyginimą galėtų naudotis kitų organizacijų ar asmenų teikiamomis paslaugomis. Skaitmeninėse platformose už atlygį atliekamos tokios užduotys kaip taksi ir kurjerių paslaugos, prekių pristatymas, namų remonto paslaugos, taip pat protiniai darbai, pavyzdžiui, tekstų rašymas ir buhalterinė apskaita. Nors tokios programėlės, kaip „Uber“ ir „Bolt“, Europos erdvėje veikia tik dešimtmetį, tai darbuotojai, teikiantys paslaugas per tokio pobūdžio platformas, dabar sudaro didelę darbo jėgos dalį (2022 m. Europos Sąjungoje - 28,3 mln. darbuotojų). Tai panašus skaičius kaip ir pramonės gamybos sektoriuose dirbančių žmonių (29 mln. darbuotojų). Be to, Europos Komisijos duomenimis, tikimasi, kad iki 2025 m. platformose dirbs dar 15 mln. darbuotojų. Populiariausios platformos ES yra „Uber“, „Deliveroo“, „Amazon Mechanical Turk“, „Fiverr“, „Upwork“, „Appjobs“, „Glovo“ arba „JustEat“ (Lenkijoje žinoma kaip „Pyszne.pl“).

Darbo platformų verslo modelis grindžiamas technologijomis, kurios naudoja algoritmus, kad veiksmingai suderintų darbuotojų ir jų teikiamų paslaugų pasiūlą ir paklausą. Be to, naudojant tinkamai parengtas taikomąsias programas, galima be kontaktų, automatizuotai priimti sprendimus ir stebėti atliekamas užduotis. Naudojant algoritmais grindžiamą valdymo sistemą, galima atsisakyti tradicinių vadovaujančių darbuotojų. Tai savo ruožtu verčia platformas tvirtinti, kad jos veikia tik kaip tarpininkas, siūlantis paslaugas, skirtas sujungti savarankiškai dirbančius asmenis su potencialiais klientais, o ne kaip darbdavys.

Kas dažniausiai ieško darbo per darbo platformas?

- jaunimas,
- vyrai,
- imigrantai (ypač dirbantys fizinį darbą),
- asmenys, turintys aukštąjį išsilavinimą, kuriems šis darbas yra papildomas pajamų šaltinis.

Be to, platformų darbuotojus darbo rinkoje galima suskirstyti į dvi kraštutines grupes. Pirmajai grupei priklauso protiniai darbuotojai, privilegijuoti pagal savo kompetenciją, pavyzdžiui, programuotojai, galintys daryti įtaką bendradarbiavimo su klientais sąlygoms (laisvai samdomi darbuotojai, IT paslaugų teikėjai). Kita vertus, antrajai grupei priskiriami žmonės, kurių kompetencija yra žema, lengvai pakeičiama ir kurių derybinė galia darbo rinkoje yra nedidelė (pvz., imigrantai, teikiantys taksi paslaugas).

Darbo su platformomis privalumai ir trūkumai

Darbo su platformomis privalumai:

- lanksčios darbo valandos ir galimybė planuoti savo darbo grafiką,
- tiesioginis bendravimas su užsakovu,
- didesnis savarankiškumas.

Tačiau šiuo metu skaitmeninės platformos turi nemažai trūkumų:

- Sveikatos ir saugos klausimai:
    - nėra reglamentuotų sveikatos ir saugos taisyklių,
    - fizinė rizika,
    - stresas, kurį sukelia nesaugus darbas;
- įdarbinimo sąlygos:
    - 5,5 mln. žmonių, dirbančių per darbo platformas ES, yra neteisingai klasifikuojami kaip savarankiškai dirbantys asmenys,
    - asmenys, neteisingai priskirti savarankiškai dirbantiems asmenims, neturi teisės į tas pačias teises ir išmokas kaip dirbantieji pagal darbo sutartį;

- problemos, kylančios dėl darbo algoritmizavimo,
- ribotos asociacijos galimybės,
- nenuspėjamas darbo užmokestis ir darbo valandos (Europos Komisijos duomenimis, 41 % platformų darbuotojų darbo laiko sudaro neapmokamos užduotys, pavyzdžiui, skelbimų peržiūra arba užsakymų laukimas).

ES teisė ir darbas platformose

Kai kurios valstybės narės jau nustatė darbo platformose taisykles nacionaliniuose teisės aktuose. Diskusijos dėl šios konkrečios įdarbinimo rūšies taip pat vyksta Bendrijos lygmeniu. Platformos darbuotojų sąvoka jau įtraukta į ES teisės aktus, pavyzdžiui, į Direktyvą dėl skaidrių ir nuspėjamų darbo sąlygų Europos Sąjungoje. Tačiau šiuo požiūriu proveržis turi būti pasiektas **Direktyva dėl platformų darbuotojų darbo sąlygų gerinimo**, kurios projektą Europos Komisija pateikė 2021 m. pabaigoje.

Pagrindinės direktyvos projekto nuostatos dėl platformų darbo sąlygų gerinimo:

- Per skaitmenines platformas dirbantiems asmenims bus suteiktas jų faktines darbo sąlygas atitinkantis įdarbinimo statusas, kuris bus tikrinamas nustatant kriterijus, reikalingus platformai pripažinti darbdaviu.
- Platforma bus laikoma darbdaviu, jei atitiks bent du iš šių kriterijų:
    - nustato atlyginimo dydį arba nustato jo viršutinę ribą,
    - elektroninėmis priemonėmis prižiūri darbo vykdymą,
    - riboja laisvę pasirinkti darbo valandas ar nedarbingumo laikotarpius, laisvę priimti ar atsisakyti užduočių arba laisvę naudotis subrangovais ar pakaitiniais darbuotojais,
    - nustatomos konkrečios privalomos išvaizdos ir elgesio su paslaugos gavėju arba darbo užsakovu taisyklės,
    - riboja galimybę plėsti klientų ratą arba atlikti darbus trečiosioms šalims.
- Platformos darbuotojams turėtų būti suteikiamos darbo ir socialinės teisės, atsižvelgiant į jų užimtumo statusą:
    - garantuotas poilsio laikas ir apmokamos atostogos,
    - minimalus darbo užmokestis,
    - kolektyvinių derybų galimybė,

- sauga ir sveikatos apsauga,
- nedarbo ir ligos pašalpos,
- įmokomis pagrįstos pensijos.

- Platforma gali užginčyti klasifikavimą, tačiau turi įrodyti, kad darbo santykiai neegzistuoja.
- Platformos turės didinti algoritmų naudojimo skaidrumą ir užtikrinti, kad darbo sąlygas stebėtų žmonės.
- Darbuotojai įgis teisę ginčyti automatizuotus sprendimus

Pastabos

Pastabos

Pastabos

Pastabos

Pastabos

Pastabos

Komisja Krajowa NSZZ „Solidarność”
ul. Wały Piastowskie 24, 80-855 Gdansk

Biuro Programów Europejskich
www.solidarnosc.org.pl

ДИГИТАЛИЗАЦИЈА НА ПАЗАРОТ НА ТРУДОТ

Модул за обука развиен во рамките на проектот
Иницирање активности за имплементирање на Рамковниот договор на европските социјални партнери за дигитализација
Кофинансиран од Европската Унија

MK

Co-funded by the European Union

NSZZ Solidarność Komisja Krajowa

KCC

Дигитализација на пазарот на трудот

Модул за обука развиен во рамките на проектот

Иницирање активности за имплементирање на Рамковниот договор на европските социјални партнери за дигитализација

Кофинансиран од Европската Унија

Co-funded by the European Union

Јуни 2023

Автори:

Бланка Вавжињак

Марта Мусидловска

Поддршка:

Ханна Сакович-Дашчињска

Редакција:

Јулиа Залеска

Графички дизајн, печатење:

PP WiB Piotr Winczewski

ph. +48 58 341 99 89, e-mail: wib1@wp.pl

Извори:

robot hand finger /rawpixel.com/freepik.com

Tesla Robot Dance / wikimedia.org

factory worker portrait / aleksandarlittlewolf/ freepik.com

AI used in this publication: freepik.com

Бесплатно издание, финансирано од средства на Европската Унија во рамките на проектот со бр. 101051759 **„Иницирање активности за спроведување на Рамковниот договор на европските социјални партнери за дигитализација (ЕФАД)“**. Оригинален наслов:

„Initiating activites to implement the European Social Partners Framework Agreement on Digitalisation (EFAD)“

Воведна забелешка

Оваа публикација е создадена во рамките на проектот „Иницирање активности за спроведување на Рамковниот договор на европските социјални партнери за дигитализација“. Таа претставува прирачник што ќе се користи и за време на обуката и по завршување на обуката од проектот. Модулот за обука има за цел да ги подготви социјалните партнери за динамичните промени што се случуваат на пазарот на трудот во врска со дигиталната трансформација. Тие, меѓу другото, вклучуваат промени во врска со автоматизацијата на производството, нови деловни модели, работа од далечина и иновативни методи на управување во компаниите. Публикацијата вклучува и дискусија за правата на вработените во дигиталната ера. Нејзината цел е да ги опреми вработените со алатки за исклучување и одржување рамнотежа помеѓу приватниот и професионалниот живот.

Содржина

Вовед

Додека вештачката интелигенција (ВИ) е широк поим што опфаќа група алгоритми што можат да ги модифицираат нивните параметри и да произведуваат нови резултати, наједноставно може да се дефинира како способност на машините да разбираат, учат, планираат и да бидат креативни.

За многу експерти, темпото на развој на вештачката интелигенција и нејзиното влијание врз светот околу нас изгледаат загрижувачки. На ова, меѓу другото, влијае фактот дека системите за вештачка интелигенција се создадени од најголемите технолошки компании од САД и Кина, кои даваат приоритет на нивниот комерцијален профит. Самите претставници на технолошката индустрија предупредуваат на опасностите поврзани со неограниченият развој на вештачката интелигенција. Во отвореното писмо во кое се повикува на суспензија на експериментите на системи со вештачка интелигенција и системите помоќни од Chat GPT-4 се потпишани, меѓу другите и, луѓе како Илон Маск (извршен директор на SpaceX, Tesla и Twitter), Стив Возниаак (ко-основач на Apple) или Јувал Ноа Харари (футурист, професор на Хебрејскиот универзитет во Ерусалим).

Контролирањето на развојот на вештачката интелигенција е од суштинско значење за да се осигура безбедноста на системите за вештачка интелигенција и гаранција дека тие го земаат предвид нејзиното влијание врз благосостојбата на луѓето. Сепак, во мноштвото информации што се однесуваат на вештачката интелигенција, најалармантните визии, што незадолжително се базираат на реалноста, доаѓаат до израз во прв план. Ова, пак, води до скептични мислења за новите технологии, страв од масовна невработеност и неподготвеност да се користат дигитални алатки. Сепак, треба да се запомни дека, технологијата сега е нераскинлив дел од секојдневниот живот. Таа не е само извор на забава, туку и достапност на алатки за олеснување на извршувањето на домашните и професионалните обврски. Поради оваа причина, усвојувањето иновативни решенија и едукацијата на општеството за нивна правилна употреба е исклучително важна.

Активностите за подигање на свеста треба, исто така (или првенствено), да се однесуваат на дигиталните алатки што се користат на работното место. Како што ќе биде наведено во понатамошниот текст на прирачникот, новите технологии се користат во многу сектори и во различни етапи од работниот однос (од регрутирање до евалуација на вработените). Тие ги олеснуваат процесите, како на управување со компанијата, така и секојдневната работа на многу луѓе (како кај физички работници, така и кај канцелариски работници). Најдобар пример за ова е широката употреба на машински јазични преведувачи, како што се Google Translate или Deepl, што ја подобруваат прекуграничната

комуникација помеѓу компаниите или овозможуваат превод на стручни текстови без потреба од користење на услугите на професионален преведувач.

Сè повеќе надежи за подобрување на работата се полагаат и во генеративната вештачка интелигенција. Апликациите како Chat GPT или DALL-E веќе се користат за креативни задачи, како што се пишување електронски пораки или спроведување анализа на податоци. На пример, користењето на генеративната вештачка интелигенција овозможува побрза анализа на содржината на статија или да се сними текот на состанокот за само еден момент. Откако ќе ја издадете соодветната команда (на пр. „дај ги главните заклучоци од дискусијата“) и ќе ги внесете основните параметри во системот, можете да очекувате генерирање на очекуваните резултати (заклучоци).

Истовремено, треба да се запомни дека јазичните модели Large Language Models (LLM), како што е Chat GPT, покрај тоа што создаваат содржини што звучат природно, сепак ги генерираат автоматски и безрефлексно. Ова, од друга страна, наложува создавање текстови од страна на алгоритми, при што е многу веродостојно да содржат многу грешки. Поради ова, од особена важност е да се развијат вештини за критичко размислување кај корисниците, способност за анализирање на реалното опкружување и филтрирање на она што е невистинито (на пример, лажни вести). Дополнително, во работата во дигиталната ера, освен подготовката на вработените во различни сектори за автоматизација и опремување со нови компетенции, неопходно е вработените да се научат како да коегзистираат со технологиите и способноста за „исклучување“. Тоа се условите за правилна рамнотежа помеѓу приватниот и професионалниот живот.

Овој труд е создаден на крајот на 2022 и на почетокот на 2023 година. Имајќи го предвид динамичниот развој на иновациите, особено на алатките за вештачка интелигенција (ВИ), авторите на прирачникот сакаат да истакнат дека некои од содржините може да станат застарени во наредните месеци и години како резултат на техничкиот напредок.

Речник на термини

AI Act/Закон за вештачка интелегенција

– Регулатива на ЕУ со која се воспоставуваат усогласени правила што се однесуваат на вештачката интелигенција.

Алгоритам

– збир на инструкции (компјутерска формула) што автономно донесуваат одлуки врз основа на статистички модели или правила за одлучување, без експлицитна човечка интервенција.

Анонимизација

– процес што се базира на трансформација на личните податоци на начин што спречува нивно доделување на веќе идентификувано лице или физичко лице кое може да се идентификува.

Автоматизација

– користење на технологијата за контрола на производството и создавање производи и услуги користејќи дигитални алатки.

Блокчејн / Blockchain

– т.н синџир на блокови, технологија што се користи за пренос и складирање информации за интернет-трансакции; регистар на децентрализирани податоци што се споделуваат безбедно. Блокчејн технологијата им овозможува на група избрани учесници да споделуваат податоци.

***Bring your own device* (BYOD)**

- тренд што се заснова врз користење приватни уреди како лаптопи, паметни телефони или таблети за извршување професионални должности.

Chat GPT

– алатка што користи вештачка интелигенција (chatbot), која што во формулата налик на

дијалог ви овозможува да добивате одговори на прашања поставени на природен јазик од корисникот.

Лични податоци – секоја информација што се однесува на идентификувано или живо физичко лице кое може да се идентификува (индивидуални информации кои, при комбинирање, може да доведат до идентификација на дадено лице, истовремено се тоа лични податоци).

Дипфејк *(анг. Deep fake)*

– од две англиски фрази: *deep learning (*длабоко учење) и *fake* (лажно/невистинито).

Станува збор за обработка на звук и слика насочена кон создавање лажна порака користејќи техники на вештачка интелигенција. Ова овозможува подготовка на материјали што ќе биде тешко или невозможно да се разликуваат од видеата или фотографиите создадени на традиционални начини и со учество на вистински лица.

Големи јазични модели (LLM*, ang. Large Language Models)*

– модели на машинско учење способни за извршување различни задачи во однос на обработка на природниот јазик. Обуката за таков систем се состои во обезбедување големи количини на податоци (на пр. книги, статии, веб-страници), благодарение на кои, може да научи фрази и поврзувања меѓу зборовите со цел генерирање нова содржина во иднина. Пример за LLM е GPT Chat, кој беше развиен од страна на OpenAI и објавен во јавноста во ноември 2022 година. Овој модел може да обработува информации и да генерира текст сличен на текстот напишан од човек, како одговор на барањата на корисниците.

Лажни вести *(анг. Fake news)*

– невистинити или делумно невистинити информации од сензационална природа што целно го водат примачот/читателот во заблуда.

Економија на споделување/економија на барање (*sharing economy*; *on-demand economy*)

– збир на деловни модели засновани врз посредување на платформи за соработка, создавајќи општо достапен пазар за привремено користење стоки или услуги што често ги обезбедуваат приватни лица.

Компетенции на иднината

– специфични вештини што овозможуваат преземање и реализирање задачи во работна средина која е фундаментално флексибилна, географски дисперзирана, склона кон чести и брзи промени и подразбира неопходност од управување со дигитални технологии и соработка со автоматизирани системи и машини што користат вештачка интелигенција.

Мобинг *(анг. Mobbing)*

– дејствија или однесувања насочени кон вработениот што се состојат од постојано и долгорочно вознемирување или заплашување.

Работа на платформа

– форма на вработување, во чиишто рамки вработениот користи дигитална платформа за да добие пристап до други организации или поединци со цел обезбедување конкретни услуги, а за возврат добива награда. Задачите што се извршуваат со плаќање преку дигитални платформи вклучуваат, меѓу другото: такси и курирски транспорт, испораки, услуги за поправки во домот, како и канцелариска работа, како што е copywriting или сметководство.

Поддржана работа

– работа при која некои активности може да бидат извршени од страна на роботи, додека други бараат учество на човечки фактор.

Право на исклучување

– право да не се вклучите во работни задачи надвор од работното време и да не учествувате во комуникација реализирана преку дигитални алатки.

Профилирање

– секој облик на автоматизирана обработка на лични податоци што се состои во нивно користење за проценка на одредени лични фактори на физичко лице. Профилирањето се користи, особено, за да се анализира или предвиди извршувањето на работата, економската ситуација, здравјето, личните преференци, интересите, кредибилитетот, однесувањето, локацијата или движењето на одредено лице.

Псевдонимизација

– обработка на лични податоци на таков начин што не е можно да се идентификува кому припаѓаат истите без пристап до други информации, што безбедно се чуваат на друго место.

Општа регулатива за заштита на податоци *(ОРЗП – анг. GDPR)*

– Регулатива на Европскиот парламент и на Советот (ЕУ) 2016/679 од 27 април 2016 година за заштита на физички лица во однос на обработката на личните податоци, за слободен проток на истите податоци и за укинување на Директивата 95/46/ЕЗ (во понатамошниот текст: Регулатива ОРЗП).

Колаборативни роботи *(collaborative robots; co-boty)*

– уреди чија задача е да го намалат обемот на работа на вработените во индустриски погони со извршување на дел од нивните задачи.

Самоучење *(ML; machine learning)*

– област на вештачка интелигенција посветена на алгоритми што постојано го подобруваат своето функционирање преку искуство, т.е. изложување на податоци. Алгоритмите за машинско учење градат математички модел врз основа на податочни примероци (наречени збирови за обука) со цел предвидување или донесување одлуки без потреба од програмирање за таа цел од страна на човечки фактор.

Фалсификување (*анг. Spoofing)*

– вид на напад во кој престапниците се претставуваат како банки, државни институции и канцеларии, компании, па дури и физички лица, со цел да изнудат податоци или пари од нивните жртви.

Стартап

– новосоздадено претпријатие или привремена организација која бара деловен модел што би обезбедил негов или нејзин профитабилен раст.

Вештачка интелигенција *(SI, AI)*

– способност на машините да разберат, учат, планираат и да бидат креативни. Во согласност со дефиницијата предложена со нацрт-законот за вештачка интелигенција (Закон за вештачка интелигенција), системот за вештачка интелигенција значи софтвер развиен со користење на една или повеќе од техниките и пристапите наведени во Регулативата што може, за одреден збир на цели дефинирани од страна на човекот, да генерира резултати, како што се содржина, предвидувања, препораки или одлуки што влијаат на опкружувањата со кои таа комуницира. Оваа дефиниција е многу широка и непрецизна, што, пак, сепак е разбирливо во контекст на технологијата, како што е вештачката интелигенција, која толку брзо се развива.

Шифрирање податоци

– збир на техники што се користат за кодирање чувствителни или лични информации со цел да се обезбеди нивната доверливост.

Носиви уреди *(анг. Wearables)*

- електронски уреди што „се облекуваат", односно се носат блиску до кожата. Тие можат да ги следат и анализираат здравствените параметри или однесувањето на корисникот. Најпопуларните уреди од овој тип моментално вклучуваат паметни часовници, спортски појаси (т.н. паметни појаси) или спортски часовници.

Work-life balance

– одржување рамнотежа помеѓу работата (како платена така и неплатена) и семејниот живот и слободното време.

Автоматизирано донесување одлуки

– работа базирана на напредни пресметки и исклучиво технички средства за обработка на информации. Издавање решенија од страна на компјутер без учество на човечкиот елемент.

1. Влијание на дигитализацијата врз работните процеси

1.1. Рамковен договор на европските социјални партнери за дигитализација – општи забелешки

Дигиталната трансформација на економијата има огромно влијание врз работодавачите, работниците и самиот работен тек. За да се олесни интеграцијата на дигиталните технологии на работното место, во јуни 2020 година беше склучен автономен Рамковен договор на европските социјални партнери (ЕФАД). Неговата цел е да ги спречи и минимизира ризиците со кои може да се соочат вработените и работодавачите. Договорот ги опфаќа сите вработени лица или тие што вработуваат лица во јавниот и во приватниот сектор, како и во сите видови стопанска дејност.

Договорот ЕФАД е независна иницијатива и резултат на преговорите помеѓу европските социјални партнери во рамките на 6-тата повеќегодишна програма за работа во годините помеѓу 2019-2021. Според чл. 155 од Договорот за функционирање на Европската Унија (TFEU), овој автономен европски рамковен договор ги обврзува членовите на BusinessEurope, SMEunited, CEEP и EKZZ (и комитетот за врски EUROCADRES/CEC) да промовираат и имплементираат алатки и мерки (на национално и секторско ниво или на ниво на компанија, каде што е потребно) во согласност со процедурите и практиките што се применуваат за социјалните партнери во земјите членки и земјите од Европската економска област.

Пример за други автономни договори склучени во последниве години е Автономниот рамковен договор на европските социјални партнери што се однесува на активно стареење и меѓугенерациски пристап или Европскиот рамковен договор за стрес поврзан со работата.

I. Главни цели на договорот EFAD

1. Подигање на свеста и подобро разбирање на работодавачите, вработените и нивните претставници по прашањето за можности и предизвици на работа што произлегуваат од дигиталната трансформација.

2. Обезбедување помош за работниците и нивните претставници, како и за работодавачите, при формирањето мерки и активности за искористување на новите можности на дигиталната технологија, а потоа и справување со предизвиците, притоа земајќи ги предвид постоечките иницијативи, практики и колективни договори.

3. Поттикнување партнерски пристап помеѓу работодавачите и синдикатите.

II. Фази на создавање партнерство со цел олеснување на транзицијата низ процесот на дигитална трансформација во компанијата

Претставниците на работниците ќе бидат обезбедени со капацитети и информации што им се потребни за ефективно вклучување во различните фази од процесот.

Фаза 1.

„Заедничко истражување/Подготовка/Поддршка“ со цел подигнување на свеста и создавање средина и атмосфера на поддршка и доверба. Овие активности имаат за цел да овозможат отворени разговори за можностите и предизвиците/заканите поврзани со дигитализацијата, како и нивното влијание врз работното место и да создадат простор за дискусија за можните активности и решенија.

Фаза 2.

„Заедничко мапирање/редовна проценка/анализа“ е задача што се заснова врз обележување тематски области во однос на придобивките и можностите, како и предизвиците и ризиците што ефективната интеграција на дигиталните технологии може да им ги донесе на вработените и компанијата.

Фаза 3.

„Заеднички преглед и усвојување стратегија за дигитална трансформација“, како резултат на првите две фази. Станува збор за основно разбирање на можностите, предизвиците/ризиците, различните компоненти што ја сочинуваат дигитализацијата на одредена компанија, како и нивна меѓусебна поврзаност, а исто така и договарање дигитални стратегии за поставување на идните цели на компанијата.

Фаза 4.

„Прием на соодветни средства/мерки“ што се базираат на заеднички преглед на ситуацијата. Тоа вклучува: можност за тестирање и пилотирање на предвидените решенија, поставување приоритети, спроведување активности во следните временски фази,

разјаснување и дефинирање на улогите и одговорностите на раководството и вработените и нивните претставници, како и ресурси и придружни мерки (на пр. експертска поддршка, надзор).

Фаза 5.

„Редовен/о заеднички/о надзор/следење, учење, евалуација“ е заедничка процена на ефективноста на акциите и дискусија за тоа дали се неопходни дополнителни анализи, подигање на свеста, поддршка или други активности.

III. Опсегот на договорот опфаќа:

1. Дигитални вештини и безбедност на работното место

Социјалните партнери треба да бидат заинтересирани за олеснување на пристапот до висококвалитетна обука и развој на вештини кај работниците. Клучниот предизвик овде ќе биде одредување кои дигитални вештини и промени во процесот треба да се воведат во одредена компанија.

Мерките кои треба да се разгледаат вклучуваат:

- Обврска на страните за преквалификација.
- Пристап до обука и нејзина организација, висок квалитет и ефективност на обуката, воведување можност за работа со скратено работно време и распределување на дел од работното време за обука.
- Јасно дефинирани услови за учество, вклучувајќи: времетраење, финансиски аспекти, вклученост на вработените и соодветен надоместок доколку обуката се одвива надвор од работното време.

2. Начини на поврзување и исклучување

Одговорност на работодавачот е да ја обезбеди безбедноста и здравјето на вработените во секој аспект поврзан со работата. Затоа, правото на исклучување е еден од главните аспекти на овој прирачник. Во однос на очекувањата на работодавачот кон вработениот при користење на дигиталните уреди, ги повикуваме синдикалците да дадат целосна и јасна слика за тоа преку колективни преговори и договори на соодветните нивоа.

Воведувањето на нови дигитални уреди во работата може да обезбеди флексибилно извршување на работните задачи во корист на работниците и на работодавачите. Истовремено, тоа може да создаде сериозен ризик поврзан со тешкото разграничување на

професионалниот и на личниот живот. Затоа, неопходно е да се фокусираме на спречување негативни појави што влијаат врз здравјето и безбедноста на вработените. За да се постигне тоа, потребно е јасно определување на правата, должностите и одговорностите, при што принципот на превенција ќе биде со највисок приоритет.

Мерките што треба да се разгледаат вклучуваат:

- Обука и други активности за подигнување на свеста на работниците.
- Создавање нова работна култура кај менаџментот, која дозволува избегнување контакт со вработениот надвор од работното време.
- Обезбедување јасни насоки на тема постоечки закони за работно време, работа на далечина и мобилна работа.
- Ефективна организација на работата, вклучително и обезбедување доволен број на вработени, со што вработените нема да бидат принудени да работат прекувремено.
- Соодветен надоместок за дополнително одработено време.
- Процедури за предупредување и поддршка што дозволуваат исклучување и заштита од санкции поради немање контакт со вработените по работното време.
- Спречување на изолација на работното место.

3. Вештачка интелигенција и гарантирање на принципот на човечка контрола

Нема сомнение дека вештачката интелигенција ќе има сè поголемо влијание врз работата на човекот. Затоа, Европскиот автономен договор поставува одредени правила и насоки за нејзино воведување на пазарот на трудот. Важен елемент што треба да се гарантира на секое работно место е човечката контрола врз вештачката интелигенција, која претставува основа за употреба на роботика и апликации базирани на вештачка интелигенција. Системот треба да биде законски и праведен и треба да ги почитува етичките стандарди во согласност со човековите права. Од техничка и социјална гледна точка, системот треба да биде безбеден и транспарентен.

4. Почитување на човековото достоинство и надзор

Поради значителното интегрирање на современите технологии во работниот процес, постои ризик да се нарушат основните вредности на лицето кое работи (на пр. со преземање чувствителни податоци – пристап до простории или документи со скенирање отпечаток од прст, зеница или вграден чип). Ваквите технологии го зголемуваат ризикот од

нарушување на човечкото достоинство, особено во случај на лично следење. Ова може да доведе до влошување на работните услови.

Минимизирањето и транспарентноста на личните податоци, заедно со јасните правила за нивна обработка, го намалуваат ризикот од наметливо следење и злоупотреба на податоците. Во контекст на вработувањето, правилата за обработка на личните податоци на вработените се утврдени во регулативата ОРЗП. Исто така, социјалните партнери во договорот ЕФАД потсетуваат и дека чл. 88 од ОРЗП се однесува на можноста за воспоставување подетални правила за чување на личните податоци на вработените преку колективните договори. Ова е за да се обезбеди заштита на правата и слободите на вработените во врска со обработката на нивните лични податоци во контекст на работниот однос.

Мерките што треба да се разгледаат вклучуваат:

- Овозможување на претставниците на работниците да ги решаваат проблемите поврзани со податоците, согласноста, заштитата на приватноста и надзорот.
- Собирање податоци за одредена и транспарентна цел. Податоците не треба да се собираат или складираат само затоа што тоа е овозможено или за неодредена цел.
- Информирање на вработените дека можат да се спротивстават на обработката на одредена група лични податоци или да ја повлечат својата претходно дадена согласност во секое време.
- Обезбедување дигитални средства и алатки за претставниците на работниците, на пример, дигитални огласни табли за извршување на нивните должности.

5. Имплементација и активности за следење

Организациите-членки ќе поднесат извештај за спроведување на договорот до Комитетот за социјален дијалог. Во првите три години од датумот на потпишување на овој договор, Комитетот за социјален дијалог беше обврзан да подготви и усвои годишен пакет со сумирање на тековната имплементација на договорот. Целосниот извештај за преземените активности за спроведување на договорот ќе биде изготвен од страна на Комитетот и ќе биде усвоен од страна на европските социјални партнери во наредните години. Договорот не ги нарушува правата на социјалните партнери да склучуваат адаптивни или дополнителни договори на начин кој ги зема предвид специфичните потреби на заинтересираните социјални партнери.

1.2. Нови технологии на работното место – работа помогната од технологијата (колаборативна) и целосно автоматизирана работа

Ставот кон роботизацијата се менува како од перспектива на работодавачите, така и од гледна точка на самите вработени. Роботот повеќе не останува само во сферата на имагинацијата, туку се појавува како производна алатка што може да им олесни на луѓето и да им помогне да решат конкретни проблеми. Меѓутоа, во зависност од секторот и фазата на производство, автоматизацијата може да се воведе во различен степен. Покрај нивото на вклученост во задачите, роботите може да се поделат на роботи што вршат главно интелектуална работа (на пример, сите алатки за вештачка интелигенција) и роботи што ги заменуваат луѓето во повторливите задачи (на пр. производи за пакување).

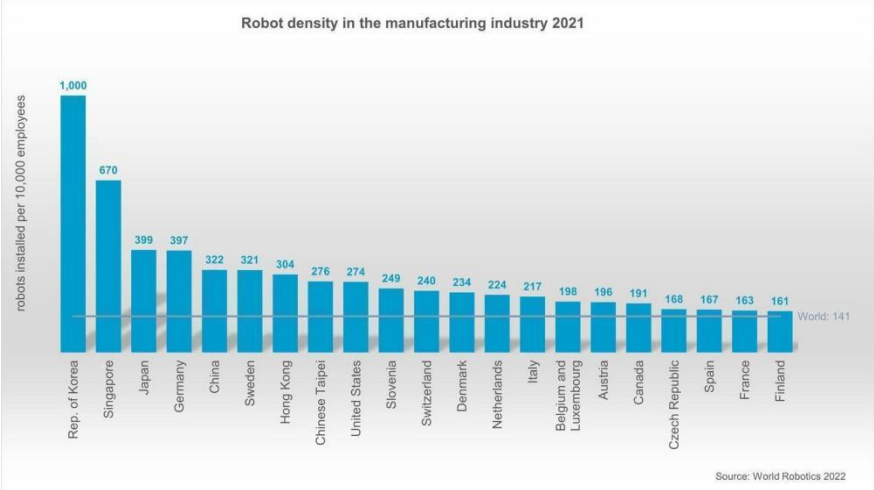
Што претставува автоматизиран систем за производство?

Автоматизацијата на производството е насока во развој на компаниите што се состои од значително намалување или целосна замена на човечката физичка и ментална работа со машини. Почетоците на овој феномен датираат од 20 век, кога во 1913 година Хенри Форд засекогаш го промени светот благодарение на мобилната линија за склопување со која управуваат специјализирани работници. Целта на ваквата работа беше да се зголеми обемот на производството, а притоа да се намали цената на финалниот производ.

Во моментов се занимаваме со следната фаза од еволуцијата на производството – подобрување на автоматизацијата преку дигитализација. Благодарение на технологиите, како што се интуитивните модули за програмирање, станува полесно да се креираат детални инструкции за роботите. Напредните сензори им овозможуваат на машините да ја разберат нивната околина и подобро да реагираат. Според Меѓународната федерација за роботика[1] (International Federation of Robotics), од 2015 до 2020 година, густината на роботите е речиси двојно зголемена на глобално ниво, растејќи од 66 единици во 2015 година до 126 единици во 2020 година.

[1] Метрика што ја користи Меѓународната федерација за роботика, мерејќи го бројот на роботи на 10.000 луѓе вработени во одредена гранка.

Држави со најголема автоматизација на производството (2021 г.)



Извор: International Federation of Robotics (*The Robot Report*, 2021).

Поддржана работа

За поддржана работа станува збор кога одредени активности во производството може да се заменат со роботи, додека други бараат учество на човечки фактор. За поддршка на производните процеси, најчесто се користат колаборативни роботи (т.н. ко-ботови), чија задача е да им олеснат на вработените во индустриските погони со извршување на дел од нивните задачи. Важна карактеристика врз основа на која ко-ботовите се разликуваат од стандардните индустриски системи (кои обично се одвоени од луѓето), е тоа што во случајот на колаборативна автоматизирана роботика, контролните системи на роботот го делат истиот работен простор со луѓето.

Методи на соработка помеѓу роботите и луѓето:

1. **Ограничена интеракција со човек** – целосно запирање на роботот кога човек ќе се појави во означената област и самостојно продолжување со работа откако работникот ќе го напушти просторот.
2. **Соработка со човек** – благодарение на вградените сензори, ко-ботот забавува или престанува да работи кога некој е во негова близина, што овозможува безбедна соработка помеѓу човекот и машината.
3. **Рачно работење** – ко-ботот е постојано контролиран од операторот. На пример, уредот го задржува товарот кога човекот ја насочува својата рака.

Целосно автоматизирана работа

Автоматизацијата во индустријата се подразбира како употреба на технологија за контрола на производството и создавање производи и услуги користејќи дигитални алатки. Во случај на целосна автоматизација, луѓето и машините престануваат да извршуваат задачи во кои се надополнуваат и почнуваат да работат во истиот опсег. Како резултат на роботизацијата, учеството на вработените во производните процеси значително се намалува или целосно исчезнува. Сите производствени процеси стануваат целосно автоматизирани и не е потребна човечка интервенција во која било фаза од создавањето на производот.

И покрај заедничкиот страв предизвикан од продлабочената автоматизација на индустриските процеси, воведувањето на овој тип на технологија може да донесе придобивки на различни нивоа поврзани со производствени процеси – меѓу другото, кога работата е ризична по животот и здравјето на луѓето.

Дискусија – дали работата на роботите треба да се оданочува?

Заедно со намалувањето на трошоците за автоматизација на производните процеси, се зголемува размерот на роботизација на индустријата. Меѓу очекуваните ефекти од ваквата состојба, може да се забележат и позитивни аспекти, како што се економски раст или зголемена продуктивност, но исто така и негативни, на пр. намалување на вработеноста во различни гранки на производниот сектор.

Трансформацијата на досегашните постоечки деловни модели покренува бројни контраверзии, а законодавците во земјите каде што автоматизацијата веќе се разви со изненадувачко темпо, се соочуваат со нови предизвици. Со оглед на значителното намалување на трошоците поврзани со вработување и остварување на профитот како резултат на користењето роботи во индустријата, се наложи прашањето за даноците што се наметнуваат на работата на роботите. Кога станува збор за набавка на нови машини и опрема, поединечните влади користат даночни олеснувања за поддршка на дигиталната трансформација и модернизација на индустрискиот сектор. На пример во Полска, од 2022 година, работодавачите имаат право на намалување дури до 150 % од трошоците за купување машини и уреди што се функционално поврзани со нив, уреди што служат за безбедност при работа на позиции, каде што се одвива интеракција човек-робот.

1. **Позитивни и негативни последици од роботизацијата**

2. **Економија**

a) **Позитивни:**

- Можност за побрзо подобрување на производите и нивно пласирање на пазарот.
- Побрз развој на нови технологии.
- Подобрување на конкурентноста на компаниите.

b) **Негативни:**

- Зголемување на невработеноста – според проценките на авторите на извештајот „*Future of Jobs*“ од 2023 година (World Economic Forum), во блиска иднина машините ќе извршуваат повеќе задачи отколку луѓето. Во 2018 година, во просек 71 % од задачите во работното време беа извршувани со учество на човечкиот фактор, додека во 2025 година овој сооднос значително ќе се промени. Луѓето ќе бидат одговорни за околу 48 % од активностите, додека останатите 52 % ќе бидат целосно автоматизирани.
- Зголемена потрошувачка на енергија, што придонесува за зголемено загадување на животната средина.

2. **Работодавач**

a) **Позитивни:**

- Намалување на трошоците за производство.
- Намалување на ризикот од грешки.
- Можност за за подобро следење на ефективноста
- Побрзо препознавање состојби на забавено производство (анг. bottleneck)”, што ја олеснува оптимизацијата на работата.
- Во некои држави (на пр. во Полска) – можност за одбивање на трошоците за купување индустриски роботи за одредена цел.

b) **Негативни:**

- Високи почетни трошоци за инсталација на опремата.
- Потреба за инвентар и високи трошоци за поправка.

- Ако процесите се високо автоматизирани, дефектите на опремата предизвикуваат прекин на производството.
- Намалена флексибилност при реакција за неочекувани проблеми или грешки во споредба со одговорот на вработениот.
- Потреба за усогласување со бараните прописи
- Високи трошоци за енергија.

3. **Работник**

a) **Позитивни:**

- Поедноставување на процесот на производство.
- Поддршка во потешки активности или активности што се повторливи.
- Зголемена ефикасност на производството со помала вклученост на работникот.
- Можност да се посвети време на посложените развојни активности како резултат на пренасочување на повторливите активности на автоматските алатки.
- Појавата на нови работни места поврзани со создавање, користење или поправка на машини.

b) **Негативни:**

- Можност за губење на работата поради автоматизација на процесот.
- Поголема веројатност за професионално исцрпување предизвикано од страв од губење на работа.
- Во случај на дефект на машините или нивна неправилна употреба – изложеност на ситуации што го влошуваат здравјето/ситуации опасни по живот.

1.3. Спречување на непропорционален и прекумерен надзор на работното место

Надзор на работното место – можности и закани

Технолошките компании со задоволство реагираат на зголемената побарувачка на работодавачите во областа на новите технологии. Насоката на развој на алатките за вештачка интелигенција, од друга страна, создава можност за преземање целосна контрола врз вработените – независно од нивното знаење и согласност. Постојат исто така, и силни

тенденции кон прифаќање на новата состојба на работите како „природна“ последица на развојот на компаниите.

Можности:

- надзорот што се врши во итни ситуации и во случај на несреќа на работа, во некои случаи може да биде во корист на работникот (на пр. кога е неопходно да се докаже дека работното место не било доволно безбедно),
- во некои сектори, надзорот е неопходен за да се обезбеди усогласеност со прописите (на пр. во банкарството може да се користи за да се спречи користењето доверливи информации)
- надзорот што се користи за време на обуката на вработените може да ги забрза процесите на негово имплементирање во структурите на компанијата (на пр. уредите за носење во градежната индустрија се паметни шлемови со сензори за вибрации што ги предупредуваат вработените за потенцијални опасни предмети /објекти во околината).

Пример Stellate

Stellate, стартап што се занимава со анализа на податоци со седиште во Сан Франциско, располага со тим од вработени распоредени низ целиот свет. Покрај алатките што се користат за заедничка работа од далечина, компанијата го следи развојот на своите вработени преку програми за обука и менторство. Наместо казни за несоодветно високи перформанси на вработените или друго несоодветно однесување, главната цел на ваквите иницијативи е да се промовираат алатки меѓу вработените во компанијата што служат за зголемување на ефикасноста на нивната работа.

Опасности:

- злоупотребата или неправилната употреба на дигиталните технологии може да доведе до повреда на правото на приватност и заштита на личните податоци на вработените,
- закана по менталното и физичкото здравје на вработените како резултат на стрес поврзан со прекумерен надзор и наметнати работни стандарди,

- попречување на здружување на вработените – следењето на работниците и препознавањето на расположението во компанијата овозможува да ги забележите движењата во корист на здружувањето (на пр. на големи работни места, се случува податоците на вработените да се користат за да се препознае нивниот однос кон работодавачот и да се утврди каде постои најголема веројатност за противење на вработените кон политиката на компанијата).

Главни принципи што се однесуваат на надзор на работното место

Познато е дека работодавачите треба да имаат можност да ги надгледуваат работните места и да ги оценуваат перформансите на своите вработени со цел да се обезбеди подобро управување со компанијата и да се заштитат деловните тајни, да се спроведе усогласеност со законските прописи и да се спречи работникот да изврши престап. Во исто време, Европската Унија и поединечните земји членки стават голем акцент на прашањата за приватноста на вработените и почитувањето на нивниот личен живот.

Надзорот на работното место е законски, но сепак…[2]

- пред отпочнување со употреба на видео надзор, треба детално да се определат целите на обработка на информациите (на пр. осигурување на безбедноста на вработените),
- работодавачот е должен да ги информира лицата кои потенцијално би можеле да бидат следени, за тоа дека се користи надзор и која област ја опфаќа.

Она што е исто така важно, целите, опсегот и начинот на користење на надзорот треба да се утврдат во колективниот договор или во правилникот за работа, на пример, во рамки на колективните преговори. Во ситуација кога работодавачот не е обврзан да има колективен договор или да утврди правилник за работа, споменатите правила треба да бидат вклучени во известувањето.

Тајниот видео надзор е дозволен само во ограничен обем, во случај кога постои основано сомневање дека е сторено сериозно недолично однесување или кривично дело што би му нанело значителна штета на работодавачот.

[2] Принципи што се однесуваат на надзор на работното место што произлегуваат од правото на Заедницата (член 8 од Европската конвенција за човекови права, регулатива ОРЗП), пресуди на судови и трибунали, Закони за работни односи на поединечни земји членки.

Работодавачот може да користи и други видови на надзор. На пример, тоа може да се:

- GPS монтиран во службено возило,
- Надзор на интернет и алатки за комуникација што се користат на службени уреди
- Геолокализатор на службен мобилен телефон или лаптоп.

Одредбите за видео надзор соодветно се применуваат за сите форми на надзор (на пример, работодавачот може да ја следи е-поштата на работникот само откако претходно ќе го извести).

Надзор на работното место и законски прописи – примери од земјите партнери

Полска

Според полскиот Закон за работни односи, надзорот е посебен надзор над просториите на работното место или областа околу работното место во форма на технички средства што овозможуваат снимање слики.

- **Надзорот во Полска е дозволен доколку е потребен за:**
- осигурување на безбедноста на работниците,
- заштита на имотот или контрола на производството,
- чување во тајност информации, чиешто откривање може да го оштети работодавачот
- надзор на електронска пошта (член 223 од Законот за работни односи), е дозволен доколку е неопходно да се обезбеди организација на работата што овозможува целосно искористување на работното време и правилна употреба на работните алатки што му се достапни на работникот; Следењето на електронската пошта не може да ја наруши доверливоста на кореспонденцијата и другите лични права на вработениот.

Работодавачот може да ги користи снимките само за целите за кои се снимени и да ги чува во период не подолг од три месеци од датумот на снимање.

Како да се спроведе надзор на законски начин? Постапка од шест чекори

Спроведувањето надзор во согласност со законот бара од работодавачот да процени какво влијание може да имаат неговите постапки врз вработените. Следниве чекори покажуваат врз кои прашања треба да се заснова ваквата анализа.

Чекори	Прашање	Постапка
Чекор 1	Доколку надзорот бил веќе воведен, врз што се заснова во тој момент?	Спроведување ревизија за да се утврди кои видови надзор се користат на работното место и кој од организацијата има овластување да ги следи вработените
Чекор 2	За што служи надзорот или зошто треба да биде спроведен?	• Разбирање на целта на следењето на вработените. Прецизно дефинирање на функцијата за следење (податоците собрани од конкретен надзор може да се користат само за целите за кои се собрани). **Исклучок**: доколку за време на надзорот, организацијата наиде на информации за активности што не може да се игнорираат (на пример, потенцијална криминална активност, мобинг), собраните податоци може да се користат за да се повикаат на одговорност соодветните лица
Чекор 3	Дали оваа цел може да се постигне без надзор?	• Откако ќе се идентификува причината поради која што се спороведува следењето, треба да се одреди дали истата цел може да се постигне без следење на вработените. **Пример:** следењето на веб-локациите што ги посетуваат вработените може да се замени со блокирање на несоодветните веб-локации или со дозволување на вработените да испраќаат пораки или датотеки само од одредени електронски адреси и во одредена големина
Чекор 4	Доколку одредена цел не може да се постигне без следење, дали постои средство за контрола што е помалку инвазивно од она што моментално се разгледува?	**Пример**: Проверката дали вработените не ја прекршуваат политиката за доверливост на компанијата може исто така да се следи и со контрола на содржината на е-пораките испратени од вработените, како и со автоматско следење, на пример, со проверка на адресите на е-пошта и темата на пораките или блокирање пораки со прилози со одредена големина
Чекор 5	Како ќе влијае надзорот врз вработените?	• Треба да се одговори на следните прашања: ○ Дали надзорот може да се смета за потценувачки или неправеден?

		○ Дали надзорот ќе има влијание врз заемната доверба помеѓу работникот и работодавачот? ○ Дали може да се сподели некоја доверлива или чувствителна информација со луѓе кои, во однос на работата немаат потреба да ја знаат? **Пример:** Тимот за сметководство може да добие информации дека лицето отсуствувало од работа поради болест (за да се овозможи исплата на надоместоци за боледување), но само менаџерот за човечки ресурси треба да ги знае медицинските причини за ослободување од работа
Чекор 6	Дали воведувањето на надзор е оправдано?	• Донесување одлука, дали воведувањето на надзор е оправдано (полесно е да се оправда надзор што е помалку инвазивен, при што за истиот се известуваат вработените). • Пред да се воведе надзор, може да се спроведе консултација со вработените, со цел заеднички да се разгледа образложението за надзор

Надзор на вработените и работа на далечина

Надзорот на вработените може да се одвива преку инсталација на апликации за контрола на компјутерите на вработените, за што често, вработените не се известени. Програмата т.н. bossware може да снима притискање на копчињата, да прави слики од екранот, па дури и да ги активира веб-камерите на вработените додека работат на далечина.

Вреди да се напомене дека постојаниот страв од следење од страна на работодавачот може да доведе до влошување на менталната состојба на вработените. Според резултатите од истражувањето, дури 56 % од испитаниците чувствуваат стрес и вознемиреност поради тоа што нивниот работодавач ја надгледува нивната електронска комуникација, 41 % постојано се прашуваат дали ги надгледуваат, а 32 % поретко прават паузи поради оваа причина.

Како ефикасно да се контролира работата без да се наруши добросостојбата на вработениот?

Совети за работодавачот:

- информирајте го вработениот за алатките за надзор што се користат,
- објаснете ги правилата за користење на надзорот и означете ги границите на истиот (на пр. во однос на видот на обработените податоци)
- наместо прекумерен надзор и увид во секојдневните активности на вработениот, воведете систем на отчет за извршената работа (на пр. неделен преглед и евалуација на задачите),
- користете апликации за управување и следење на текот на работата (на пр. Connecteam) и подобрете ја далечинската комуникација помеѓу работните тимови овозможувајќи заедничко планирање.

1.4. Разлика помеѓу работа надвор од канцеларија и работа од далечина – влијание врз односите на вработените

Според истражувањето на Европската комисија, во годината пред избувнувањето на КОВИД-19 пандемијата, само 5,4 % од вработените во ЕУ-27 работеле од дома – дел што не е променет од 2009 година. Како резултат на пандемијата, овој процент се зголеми повеќе од двојно – на 12,3 %. Во некои земји членки, оваа бројка надмина вкупно дури 1/4 од вработените, без разлика на гранката или економскиот сектор.

И покрај првичните потешкотии со приспособувањето кон новата реалност (главно предизвикани од недостатокот на соодветна ИКТ инфраструктура или обука од областа на дигитализација на работните процеси), вработените денес не можат да замислат враќање на начинот на работа од пред пандемијата. Тие ја ценат поголемата флексибилност за работа, можноста да поминуваат време со семејството и зголемувањето на работната ефикасност.

Сепак, и покрај популарноста на хибридната работа, многу работодавачи и вработени и понатаму се одлучуваат за враќање во своите канцеларии. Оваа одлука ја оправдуваат со подобрување на односите и соработката со вработените и колегите, како и со можноста за создавање средина погодна за заеднички иновации и подобра продуктивност, јасно одделувајќи го приватниот од професионалниот живот.

Работа на далечина – основни поими

Зголемувањето на популарноста на работата користејќи дигитални алатки и разновидните можности што тие ги нудат, ја наметна потребата од користење низа нови термини. За да се олесни снаоѓањето во лавиринтот на дефиниции, создадена е табела која ги прикажува разликите помеѓу поединечните начини на работа.

Вид на работа со помош на дигитални алатки	Дефиниција
Работа надвор од канцеларија	Работата надвор од канцеларија се однесува на секој вид работа што се одвива надвор од седиштето на работодавачот, независно од технологијата што се користи. Според измената на полскиот закон за работни односи, тоа е: работа извршена целосно или делумно на место назначено од работникот и истата е секој пат договорена со работодавачот
Работа на далечина (анг. telework)	Работа на далечина е секој облик на организирање и/или извршување работа со користење информатичка технологија, врз основа на договор за вработување, според кој работата може да се врши и во просториите на работодавачот, но сепак редовно се врши надвор од оваа просторија.
Работа на далечина со редуцирано работно време	Овој работен систем ги комбинира работните денови на далечина со работните денови во канцеларија и првпат беше користен во пракса од страна на Џек Нилс на почетокот на 1970-те години во САД.

Работа од далечина и мобилна работа базирана на информатичко-комуникациски технологии (ТІСТМ)	ТІСТМ се однесува на користење информатичко-комуникациски технологии како што се паметни телефони, таблети, лаптопи и статични компјутери за работа надвор од просториите на работодавачот. Ги опфаќа сите форми на работа од далечина, но се труди да направи разлика помеѓу работа од дома или фиксна локација (работење на далечина) и мобилна работа базирана на ИКТ. Последниот термин се користи во Германија за да се разграничи далечинската работа што се изведува дома со форма на работа која што е повеќе мобилна
Паметна работа/агилна работа	Паметната работа се однесува на флексибилен работен систем што им овозможува на вработените да работат удобно и ефикасно без временски и просторни ограничувања (во кое било време и на кое било место) користејќи информациски и комуникациски технологии во мрежата. Сличен термин („агилна работа“) се користи во Италија
Флексибилни услови за работа	Флексибилна работна организација опфаќа алтернативни работни опции што дозволуваат вршење на работите надвор од традиционалните временски и/или просторни граници на еден стандарден работен ден
Виртуелна работа	Виртуелна работа е платена или неплатена работа што се изведува при комбинирана употреба на дигитални и телекомуникациски технологии или изготвување содржина за дигитални медиуми
Хибридна работа	Тоа е работен систем во кој работата може да се врши делумно од просториите на работодавачот, а делумно од дома или од други места

Работа надвор од канцеларија и работа на далечина – како е според закон?

Регулативи на ниво на ЕУ

Во моментов, не постојат обврзувачки правни акти што се фокусираат на работа на далечина, иако неколку директиви и регулативи се занимаваат со прашања за обезбедување добри услови за работа за лицата што работат на далечина. Сепак, постои Европски рамковен договор за работење на далечина (2002). Овој документ е автономен договор помеѓу европските социјални партнери (ETUC, UNICE, UEAPME и CEEP) и ги обврзува поврзаните национални организации да го спроведат тој договор во согласност со „процедурите и практиките“ специфични за секоја земја членка.

Работа надвор од канцеларија/работа од далечина и законот – пример Полска

Законот од 1 декември 2022 година за изменување и дополнување на Законот за работни односи и други одредени акти го воведе концептот на работа надвор од канцеларија (анг. remote work) во полскиот закон за работни односи, истовремено укинувајќи ги одредбите што се однесуваат на работа од далечина (анг. telework). Во согласност со овие измени и дополнувања, работа надвор од канцеларија е **работа што се извршува целосно или делумно на место назначено од работникот и секој пат е претходно договорено со работодавачот**, вклучително и домашната адреса на работникот, на пр. користејќи средства за директна далечинска комуникација.

Работа од далечина, пак, е каква било форма на организирање и/или извршување работа со користење информатичка технологија, врз основа на договор/работен однос, **во која работата што може да се врши во просториите на работодавачот, редовно се врши надвор од просториите на седиштето**. И покрај тоа што работата надвор од канцеларија може да биде привремена, работата од далечина, по правило, се заснова врз постојано извршување на должностите од дома.

Правилата за работата од далечина треба да се дефинираат во договор со синдикатите, во рамките на правилникот за работа или во индивидуален договор со работникот. Покрај тоа, работодавачот не може да одбие работа од далечина на родители кои воспитуваат дете до четири години, родители или старатели на лица со посебни потреби или бремени жени (освен ако природата на должностите што се вршат не го дозволува тоа). Работодавачот, исто така, е должен да му ги обезбеди на работникот потребната опрема и алатки за вршење работа од далечина и да ги надомести, меѓу другото, трошоците за струја и интернет.

Работата надвор од канцеларија може да се врши по барање на работникот или по налог на работодавачот. Работодавачот исто така може да наложи работа надвор од канцеларија во случај на вонредна состојба, состојба на закана од епидемија или епидемија, како и поради виша сила, на пример, уништување на работното место како резултат на пожар или поплава.

Измената на Законот за работни односи, исто така, содржи предлог за т.н повремена работа надвор од канцеларија, според која, на барање на вработениот, тој ќе може да работи надвор од кацеларија до 24 дена во една календарска година. Меѓутоа, барањето на работникот за повремена работа од далечина не е обврзувачко и работодавачот може да го одбие.

Важно е тоа што на работодавачот му е забрането да дискриминира вработен поради работата од далечина, како и поради одбивање да ја изврши истата работа. Дополнително, работодавачот е должен на работникот кој работи работата од далечина да му овозможи престој во просториите на работодавачот, контакт со други вработени и да му дозволи користење на просториите и опремата на работодавачот, друштвените простории на компанијата, како и да учествува во друштвените активности на компанијата – под исти услови како и останатите вработени.

1.5. Алгоритми и дискриминација на работно место

Во светот воден од информации, сè почесто слушаме за вештачка интелигенција (*artificial intelligence* – AI), чија што употреба може да се најде речиси насекаде. Може да се очекува дека таа сè повеќе ќе се користи и во сферата на работата. Според истражувањето на Форбс, околу 4 од 5 компании сметаат дека вештачката интелигенција е највисок приоритет во нивната деловна стратегија. Сепак, надежите за оптимизација на трошоците и зголемена ефикасност во производството се придружени со стравот на вработените дека ќе ги загубат своите работни места – според Форестер во извештајот „Future of Jobs Forecast", бројот на работни места изгубени поради автоматизација ќе достигне 12 милиони само во Европа до 2040 година.

И покрај тоа што буди бројни емоции, во јавната дебата сè уште недостасува сигурно објаснување за тоа како функционира вештачката интелигенција и дали секој тип на автоматизација може да се класифицира како вештачка интелигенција. За целосно разбирање на проблемот, неопходно е да се разгледа и која е разликата помеѓу системот за вештачка интелигенција и алгоритмите, бидејќи овие термини често се користат наизменично.

ВИ (Вештачка интелигенција) е исклучително широк поим што опфаќа група алгоритми што можат да ги модифицираат своите параметри и да создадат нови алгоритми како одговор на проучените влезни податоци. Оваа способност за промена, приспособување и растење врз основа на нови податоци се определува токму како „интелигенција“.

Со наједноставни зборови, вештачката интелигенција може да се дефинира како **способност на машините да разбираат, учат, планираат и да бидат креативни**. Според дефиницијата предложена со нацрт-регулативата за вештачка интелигенција (AI Act/Закон за вештачка интелигенција), систем за вештачка интелигенција значи софтвер развиен со користење на барем една од техниките и пристапите наведени во регулативата[3], што може – за одреден збир на цели дефинирани од човекот – да генерира резултати како што се содржина, предвидувања, препораки или одлуки што влијаат врз средините со кои се во интеракција.

Алгоритам е збир на инструкции, поточно пресметковна формула, што автономно донесува одлуки врз основа на статистички модели или правила за одлучување без експлицитна човечка интервенција. Алгоритмот претставува низа од инструкции што му кажуваат на компјутерот што треба да прави во рамките на сет од прецизно дефинирани чекори и правила дизајнирани со цел извршување на работата. Така, тоа е однапред одредено, ригидно, кодирано однесување што се активира откако ќе сретне одреден елемент.

Прашање што припаѓа во областа на вештачката интелигенција е **машинското учење** (*machine learning*, ML). Неговата главна цел е да создаде систем што ќе работи автоматски, што ќе може да се подобрува врз основа на искуство во форма на податоци и што може стекне нови знаења врз основа на тоа. Овој процес се заснова врз наоѓање шема во дадените податоци, којашто треба да се користи за да се одговори на прашањето за непознатото множество. Значи, тоа е еден вид предвидување на иднината со помош на веројатност и статистика.

[3] Техники и пристапи во областа на вештачката интелигенција наведени во регулативата:

а) механизми за машинско учење, вклучувајќи надгледувано учење, учење на машините без надзор и учење за зајакнување, со користење широк опсег на методи, вклучувајќи длабоко учење,

б) методи базирани на логика и знаење, вклучително претставување на знаењето, индуктивно (логичко) програмирање, бази на знаење, пребарувачи за заклучување и дедукција, (симболичко) расудување и експертски системи,

с) статистички пристапи, баесова проценка, методи за пребарување и оптимизација.

Можноста за самостојно учење не е карактеристика за секоја вештачка интелигенција. Понекогаш, алгоритам може да се напише на таков начин што програмата во која е поставен извршува команди без да мора да учи од нови податоци (како во случајот со ML).

Пример за алгоритам кој веќе бил правилно програмиран е оној што го користел познатиот суперкомпјутер IBM Deep Blue. Оваа машина стана позната откако пред 25 години успеа да победи во шах против мајсторот Гари Каспаров. Deep Blue, исто така, ги зачувал сите можни потези во зависност од позицијата на фигурите на шаховската табла и стратегијата на противникот. Благодарение на ова и на големата компјутерска моќ, тој можеше успешно да се снаоѓа во секоја ситуација.

Спротивно на алгоритмот имплементиран во програмата IBM Deep Blue беше програмата AlphaGo креирана од DeepMind. Користејќи механизми за самостојно учење, овој систем научил да игра GO (стара кинеска игра на табла во која целта е да обележи што е можно повеќе територија со свои камења на првично празна табла) и дури го победил играчот кој се сметал за најдобар во светот.

Општа вештачка интелигенција, од друга страна, е самосвесен систем што располага со сеопфатно знаење или когнитивни вештини, систем способен за самостојно размислување и извршување задачи. Создавањето технолошка сингуларност со години предизвикува бројни контроверзии – пред сè во однос на тоа дали тоа воопшто е можно. Според еден од водечките критичари за настанувањето на општата вештачка интелигенција, филозофот Хуберт Драјфус, компјутерите немаат тело, не минуваат низ детство и адолесценција и не учествуваат во културните искуства, па воопшто не можат да стекнат човечка интелигенција. Еден од главните аргументи на Драјфус беше дека развојот на човечката интелигенција се одвива во делови на несвесен начин, со што не може да се артикулира и да се вгради во компјутерска програма.

Алгоритми на работа

1. Анализа на CV на кандидат со помош на алгоритам пред стапување во работен однос

Алгоритамското вработување се базира на користење на системите за вештачка интелигенција и машинско учење за наоѓање кандидати, регрутирање, спроведување интервјуа и вработување. Оваа техника користи многу критериуми за оценување на кандидатот, вклучувајќи: неговото искуство и образование, а биографиите што ги добива често ги филтрира користејќи клучни зборови. Алгоритмите, исто така, можат да помогнат во проценатa на меките вештини, како што е склоноста на кандидатот за брзо учење и тимска работа.

Компаниите што користат различни алатки за вештачка интелигенција за време на регрутирањето, сакаат на тој начин да се осигурат дека процесот се спроведува праведно. Теоретски, при првото автоматско оценување, нема простор за човечкиот фактор и евентуална дискриминација. Сепак, овие системи честопати се критикувани дека ги одразуваат предрасудите на луѓето кои ги програмирале.

Важно е дека алгоритмите не ја носат конечната одлука за вработување. Тие првенствено се наменети за стеснување на големиот избор на кандидати.

Методи на анализа на CV преку алгоритам:

- **Доделување поени на CV-то** – алгоритмот доделува поени според критериумите претходно поставени од регрутерот,
- **Рангирање** – подредување на биографиите врз основа на присуството на клучни зборови,
- **Усогласување** – препознавање на клучните зборови што одговараат на оние во огласот за работа,
- **Анализа** – алгоритмот ја анализира семантиката на CV-то, ги извлекува главните информации и ги дели во различни категории: искуство, вештини, податоци за контакт.

2. Карактеристики и области на користење алгоритми на работното место

Видови алгоритми:

- **Описни** – се користат за евидентирање настани од минатото и за анализа на нивното влијание врз сегашните настани, како на пример алгоритми за евалуација на перформанси што имаат цел собирање различни видови податоци поврзани со ефективноста на вработените и давање општа процена.
- **Предвидувачки** – имаат за цел предвидување на идното однесување или процена на веројатноста за појава некој настан (на пример, предвидување пораст на побарувачка за нови вработени).
- **Алгоритми што предложуваат/препорачуваат** – нивна задача е да го изберат најдоброто сценарио од разните можности и да препорачаат одредена акција или едноставно, нејзино спроведување (на пр. донесување одлуки во врска со човечките ресурси, распределба на задачи или распоред).

Употребата на алгоритми на работа се поврзува со т.н **алгоритамско управување**. Се однесува на „системот за контрола во кој на алгоритмите им се доделува одговорност за

донесување и извршување одлуки што влијаат врз работата, ограничувајќи го на тој начин човечкото учество и надзор над работниот процес“.

Шест клучни функции во областа на управување со работните процеси, за чијашто реализација се користени алгоритми:

1. Надзор/контролирање на вработените.
2. Утврдување цели.
3. Управување со резултати.
4. Создавање распоред.
5. Надомест.
6. Престанок на работен однос.

Зголемување на контролата на работодавачот врз вработените со помош на алгоритми

- **Препорачани алгоритми** – работодавачите користат алгоритми за да ја оценат дадената ситуација, како и да дадат предлози за да го поттикнат вработениот да преземе дејствија означени со алгоритмот.
- **Алгоритамско пригушување** – употреба на алгоритми за прикажување само одредени информации, дозвола за покажување одредени однесувања, додека е оневозможено прикажувањето на други.

Таквата употреба на алгоритми може да ја зголеми фрустрацијата на вработените, кои поради потребата да се приспособат на неразбирливите препораки, може да почувствуваат дека нивниот глас не вреди.

Алгоритми што се користат за евалуација на работата

- **Алгоритамска евиденција** – користење пресметковни процедури за следење, собирање и известување, често во реално време, широк опсег на прецизно избрани податоци од внатрешни и надворешни извори.
- **Пресметковни технологии** – се користи за собирање рејтинзи и рангирања со цел пресметување одредена мерка за ефективноста на вработените; исто така, предвидувачка аналитика со цел предвидување на нивните идни перформанси.

Оценувањето на работата со помош на алгоритми може да доведе до одредени проблеми – не само поврзани со дискриминација, туку и со губење на чувството за приватност на вработените, безбедноста на информациите итн.

Алгоритми што се користат за наградување

Алгоритамското наградување може да обезбеди награди во реално време за однесувања што ги исполнуваат однапред дефинираните упатства. Може да користи и принципи на гејмификација, за да го направи работното искуство попозитивно и позабавно за вработените.

Дисциплина на работно место

Алгоритамската замена (*algorithmic replacing*) е базирана на брзо или дури и автоматско отпуштање вработени со ниски резултати, како и нивна замена со поефикасни вработени.

Автоматско донесување одлуки и профилирање

Членот 22 од ОРЗП потврдува дека, лицето на коешто се однесуваат податоците има право да не биде предмет на одлука заснована исклучиво врз автоматска обработка, вклучително и профилирање, што доведува до правни последици што се однесуваат на истото лице или на сличен начин имаат влијание врз одлуката. Правото на едно лице да ја оспори автоматизираната одлука што се однесува на него се заснова врз две тези за квалификувано профилирање: автоматизирана обработка и правни последици или фактори што значително влијаат врз одредено лице.

Што претставува автоматско донесување одлуки?

Благодарение на кодифицираното знаење и прецизната анализа на условите на животната средина, компјутерот може да издава инструкции без учество на човечкиот елемент. Оваа операција се заснова врз напредни пресметки и исклучиво технички средства за обработка. На тој начин се минимизира човечкото учество во процесите на донесување одлуки, а резултатите се издаваат на автоматизиран начин.

Меѓутоа, за обработката на податоците да се смета за целосно автоматизирана, во процесот на донесување одлуки не треба да има човечка интервенција. Треба да се забележи дека уделот на човекот при донесување на одлуката, којашто се состои, на пример, само од одобрување на одлуката наведена од алгоритмот, нема да претставува основа за исклучување од опфатот на употреба на забраната според член 22 од ОРЗП. Меѓутоа, доколку лицето кое има овластување и компетенција да ја промени одлуката би преземало акција за да ја смени одлуката, во тој случај нема да има автоматско одлучување.

Што се однесува до ситуациите од чл. 22 од ОРЗП, тие ги опфаќаат двете ситуации во кои одлуката предизвикува правни последици (т.е. влијае врз правата на поединецот во согласност со прописите; на пр. право на бенефиции за невработеност) или има „слично

значајно влијание“ (на пр. се однесува на финансиската состојба или здравствената состојба на даден субјект).

Што претставува профилирање?

Во чл. 22 од ОРЗП е вклучена и посебна категорија на автоматско донесување одлуки, односно врз основа на профилирање. Терминот „профилирање“ (член 4 од ОРЗП) се дефинира како каква било форма на автоматизирана обработка на лични податоци што се состои од нивна употреба за анализа или процена на одредени лични аспекти на физичко лице. Конкретно, ова се однесува на анализа или на предвидување аспекти што се однесуваат на **ефективноста на работата на тоа физичко лице**, економска и здравствена состојба, лични преференци, интереси, кредибилитет, однесување, локација или движење[4].

Практични примери за профилирање:

- **Маркетинг** – креирање профили на потрошувачи преку собирање информации за нивните преференци за купување и предложување производи индивидуално адаптирани на клиентот
- **Позајмици и кредити** – креирање профили на кандидати и донесување потврдна одлука за кредит во зависност од анализата на личните податоци доставени до алгоритмот,
- **Придобивки од социјална помош** – користење профилирање со цел правична распределба на средствата од државната помош,
- **Регрутација и човечки ресурси (HR)** – процесите на масовно регрутирање често се спроведуваат со користење системи што самостојно ја анализираат биографијата на кандидатот и другите податоци, и врз основа на таквата анализа, донесуваат одлуки за отфрлање или прием на кандидатот (на пр. по пребарувањето на CV-то со клучни зборови). Во областа на човечките ресурси, профилирањето се користи и за оценување на работата.

Ризици поврзани со профилирање

- **Нарушување на приватноста и недостаток на транспарентност** – иако многу луѓе се свесни дека одредени видови податоци (на пример, медицински) се особено чувствителни и треба да бидат заштитени, голем дел од општеството не е свесно за

[4] Треба да се напомене дека, и покрај сличностите, профилирањето и автоматското донесување одлуки се две различни активности, што може или не мора да бидат меѓусебно поврзани.

фактот колку информации за нив може да се добијат од бихејвиоралните податоци што се користат за непосакувано профилирање. Освен тоа, самиот процес на профилирање често е нетранспарентен и неразбирлив за засегнатите лица.

- **Дискриминација** – Алгоритмите проектирани од човекот можат да ги пренесат насоките на нивните креатори. Со тоа, системот може понеповолно да ги третира, на пример, луѓето со различни религиозни погледи, сексуална ориентација или боја на кожа.
- **Ограничување на разновидноста** – профилирањето има цел да врши процена, да ги окарактеризира и препознае групите на примателите на дадена содржина со цел да се совпаднат материјалите во однос на интересите или верувањата (на пр. политички) на одредени луѓе. Затоа, го намалува обемот на информации што му се даваат на корисникот, ограничувајќи ја притоа разновидноста на содржините и создавајќи т.н. меурчиња со информации и стеснување на виртуелниот хоризонт на примателот.

Профилирање во работниот процес – студија на случај

Од 2020 година, Австриската јавна служба за вработување (AMS) користи алгоритамско профилирање за лицата што бараат работа, со цел зголемување на ефективноста на процесот на советување и приспособување на тековните програми на потребите на пазарот на трудот. Системот е проектиран да ги класифицира барателите на работа во три категории:

- Група А. Добри изгледи за наоѓање работа во периодот што следи.
- Група Б. Просечни изгледи.
- Група В. Ниски изгледи на долг рок

Потоа, во зависност од назначената категорија, алгоритмот ја приспособува помошната програма кон потребите на единицата.

Прашање за дискусија: Дали е оправдано алгоритамското профилирање на луѓето без работа, со цел усогласување со програмите за поддршка на нивните потреби?

Пример: во Њујорк беше објавен закон за ограничување на употребата на алатки за вештачка интелигенција во процесите на регрутирање. Како што беше наведено, главниот проблем на проценатa со вештачка интелигенција беше исклучувањето од процесот на групите кои не одговараат на програмираниот клуч. Примерите вклучуваат дисквалификување лица со пречки во говорот што е проценето од страна на компјутерот за време на видеоповик или одбивање апликанти со артритис или други состојби што ја ограничуваат нивната физичка подготвеност (во случај на тестови на време).

Прашање за дискусија: Дали треба да се забранат сите видови алгоритамска процена во процесот на регрутирање?

Пример: Некој работодавач работел на создавање и имплементација на алатка за вештачка интелигенција во својата компанија, која требало да помогне при вработување луѓе со соодветен профил за дадената позиција. Работата била прекината кога компанијата сфатила дека системот ги дискриминира жените. Причината за почестото отфрлање на женските профили била тоа што вештачката интелигенција се базирала на податоците од биографиите на луѓето кои работеле во компанијата во последните 10 години (најчесто мажи). Како резултат на тоа, компјутерот проценил дека треба да им даде приоритет на мажите, што автоматски ги намалува шансите на жените-апликанти.

Прашање за дискусија: Дали можете да идентификувате други примери на дискриминација што може да се појават при регрутирање со помош на алгоритми за профилирање?

Закани и придобивки од користењето на алгоритми во однос на вработените

Закани:

- поголема контрола на работодавач на сметка на приватноста на работникот (недостиг на соодветна согласност од работникот),
- ерозија на човековата автономија преку замена на директниот контакт помеѓу менаџерите и нивните подредени, т.е. „дехуманизација“ на системите за управување,
- алгоритамска предрасуда и дискриминација.

Придобивки:

- зголемена продуктивност благодарение на заштедено време и поефикасно одлучување,
- поефективно планирање на смените и распределување на одговорностите,

- можност за спроведување побрзо регрутирање,
- разбирање на проблемите што се јавуваат на работното место преку подобар увид во работната средина,
- поретко фаворизирање на вработените и елиминирање на предрасудите што може да се појават во директните односи со вработените,
- автоматското донесување одлуки ја ограничува можноста за мешање во одлуките на менаџментот во врска со плата, одобрување одмор или распоредувањето во смена.

Алгоритмизација на односот работник – работодавач

Алгоритмизацијата на работните процеси е веќе реалност во многу компании. Сепак, често работи против вработените за прашања како што се:

- **Автоматско отпуштање вработени** (прашање што треба да се дискутира како дел од дискусиите на обуката).
- **Алгоритамска пресметка на плата:**
    - Алгоритмот на курирската апликација издал налог на лицата задолжени за доставување на нарачките, без оглед на оддалеченоста од местото на подигање на нарачката. Возачите не добиле надомест за растојанието до местото на подигање. Работодавачот ги покривал само трошоците за патување на пократко растојание, како резултат на што, кога ќе се одбијат трошоците за гориво и амортизација на автомобилот, возачите не остварile никаков профит.
    - Компанијата тврди дека заработката зависи од бројот на поминати километри и дека за секоја нарачка се исплаќа фиксна стапка наречена „основна стапка“, која може да варира во зависност од градот.
    - Меѓутоа, проблем беше и несигурноста на вработените во однос на стапката за саатницата – за време на пандемијата, куририте добиваа информации за промена на тарифата во рок од еден ден, поради што често беа принудени да „доплаќаат“ наместо да заработуваат од извршената работа.
    - Неколку промени им беа ветени на куририте по штрајкот, меѓу другото, можност за одбивање нарачка трипати на ден, а не само еднаш. Врз основа на ова, во случај на неповолна промена на основната цена, куририте имаат можност да одбијат да ја реализираат нарачката. Сепак, поголема стабилизација на стапката не беше прогласена.

Алгоритамска идентификација на вработените

- Апликациите за такси користат софтвер што служи за утврдување на идентитетот на нивните возачи врз основа на селфи сликите што ги поставуваат. Во 2018 година, беше потврдено дека овој тип на софтвер, кој го користи една од компаниите, е склон да направи грешки во случајот кај лицата со темен тен на кожата (вреди да се напомене дека огромно мнозинство возачи кои користат такси апликации се мажи, а многу од нив се со BAME потекло (црни, азиски и малцински заедници).
- Во врска со проверката на идентитетот, неколку курири пријавиле дека, поради проблеми со алгоритмот, им се заканувало раскинување на договорите за вработување, замрзнување на сметките или трајно отпуштање од работа откако селфито што го направиле не ги исполнило критериумите за идентификацијата според *Real Time ID Check*. Некои луѓе биле отпуштени од работа откако функцијата за селфи воопшто не работела. Овој процес не го вклучува правото на жалба.

- **Алгоритамска оцена (не само перформанси) на вработените** (прашање што треба да се дискутира како дел од дискусијата за време на обуката).

Алгоритмизација и заштита на личните податоци

Како што веќе беше напоменато, алгоритам е серија инструкции за тоа како збир на факти за светот да се претворат во корисни информации. Кажано уште поедноставно, фактите се третираат како податоци, а информацијата како знаење, што подоцна може да се користи од луѓето или други машини.

Податоци на работно место и заштита на истите

За да се избегнат конфликти во врска со приватноста, работодавачите треба да спроведат соодветни мерки за заштита на личните податоци, особено кога овие податоци се користат за автоматско одлучување што директно влијае на работникот. Затоа, потребно е соодветно да се балансира интересот на работодавачот кој се грижи за имплементација на технологии базирани на податоци, како и интересите на субјектот на којшто се однесуваат податоците, и се постапува во согласност со основните принципи на ОРЗП.

- **Работодавачите треба да собираат податоци за вработените исклучиво кога е неопходно да се управува со работното место и да се извршуваат задачите на вработените**

Согласно со принципот за минимизирање на количината на податоци, работодавачите треба да го ограничат собирањето на податоци за вработените, односно какви било информации што се однесуваат на нивниот идентитет, здравје и биометрика, податоци поврзани со активности преземени на работното место (на пр. податоци што се однесуваат на продуктивноста), но исто така и информации што произлегуваат од активноста на вработените на социјалните мрежи. Неограниченото собирање податоци непотребно ги изложува вработените на ризици, како што е злоупотреба на личните податоци од страна на работодавачите или нивно неконтролирано истекување.

- **Вработените треба да имаат право на преглед, корекција и преземање на нивните податоци**

Вработените треба да имаат можност за добивање на сите релевантни информации за нивните податоци – вклучително и информација зошто и како се собрани нивните податоци, што е заклучено за вработениот врз основа на нив и дали податоците биле користени за донесување одлуки поврзани со нивното вработување. Работодавачите треба да бидат одговорни за корекција на сите неточни податоци.

- **Податоците на вработените треба да бидат заштитени од злоупотреба**

Во ниту еден случај работодавачот не смее да дозволи продажба или лиценцирање на податоците за вработените на трети лица. Да не беше ова предупредување, ветувањето за профит од „монетизацијата" на податоците за вработените ќе претставуваше преголем ризик, бидејќи работодавачите ќе ги користат податоците несоодветно за дополнителна заработка.

- **Согласност за обработка на лични податоци**

Во рамките на работните односи, согласноста за обработка на лични податоци покренува многу контроверзии, бидејќи поради немање рамнотежа на страните, лесно може да се доведе во прашање доброволната природа на давањето таква согласност од страна на вработениот. Треба да се забележи дека работодавачот лесно може да го принуди работникот да ги исполни неговите очекувања под закана од негативни последици поврзани со вработувањето. Сепак, во согласност со чл. 155 од ОРЗП, земјите членки може да воведат детални прописи во врска со обработката на личните податоци на вработените во контекст на вработувањето, а особено условите под кои личните податоци може да се обработуваат со согласност на вработениот.

На пример, во Полска, работодавачот може да собира лични податоци наведени во Законот за работни односи, само ако работникот се согласи со тоа. Сепак, треба да се напомене дека, согласноста треба да се даде доброволно и нема да биде ефективна

доколку вработениот нема да има можност да ја одбие поради страв од негативни последици. Покрај тоа, согласноста може да се отповика во секое време.

Видови податоци што се користат во различни фази на работа

Фаза I. Барање работа

Што може да очекува работодавачот?

Работодавачот може да очекува од кандидатот да му ги даде основните податоци што се неопходни за преземање чекори за склучување на договорот. Таквите податоци може да бидат:

- Идентификациски (име, презиме, имиња на родители, датум на раѓање),
- податоци за контакт назначени од такво лице;
- Податоци што се однесуваат на образование, вештини, професионално искуство (за завршено образование, поминати обуки и курсеви, претходни работодавачи, работни позиции и професионални обврски).

Поважно е дека, во случај на учество во процесот на регрутација, и покрај споделените податоци, може воопшто да не дојде до склучување на договорот.

Што може да очекува кандидатот?

Веќе во првата фаза од регрутацијата, потенцијалниот работодавач кој собира податоци од кандидатите, е должен да ги информира овие лица за:

- целосниот назив и адресата на седиштето на компанијата,
- податоците за контакт на лицето одговорно за заштита на податоците (доколку е назначено),
- целта на обработката на податоците и правната основа за таквата обработка која му била позната во моментот на собирањето на податоците, примателите на податоците (широко разбрани) или нивните категории,
- намерата за прекугранична обработка на податоци (доколку постои),
- периодот во кој ќе се обработуваат податоците или критериумите за утврдување на овој период

- правото што го има кандидатот за барање пристап до податоците, вклучително и добивање копија од нив, како и корекција, бришење или ограничување на обработката на податоците,
- правото да се повлече согласноста во одреден момент без да влијае на законитоста на обработката, врз основа на согласност дадена пред повлекување на согласноста (доколку податоците се собрани врз основа на согласност),
- право да поднесе жалба до раководителот на Управата за заштита на лични податоци,
- добра волја или обврска за давање податоци и последиците од истото доколку податоците не бидат споделени.

Фаза II. Процес на регрутација

За време на интервјуто, регрутерот може да постави многу подетални прашања во врска со информациите што кандидатот за вработување ги вклучил во своето CV. Меѓутоа, важно е тие да се однесуваат само на прашања поврзани со позицијата за која што аплицира. Неприфатливи се прашања што можат да го засрамат кандидатот, да го нарушат неговото право на приватност или лични права (на пр. во врска со приватен живот, религија, сексуална ориентација, политички убедувања итн.).

Временска рамка за чување на податоците

Периодот на чување на податоците на кандидатот треба да биде во согласност со правилата за обработка на податоците однапред определени од администраторот. Според правилата, работодавачот треба трајно да ги избрише личните податоци на кандидатот за кој одлучил да не склучи договор за вработување веднаш по завршувањето на процесот на регрутација, односно по потпишувањето на договорот за вработување со нововработениот (на пр. со бришење или враќање на податоците).

Фаза III. Период на вработување

Со засновањето работен однос, како за работодавачот така и за работникот, се создаваат одредени права и обврски. Нивното спроведување очигледно се поврзува со потребата од обработка на личните податоци на вработениот. Администрирањето на личните податоци, иако генерално е регулирано во ОРЗП, во случај на работен однос, дополнително е специфицирано и во рамките на националните регулативи.

На пример, во Полска, согласно чл. 221 став 2 и 4 од Законот за работни односи, работодавачот има право да бара од работникот што одлучил да го вработи да обезбеди

(без разлика на личните податоци што можеби ги добил од него при регрутирањето) исто така и:

- адреса на живеење,
- ЕМБГ,
- други лични податоци, вклучувајќи имиња и презимиња и датуми на раѓање на неговите деца, доколку давањето такви податоци е неопходно за исполнување соодветни критериуми за користење посебни права предвидени во трудовото право,
- образование и преглед на претходен работен однос, доколку не биле побарани од кандидатот при регрутирањето,
- број на трансакциска сметка, доколку работникот не поднел барање за исплата на надоместокот на рака.

Обврска на работадавачот за информирање на работникот

Податоците на работникот може да бидат обработени од страна на работодавачот за различна цел отколку во случајот со кандидатот, за што работникот треба да биде соодветно информиран. Оваа цел може да се постигне со вклучување на таквите информации во информативната клаузула што им се дава на кандидатите при регрутирањето, преку дополнување на клаузулата со информации што се однесуваат на целта на обработка на податоците и со наведување на примателите на податоците во случај на вработување на кандидатот или, пак, со дополнување на оваа информација веднаш по вработувањето на кандидатот.

Контрола на алгоритмите што се користат во работата (транспарентност на алгоритми)

Следниве примери за употреба на вештачка интелигенција на работното место покажуваат дека неконтролираното користење алатки за вештачка интелигенција од страна на компаниите може да доведе до зголемена несигурност кај вработените, а со тоа да има негативно влијание врз животот на вработените. Во исто време, според проценките на McKinsey Global Institute, дури 70 % од компаниите ќе имплементираат одредени форми на системи за вештачка интелигенција до 2030 година. Поради оваа причина, многу е важно критички да се проценат новите технологии и да се овозможи надзорните органи и независните организации да спроведат ревизии во областа на вештачката интелигенција.

- Во Велика Британија, софтверот Horizon што го користи националната пошта, лажно обвини поединечни вработени за кражба на дури десетици илјади британски фунти. Како резултат на грешката на вештачката интелигенција, обвинети беа дури 736

поштенски работници, а против некои од нив биле покренати обвинениja и биле осудени.

- Во Холандија, возачите на апликацијата за такси ја тужат компанијата, откако алгоритам им ги блокирал сметките за наводна измама. Судот ги отфрли нивните барања бидејќи утврди дека повредите не спаѓаат во дефиницијата за целосно автоматизирано одлучување предвидена во ОРЗП. Како резултат на тоа, вработените останаа без никаква правна заштита.
- Во Италија, судот ѝ нареди на една компанија за испорака на храна да го открие алгоритмот на апликацијата и да ги елиминира елементите што, поради недоволно разгледување на прашањата регулирани во законот за работни односи (како боледување или право на штрајк), го направија дискриминаторски.

Алгоритам и деловна тајна

Во согласност со правото на ЕУ, информациите на тема технологија или кои било други аспекти што се однесуваат на компанијата, може да бидат заштитени како деловна тајна. Сепак, тие мора да ги исполнуваат следниве услови:

- информациите за алгоритмот не се широко познати ниту меѓу експертите во одреден сектор,
- информациите за алгоритмот имаат комерцијална вредност,
- преземени се мерки за да се обезбеди доверливост на информациите, на пример, информациите се чуваат на безбедно место и секој што има пристап до нив или за кого се достапни информациите, потпишал договор за доверливост.

Во случајот на нови технологии што се користат во работните процеси, исполнувањето на овие услови не е тешко. Компаниите често цитираат трговски тајни, истакнувајќи ја нивната загриженост за губење на конкурентноста како резултат на откривање на нивните внатрешни системи. Поради оваа причина, увидот во алгоритмите и валидацијата на алатките за вештачка интелигенција во приватниот сектор се особено проблематични. Покрај тоа, дополнителните форми на законски заштитни мерки во форма на клаузули за доверливост спречуваат внатрешни лица (сегашни или поранешни вработени) да споделуваат информации за механизмите што ја координираат нивната работа.

Закон за вештачка интелигенција (AI Act)

Зачестените обвинувања за дуплирање, предрасуди, неточност или дискриминација од страна на алгоритмите на вештачката интелигенција резултираа со фактот дека Европската

комисија се обврза да воведе регулатива насочена кон контрола на алатките за вештачка интелигенција и спречување на негативните последици од нивната употреба.

На 12 април 2021 година, ЕК претстави нацрт-регулатива за вештачка интелигенција на ЕУ – прв таков комплексен правен акт што се однесува на алатки за вештачка интелигенција. Целта на регулативата е обезбедување соодветна средина за развој на вештачката интелигенција во Европската Унија, притоа земајќи ги предвид ризиците поврзани со развојот на најновите технологии. Сепак, пред сè, Законот за вештачка интелигенција има за цел, алгоритмите имплементирани во ЕУ да ги направи безбедни, транспарентни, етички, непристрасни и контролирани од луѓето.

Пристап заснован врз ризик

Главна претпоставка на законот е дефинирање на ризикот што го носи даден систем на вештачка интелигенција и да зависи од тоа на кои регулаторни обврски и барања ќе подлежат и креаторите и субјектите што спроведуваат вештачка интелигенција.

- **Неприфатлив ризик** – забрана за вештачка интелигенција

Забрана за особено штетни примени на вештачка интелигенција, спротивни на вредностите на ЕУ, што создаваат ризик од прекршување на основните права на поединците, на пр. оценување на влијанието на поединци врз основа на нивните социјални мрежи (т.н *social scoring*), искористување на слабостите на одредена група на луѓе од аспект на возраста, физичка попреченост или ментално растројство, употреба на сублиминални техники, употреба на биометриска идентификација на јавни простори, како и за цели на спроведување на законот (со неколку исклучоци).

- **Висок ризик -** вештачката интелигенција е дозволена, но под одредени услови

Алатките што имаат негативно влијание врз безбедноста на луѓето или нивните основни права, се системи што се класифицираат како системи со висок ризик, т.е. тоа се системи од следните области:

- биометриска идентификација и категоризација на физички лица,
- управување со критична инфраструктура,
- стручно образование или професионална обука – можност да се одлучи за пристап до стручно образование и обука за одредено лице (на пр. оценување испити),
- безбедност на производи (на пр. употреба на вештачка интелигенција во хирургија со помош на роботи),

- вработување, управување со вработени и пристап до самовработување (на пр. софтвер за анализа на CV за потребите на процедурата за регрутирање),
- основни приватни и јавни услуги (на пр. проценка на кредитната способност, кредитно бодување),
- спроведување закон – конфликт со основните права на луѓето (на пр. верификација на автентичноста на документите),
- миграција, азил и управување со граничната контрола (на пр. оценување на барањата за доделување азил),
- спроведување правда и демократски процеси (на пр. сугерирање на видот и тежината на казната за лице осудено за кривично дело).

Примери за специфични барања за системи со висок ризик:

- **Барања што се однесуваат на транспарентност** – функционирањето на високоризичните системи за вештачка интелигенција треба да биде доволно транспарентно за да им овозможи на корисниците да ги толкуваат информациите што се однесуваат на нивните резултати. За високоризичните системи со вештачка интелигенција треба да се изготви упатство за употреба.
- **Задолжителен човечки надзор над системите со висок ризик** – неопходно е обезбедување ефективен надзор над високоризичната вештачка интелигенција од страна на луѓето, вклучително и разбирање на можностите и ограничувањата на предметниот систем на вештачка интелигенција. Соодветните мерки за надзор може да вклучуваат донесување одлука да не се користи системот за вештачка интелигенција во дадена ситуација, игнорирање на одлуката донесена од системот за вештачка интелигенција или запирање на системот користејќи го копчето СТОП.

Работни прашања за вештачка интелигенција покренати во Законот за вештачка интелигенција

Системите со висок ризик што влијаат врз пазарот на трудот и подлежат на посебен надзор се наведени во Анекс III на нацрт-законот во однос на вештачката интелигенција. Системи за вештачка интелигенција се следниве:

1. Системи што се користат во процесот на регрутирање или избор на одредени лица, особено оние што се користат за објавување огласи за работа, влезна селекција или филтрирање апликации, оценување на кандидатите за време на интервјуа или тестови.

2. Системи што донесуваат одлуки за нечие унапредување или отпуштање, утврдување и распределба на задачи и следење на ефективноста на вработените и нивното однесување.
3. Системи што одлучуваат за пристап до стручна обука или оценување на учесниците во обуката.

Како што е наведено погоре, горе споменатите системи за вештачка интелигенција може да имаат значително влијание врз професионалните перспективи на луѓето чии податоци ги обработуваат, а со тоа може да влијаат врз нивниот извор на егзистенција и врз висината на приходите. Европската комисија, исто така, посвети внимание на тоа дека, лошо дизајнираните и користени системи може да ги овековечат дискриминаторските обрасци (на пример, врз жените, постарите лица, лицата со посебни потреби, луѓето од различна расна, етничка или сексуална ориентација). Покрај тоа, системите за вештачка интелигенција што се користат за проверка на перформансите (особено системите базирани на биометрика) може да имаат влијание врз заштитата на личните податоци и правото на приватност. Поради оваа причина, тие треба да подлежат на особено рестриктивни услови, а вработените секогаш треба да имаат можност за жалба против одлуката на алгоритмот.

Критика на Законот за вештачка интелигенција

Се појавија многу критики во врска со примената на Законот за вештачка интелигенција во контекст на прашањата за вработување. Според експертите, регулативата посветува премалку внимание на прашањата на вработените, а контролата на транспарентноста на алгоритмите се сведува на општите барања за транспарентност наведени во чл. 52 од предлог-законот. Згора на тоа, сомнително е дека регулативата ќе стапи на сила пред 2025 година.

Страв од губење на работата поради алгоритмизација/роботизација

Според проценитe на McKinsey, автоматизацијата во различни гранки на економијата, до 2030 година, ќе доведе до потребата од преквалификација на дури 375 милиони работници. Малку поинакви прогнози, иако подеднакво вознемирувачки, беа претставени во извештајот од страна на Светскиот економски форум, кој во публикацијата „*Future of Jobs*“ посочи дека во наредните години напредокот во областа на алгоритмизацијата и техниките на пресметување може да резултира со преземање на 75 милиони работни места од страна на машините.

Кога станува збор за последиците од роботизацијата, може да се претпостави дека, најмногу ќе бидат погодени луѓето кои вршат физичка работа, особено оние типови

базирани на предвидливи секвенции. Сепак, автоматизацијата може негативно да влијае и врз ситуацијата на некои професионалци. Според цитираниот извештај „*Future of Jobs*“, меѓу професиите засегнати од вештачката интелигенција, како што се механичар, магационер и менаџер на производство, ќе се вброи и професијата правник или финансиски аналитичар. Уште повеќе, ефектите од автоматизацијата ќе ги почувствуваат и луѓето чии професии се потпираат на собирање и процесирање податоци, односно задачи што многу побрзо и попрецизно се извршуваат со помош на машините.

Дури 60 % од вработените се сведоци дека 1/3 од задачите од нивното тековно работно место се автоматизирани. Затоа, не треба да изненадува тоа што вработените се загрижени за нивните досегашни работни места. Според извештајот на Procontent Communication „*Пандемијата ја автоматизира Полска?“*, речиси секој петти испитаник (18,7 %) се плаши од автоматизирање на своето работно место, а потоа и од негово губење. Сепак, експертите ги разладуваат стравовите – гледајќи на глобално ниво, само 5 % од работните места може целосно да исчезнат. Уште повеќе, иако многу работни места ќе бидат заменети со машини, може да се очекува дека на нивно место ќе се појават нови професии како резултат на зголемувањето на побарувачката за меки вештини кои бараат креативност, емоционална интелигенција и критичко размислување.

Дополнително, развојот на технологијата ќе придонесе за континуирано создавање на нови, високо платени работни места во ИТ секторот – на глобално ниво до крајот на деценијата тоа би можело да изнесува дури 50 милиони работни места. Горенаведениот оптимистички пристап се чини го потврдува и веќе споменатата анализа на Светскиот економски форум, во која беше посочено дека со напредната автоматизација, ќе се појават до 133 милиони работни места. Додека, поради динамиката на промените предизвикани од дигитализацијата, колку е тешко прецизно да се одреди обликот на идното ниво на вработеност, толку, според експертите, е сомнително дека феноменот на технолошка структурна невработеност ќе се појави во блиска иднина.

Технологијата на услуга на инклузивноста

Дигитализацијата на работните места придонесува за поефективно вклучување на пазарот на трудот на оние социјални групи кои претходно биле привремено или трајно исклучени од него.

За **лицата со посебни потреби** може да се забележат следниве придобивки:

- помалку тешкотии поврзани со транспортот до работното место со кои претходно се соочиле лица со одредена физичка попреченост,

- помалата изложеност на стимули и поспокојниот начин на работа од далечина придонесуваат за поефикасна работа на лицата со интелектуална попреченост, хиперактивност или со тешкотии со концентрацијата и учењето,
- употребата на електронски телекомуникациски средства (е-пошта, инстант пораки) им овозможува на луѓето кои страдаат од говорни пречки да учествуваат активно во дискусијата.

Примери за придобивки за **родителите**:

- можност да поминуваат повеќе време со децата,
- намалување на изложеноста на целото семејство на вообичаени заразни болести (грип, настинка, КОВИД-19),
- можност за ефективно усогласување на приватниот и професионалниот живот за младите родители.

Работата од далечина исто така има големо влијание врз младите мајки кои остануваат на пазарот на трудот (дури 49 % од мајките кои работат признаваат дека познаваат барем едно лице кое ја напуштило работата или планира да го стори тоа поради барањето да се вратат во канцеларија).

Примери за придобивки што произлегуваат од **користење на апликации за такси**:

- дејствувајќи за родова еднаквост (во повеќето американски градови, жените сочинуваа помалку од 5% од таксистите досега, во случај на апликации за споделување економија, тоа е веќе околу 20-30 %),
- олеснување на влезот на пазарот на труд за мигранти (на пр. од Украина),
- нуди попристапни цени за возење – на пример, апликацијата Uber во Лос Анџелес е достапна во 21 област со ниски приходи, каде што овозможува многу поевтини возења од традиционалните такси компании.
-

1.6. Влијанието на новите технологии врз договорните односи (влијание врз релациите со работодавачот и создавање на тип на договор)– дискусија околу паметните договори (анг. smart contracts) и нивна идна применаво односотвработен – работодавач

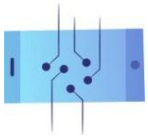
Дигитализацијата веќе ги опфати речиси сите области од нашето секојдневие и приватен живот. Ова исто така важи и за договорните односи што претходно се склучуваа усно или писмено, а сега често се зајакнуваат или дополнуваат со помош на дигитални алатки. Поради огромното количество информации на веб страните и сè почестото завршување на меѓусебните обврски вклучувајќи го и дигиталниот елемент, во блиска иднина најголемо влијание врз договорните односи секако ќе имаат алатките што користат блокчејн технологија, на пр. паметни договори (*smart contracts*).

Што претставува blockchain?

Блокчејн или верига од блокови со заштита (ang. *blockchain*) е технологија што се користи за испраќање и складирање информации за трансакции склучени преку интернет. Индивидуалните информации се распоредени во последователни блокови на податоци. Откако блокот ќе се исполни со одреден број трансакции, новите информации за трансакциите се запишуваат во следниот блок. Благодарение на преносот на информациите содржани во претходниот блок на следниот блок во ланецот, станува невозможно да се промени или избрише записот на една трансакција без истата промена да се забележи во сите следни блокови. Ова решение ја промовира транспарентноста на трансакциите и спречува измами и манипулација со информации.

Што претставуваат *smart contracts (паметни договори)*?

Паметниот договор е „самоизвршувачка“ програма базирана на логиката „ако-тогаш“ (анг. *if-then)*. Тој е целосно напишан на програмски јазик и може да работи со помош на технологија за дистрибуиран регистар (DLT) или блокчејн. Во вториот случај, програмата се зачувува на блокчејнот и се вклучува кога одредени услови предизвикуваат друго дејство – на пример, може да активира плаќање или да обезбеди одредена услуга. Значи, тоа е поврзување на **реалноста создадена врз основа на даден договор со реалниот свет користејќи технологија**. Благодарение на ова, договорот е потранспарентен и кредибилен, обезбедувајќи им на страните сигурност во исполнувањето на условите на истиот, кога ќе се појави одредена ситуација.



Примери за користење паметни договори:

- Купување недвижности – благодарение на паметните договори, процесот што обично е многу сложен и бара вклучување на многу посредници (нотар, агент за недвижности, правен советник, кредитна институција), значително е упростен и не бара учество на горенаведените субјекти, овозможувајќи стекнување на сопственост во електронска форма.
- Купување преку интернет – во овој случај, паметните договори обезбедуваат итно извршување на плаќањето, а со тоа и побрза испорака на производот до купувачот.
- Обработка на лични податоци – поради складирањето лични податоци и дигитални лични карти на блокчејн, ризикот од кражба на идентитетот е многу помал.
- Запишување резултати од избори или референдуми – минимизирање на ризикот од фалсификување на резултатите од гласањето. Употребата на паметни договори за оваа намена може да се забележи во пракса, на пр. во Естонија.
- Плаќање обесштетување и исплата на придонеси – автоматско подмирување на обесштетување, пресметка на висина на придонеси.

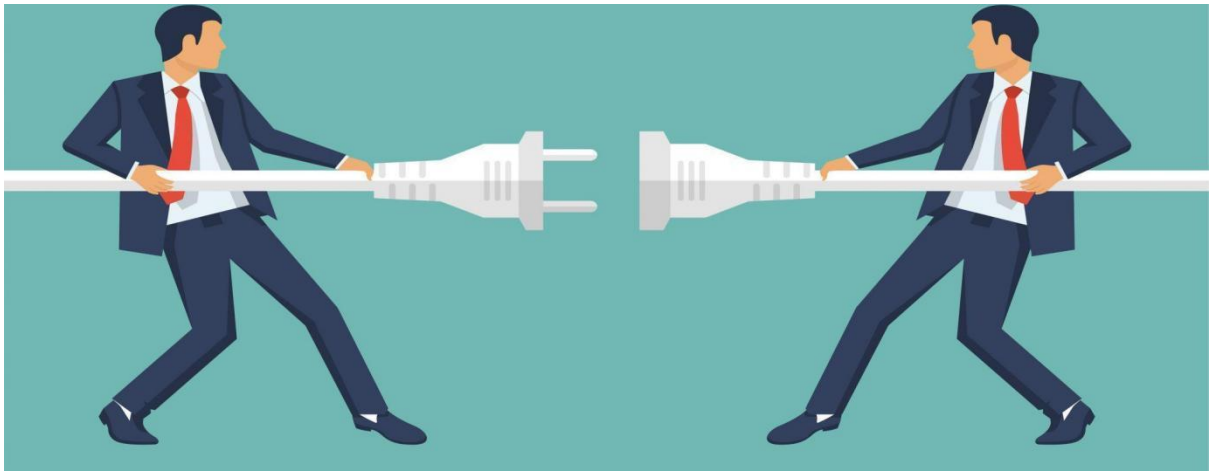
2. Влијание на дигитализацијата врз приватниот живот на вработените

2.1. Заштита на работното време на вработените при работа од далечина. Работа од далечина и рамнотежа помеѓу работата и приватниот живот (work-life balance)

Според истражувањето на Eurofound, 1/3 од вработените во Европската Унија почнале да работат од дома за време на пандемијата, а што се однесува на преминот кон работа од далечина, дури 27 % од нив се изјасниле дека извршуваат професионални обврски во слободното време. За време на карантинот/изолацијата, границата помеѓу приватниот и професионалниот живот почна да избледува. Вработените се стекнаа со можност сами да си го организираат времето, но беа изложени и на ризик да бидат постојано достапни и да не можат целосно да се исклучат од електронските уреди надвор од работното време.

Важно е тоа што, во режимот на задачи или период на работно време (незаснован на фиксно работно време), важат истите правила како во традиционалниот систем, односно, работникот треба да ги извршува своите должности во рамките на 8 часа работно време во текот на денот, 5 дена во неделата. Задачите што се извршуваат надвор од оваа рамка треба да се сметаат за прекувремена работа. Сепак, иако флексибилното работно време е несомнено корисно за вработените, тие често погрешно веруваат дека, бидејќи не се во канцеларија во фиксни часови, тие треба да бидат достапни во секое време од денот.

2.1.1. Право на исклучување



Извор: Shutterstock.

Како што е наведено во чл. 24 од Универзалната декларација за човекови права, секој човек има право на одмор и слободно време, вклучувајќи разумно ограничување на работното време и периодични платени одмори. Покрај тоа, во согласност со чл. 31 од Повелбата за основните права на ЕУ, секој работник има право на работни услови што го почитуваат неговото здравје, безбедност и достоинство и има право на дневен и неделен одмор, на годишен платен одмор и, пред сè, на ограничување на максималното работно време.

Новата постпандемиска реалност во која границата помеѓу приватниот и професионалниот живот е често замаглена, ја истакна потребата од спроведување регулатива што им дава доверба на вработените да можат, без негативни последици, да се одјават од работа и да не одговараат на е-пошта од нивните претпоставени по завршување на работното време. Поради оваа причина, во 2021 година Европскиот парламент донесе резолуција во корист на правото на исклучување, со што ја повика Европската комисија да подготви директива во однос на правото да се биде исклучен.

Вреди да се напомене дека, резолуциите на Европскиот парламент не се обврзувачки. Со тоа, Европската комисија не е обврзана да преземе активности за спроведување на директивата предложена од Парламентот. Сепак, земајќи ја предвид природата на предметот, може да се очекува дека Комисијата ќе се обиде да го регулира правото на исклучување и да обезбеди еднообразно ниво на заштита за работниците низ Европската Унија.

Како што е предложено од Европскиот парламент, директивата за правото да се биде исклучен треба да гарантира:

1) минимум правила со кои на вработените кои користат средства за далечинска комуникација во нивната секојдневна работа, им се гарантира правото на исклучување,
2) забрана за дискриминација или понеповолен третман на вработените кои го користат правото на исклучување (вклучувајќи ја и забраната за раскинување на договори за вработување),
3) еднаков третман на сите вработени, како од јавниот така и од приватниот сектор, вработените од пониско ниво и раководниот кадар (иако во вториот случај тоа може да биде тешко поради специфичните регулативи во врска со раководниот кадар),
4) ефикасна судска постапка и можност за поднесување тужби поврзани со повреда на дадените права (пристап до судска заштита од реперкусии).

Одговорности на работодавачите во однос на правото на на исклучување на вработените

Новите права за вработените повлекуваат и дополнителни обврски за работодавачите. Тие ја вклучуваат, на пр., потребата да се обезбеди внатрешен систем кој овозможува прецизно мерење на времето одработено секој ден од страна на вработениот (почитувајќи го правото на приватност и заштитата на личните податоци). Исто така, важно е да се поддржат вработените при правилно спроведување на правото да се исклучат – јасно да се соопштува новиот закон во политиката на компанијата, да се спроведуваат обуки и информативни кампањи во оваа област. Меѓутоа, во однос на подигањето на свеста, најважна обврска на работодавачот е писмено информирање на секој од вработенте за своите права.

Дополнително, работодавачите треба да избегнуваат промовирање на моделот „секогаш достапни“ и наградување на вработените кои не го користат своето право на исклучување. Проценатa на здравјето и безбедноста при работа во однос на правото на исклучување (на пр. во однос на психосоцијалните ризици) исто така треба да биде важно прашање.

2.1.2. Рамнотежа помеѓу приватниот и професионалниот живот - улогата на државата

Извор: Technology Headlines.

Важна улога во оформувањето на односот меѓу работникот и работодавачот има државата и нејзината трудова политика. Некои земји преземаат иницијативи за промовирање добри практики за вработување во однос на рамнотежата помеѓу работата и приватниот живот. Од една страна, ова се однесува на имплементацијата на државните прописи, а од друга страна, на инструментите поврзани со правото што немаат правно обврзувачка моќ, туку имаат за цел обликување одредени однесувања.

Ваквите „меки“ мерки може да се засноваат, на пример, врз имплементација на кодекси за добро однесување или давање добар пример на другите работодавачи преку промовирање потрудољубив пристап во структурите на државната администрација. Овој пат изборот падна на Малта, која во 2020 година објави *Прирачник за мерки за постигнување рамнотежа помеѓу работата и приватниот живот*. Оваа публикација ги сумира и детално ги опишува правата на вработените, заедно со упатствата за тоа како правилно да работите во ерата на дигитализација (на пр. како да ја организирате вашата работа додека ги извршувате вашите професионални обврски од далечина). Сепак, прирачникот не е корисен само за подобро познавање на привилегиите на вработените или дополнително знаење од областа на дигитализацијата. Ваквите прирачници за добри

практики, обврзувачки на работното место (или одреден сектор), исто така може да бидат еден вид „карта за договарање“ во преговорите со работодавачот.

Во случајот со прирачникот од Малта, иницијаторите на проектот посочија дека нивната главна цел е да обезбедат рамнотежа помеѓу работата и приватниот живот на луѓето кои се вработени во јавниот сектор преку зголемување на свеста на вработените. Сепак, вреди да се напомене дека прирачникот на никаков начин не го проширува опсегот на правата на вработените, туку само посветува внимание на соодветните практики за вработување и ги освестува вработените за можноста за преговарање за работните услови во согласност со одредбите од документот.

Примери за популаризирање на правото на исклучување во земјите на ЕУ

Иако во моментот не постои општо-европска правна рамка што го регулира правото на исклучување, сепак, во рамките на Европската Унија, веќе има некои примери на законодавно дејствување во оваа област. Ова е комбинирано со промовирање на правото на исклучување преку колективните договори. Покрај тоа, некои земји членки веќе имаат имплементирано сопствено законодавство за правото на исклучување.

Франција

Франција се смета за пионер во правото на исклучување. Уште во 2013 година усвои меѓусекторски договор за квалитет на животот на работа, со кој на компаниите им беше посочено да избегнуваат упад во приватниот живот на вработените и го прецизираше времето кога треба да се исклучат уредите што се користат за контакт со вработениот. Овие одредби потоа беа донесени на 8 август 2016 година и беа вклучени во францускиот работен законик. Дополнително, од јануари 2017 година, во Франција законски се бара работодавачите да преговараат за договори со синдикатите во врска со правото на исклучување.

Италија

По Франција, следеше Италија, која одлучи да го воведе правото на исклучување во 2017 година. Регулативата се фокусира на луѓето кои работат од далечина (анг. *smart working*, ит. *lavoro agile*) и утврдува дека вработените кои работат од далечина имаат право да се исклучат од технолошките уреди и онлајн платформите без да имаат никакви последици од работодавачите. Во Италија има и гански колективни договори и колективни договори на ниво на работодавач кои предвидуваат право на исклучување.

Шпанија

Следната земја која го усвои правото на исклучување во државното законодавство беше Шпанија. Во 2018 година, со транспонирањето на ОРЗП во шпанскиот закон, беше воведен нов пакет на дигитални права. Со него, вработените кои работат и во приватниот и во јавниот сектор добија право на исклучување чија цел беше да се одржи рамнотежа помеѓу приватниот и професионалниот живот. Според регулативата, работодавачите треба, откако ќе ги слушнат претставниците на вработените, да воспостават внатрешни правила со кои ќе се прецизира како вработените можат да го остварат правото на исклучување и да им обезбедат на вработените обука за правилна употреба на новите технологии.

Белгија

Во Белгија, во 2018 година, сите работодавачи со повеќе од 50 вработени требаше да разговараат со Комисијата за здравје и безбедност во однос на безбедното користење на дигиталните алатки и за правото на работниците да се исклучат. Вреди да се напомене дека со воведувањето на правото на исклучување, самите вработени не добија нови права, туку само поголеми можности да преговараат со работодавачот. Меѓутоа, во 2022 година, сепак беше усвоена нова регулатива која им овозчожи на службениците да ги исклучуваат службените електронски адреси и да не одговараат на СМС-пораки и телефонски повици надвор од работното време, без страв од негативни последици. Се разговара и за планови за проширување на новите правила на работниците од приватниот сектор.

Ирска

Во април 2021 година, ирската влада објави кодекс на однесување, според кој сите вработени имаат право да се исклучат и да не одговараат веднаш на електронски пораки, телефонски повици или други пораки од нивниот работодавач, по работното време. Во Кодексот, исто така, е утврдено дека работникот, по правило, не треба да биде принуден да врши работа надвор од стандардното работно време и не треба да биде одговорен доколку одбие да извршува деловни работи по работното време.

2.1.3. Спроведување на континуирана достапност од страна на работодавачот и мобинг

Извор: jobs.ca.

Мобингот е постапување/однесување насочено кон вработениот, засновано врз постојано и долгорочно вознемирување или заплашување. Се појавува во случаи кога одредени постапки се насочени кон понижување или исмевање на вработениот, но и кога треба да предизвикаат потценување на бенефитот од неговата професионална способност.

Поради фактот што мобингот може да има различни форми на агресија, збирот однесувања класифицирани во овој вид насилство останува отворен. Затоа, очекувањето вработениот да биде постојано достапен под закана од негативни последици може да се смета за вид на мобинг. Сведоштво за тоа наоѓаме, на пример, во пресудите во кои судовите се согласиле со вработените кои посочиле дека напорното и постојано примање пораки кои содржат работни налози по работното време или во слободните денови треба да се третира како мобинг.

Пресуда на Основен суд во Лублин од 20 јуни 2018 година (VIII Pa 86/18)

На вработените во општината, Судот им додели 25 илјади злоти од работодавачот како компензација за здравствено нарушување предизвикано со упорно испраќање електронски

пораки по работното време. Случајот се однесувал на жена вработена на работно место државен службеник на неопределено време со полно работно време. По смената на градоначалникот во општината, новиот градоначалник ја усвоил електронската пошта, т.е. праќање електронски пораки во форма на e-mail на службени и приватни електронски адреси, како основен начин за комуникација со вработените. Од 01.01.2015 година, тужителот добил околу 200 e-mail пораки од градоначалникот, од кои над 100 се испратени по работното време, вклучително и ноќе и во слободни денови, за време на празници или боледувања. Како резултат на постапката, беше донесена пресуда од Основниот суд во Лублин, во која Судот одлучи дека наметнување должности на вработен и испраќање е-пораки со налози за работа во слободни денови, за време на боледување и празници, како и несоодветна пресметка за неизвршената задача, може да се смета за **мобинг**.

Прекршување на правото на исклучување – последици за работодавачот и механизми за поднесување жалби

Казните за прекршување на правото на исклучување може да варираат од една до друга земја членка на ЕУ. Ова се должи на фактот што секоја земја членка треба поединечно да ја одреди висината на казната што треба да му биде изречена на работодавачот за непочитување на слободното време на своите вработени.

Во Полска сè уште не е воведено право на посебен вработен да се исклучи, но тоа може да се изведе од општите прописи за работното време и судските одлуки. Затоа, општо прифатено е дека вработениот нема обврска да одговара на телефон или да одговара на е-пораки по работното време или за време на одмор. Исклучок е ситуацијата кога е должен да врши дежурство, односно да остане во готовност надвор од стандардното работно време.

Најчести прекршоци што ги прават работодавачите во рамките на работниот однос се неправилностите поврзани со раскинување на договорите за вработување, прекршување на прописите за работното време, неправилна исплата на надомест или неправилно доделување одмори. Во зависност од обемот и видот на прекршокот, работодавачот може да биде казнет со парична казна од 1.000 до 30.000 злоти.

Со тоа, може да се очекува дека во Полска, непочитувањето на правото на исклучување ќе биде санкционирано на ист начин како и секое друго прекршување на прописите за работното време, односно работодавачот може биде казнет со парична казна до дури 30.000 злоти. Дополнително, во случај на полош третман на вработениот поради неговата ограничена достапност надвор од пропишаното работно време, може да се појават

прашања за обесштетување за дискриминација (во износ не помал од применливата минимална плата).

Според истражувањето на јавното мислење[5], 23,9 % од вработените во Полска добиваат е-пораки, текстуални пораки или други пораки од нивните претпоставени по работното време. Иако, како што забележуваат експертите, тоа не е забрането, ваквата постапка може да се смета за наредба за прекувремена работа (особено кога контактот го принудува вработениот да изврши дадена задача). Доколку е потребно да се одговори на е-пораки или телефонски разговор за деловни прашања, во согласност со чл. 151 (1) и 151 (2) од Законот за работни односи, таквата постапка мора да се компензира со дополнителен паричен надомест или одмор.

Што треба да направи полскиот работник чии што права се повредени?

a) Разговор со работодавачот

Пред да се донесе одлука за пријавување на нарушувањето на правата до надворешни органи, се препорачува работникот да се обиде да комуницира со работодавачот. Важно е, директорот или сопственикот на компанијата да се приклучат на разговорот, бидејќи може да излезе дека раководниот персонал не е свесен за неправилностите од претпоставените кои работат на пониско ниво.

b) Барање поддршка од синдикатите

Ако разговорот со работодавачот не ги донесе посакуваните резултати, работникот може да побара поддршка од синдикатите, доколку тие се активни на одредено работно место. Работата на синдикатот е да ги застапува работниците и треба повторно да се обиде да постигне договор со директорот/сопственикот на компанијата или нејзиното раководство.

[5] анкета спроведена од UCE RESEARCH и ePsychologii.pl, https://uce-pl.com/news/blisko-24-proc-polakow-twierdzi-ze-pracodawca-kontaktuje-sie-z-nimi-w-czasie-wolnym-od-pracy.

c) Пријавување прекршоци до Државниот трудов инспекторат (PIP)

Државниот трудов инспекторат (PIP) е најважната институција која се занимава со прашања за работните услови и правата на вработените во Полска. Тоа е првата институција до која треба да стигнат формалните пријави за прекршување на правата на вработените. Контакт податоци за инспекторатот може да се најдат на веб-локацијата www.pip.gov.pl, а жалбата може да се поднесе во писмена форма, преку телеграф, по факс, е-пошта, формулар за е-поплака, како и усно за евиденција. Деталите за вработениот кој поднесува жалба може да останат анонимни. Согласно Законот за државен трудов инспекторат[6], трудовиот инспектор е должен да не открива информации дека инспекцискиот надзор се врши по претставка од поднесена жалба, освен кога тужителот дава согласност за истото во писмена форма. Сепак, важно е да се запомни дека треба да се поднесе соодветното оправдување на наводите и презентирањето на веродостојни докази, а потоа инспекторатот ќе одлучи дали пријавата е веродостојна и дали ќе биде проверена.

d) Поднесување на случајот до окружниот суд

Материјалите доставени до инспекторатот, исто така, може да претставуваат доказ, ако случајот оди до окружниот суд. Сепак, покренувањето на судска постапка е последното средство што се користи само доколку претходните методи не успеале.

[6] Член 44 став 3 *Закон за државна трудова инспекција донесен на 13 април 2007 г.* (Сл.весник од 2017 г. поз. 786 со измените).

2.1.4. Work-life balance – што претставува рамнотежа помеѓу приватниот и професионалниот живот?

Извор: zapier.com.

Во согласност со извештајот „OECD How's Life? Measuring Well-being“, поимот *work-life balance* претставува одржување рамнотежа помеѓу работата (како платена, така и неплатена) и семејниот живот и слободното време. Тоа е поврзано со способноста на вработениот да ги организира должностите на таков начин што тие нема да го попречуваат неговото слободно време. Сепак, правилната рамнотежа помеѓу различните области од животот не зависи само од вработениот, туку и од работодавачот. Токму тој најчесто ја создава работната култура во компанијата и наметнува одредени стандарди.

Почитувањето на слободното време на вработените кои работат од канцеларија, работат работа на далечина или хибридно, е од огромно значење. Благосостојбата на секој вработен зависи од соодветната рамнотежа помеѓу работата и приватниот живот (добросостојба, ментална состојба). Како што покажуваат истражувањата, преоптоварувањето со должности и постојано работење (вклучувајќи домашни активности и грижа), може да доведе до исцрпеност на телото и здравствени проблеми, хроничен стрес или намалување на продуктивноста.

Пред пандемијата, времето што вработените со полно работно време го поминуваа во одмор и грижа за својата благосостојба се движеше од околу 14 до 16,5 часа на ден. Мажите со полно работно време земале 30 минути помалку одмор во споредба со жените. Сепак, статистиката изгледа поинаку во случај на работа од далечина, која стана популарна

за време на карантинот поради пандемијата на КОВИД-19. Времето поминато пред компјутерот тогаш беше значително продолжено (до два дополнителни часа дневно), а квалитетот на одморот се намали. Поверојатно е дека вработените кои работат од дома ќе се согласат на прекувремена работа и ќе ги извршуваат задачите навечер или за време на викендите, а со тоа ја замаглуваат границата помеѓу приватниот и професионалниот живот.

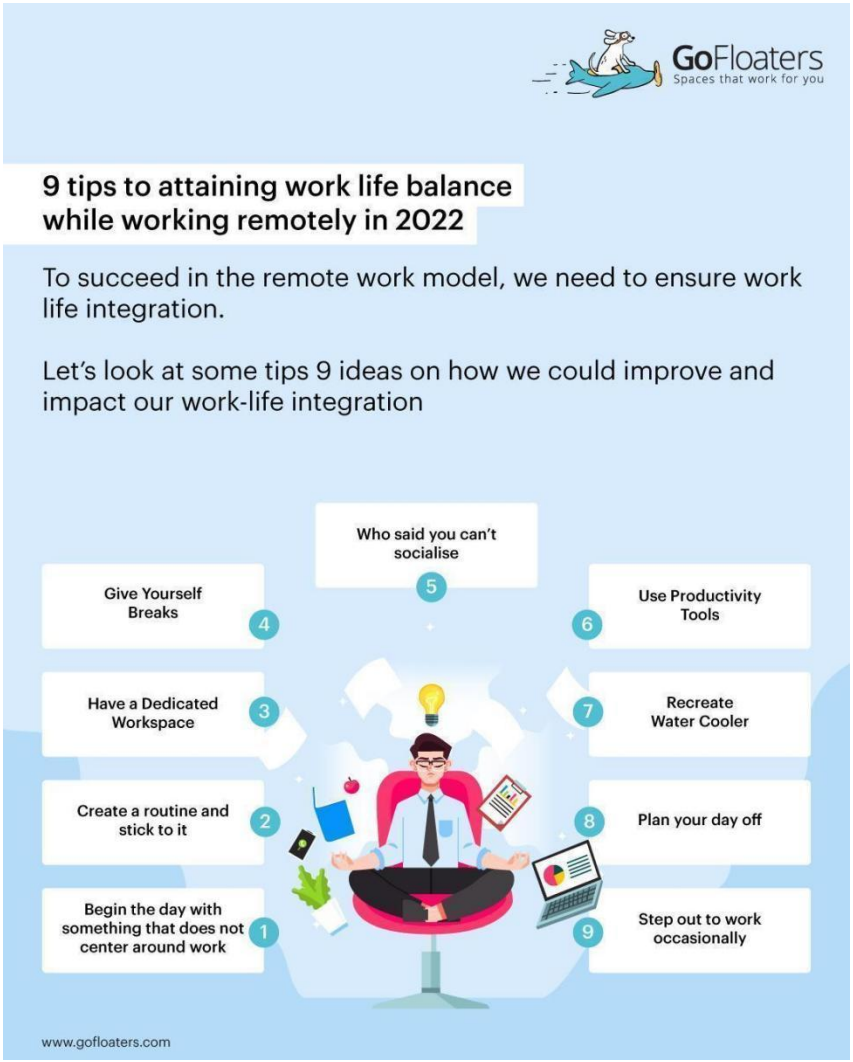
Сепак, одржувањето на споменатата рамнотежа е исклучително важно. Тоа овозможува да се избегне професионално исцрпување, поттикнува поголема мотивација на вработените и нивно ангажирање во активностите на компанијата. Тоа придонесува и за само-развој и поголема отвореност кон нови предизвици. Со тоа, и покрај помалиот број одработени часови, се зголемува ефикасноста на работниот кадар, а се намалуваат потребите за медицинска нега и боледување.

Како работодавачот може да ја поправи *рамнотежата помеѓу работата и приватниот живот* на своите вработени?

Рамнотежата помеѓу работата и приватниот живот на вработените често зависи од работодавачите и раководниот кадар. Тие се оние кои промовираат одредено однесување и ја формираат политиката за работење на работното место. Затоа е толку важно да се поддржуваат добрите навики кои им овозможуваат на вработените да се оттргнат од секојдневните професионални обврски. На пример, работодавачите можат да ги охрабрат своите вработени да прават паузи од работа, да работат флексибилно работно време кое е поволно за нив, да го користат правото на исклучување, јасно да ги соопштуваат своите потреби (на пр. да информираат за преоптоварување со должности и потребата да се намали работното темпо).

Исто така, важно е да се промовира здрава работна култура со избегнување да се наградува за постојана достапност или воведување на правилото за не одговарање на е-пошта и пораки по работното време. Исто така, добра идеја е да се спроведуваат обуки за вработените на темата рамнотежа помеѓу работата и приватниот живот и правото на исклучување, како и давање совети за тоа како лесно да се ограничи прекумерната употреба на дигитални алатки.

2.1.5. Дигитална безбедност и здравје при работа, или како самостојно да се ограничите да бидете постојано поврзани



Совети за вработените

1. **Исклучете ги известувањата на вашиот телефон**

Доколку имате комуникатори и апликации што се користат на работното место, а се инсталирани на вашиот приватен телефон или ако сандачето за службената електронска пошта е поврзано со приватното, исклучете ги сите известувања што може да ви го нарушат спокојот во слободното време. Исто така, добар начин е поставување временски ограничувања што ги стишуваат сите пораки по стандардните работни часови.

2. **Користете го службениот компјутер во работното време, а приватниот по работното време**

Изборот на службен компјутер за работа наместо личен уред е покорисно не само поради безбедност, туку и поради можноста да се ограничи вашата изложеност на комуникациите и пораките што ги добивате од колегите по работното време. Ако вашата компанија има политика BYOD (*bring your own device*), можете да креирате две сметки на вашиот уред (професионална и приватна) и да се префрлате помеѓу нив во зависност од времето од денот и вашите потреби.

3. **Аналогни утра и вечери**

Зрачењето на телефонот или лаптопот е слично на сончевата светлина која го намалува лачењето на мелатонин во мозокот. Ова, пак, го отежнува заспивањето, го намалува квалитетот на вашиот одмор и води до дополнителни проблеми со спиењето. За доброто на вашата благосостојба, обидете се да не ги користите телефонот и лаптопот барем еден час пред спиење. Исто така, не започнувајте го утрото со нервозно проверување на вашата е-пошта или социални мрежи.

4. **Внесете временска рамка во која користите дигитални алатки**

Дури и ако работите со флексибилно работно време, известете ги вашите претпоставени и луѓето со кои работите кога може да ве контактираат и кога вашата достапност ќе биде ограничена.

5. **Внесете целодневна детоксикација**

Иако дигиталната детоксикација не е главната и единствена компонента на идејата за рамнотежа помеѓу работата и приватниот живот, сепак целосното исклучување од мрежата и друштвените медиуми подолго време може да донесе огромни придобивки за благосостојбата на поединецот. Искуството на оставање на електрониката нѐ прави свесни колку време всушност поминуваме на интернет. Ова овозможува да се воспостават здрави граници помеѓу работата и приватниот живот. Исто така, ве мотивира да се ослободите од лошите навики, како што е компулсивна проверка на вашата е-пошта или посегнување по телефонот веднаш после будење. Затоа, се препорачува да користите циклична детоксикација (на пр. целосно исклучување за време на викендите) и слободното време да го поминувате на одмор, средби со семејството и пријателите или физичка активност, наместо да прелистувате на социјалните мрежи.

2.2. Комодификација на приватни ресурси – принудни или доброволни

2.2.1. Што претставува политиката BYOD (bring your own device)

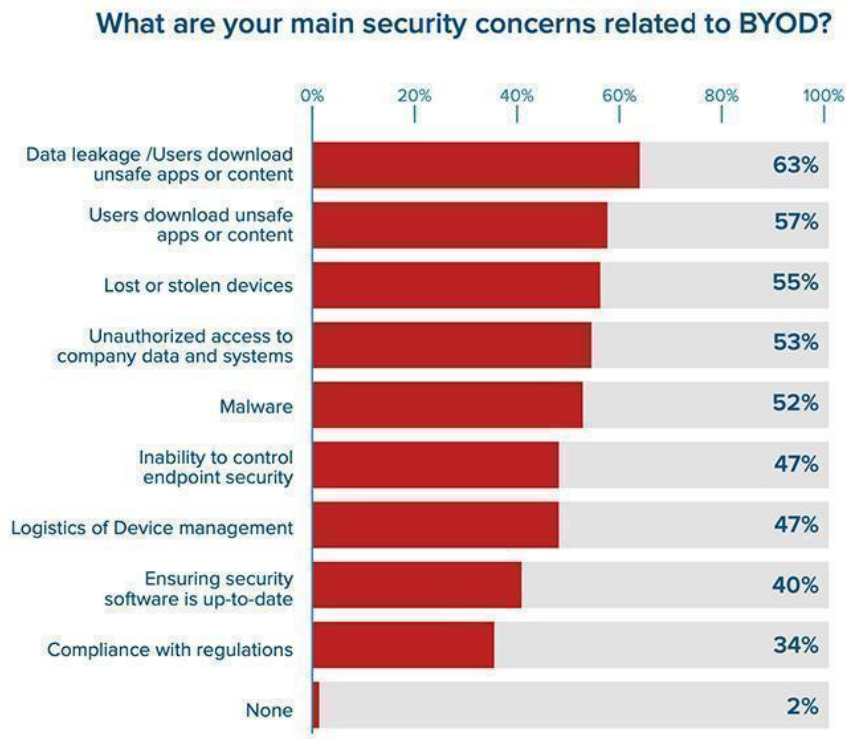
Формулацијата *bring your own device (д*онесете свој уред) е исто така позната под кратенката BYOD. Тоа е тренд на користење приватни уреди, како што се лаптопи, паметни телефони или таблети, за професионални обврски. Следењето на овој тренд често произлегува од волјата на самите вработени (доброволна комодификација на приватни ресурси). Понекогаш, сепак, политиката на BYOD ја претпочитаат и работодавачите (принудна комодификација на приватни ресурси). Иако овој тренд има многу предности, сепак, пред да се примени во претпријатието, треба да се земат предвид потенцијалните ризици, како што се прашањата за безбедност и приватност .

Вреди да се додаде дека BYOD е сосема спротивно од традиционалниот стил на работа наречен *here's your own device* (HYOD), во кој компаниите им ги даваат на своите вработени сите електронски уреди што им се потребни за работа.

Предности на политиката BYOD:

- **Флексибилност** – BYOD се врзува со согласност од страна на работодавачот за пристап до документите на компанијата на приватните уреди на вработениот. Така, извршувањето на професионалните обврски станува возможно секаде и во секое време. Дополнително, поголема флексибилност се манифестира во можноста за тестирање нови решенија, програми, дигитални алатки, бидејќи вработените не се ограничени на користење уреди од еден тип или бренд.
- **Комфорт** – една од придобивките на BYOD е тоа што вработените можат да користат уреди што ги знаат и се чувствуваат удобно додека ги користат.
- **Поголема продуктивност** – користењето на вашиот сопствен лаптоп или паметен телефон може да го олесни процесот на вклучување нови вработени, како и да ја зголеми продуктивноста на постојаните вработени.
- **Пониски трошоци (корист на работодавачот)** – согласувајќи се со политиката на BYOD, работодавачите често ја избегнуваат обврската да му обезбедат на работникот работна опрема, со што може да се избегнат дополнителни трошоци.
- **Децентрализација на податоци (корист на работодавачот)** – чувањето деловни документи на приватен лаптоп (под услов да се добро обезбедени) може да биде корисно за компанијата поради повисокото ниво на децентрализација на податоците. Во случај на протекување податоци или напад на малициозен софтвер на системот на компанијата, датотеките што се наоѓаат на уредите на вработените

нема да бидат пресретнати заедно со централната база на податоци на работодавачотот.



Извор: helpnetsecurity.com, *BYOD adoption is growing rapidly, but security is lagging*, https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/.

Недостатоци на политиката BYOD:

- **Сајбер(не)безбедност** – освен придобивките од децентрализацијата на податоците, прашањата за сајбер-безбедноста се најголемиот недостаток на политиката на BYOD. Користејќи приватни уреди, вработените се подготвени да складираат доверливи документи на нивните дискови, кои обично се помалку безбедни од оние на компанијата. Уште повеќе, кога работат од далечина од јавни места (на пример, кафулиња, библиотеки, транспортни средства), тие често се поврзуваат на туѓа интернет-мрежа, со што се зголемува веројатноста за хакирање на компјутерите и инсталирање малициозен софтвер. Покрај тоа, постои ризик од кражба или губење на уредот од страна на вработениот.
- **Некомпатибилност** – флексибилноста во изборот на работни алатки може да се претвори во проблем со нивната компатибилност со системите што се користат стандардно во компанијата. Така, во случајот на BYOD, може да се појават проблеми поврзани со некомпатибилноста на форматите и тешкото користење на деловните документи (на пр. поради различно зачувување на датотеки во случај на Windows и различно во MacOS).

- **Враќање на податоците** – Политиките на BYOD може да предизвикаат проблеми поврзани со враќање на податоците зачувани на уредот на работникот по истекот на работниот однос. Истото се должи на фактот што вработените имаат целосна контрола врз нивните уреди и можат самостојно да управуваат со датотеките зачувани на нив.

Права и обврски поврзани со BYOD

При работа на приватен уред, неопходно е тој да ги исполнува барањата поврзани со здравјето и безбедноста при работа. Сепак, осигурувањето на таквата опрема не е задолжително – работникот и работодавачот можат да се договорат за опсегот на осигурувањето и правилата за користење на опремата неопходна за извршување на работата од страна на вработениот.

Примерот на Полска – измена на Законот за работни односи и нови прописи што се однесуваат на работа од далечина

Вреди да се напомене дека работникот вработен врз основа на договор за вработување има право да побара компјутер од фирмата, а работодавачот е должен да му го обезбеди. Меѓутоа, доколку се користи приватна опрема за извршување на работата, тогаш работникот има право на соодветен паричен надомест. Дополнително, работодавачот треба да ги покрие трошоците за електрична енергија и телекомуникациските услуги неопходни за вршење работа од далечина. Надоместувањето на трошоците може да се случи во реална вредност или во форма на паушален износ договорен меѓу страните. При утврдување на висината на противвредноста и на паушалот, работодавачот мора да ги земе предвид цените на материјалите и опремата, како и услугите за електрична енергија и телекомуникации[7].

Доколку работата се врши дома, работодавачот ги исполнува обврските кон работникот во однос на здравјето и безбедноста при работа, со исклучок на:

- обврска да се грижи за безбедна и хигиенска состојба на местото каде што се работи,
- обврски што се однесуваат на изградба или реновирање на објект во којшто се наоѓаат работни простории,
- обврска за обезбедување соодветни хигиенско санитарни апарати.

[7] *Закон донесен на 1 декември 2022 г. за измените – Кодекс за работа и некои други закони* (Сл. весник од 2022 г. поз. 240).

Ваквите обврски на работодавачот да обезбеди соодветни работни услови за своите вработени имаат влијание и врз прашањата поврзани со концептот „несреќа при работа“ и социјално осигурување. Работникот кој ќе доживее незгода на работа, без разлика каде ги извршува своите должности – работи од далечина или на работното место – има право на **надомест од социјално осигурување**.

Пред да дозволи работа од далечина, работникот потврдува со изјава (доставена во хартиена или електронска форма) дека ја прочитал проценатa на професионалниот ризик направена од страна на работодавачот и информациите што ги содржат правилата за безбедност и дисциплина при работа од далечина, при што се обврзува дека ќе ги почитува.

При процена на професионалниот ризик, особено се зема предвид влијанието на работата од далечина врз видот и мускулно-скелетниот систем на вработениот. Исто така, предвид се земаат и психосоцијалните услови на одредено работно место. Врз основа на резултатите од оваа процена, работодавачот развива информации што ги содржат правилата и методите за правилна организација на работната позиција за работа од далечина. Тие треба да ги земат предвид барањата за ергономија, безбедност и дисциплина при работа од далечина, активностите што треба да се извршат по завршувањето на работата од далечина, како и правилата за однесување во итни ситуации што претставуваат закана за животот или здравјето на луѓето. Работодавачот може да подготви и универзална процена на професионалниот ризик за поединечни групи на работни позиции за работа од далечина.

2.3. Приватност на личните податоци и безбедност на лицата кои работат на интернет

2.3.1. Работа од далечина

Од аспект на зголемената популарност на хибридната работа или работата од далечина со полно работно време, законодавците на многу земји членки одлучија да воведат соодветни измени во законот за работни односи. Должностите на работникот и работодавачот бараа адаптација на новите облици на работа. Тие произлегуваат од потребата да се обезбеди соодветна ИТ-инфраструктура или работен простор на местото на работа од далечина на таков начин што ќе ги задоволат барањата за здравје и безбедност при работа.

Работа од далечина и трудовото право - примерот на Полска

1. **Алатки за работа од далечина**

Според предложената измена на ЗРО, чл. 67 (24) став 1, работодавачот е должен на работникот кој врши работа од далечина да му обезбеди:

- **Материјали и алатки за работа** – ова, меѓу другото, се однесува на технички уреди неопходни за работа од далечина (во зависност од спецификите на дадената работа, покрај компјутерот, тоа може да бидат на пр. соодветни слушалки за онлајн-состаноци, микрофон итн.).
- **Инсталација, сервис и одржување на уредите за работа** – вклучувајќи технички уреди неопходни за работа од далечина. Алтернативно, работодавачот може да ги покрие и потребните трошоци поврзани со овие услуги.
- **Обука и техничка поддршка** неопходна за извршување работа од далечина.
- **Покривање на трошоците за електрична енергија –** работодавачот е должен да ги покрие и трошоците за енергија и телекомуникациски услуги потребни за вршење работа од далечина.

Колективниот договор склучен помеѓу работодавачот и синдикалната организација на компанијата или правилникот за работа може да го обврзат работодавачот да покрива други трошоци директно поврзани со извршување на работата од далечина.

2. **Уредување простор за работа од далечина – контрола на работодавачот**

Работникот е должен да организира работна позиција за работа од далечина, земајќи ги предвид ергономските услови. Ова вклучува на пр. избор на удобен стол, биро со соодветна висина, правилно поставување на мониторот во однос на очите и соодветно осветлување.

Доколку работата се врши во домот на работникот, работодавачот ги исполнува своите обврски во однос на здравјето и безбедноста при работа, со исклучок на:

- обврската да се грижи за безбедноста и хигиената на работното место,
- обврската утврдена во Поглавје III, Дел десет од Законот за работни односи (одредби што се однесуваат на згради и работни простории),
- обврската за обезбедување соодветни хигиенско-санитарни апарати.

Споменатите обврски на работодавачот во однос на обезбедувањето соодветни работни услови за своите вработени, имаат влијание и врз прашањата поврзани со опфатот

на концептот „несреќа при работа“ и социјалното осигурување. Работникот кој ќе доживее незгода на работа, без разлика каде ги извршува своите работни задачи (работа од далечина или на работното место), има **право на надомест од социјално осигурување.**

Од аспект на обврските на работодавачот во врска со:

- примена на соодветни мерки за спречување несреќи при работа од далечина,
- преземање на потребните активности за елиминирање или намалување на ризикот од таква несреќа,
- давање прва помош на повредените како и околностите и причините за несреќата во согласност со колективниот договор склучен со синдикалната организација на институцијата/организацијата или со правилникот за работа;

работодавачот има право да спроведе контрола во следниот опсег:

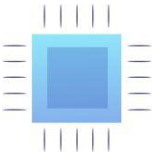
- Безбедност и дисциплина при работа,
- **Примена на прописите за безбедност и заштита на информациите**, вклучително и процедурите за заштита на личните податоци.

Во согласност со новите прописи од Законот за работни односи, работодавачот ќе може да воведе контрола на трезност на вработените само тогаш кога тоа е неопходно за да се обезбеди заштита на животот и здравјето на вработените, други лица или заштита на имот.

Секоја контрола на трезност треба да биде:

- спроведено во консултација со вработениот,
- извршена на местото на работа од далечина и во тек на работното време на работникот,
- адаптирана на местото на работа од далечина и типот на работа што се врши,
- не се препорачува користење на просториите за домаќинство на начин што е во согласност со нивната намена,
- во случај на повремена работа од далечина, контролата на трезноста треба да се одвива според условите договорени со вработениот,
- спроведена со почитување на приватноста на вработениот и другите луѓе (на пр. други членови на домаќинството или станари).

Ако за време на контролата, работодавачот констатира недостатоци во областа на здравјето и безбедноста при работа, безбедноста и заштитата на информациите,



вклучително и заштитата на личните податоци, постојат две опции. Може да му постави краен рок на вработениот да ги отстрани недостатоците или да ја повлече согласноста за работникот да врши работа од далечина.

3. Заштита на личните податоци при работа од далечина според измените на Законот за работни односи

Со оглед на зголемениот ризик од губење на личните податоци и други видови прекршувања во овој поглед, работодавачот треба да дефинира процедури за заштита на личните податоци. Исто така, неопходно ќе биде спроведување соодветна обука во дадената организација. Работникот кој работи од далечина, пак, треба да потврди дека ги прочитал стандардите поставени од работодавачот во писмена или во електронска форма.

И работникот и работодавачот треба да се договорат и како и со кои алатки ќе комуницираат од далечина и ќе даваат информации во врска со извршувањето на работата.

2.3.2. Како, согласно со Општата регулатива за заштита на податоци (GDPR), да ги заштитите личните податоци при работа од далечина?

Зголемената популарност на работата од далечина го зголеми ризикот од протекување/губење чувствителни информации за компанијата. Ова се должи на фактот што може да биде тешко и за работникот и за работодавачот да одредат точно под кои услови се прекршени принципите за заштита и безбедност на информациите на компанијата и личните податоци. Бидејќи работата од далечина (барем делумно) веројатно ќе остане со нас подолго време, неопходно е да се потсетиме на најчесто прекршените принципи за заштита на личните податоци. Исто така, вреди да се разгледаат заканите што ги демнат луѓето кои работат од далечина и начините за ублажување на ризикот од нивно појавување.

ЗАПОМНЕТЕ!

Според чл. 32 од ОРЗП, работодавачот, како администратор на вашите лични податоци, треба да спроведе соодветни технички и организациски мерки за да обезбеди ниво на безбедност што одговара на степенот на ризик од повреда на правата или слободите на физичките лица со различна веројатност и тежина.

За таа цел, работодавачот може да ги преземе следниве активности:

a) псевдонимизација и шифрирање на личните податоци,

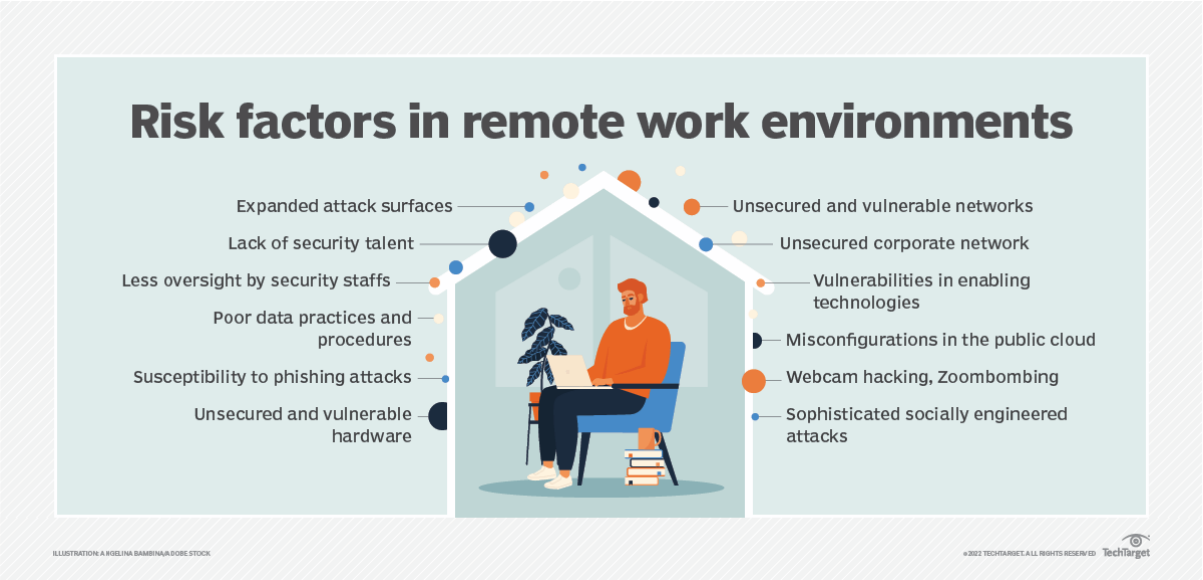
b) обезбедување доверливост, интегритет, достапност и отпорност на системите и услугите за обработка на податоци,

c) обезбедување можност за брзо враќање на достапноста на личните податоци и пристап до нив во случај на физички или технички инцидент,

d) обезбедување можност за редовно тестирање, мерење и оценување на ефективноста на техничките и организациските мерки за осигурување на безбедноста на обработката на личните податоци.

Според објаснувањата на Европската комисија, вработените кои обработуваат податоци како дел од својата работа во организацијата, всушност на тој начин ги извршуваат задачите на администраторот на податоци. Затоа, тие се одговорни и за осигурување на безбедноста на личните податоци.

2.3.3. Интернет-закани и работа од далечина



Иако сајбер-безбедноста е еден од најважните предизвици со кои се соочуваат државните институции денес, јавната свест во оваа област сè уште останува ограничена. Речиси сите слушнале за сајбер-безбедноста и нејзината важност, но однесувањето на граѓаните не секогаш одразува високо ниво на знаење на оваа тема. Според истражувањето

на веб-страницата ChronPESEL.pl и Националниот регистар за долгови спроведено во 2022 година, секој трет Полјак се плаши од протекување на неговите лични податоци, но помалку од половина од испитаниците би знаеле што да прават во таква ситуација.

Иако е невозможно да се обезбеди 100 % заштита на податоците и безбедност на информациите, постојат голем број превентивни мерки што можат соодветно да го намалат ризикот од протекување на податоци и други видови опасности.

Заканите кои демнат за вработените при вршењето работа од далечина не се разликуваат многу од оние на кои секој корисник на интернет треба да внимава. Нивната цел е најчесто да украдат заштитени информации или податоци за одредена личност или компанија, благодарение на што напаѓачот ќе стекне финансиска корист, конкурентска предност или други цели. Според извештајот на Агенцијата за сајбер-безбедност на Европската Унија (ENISA), најчестите и опасни закани во сајбер-просторот се:

1. **Малициозни софтвери** (*malware*) – тоа се штетни кодови или апликации што го отежнуваат или целосно го оневозможуваат нормалното користење на крајниот уред (на пр. компјутер или принтер). Со инфицирање на вашиот хардвер со малициозен софтвер, криминалците можат да дојдат до вашите податоци или да добијат пристап до други функции на вашиот уред. Тие, исто така, може да имаат за цел целосно да го блокираат уредот, под услов корисникот или друго лице делумно погодено од нападот да плати откуп за да се одблокира.
2. ***Ransomware*** – вид на малициозен софтвер со кој криминалецот го блокира пристапот на корисниците до нивните системи или лични датотеки, а потоа бара плаќање такса во замена за негово обновување.
3. **Напади преку интернет-страници** – Метод, со кој хакерите ги мамат жртвите на нивните напади со користење интернет-системи и услуги како канал за подготовка и извршување на нападот. Конкретно, овде може да се разликува споделување или олеснување на пристапот до малициозните URL-адреси или скрипти кои имаат за цел да го насочат корисникот до саканата веб-страна или преземањето малициозна содржина. Резултатот е дека малициозниот код се имплементира во вистинска веб-страница со цел да се украдат информации и да се добие финансиска добивка.
4. ***Фишинг*** – Слично како во случаите со другите сајбер-напади, целта на овој вид напад е добивање вредни информации преку сајбер-криминалците, кои првенствено вклучуваат кориснички имиња за најавување, лозинки, ЕМБГ броеви или броеви на кредитни картички. Името доаѓа од фактот дека криминалците користат специфична мамка подготвена за одредена личност чии податоци сакаат да ги украдат. Тие обично користат лажни е-пошта или СМС-пораки, како и канали за

комуникација на друштвените мрежи. Со цел да добијат доверба, сајбер-криминалците се претставуваат како телекомуникациски компании, курирски компании, банки, аукциски портали, па дури и институции. Постапувајќи според емоциите на жртвата, тие се обидуваат да ги убедат да кликнат на линкот што го подготвиле на веб-страница која иако е слична на вистинската, ја создал криминалецот и е негов канал за извршување измама.

5. **DDoS** - (ang. *distributed denial of service*) – Дистрибуирано одбивање на услугата е тип на напад кој ги таргетира мрежните услуги или компјутерските системи. Нивната задача е да ги окупираат сите достапни и бесплатни ресурси за да спречат функционирање на целата услуга на интернет. Нападот може да се однесува на веб-страницата на компанијата, хостирањето на е-поштата на вработениот итн. Се врши од различни компјутерски уреди во исто време – главно од оние кои биле преземени од специјални вируси – ботови или тројанци. Опасноста во овој тип на напад се заснова врз тоа што корисникот на дадената опрема можеби не е свесен дека неговиот компјутер се користи за извршување DDoS.
6. **Кражба на идентитет** – со помош на ЕМБГ бројот, личните податоци или личната карта, криминалецот се претставува како одредена личност за да земе, на пример, заем или на друг начин да го користи неговиот идентитет за своја корист.
7. **Повреда на безбедноста на податоците** – е вид на инцидент поврзан со сајбер-безбедност, при што, се пристапува до информации (или дел од ИТ-систем) без соодветно овластување, обично со злобна намера. Ова води до потенцијална загуба или злоупотреба на овие информации. Причината за овој тип на закана често е т.н човечка грешка, што може да се појави при конфигурација и распоредување на одредени услуги и системи, што може да резултира со ненамерно изложување на податоците.
8. **Протекување на информации** – чест резултат на прекршување на податоците кој опфаќа широк опсег на информации изложени на ризик – од лични податоци за идентификација, преку финансиски податоци складирани во ИТ-инфраструктура, до лични здравствени податоци складирани во складишта на даватели на здравствени услуги.
9. **Внатрешна закана** (злоупотреба на привилегии) – е акција преземена од лице или група луѓе поврзани со жртвата на напад во професионална или друга врска, каде што и напаѓачот и жртвата остануваат на иста мрежа или инфраструктура, или се во можност да добијат информации преку меѓусебно поврзување. Постојат неколку модели поврзани со овие видови закани. Тие можат да се појават и кога надворешни

лица работат со внатрешни лица од компанијата со цел добивање неовластен пристап до ресурсите. Внатрешните лица, исто така, ненамерно, може да предизвикаат штета преку невнимание или недостаток на знаење. Бидејќи луѓето во процесите на компанијата често уживаат во довербата на колегите, а исто така ги познаваат процесите и процедурите на организацијата, тешко е да се направи разлика помеѓу легитимен пристап до податоци и системи со лоша намера.

10. **Ботнет** – мрежа на поврзани уреди заразени со малициозен софтвер од типот бот. Тие обично се користат за извршување DDoS напади. Ботнетите може да бидат далечински контролирани од страна на криминалецот, за да може да дејствува на синхронизиран начин за да постигне одреден резултат.

2.3.4. Сајбер-дисциплина - како да бидете безбедни на интернет секој ден?

1. **Доколку можете, работете во безбеден, приватен простор**

Протекување на податоците може да настане не само како резултат на хакерски напад, туку и преку помалку сублимирани, конвенционални методи – меѓу другото, сомнителна содржина на екранот или сликање на нашиот монитор. Несомнено е дека, освен местото подготвено од работодавачот за извршување одредена работа, најбезбеден простор за работа од далечина се чини дека е вашиот дом. Идеално би било тоа да биде просторија заклучена со клуч, каде што можете безбедно да се одделите од останатите во домот.

Доколку не постои можност за работење во изолирана просторија (на пример, за време на службено патување), прашањето за одржување на безбедноста станува многу покомплицирано. Посебно, треба да се внимава на отворени простори (кафулиња, возови, аеродроми), каде што луѓето наоколу постојано се менуваат. Покрај тоа, на многу места од овој тип е инсталиран надзор, кој може да ги сними не само активностите на луѓето во неговиот опсег, туку и сите видови други елементи на околината, вклучително и компјутерските екрани.

Решение: обезбедете филтер/обвивка за приватност

Благодарение на оваа алатка, содржината на екранот е видлива само за лицето кое го користи компјутерот/телефонот. Оваа технологија работи слично како и микро-решетките - филтерот се состои од микроскопски канали насочени директно пред лицето кое го користи

екранот на мониторот. Луѓето кои гледаат на екранот од различен агол нема да ја видат истата содржина.

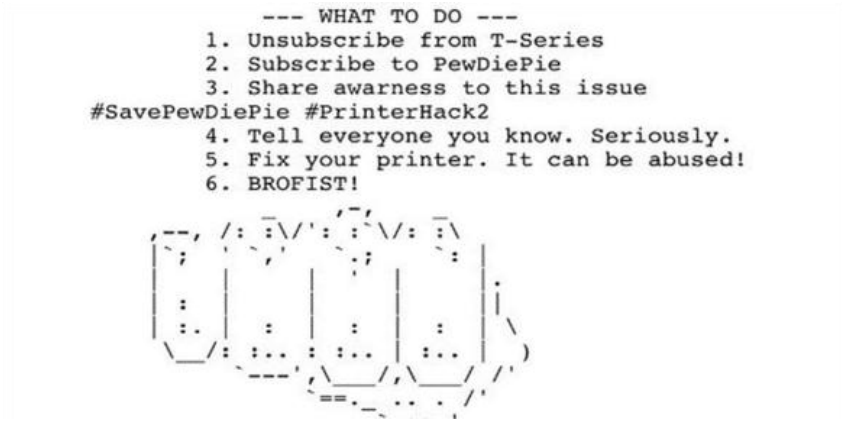
2. **Чувајте ги документите во безбеден, заклучен простор на местото каде што работите од далечина**

Т.н. политика за чисто биро или за чист екран која што е обврзувачка на многу работни места, треба да се применува и на местото каде што се врши работа од далечина. Дури и ако имате доверба во членовите од семејството или цимерите, не треба да се оставаат никакви документи што содржат лични податоци за време на отсуство. Исто така, лозинките за работните уреди не треба да се чуваат на видно место.

Решение: опремете го вашиот простор за работа од далечина со фиока или шкаф што може да се заклучува

Тоа ќе биде место, каде што можете безбедно да ги складирате сите материјали што се користат за извршување на задачите додека работите. Доколку е можно, чувајте го клучот со себе постојано или сокријте го на место што само вие ќе го знаете.

3. **Не печатете документи дома или во јавни продавници за копирање освен доколку тоа е неопходно**



Експертите за сајбер-безбедност веќе подолго време предупредуваат дека најзапоставениот уред во однос на потребата од спроведување соодветни безбедносни мерки е... печатачот. Според истражувањето на InfoSecurity Magazine, околу 66 % од испитаните луѓе кои работат од далечина печателе во просек по пет документи неделно. Една четвртина од нив сè уште не ги уништиле печатените документи, со образложение

дека планираат да ги вратат во канцеларија. Само 24 % користат домашен уништувач, но признаваат и дека фрлаат документи во корпата за отпад од домаќинството. Дури 12 % од испитаниците исто така тврдат дека немаат познавање на ОРЗП.

Денешните печатачи се повеќе наликуваат на компјутери – наместо на еднонаменски, едноставни уреди, тие често претставуваат дел од интернет на нештата (ang. *Internet of Things,* IoT) и се мултифункционални работни алатки. Еден од попознатите напади на домашните печатачи, кој го истакна проблемот со недостатокот на соодветна безбедност на овие уреди, беше нападот поврзан со познатиот креатор на YouTube PewDiePie. Во 2018 година, хакер (или група од многу фанови на PewDiePie) нападна десетици илјади принтери ширум светот. Без интервенција на нивните сопственици, уредите почнале да печатат брошура за промовирање на содржината објавена од PewDiePie, поттикнувајќои поддршка за активности на истата.

Денешните, сè понапредни технолошки печатачи, поседуваат кеш-меморија каде што се чуваат документите што треба да се печатат. Модерните печатачи работат и безжично, што значи дека, секој, со соодветни драјвери на својот компјутер и пристап до мрежата каде што се наоѓа печатачот може да се поврзе на него. Во случај да ја преземе контролата над печатачот (на пр. во компанија), хакерот може да добие пристап до документите кои што се веќе испечатени, како и до други ресурси складирани на компјутерот или дури и до лозинките на уредите што ги користеле услугите на печатачот.

Решение: печатете документи само на работа, а доколку мора да го правите тоа дома, проверете дали имате соодветно обезбедување на опремата што ја користите

Ова може да се направи со поставување безбедна лозинка за Wi-Fi за печатачот (ако е можно). Ако отпечатените документи повеќе не се потребни, не фрлајте ги во ѓубре дома – однесете ги во фирмата, каде што треба да има уништувач на хартија. Ако тоа не е можно, прашајте го вашиот работодавач или одделот за човечки ресурси за постапката за уништување документи на компанијата.

4. Покривка на веб-камера

Работата од дома обично значи учество во телеконференции и видео повици за кои е потребна употреба на веб-камера. За жал, хакерите можат лесно да пристапат до вашата веб-камера, загрозувајќи ја вашата приватност. Дополнително, доколку има доверливи документи на физичкото работно место што може да ги сними веб-камерата, криминалците ќе можат да пристапат до нив.

Решение: ограничување на приказот на предмети што содржат лични податоци

Кога веб-камерата е вклучена, погледот околу неа, каде што има елементи што содржат лични информации, треба да биде ограничен. Дополнително, ако веб-камерата е одвоена од уредот, исклучете ја кога не ја користите. Ако камерата е вградена, вреди да се преземат дополнителни мерки за заштита, на пример, да се набави покривка за камерата. Во продавниците можете лесно да најдете лизгачки капаци за веб-камери од различни типови. Тие обично се лесни за инсталирање бидејќи повеќето имаат леплив слој што се лепи за камерата. Можете исто така да користите функции како **замаглување на позадината** кога користите програми и апликации за видео-конференции.

5. **Земете активно учество во обуката на компанијата од областа на сајбер-безбедност и промените во политиката на работодавачот во однос на заштитата на податоците и информациите**

Според ОРЗП, доколку се усвојат нови процедури за заштита на личните податоци во компанијата, пред истите да бидат имплементирани, работодавачот треба да им дозволи на своите вработени да се запознаат со тие процедури.

Доколку работодавачот не спровел соодветна обука за користење на уредите, користење внатрешни и надворешни алатки за комуникација или не ги претставил основните принципи поврзани со заштитата на податоците во компанијата, работникот има право да побара од работодавачот да го стори тоа. Доколку, дури и по обуката, работникот сè уште не е сигурен за процедурите што треба да се следат во дадена ситуација, треба да го пријави тоа кај својот работодавач или кај лицето во компанијата одговорно за управување со ИТ-инфраструктурата, одделот за човечки ресурси итн.

Сајбер-дисциплина при работа од далечина

Што друго можете да направите за да го заштитите вашиот компјутер?

Шифрирајте ги личните податоци

Особено доколку станува збор за чувствителни податоци или ги испраќате надвор од организацијата. Како што беше споменато претходно, вработените кои обработуваат податоци како дел од нивните професионални задачи, всушност ги извршуваат задачите на контролорот на податоци, а тоа е работодавачот. Според чл. 32 од ОРЗП, контролорот и обработувачот спроведуваат соодветни технички и организациски мерки за да обезбедат ниво на безбедност на податоците што одговара на обемот, контекстот и целите на

обработката на податоците, како и ризикот од повреда на правата или слободата на физичките лица. Како безбедносни мерки, ОРЗП, меѓу другото, наведува: псевдонимизација и шифрирање на личните податоци.

Иако не постојат експлицитни барања во ОРЗП за најефективниот метод на безбедност, регулативата постојано нагласува дека **шифрирањето и псевдонимизацијата** се соодветни технички и организациски мерки за одржување на безбедноста на личните податоци.

Шифрирањето има за цел кодирање на одредена содржина на таков начин што, само примачот кој го има соодветниот клуч ќе ја разбере. Наједноставно кажано, идејата е, на пример, да се смени низа од букви во низа од други букви или броеви, да се додадат дополнителни низи од букви или бројки итн.

Псевдонимизација е обработка на личните податоци на таков начин што, невозможно е, без пристап до информации зачувани безбедно на друго место, да се идентификуваат кому му припаѓаат. Се состои во маскирање на податоците со замена на информации за дадена личност со измислени идентификатори.

Која е разликата помеѓу наведените методи?

Како и псевдонимизацијата, така и шифрирањето ги крие информациите со замена на идентификаторите со нешто друго. Сепак, како што псевдонимизацијата му овозможува на секој што има пристап до податоците да прегледа дел од збирот на податоци, така шифрирањето им дозволува само на одобрените корисници да пристапат до целосната база на податоци. Псевдонимизацијата и шифрирањето може да се користат истовремено или одделно.

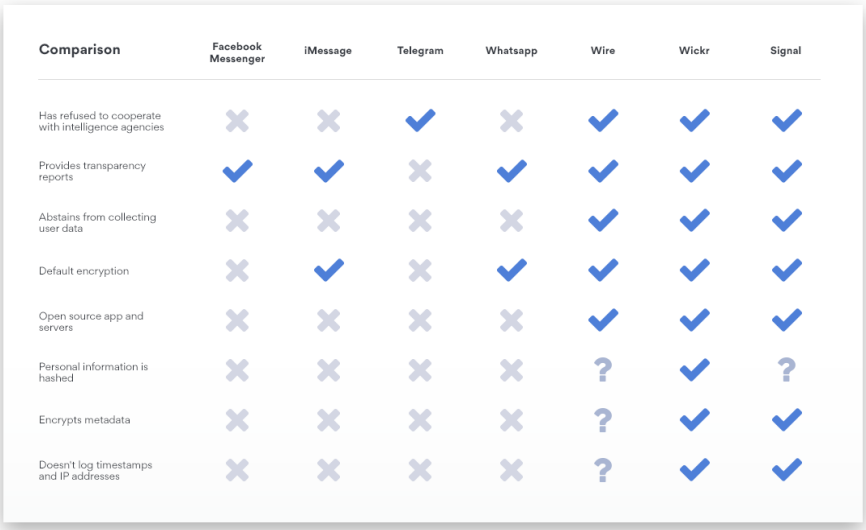
Методи за заштита на податоците/шифрирање во внатрешната комуникација како и во комуникацијата со надворешни субјекти

а. **Внатрешна комуникација – користење на шифрирани комуникатори и безбедни платформи**

Иако е-поштата останува еден од најпопуларните методи за деловна комуникација (во 2021 година, 316,9 милијарди електронски пораки се испраќаа и примаа секој ден, а се очекува овој број да се зголеми на 376,4 милијарди до 2025 година), тоа не е најбезбедниот систем за размена на доверливи информации. Поради големата популарност, е-поштата е главен канал и за хакерски напади. Deloitte откри дека 91 % од сите сајбер-напади доаѓаат

од phishing-пораки. Трошоците што ќе ги сносат организациите како резултат на таков напад може да бидат многу високи.

Во случај на внатрешна комуникација, каде што често се разменуваат доверливи информации за компанијата, нејзините вработени или клиенти, може да се користат други, побезбедни алатки.



Comparison	Facebook Messenger	iMessage	Telegram	Whatsapp	Wire	Wickr	Signal
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓
Open source app and servers	✗	✗	✗	✗	✓	✓	✓
Personal information is hashed	✗	✗	✗	✗	?	✓	?
Encrypts metadata	✗	✗	✗	✗	?	✓	✓
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	?	✓	✓

Whatsapp и Messenger – најчесто избирани комуникатори и нивните особини

1. **WhatsApp:**
   - користи шифрирање на **Signal**,
   - повеќето луѓе во Европа веројатно ја користат оваа апликација,
   - прифатлива апликација за корисниците, која нуди дополнителни функции,
   - во сопственост на Facebook,
   - апликацијата претходно доживеа сериозни прекршувања на заштитата на личните податоци.
2. **Messenger:**
   - широк опсег – поради поврзаноста со Facebook, повеќето луѓе го имаат овој комуникатор,
   - можете да се користи дури и по деактивирање на вашата сметка на Facebook,
   - шифрирањето не е стандардно,

- не ги шифрира минатите повици,
- апликацијата го следи однесувањето на корисникот.

Најдобри апликации од аспект на безбедност на податоците:

1. **Signal:**
   - поддржува групни разговори, СМС-пораки, гласовни и видеопораки, овозможува префрлување документи и фотографии,
   - нуди пораки што исчезнуваат (со тајмер),
   - користи протокол за сигнализација – користи сигнален протокол – криптографски протокол, што може да се користи за шифрирање гласовни повици и разговори преку инстант-пораки, во кои пораките во јасна форма можат да ги читаат само лицата кои комуницираат,
   - софтвер од типот *open source* (т.е. чиј изворен код е достапен бесплатно и може да се дистрибуира и модифицира без да се плаќа надомест),
   - не складира кориснички податоци или метаподатоци,
   - пропагиран од страна на Едвард Сноуден
   - бара внесување телефонски број при регистрација.

Безбеден софтвер и платформи за работниот простор:

1. Microsoft Teams.
2. Google Workspace.
3. Slack.
4. Asana.
5. Trello.

b. Надворешна комуникација – шифрирање датотеки што содржат лични податоци и списоци на адреси на е-пошта

Се препорачува, доколку е можно, секогаш кога податоците се пренесуваат од една локација на друга, тие да бидат псевдонимизирани или шифрирани, за да се спречи протекување.

Пренесување лични податоци во мејлинг листа

Користете го полето БЦЦ (ang. BCC). Полето БЦЦ ви овозможува да испраќате пораки на таков начин што примателите не ги гледаат адресите меѓусебно. Оваа опција може да се најде во секоја е-пошта.

Пренос на лични податоци во датотеки испратени по електронска пошта

Документите испратени преку е-пошта може да содржат многу лични податоци или други законски заштитени информации, па затоа треба дополнително да се обезбедат. Методите за шифрирање датотеки може да се разликуваат во зависност од форматот во кој се зачувани. Сепак, сите тие имаат еден основен заеднички принцип: пренесување на лозинката на шифриран документ со помош на друго средство за комуникација различно од е-пошта.

За правилно шифрирање на датотеката, најчесто избраните програми се **WinRAR** и **7-zip**. На секоја од нив, откако ќе ја изберете опцијата „додај во архива“, ќе се отвори прозорец што овозможува, меѓу другото, да се постави лозинка за пристап до документот.

Редовно правете резервна копија од вашите податоци и складирајте ги на надворешни дискови

Во случај вашиот хардвер да е заразен со вирус или други настани што може да доведат до бришење на податоците од вашиот компјутер и неможност за враќање, најдобро е да правите редовни **резервни копии**.

Резервните копии, познати и како backup, се копии на информации кои се складирани на друго место освен во рамките на оригиналот. Првиот чекор треба да биде да одлучите дали сакате да направите резервна копија:

1. Конкретни податоци, што се важни поради некоја причина.
2. Целиот оперативен систем.

Повеќето алатки за резервна копија се стандардно конфигурирани за првата цел и прават резервна копија на вашите податоци врз основа на тоа кои документи најчесто ги користите. Доколку не сте сигурни на кои датотеки да направите резервна копија, се препорачува архивирање на сите документи.

Колку често да се прават резервни копии?

Одговорот зависи од индивидуалните преференции и зачестеноста на воведените промени. Некои го прават тоа на 1 час, некои еднаш дневно, а трети еднаш неделно. Сепак, се препорачува секојдневно правење резервни копии на вашите документи.

Како да направите резервна копија на документи?

Во зависност од оперативниот систем на вашиот компјутер, се препорачуваат програми што ќе ви овозможат да го поставите периодот во кој автоматски ќе се креира резервна копија. Тука се вбројуваат на пр. Backup and Restore на Microsoft Windows или Time Machine на Apple. Овие програми работат и кога уредот е активен и се користи, но исто така и кога не е активен.

Податоци на надворешен уред или податоци во облак?

Најдобро и едното и другото. Надворешниот уред може да биде УСБ-диск, преносliв надворешен диск или други уреди што можат да се поврзат преку Wi-Fi мрежа. Предноста од нивното користење со сигурност е тоа што тие можат да складираат големи збирки податоци за релативно кратко време. За жал, бидејќи ова е метод на физичко креирање резервна копија, може да не успее или да се расипе исто како и вашиот компјутер. Резервната копија на надворешен диск може да биде украдена, дискот може да се изгуби, поплави, прегрее итн. Уште повеќе, ако уредот од кој доаѓаат податоците претходно бил заразен со малициозен софтвер, за жал постои ризик од инфицирање на дискот и, како последица од тоа, и на самата резервна копија.

Од друга страна, правењето резервна копија на облак вклучува поставување копии од документи или други датотеки на интернет. Поточно, тие се збирки на сервери и центри за податоци расфрлани низ светот каде што се чуваат податоците. Ова се случува автоматски, обично преку стандардната алатка на платформата за уредување текст (на пр. Google Docs), која создава резервна копија во одредени периоди или по секоја промена на датотеката. Дефинитивна предност за складирање копии од датотеки во облакот е нивната издржливост и можноста за пристап до резервната копија од кој било друг уред (се разбира, под услов да ја имаме лозинката на сметката, под која постои облакот). Сепак, ова решение не е целосно без недостатоци – ако сакаме брзо да направиме резервна копија на голема количина на податоци, нивниот пренос на облак може да биде многу побавен отколку во случај на физички креираната резервна копија на надворешен диск. Исто така, може да се случи да снема простор во облакот за собирање нови податоци, при што ќе се

јави потреба од бришење дел од податоците или ќе треба да купите пристап до дополнителни ресурси од доставувачот на облакот.

Безбеден пристап до вашиот компјутер, телефон, па дури и онлајн-состаноци

Како што е неопходно шифрирање на податоците со цел осигурување на безбедноста на личните податоци, така е исклучително важно правилно да се обезбеди и опремата што ја користиме. Употребата на лозинки или други видови шифрирање гарантира дека само овластени лица имаат пристап до одредени ресурси.

Постојат неколку начини за обезбедување на опремата:

- **Силна лозинка или лозинка:**
  - **Долга** – содржи најмалку 8 карактери (колку подолга толку подобро),
  - **Комплексна –** содржи најмалку еден знак од следните категории: голема буква, мала буква, специјални знаци (пр. !, ?), број,
  - **Тешка да се открие** – доколку сакате да изберете фраза, цитат или изрека, погрижете се таа да не е директно поврзана со вас, вашата работа или вашата околина; сепак, ако знаете дека без лесни асоцијации нема да ја запомните лозинката – заменете ги зборовите со соодветни симболи или бројки од тастатурата, пр. „Ala ma kota” може да се запише како „4LaM@k0T@”,
  - **различна од претходната лозинка за одреден уред** – во случај на промена на лозинката за постоечка сметка, таа не треба да биде иста како претходната; исто така, лозинката не треба само површински да се менува, на пример со додавање цифра на крајот или почетокот.

Совет: Користете уреди за управување со лозинки за да складирате шифрирани лозинки на интернет – ќе ви овозможи да креирате сложени лозинки што содржат големи и мали букви, бројки, разни специјални знаци итн. Благодарение на овој метод, може да се креира бесмислена низа знаци што ќе биде тешко да се пробие.

ЗАПОМНЕТЕ!

- не користете лозинка која истовремено е назив или е слична на името на корисникот, компанијата итн.,
- не користете низа букви или броеви од тастатурата или азбуката,

- не користете повеќе од две букви или бројки што се повторуваат (на пр. abba),
- не користете туѓи лични податоци за да креирате лозинка,
- не користете обратно напишани зборови (на пр. janek1 како 1kenaj),
- не внесувајте ја вашата лозинка во присуство на други луѓе,
- не запишувајте ја лозинката на хартија – доколку мора да ја запишете, користете алатка за управување со лозинка на USB-уред и носете ја со себе,
- не користете иста лозинка за сите уреди или веб-страници,
- не најавувајте се на уреди што не се ваши
- не праќајте лозинка по електронска порака,
- не споделувајте лозинки преку интернет – ако треба да споделите информации за најавување со колега, јавете се по телефон, наместо да ја испраќате лозинката преку е-пошта, СМС или друга алатка за комуникација,
- ако вашиот компјутер/веб-страница е хакиран/а, веднаш сменете ја лозинката.

Антиводич – список на најмалку безбедни лозинки за пристап[8]:

1. password
2. 123456
3. 123456789
4. guest
5. qwerty
6. 12345678
7. 111111
8. 12345
9. col123456
10. 123123

[8] Според истражувањата спроведени од фирмата NordPass, Top 200 most common passwords, https://nordpass.com/most-common-passwords-list/.

11. 1234567
12. 1234
13. 1234567890
14. 000000
15. 555555
16. 666666
17. 123321
18. 654321
19. 7777777
20. 123

Автентикација со повеќе компоненти

Повеќекомпонентно автентицирање (MFA или 2FA) е безбедносен метод, за кој е потребно да се употребат најмалку две независни компоненти за автентикација на дејство (на пр. внесување лозинка на вашата сметка, а потоа внесување СМС-код). Овој метод ги спречува повеќето напади врз основа на идентитет.

Многу апликации или платформи веќе нудат опција за овозможување на овој тип на заштита (на пр. Apple ID, Microsoft, Google, Twitter или Facebook). Вториот фактор за автентикација може да биде: СМС-код, еднократен код од апликацијата (Google Authenticator или Microsoft Authenticator) или постојан код предложен од добавувачот на дадена алатка и избран од корисникот.

Клуч U2F

Според специјалистите за сајбер-безбедност, клучот U2F е единствениот метод за автентикација со две компоненти, што е 100 % заштитен од напади на *фишинг* (но, не и од други напади, на пример, малициозен софтвер). Ако лице со клуч U2F биде измамено од сајбер-криминалци и ги внесе најавата и лозинката на лажна веб-локација, напаѓачот нема да може да ги преземе податоците на сметката на корисникот.

Ова се должи на *secure element* (т.н. мал компјутер) вграден во клучот U2F. Работи на таков начин што, откако ќе го вметнете клучот во USB-портата (или ќе го доближите до читачот во паметниот телефон), клучот се активира и може да врши криптографски операции во неговиот внатрешен систем, а не на уредот на корисникот.

Покрај тоа, вреди да се добијат два клуча – иако истиот клуч може да се поврзе со различни услуги, вреди да се има еден резервен. По купувањето, клучот мора да се конфигурира. Многу сервиси нудат можност за додавање клуч како форма на повеќефакторска автентикација. Ова решение го препорачуваат и разни видови социјални медиуми, Amazon, GitHub и сметки на електронски пошти. Ако одлучите да користите клуч U2F, треба да ги отстраните другите методи за двокомпонентна автентикација од дадената услуга.

Обезбедување на онлајн-состаноците

Не само опремата, туку и состаноците и видео конференциите во мрежа бараат безбедност. Работата од далечина често значи потпирање на софтвер за видео конференции, што пак, од своја страна, создава потенцијални безбедносни ризици на уредот. По серијата напади на платформата Зум, засновани на упаѓање на непоканети луѓе на видео конференции со цел да ги заплашат или малтретираат нејзините учесници (*zoom bombing*), компанијата беше принудена да ги поправи безбедносните пропусти. И покрај називот, *zoom bombing* може да се случи и на други платформи. Како резултат на овој тип на напад, може да дојде до протекување доверливи информации за компанијата, клиентите, другите вработени или корисникот.

Како одговор на ваквите напади во Зум, ФБИ објави совети со цел да им помогне на корисниците да се заштитат за време на користење софтвер за видео конференции:

1. Проверете дали состанокот е приватен, ако е ќе ви побара лозинка за да се придружите или, пак, дали е со контролирање на пристапот на гостите од лобито.
2. Размислете за безбедносните барања при изборот на добавувачи. Шифрирањето *end-to-end* (криење на пораката кај испраќачот и само дешифрирање кај примачот)

обезбедува приватност и безбедност – затоа проверете дали вашиот софтвер за видео конференции ја има оваа функција.

3. Проверете дали вашиот софтвер е ажуриран, инсталирајќи ги најновите поправки и ажурирања.

Во моментов, најбезбедната платформа за видео конференции е Microsoft Teams. Беспрекорната интеграција на сите апликации на Office, исто така, овозможува дополнителни безбедносни поставки за да можат сите во организацијата да работат заедно, оддржувајќи безбедност дури и во домашната канцеларија.

Инсталирајте и ажурирајте антивирусни програми, како и заштита од малициозен софтвер

Ажурирањето на системи, апликации и пребарувачи често се занемарува и одложува за подоцна. Всушност, ако тоа се направи во вистинско време може да спречи голем дел од нападите. Затоа, погрижете се да користите ажуриран и модерен антивирусен софтвер. Ажурирањата содржат важни промени што ги подобруваат перформансите и безбедноста на уредот. Во моментов, ажурирањата се објавуваат дури и секој месец, но вреди да се активира дневен режим за креирање резервна копија. Ова значително ја зголемува безбедноста, бидејќи програмерите можат брзо да ги елиминираат безбедносните празнини, што уште подобро ќе ги заштитат уредите од малициозен софтвер.

Едноставен чекор што треба да се следи е, исто така, осигурување дека софтверот против *malware* е инсталиран и користен како додаток на вашиот стандарден антивирусен софтвер. Оваа алатка не само што може да обезбеди заштита од напади, туку и да го предупреди корисникот, кога има ситуација на обид за напад.

Избегнувајте поврзување на вашите уреди на јавни мрежи

Користењето јавна мрежа, т.е. онаа на која секој може да се поврзе, со самиот факт на целосна отвореност, може да биде канал за бројни напади и е поврзан со ризик од протекување на податоци. Доколку треба да работите на јавен простор, не заборавајте да се поврзете само на доверливи мрежи и секогаш да користите VPN или да се поврзувате од вашиот телефон (преку т.н. хотспот).

Што претставува VPN?

Ова се виртуелни приватни мрежи, кои обезбедуваат сигурни, директни врски со компјутерската мрежа на вашата организација. Тие може да бидат неопходни кога пристапувате до датотеки, работите со доверливи информации или користите одредени веб-страници. VPN ги шифрира врските на корисниците со своите сервери, овозможувајќи

безбеден и сигурен пристап до мрежата на организацијата. Шифриран тунел на корпоративната мрежа VPN исто така ќе ви помогне да ги одржувате вашите податоци безбедни при транспорт. Може да ги спречи напаѓачите кои немаат корпоративна мрежа VPN да пристапат до серверите.

Безбедноста на VPN може да се подобри со користење на робустен метод за автентикација. Многу VPN користат корисничко име и лозинка, но може да размислите и за надградба и користење на паметни картички (*smart cards*), што овозможуваат заштита на процесот на најавување на вашите корисници и подобра контрола на пристапот до вашата сметка.

Се разбира, не е важно колку е силна мрежата VPN. Ако лозинката е компромитирана, хакерите лесно можат да дојдат до неа. Затоа треба редовно да ја ажурирате. Вреди да се ограничи употребата на VPN само во ситуации кога тоа е неопходно. Ако вашите работни уреди за лична употреба се користат навечер или за време на викендите (ако тоа е политика на компанијата), најдобро е да го исклучите VPN.

Што освен VPN?

Друга опција е користење на мрежата 5G. Нуди подобра поврзаност и ветува поголема безбедност отколку користење wi-fi или дури и VPN. Најавените, поретки одложувања во случајот на 5G, може да придонесат да стане реална алтернатива на Wi-Fi. Оваа технологија има вградено шифрирање преку алатки против следење или *spoofing*.

За време на работа од дома, од суштинско значење е да го обезбедите и вашиот домашен рутер. Треба да се ажурира и да биде обезбеден со долга, единствена лозинка – различна од автоматската лозинка што доаѓа со секој рутер. За да го направите ова, можете да отидете на страницата за поставки на рутерот со внесување на соодветната фраза во прелистувачот и да ја смените лозинката таму. На истата страница, најчесто можете да го смените и SSID, т.е. името на безжичната мрежа, за да ја отежните идентификацијата и пристапот до вашата домашна wi-fi мрежа од страна на трети лица. Не треба да се користи вашето име, домашна адреса или нешто што може да послужи за да ве идентификуваат.

Исто така, треба да се осигурите дека е овозможено мрежно шифрирање, што обично може да се направи во безбедносните поставки на страницата за конфигурација на безжичната мрежа. Постојат неколку безбедносни методи за избор, како што се WEP, WPA и WPA2. Најсилниот од нив е WPA2, кој бара хардвер понов од 2006 година.

3. Влијание на дигитализацијата на пазарот на трудот

3.1. Дискриминаторски третман во процесите на регрутирање

Во светот, пред напреднувањето на технологијата, сите одлуки за вработување и оценување на вработените ги донесуваа луѓе. Овие одлуки обично ги земаа предвид тековната ситуација, етичките прашања, правните аспекти во однос на транспарентноста на процесот и исправноста на изборот на раководниот кадар. Меѓутоа, денес многу компании користат ИТ-системи, кои нудат поголема ефикасност и овозможуваат намалување на мачната анализа на документите во потрага по конкретни информации.

Овие системи, познати како ADS (алгоритамски системи за одлучување / ang. *algorithmic decision systems*), се засноваат врз анализа на големи количини на обработени податоци со цел добивање на потребните резултати, кои потоа ќе бидат основа за донесување одлуки. Човечката интервенција во овој процес е обично занемарлива, а во некои случаи може целосно да се елиминира. Сепак, влијанието на дадена одлука врз одредена личност може да биде од големо значење, бидејќи ќе ја обликува нивната животна ситуација.

Оттука, целосното потпирање на ADS во процесот на донесување одлуки се поврзува со многу сомнежи од етичка, политичка и правна природа. Поради ризикот алгоритамските системи да ги пренесат предрасудите на нивните креатори, неограничената доверба во технологијата е контроверзна, особено во однос на областите како вработување или пристап до приватни и јавни услуги (на пр. здравствена заштита, системи за кредитен рејтинг).

3.1.1.Што може да направи лице кое е засегнато од алгоритамска дискриминација?

Се претпоставува дека, во процесот на вработување треба да се применуваат одредби што се однесуваат на еднаков третман при вработувањето (во Полска, ова прашање е покриено со член 18, точка 3а од ЗРО) и забраната за дискриминација (член 11, точка 3 од ЗРО). Ова значи дека, секоја дискриминација при вработување (особено поради пол, возраст, попреченост, раса, религија, националност, политички убедувања, членство во синдикат, етничко потекло, религија, сексуална ориентација) е неприфатлива.

Сепак, се појавуваат случаи на дискриминаторско третирање во процесот на регрутација. Се работи, меѓу другото за фаворизирање на машки кандидати, одбивање да се вработат млади мажени жени или жени со деца или вклучување клаузули за

дискриминација на странците во понудите за работа. Колку почесто компанијата користи електронско регрутирање врз основа на автоматизирани системи за одлучување, толку се поприсутни критериумите за исклучување. Истовремено, не само што може да има ненамерна дискриминација на кандидатите преку пристрасна вештачка интелигенција, туку управниот одбор на компанијата може намерно да воведе критериуми за дисквалификување во системот.

Во случај на појава на дискриминација во процесот на регрутирање, манифестирана со исклучувачка содржина на огласот или недискретни прашања за приватниот и семејниот живот, оштетеното лице може да побара заштита на својот интерес пред суд. Товарот на докажување во таквата постапка паѓа на работодавачот, а потенцијалниот кандидат треба само да докаже дека имало дискриминација (член 18, точка 3б од ЗРО). Доколку судот го потврди прекршокот, работодавачот ќе биде должен на дискриминираното лице да му исплати оштета во висина на износ не помал од минималната плата.

Меѓутоа, при алгоритамско одлучување, демонстрирањето на неоправдано отфрлање во процесот на регрутирање и следењето на барањата во овој поглед е многу потешко. Истото е поврзано со т.н проблемот со црната кутија (*black box problem)*, односно недостаток на транспарентност во работењето на алатките за вештачка интелигенција. Тоа значи дека, често дури и самите креатори, а со тоа и работодавачите кои користат или имплементираат одредена алатка за вештачка интелигенција, не се свесни за нејзините несакани ефекти. Сепак, тоа не значи дека тие се ослободени од одговорност за прекршоци. Лицето кое се сомнева дека е неправедно одбиено од алгоритмот може да преземе конкретни чекори за да го заштити својот интерес и за да ја промени одлуката донесена од системот.

Во тој поглед, член 22 од ОРЗП има клучно значење. Во согласност со оваа одредба, на контролорот на податоците му се наметнува обврска за спроведување соодветни мерки за заштита на правата, слободите и законските интереси на субјектите, чии што податоци (а со тоа и одлуки) се засегнати, а исто така и механизми кои на конкретното лице му овозможуваат да ја оспори одлуката заснована само врз автоматска обработка.

Доколку, според вашето мислење, вашата кандидатура е погрешно одбиена во процесот на е-регрутирање:

1. Потврдете дали одлуката била целосно автоматизирана. За да го направите тоа, внимателно прочитајте ги условите за вработување или контактирајте со одделот за човечки ресурси на компанијата и утврдете како функционира алгоритмот во контекст на процесот на аплицирање за работа.

2. Побарајте од компанијата (администраторот на податоци) можност да го претставите вашето мислење и причината зошто сметате дека одбивањето е неправедно.
3. Побарајте објаснување од компанијата и повторно разгледување на вашата апликација, но овој пат од страна на одредено лице. Администраторот е должен да одговори на таквото барање во најкраток можен рок (најмногу во рок од еден месец). Во рок од еден месец, администраторот треба да информира и за неисполнувањето на барањето и неговите причини.
4. Меѓутоа, доколку контролорот сепак го игнорира барањето или одговорот е незадоволителен, можете да побарате поддршка од органите за заштита на лични податоци и да поднесете жалба.
5. Дополнително, независно од постапката пред органот за заштита на лични податоци, имате право да ги заштитите вашите права пред граѓански суд. Доколку констатирате дека обработката на вашите податоци го прекршува законот, можете да го тужите контролорот или обработувачот на податоците. Пред судот можете да барате надомест за повреда на прописите за заштита на лични податоци, како и да покренете прашања за дискриминација што предизвикала материјална или нематеријална штета.

3.1.2. Регулативите на ЕУ за вештачка интелигенција и процесот на регрутирање

Како што веќе беше споменато, во нацрт-регулативата за вештачка интелигенција (Закон за вештачка интелигенција / AI Act), прашањата поврзани со вработување и управување со човечките ресурси се вклучени во листата на системи со високо ниво на ризик. Ова значи дека алатките што се користат, на пример, за автоматско оценување на кандидат за дадена позиција, ќе мора да поминат низ посебен пат за да бидат пуштени во употреба.

Многу одговорности ќе паднат на набавувачите на системи за вештачка интелигенција, кои ќе подлежат на строги барања за дизајнирање, тестирање, ревизија и сертификација на системите за вештачка интелигенција. Покрај тоа, субјектите кои користат системи за вештачка интелигенција предложени од набавувачите (на пример, компании), ќе бидат обврзани да ги користат во согласност со законот и прирачникот за користење, како и да обезбедат точност на податоците внесени во системите, нивно следење и водење евиденција за настаните во случај на инциденти.

Новите ограничувања се очекува да обезбедат дополнителни заштитни мерки против дискриминирачките, нечовечки одлуки. Во исто време, Законот за вештачка интелигенција (AI Act) не дава дополнителни овластувања на субјектите засегнати од таквите одлуки. Сепак, рамката на ЕУ ќе биде дополнета со планираната Директива за одговорност за вештачка интелигенција (*AI Liability Directive*, AILD), која за прв пат ќе воведе одредби што се однесуваат на штети предизвикани од системите за вештачка интелигенција. Целта на истата е воспоставување поголема заштита на луѓето кои се оштетени од употребата на вештачка интелигенција и да им го олесни поднесувањето на жалба. Нацрт-одредбите претставуваат чекор напред во обезбедувањето ефективен пристап до правни лекови во случај на дискриминација при примената на системите за вработување. Тие претпоставуваат дека, работодавачот е тој кој што не ја исполнил должноста за длабинска анализа, а притоа користел систем за вработување што дискриминирал одредени категории на луѓе.

Работата на нацрт-регулативата за вештачка интелигенција (AI Act), како и на Директивата за одговорност за вештачка интелигенција, се во напредна фаза. Сепак, според сегашната формулација на новите регулативи, нивните одредби ќе се применуваат во сите земји-членки на ЕУ дури две години после нивното усвојување.

3.2. Иднина на работата

3.2.1. Професии кои исчезнуваат, компетенции на иднината и одговорност на работодавачот да ги приспособи вештините на вработените со автоматизацијата

Според најновите истражувања на Центарот за истражување на економска политика (CEPR), дури 40% од испитаниците тврдат дека веројатноста да бидат заменети со машина, робот или алгоритам во следната деценија е повеќе од 50%. Стравувањата од технолошка невработеност не се целосно неосновани. Според извештајот Future Jobs, уделот на новите технологии во извршување на задачи значително се зголемува. Во 2018 година, во просек, 71% од работното време го вршеле човечки активности, а 29% машини. Се предвидува дека до 2025 година овие пропорции значително ќе се променат. Луѓето ќе бидат одговорни за околу 48% од активностите, додека останатите 52% од задачите ќе бидат целосно автоматизирани.

Што се однесува до последиците од автоматизацијата, може да се претпостави дека, тоа најмногу ќе го почувствуваат луѓето кои вршат физичка работа што лесно може да биде заменета со роботи (т.е. врз основа на предвидливи секвенции). Сепак, дигитализацијата

може да влијае и на ситуацијата на одредени специјалисти. Според извештајот Future of Jobs, меѓу непотребните професии, како механичар, магационер и менаџер на производство, ќе најдеме и финансиски аналитичар или службеник. Експертите на Глобалниот институт McKinsey, сепак, ги намалуваат овие стравови - се проценува дека на глобално ниво, само 5% од професиите ќе бидат целосно ликвидирани.

Несомнено е дека, начинот на извршување на професионалните обврски (поголем удел на ИТ системите и машините во извршените обврски) и посакуваните компетенции на вработените значително ќе се променат. Имајќи предвид дека многу задачи ќе ги извршуваат машини, ќе се појави зголемена побарувачка за вештини кои компјутерите не можат прецизно да ги реплицираат. Станува збор за меки вештини, односно за оние, кои бараат креативност, емоционална интелигенција и критичко размислување. Дигитализацијата, исто така, ќе ја зголеми побарувачката за технички вештини и ќе создаде работни места за добро квалификувани работници со знаење, способни да работат со нови системи. Ова, пак, може да предизвика загриженост за растечката поларизација на пазарот (полоша положба на физичките работници за сметка на зголемување на важноста на најдобро образованите). Оваа загриженост се чини дека ја потврдуваат и резултатите од студијата на Европскиот центар за развој на стручното образование (Cedefop), која покажа дека на над 70% од вработените им требаат барем основни ИТ вештини за да се вклопат на денешниот пазар на труд, а дури 30% од нив се изложени на ризик трајно да не можат да ги стекнат посакуваните компетенции (а со тоа и да ја загубат работата).

3.2.2. Компетенции на иднината и непотребни професии во ерата на дигитализација

Се поголемото користење на технологијата ќе значи дека, компетенциите посакувани на пазарот на труд значително ќе се променат во следните години. Се очекува дека заедно со автоматизацијата и алгоритмизацијата, ќе се намали побарувачката за вештини кои лесно се заменуваат со машини. Тука станува збор и за мануелни вештини (во случај на физички работници, работници во производство), како и за оние поврзани со ментална работа (на пр. Броење или креативно пишување). Од друга страна, **побарувачката за компетенции** на иднината ќе се зголеми, дефинирана во извештајот DELab *(Компетенции на иднината. Како да се оформат во флексибилен образовен екосистем?) како: специфични вештини кои овозможуваат преземање и извршување задачи во работната средина која е фундаментално флексибилна, географски дисперзирана, подложна на чести и брзи промени, има потреба од работа со дигитални технологии и соработка со автоматизирани системи и машини кои користат вештачка интелигенција.*

Компанијата McKinsey ги подели овие компетенции во три групи: технички и дигитални, социјални и когнитивни.

Компетенции на иднината	
Технички и дигитални	• Се посочува дека побарувачката за **основни** дигитални вештини ќе се зголеми за 65%. Станува збор за способноста за користење на технологија во секојдневната работа, особено во областа на решавање проблеми и пронаоѓање информации. • До 2030 година, вработените во Европа ќе трошат над 40% повеќе време на активности кои користат напредни дигитални вештини. Уште повеќе, побарувачката за програмирање и ИТ вештини ќе се зголеми за 90%
Социјални	• До 2030 година, на европскиот пазар на труд, побарувачката за социјални компетенции, првенствено претприемништвото и способност за преземање иницијативи, ќе се зголеми за 22%.
Конгитивни (повисоки): критичко размислување, креативност, вештини за управување со луѓе	• Побарувачката за повисоки когнитивни вештини ќе се зголеми за 14% до 2030 година. Истовремено, важноста на основните когнитивни вештини како што се читањето, пишувањето и основна обработка на податоци ќе се намали за 23%.

Kompetencje przyszłości w podziale na trzy grupy umiejętności: poznawcze, społeczne i techniczne

Светскиот економски форум (СЕФ) укажува дека, во следните години, најважни ќе бидат вештините како што се:

- **Човечки ресурси (HR)** – мотивирање и управување со луѓето на работа, градење на работни кадри преку барање на најдобри луѓе за извршување на конкретни задачи; мотивирање и управување со луѓето за време на работа,
- **Вештини за преговарање** – способност за решавање на конфликти и надминување на разликите во мислењата; покажувајќи ја моќта на убедување,
- **Емоционална интелигенција** – способност за идентификување и именување на сопствените и туѓите емоции; способност за управување и користење на емоциите при донесување судови и одлуки; разбирање на потребите на другите (вработени и клиенти),
- **соработка со други - способност за работа во група,**
- **когнитивна флексибилност** - способност за „префрлање“ помеѓу задачите што се извршуваат,
- **решавање на сложени проблеми** – способноста за разработување на неочигледни решенија во различни контексти,
- **критичко размислување** – користење логика и расудување за да се идентификуваат предностите или слабостите на алтернативните решенија, заклучоци или пристапи кон проблемите,

- **Креативност** – способност да не се размислува шаблонски, пронаоѓање на иновативни идеи, решавање на проблемите на неочигледен начин.

Уште повеќе, во извештајот на светскиот економски форум, наведени се и **професиите кои ќе ја изгубат својата важност во ерата на дигитализација**. Тука се вбројуваат професии како што се: вработен во внесување податоци, вработен во сметководство и платен список, административен и извршен секретар, вработен во монтажа и производство, вработен за информации и услуги за клиенти, менаџер за административни и деловни услуги, сметководител и ревизор, чувар на складиште, генерален и оперативен раководител, поштенски службеник, финансиски аналитичар, касиер и инспектор за билети, механичар, телемаркетинг, инсталатер на електроника и телекомуникации, банкар, возач, брокер и агент за продажба, мобилен продавач и продавач, вработен во секторот за осигурување, статистичко и финансиско осигурување, адвокат.

Zawody – prognoza na 2020 r.

Stabilne zawody	Nowe zawody	Zbędne zawody
Dyrektor zarządzający i prezes	Analityk danych i data scientist*	Pracownik wprowadzający dane
Główny menadżer i kierownik operacyjny*	Specjalista AI i ML	Pracownik księgowości i listy płac
Programista i analityk oprogramowania*	Główny menadżer i kierownik operacyjny*	Sekretarz administracyjny i wykonawczy
Specjalista działu sprzedaży i marketingu*	Specjalista Big Data	Pracownik montażu i produkcji
Przedstawiciel handlowy	Specjalista ds. transformacji technologicznej	Pracownik działu informacji i obsługi klienta*
Specjalista ds. zarządzania zasobami ludzkimi	Specjalista działu sprzedaży i marketingu*	Menadżer administracji i usług biznesowych
Doradca finansowy i inwestycyjny	Specjalista ds. nowych technologii	Księgowy i rewident
Specjalista ds. baz danych i sieci	Specjalista ds. rozwoju organizacji*	Magazynier
Specjalista ds. logistyki i łańcucha dostaw	Programista i analityk oprogramowania*	Główny menadżer i kierownik operacyjny*
Specjalista ds. zarządzania ryzykiem	Specjalista ds. automatyzacji procesów	Urzędnik pocztowy
Analityk bezpieczeństwa danych*	Specjalista ds. innowacji	Analityk finansowy
Analityk zarządzania i organizacji	Analityk bezpieczeństwa danych*	Kasjer i kontroler biletów
Inżynier elektrotechniki	Specjalista działu e-commerce i mediów społecznościowych	Mechanik
Specjalista ds. rozwoju organizacji*	Projektant UX i interakcji maszyna-człowiek	Telemarketer
Operator zakładu przetwórstwa chemicznego	Specjalista ds. szkoleń i rozwoju	Elektronik i instalator telekomunikacyjny
Nauczyciel uniwersytecki i szkolnictwa wyższego	Specjalista i inżynier robotyki	Bankier
Urzędnik ds. zgodności	Specjalista ds. ludzi i kultury	Kierowca
Inżynier energetyki i naftowy	Pracownik działu informacji i obsługi klienta*	Broker i agent sprzedaży
Specjalista i inżynier robotyki	Projektant usług i rozwiązań	Obwoźny sprzedawca i akwizytor
Operator i pracownik rafinerii ropy naftowej i gazu ziemnego	Specjalista ds. marketingu i strategii online	Pracownik ubezpieczeń, działu statystycznego i finansowego
		Prawnik

Źródło: World Economic Forum (2018) The Future of Jobs Report 2018, s. 9. Zawody oznaczone * występują w więcej niż jednej kolumnie tabeli, co spowodowane jest różnicami między poszczególnymi sektorami.

3.2.3. Дигитализација и трендови во областа на бизнис менаџментот - улогата на работодавачите

Со цел целосно искористување на предностите од дигитализацијата и придобивките од имплементацијата на новите технологии, компаниите ќе мора да ги реорганизираат своите структури и да го променат нивниот сегашен пристап кон работата. Ова ќе бара

редизајнирање на формалната организација на компанијата, дополнување на персоналот со вработени со нови компетенции, преквалификација или развивање на постоечките квалификации. Според McKinsey, од аспект на промената на бараните работни места и најценетите вештини, од организациите ќе се бара да направат **ажурирање во пет клучни области** - начин на размислување, организациска структура, распределба на работата, состав на работната сила и одговорности на раководството на човечките ресурси.

Кога станува збор за начинот на размислување во компанијата, клучот за идниот успех на организацијата ќе биде промовирање на т.н. доживотно учење (*lifelong learning*), односно нудење можност на вработените да стекнат нови вештини и знаења и во текот на нивната кариера, а не само на почетокот. Во однос на организациската структура, се посочува дека приоритет во наредните години ќе биде воведувањето на подинамични и иновативни методи на управување, како и почеста соработка меѓу тимовите и размена на знаења и функции од страна на вработените.

Компаниите кои имплементираат автоматизација во голем обем, исто така, очекуваат да ги префрлат задачите што моментално ги извршуваат висококвалификувани вработени на вработени со пониска вештина (поддржани од машини и компјутери). Што се однесува до работниот кадар, се очекува почесто да се бара помош од разни видови хонорарци и привремени работници. Ова ќе резултира од раст на т.н економија на споделување /економија на барање (*sharing economy; on-demand economy*), т.е. бизнис модели засновани на посредништво на платформи за соработка, создавајќи јавно достапен пазар за привремено користење на стоки или услуги, често обезбедени од приватни лица.

Одржување на конкурентност на компанијата при истовремена поддршка на вработените во процесот на дигитализација

Во извештајот *Надвор од вработувањето. Како компаниите менуваат квалификации, за да се справат со проблемот со недостиг на таленти*, McKinsey наведе различни тактики за одржување на конкурентноста помеѓу компаниите и затворање на јазот помеѓу потребните и достапни вештини за работниците во приватниот сектор. Практиките што треба да ги земат предвид работодавачите кои сакаат да ја развијат својата компанија и да изградат компетентна работна сила вклучуваат:

- **Преквалификација** – поттик за стекнување нови компетенции и надградба на постоечките вештини од страна на вработените, како и воведување и обука на нововработените во областа на посакуваните вештини. Клучно прашање за компаниите ќе биде одлуката за начинот на спроведување на обуката: внатрешно (со користење на достапни ресурси и програми) или надворешно (како дел од соработка со образовна институција или центар за обука). Што се однесува до

областите во кои работодавачите планираат да инвестираат, најчесто се однесуваат на градење стратешки вештини за нивната компанија, односно напредни ИТ компетенции, вештини за креативно пишување, критичко размислување, вештини за решавање проблеми. Од друга страна, во случај на помалку сложени вештини, работодавачите изјавуваат можност за вработување луѓе надвор од организацијата.

- **Трансфер во рамки на компанијата** – префрлање на вработени со специфични вештини во одделенија/тимови каде што можат подобро да ги искористат своите вештини. Во анкетата на McKinsey спроведена во февруари 2018 година на раководители на компании, 55% од испитаниците рекле дека повеќе би сакале да преместат некои вработени на различни или сосема нови позиции отколку целосно да ги отпуштат.

- **Вработување** – Барање на поединци или цели тимови кои ги поседуваат потребните, специфични вештини (иако понудата на експерти на пазарот може да биде недоволна за сите компании да ја имплементираат оваа стратегија). Од една страна, трошоците за вработување може да бидат пониски од преквалификацијата, но од друга страна - регрутирањето на нови членови на тимот е поврзано со ризикот како одредена личност ќе ја врши својата работа. Со цел успешно стекнување на нови, клучни вештини, компаниите треба да воведат иновации во начинот на кој регрутираат кандидати, како и да понудат атрактивна работна култура и бенефиции надвор од надоместокот за плата.

- **Создавање нови форми на соработка** - компаниите можат да користат вештини што ги носат луѓето надвор од организацијата (хонорарци, експерти, привремени агенти од агенции за вработување). Негативната страна на овој модел, сепак, е ризикот од откривање на трговски тајни (на пр. know-how, дела покриени со права на интелектуална сопственост) на трети лица, како и тешкотии во приспособувањето кон културата на компанијата и начинот на работа. Поради оваа причина, работодавачите изјавуваат дека пополнуваат позиции со независни изведувачи кои не се поврзани со клучните активности на компанијата или бараат ниски квалификации.

- **Можни отпуштања** – отпуштањето на вработените може да биде неизбежно во некои компании, особено во сектори/гранки кои не се развиваат доволно динамично и каде што автоматизацијата може во огромен степен да ја замени работната сила. Стратегијата за технолошки вишок може да се имплементира со ограничување или запирање на вработувањето на нови вработени, притоа

овозможувајќи да продолжи нормалниот процес на повлекување и пензионирање на постојните вработени.

Иако се можни отпуштања поради зголемената употреба на машини, тешко е да се очекува работниците во сите сектори да се плашат за своите работни места. Несомнено, сепак, ќе има нови технологии, системи и програми кои ќе бараат дополнителни вештини во областа ИТ.

Како работодавачите можат да ги поддржат своите вработени во процесот на дигитализирање на компанијата?

Пред се, тие можат:

- Да ги запознаат вработените со новите алатки - да го елиминираат стравот и конзервативноста кон новите технологии и да им покажат како може да се користат дигиталните алатки во секојдневната работа,

- Да ја подигнат свеста на вработените - да објаснат зошто и на каков начин компанијата ја користи дадената технологија; имајќи информации за таа област, вработените подобро ќе ги разберат новите работни алатки и ќе бидат мотивирани да ги користат,

- Да го обучат добро раководниот кадар за претстојните промени - раководството треба да ги знае одговорите на основните прашања за новите работни алатки и да им покаже на другите членови на тимот како да ги користат имплементираните технологии;

- Да спроведе обука за новите системи - дури и на моменталните работници со технолошки вештини им треба време да се запознаат со новите програми и дигитални алатки што не ги користеле досега; компанијата треба да обезбеди стручна обука за сите вработени.

3.2.4. Други субјекти кои играат важна улога во процесите на дигитализација на работата и преквалификација на вработените

Едукативни институции

Улогата на образованието во процесот на дигитализација веќе е забележана од властите на Европската Унија.

Во заклучоците на Европскиот совет беше истакнато дека, пристапот до висококвалитетно образование поддржано од дигитални технологии е предуслов за трансформација на одделните сектори и натамошен економски раст.

Исто така, Европската комисија го зеде предвид и создавањето на акционен план за дигитално образование за период од 2021-2027 година, дефинирајќи визија за дигитално образование во Европа.

Целта на двете иницијативи беше да се поттикнат универзитетите, училиштата и наставниот кадар да играат поактивна улога во градењето дигитални компетенции и задоволување на потребите на пазарот на трудот. Улогата на овие институции во дигиталната трансформација се чини дека е потврдена и со економските публикации, како што се извештајот PwC и ЕСФ *Подигнување на квалификации за заеднички просперитет (2021)*, кој нагласува дека институциите за високо образование имаат потенцијал да поттикнат промени - да го подигнат општото ниво на знаење, вештини и компетенции кај учениците и општеството.

Јавна власт

Улогата на државата е во подеднаквото поддржување на работодавачите и вработените во процесот на дигитализација. Поради тоа, важно е носителите на одлуки да спроведуваат политики кои придонесуваат за стекнување дигитални вештини или преквалификација на вработените (на пр. како дел од програмите за кофинансирање на обука за мали и средни претпријатија). Згора на тоа, важно е да се стимулира пазарот на трудот и да се избегне невработеноста преку активни политики/мерки за вработување - наместо да се потпира на бенефиции за невработени, државата треба да инвестира во агенции за вработување кои ќе станат центри за вработување и ќе ја олеснат преквалификацијата на невработените.

Невладини организации

Невладините организации често дејствуваат како инкубатори на решенија корисни за општеството. Тие обично имаат поголема слобода на дејствување отколку државните институции и може да излезат со предлози за различни решенија за проблемите. Поради оваа причина, некои компании преземаат филантропски иницијативи или соработуваат со фондации во областите поврзани со стекнување нови вештини од страна на вработените. Пример е иницијативата Generation, која се бори против невработеноста преку затворање на јазот во вештините кај младите луѓе, како и поддршка на возрасните да најдат соодветни позиции преку регрутирање, обука и менторство.

Синдикати и трговски здруженија

Дејствувајќи како социјални партнери, трговските здруженија и синдикатите играат важна улога во дигитализацијата на пазарот на трудот. На пример, во Шведска се формираат совети за заштита на трудот, финансирани од компании и синдикати. Овие субјекти обучуваат лица кои останале без работа - им обезбедуваат привремена финансиска поддршка и го олеснуваат процесот на преквалификација за невработените побрзо да се вратат на пазарот на трудот.

3.3. Нови бизнис модели и нивното влијание на пазарот на трудот

3.3.1. Ерозијата на преговарачката моќ на работниците - како новите технологии го попречуваат здружувањето на работниците

Новите технологии ја олеснуваат комуникацијата и ги поврзуваат корисниците, и покрај растојанието што ги дели. Меѓутоа, во исто време, тие водат до поголемо оттуѓување и сè помала интерперсонална интеракција. Овој феномен се однесува не само на сферата на приватниот живот, туку и на професионалниот живот. Дигитализацијата и префрлањето на работата во онлајн светот значеше дека, вработените понекогаш воспоставуваат трајни односи и поретко се среќаваат и разговараат за проблемите на работното место.

Новите технологии се погодни за изолација не само во случај на работа од далечина. Алатките за вештачка интелигенција што ги користат работодавачте за да ги контролираат вработените и да ги мерат нивните перформанси, исто така, често се користат за шпионирање и спречување на вработените да се здружат.

Се случува деловните модели на големите компании да се засноваат на голема контрола на вработените и постојано зголемување на темпото на работа. Здружувањето на вработените со цел застапување на нивните колективни и индивидуални права и интереси претставува реален ризик за системот, во кој единственото нешто што е важно е зголемување на профитот на работодавачот. Поради оваа причина, компаниите превземаат мерки за да ги спречат работниците да се здружуваат. Оваа практика се интензивираше за време на пандемијата на КОВИД-19, кога препораките за здравје и безбедност воведени во овој период почнаа да се користат за имплементација на алатки за мерење на растојанието меѓу луѓето во магацините, притоа забранувајќи им да останат премногу блиску еден до друг. Компаниите почнаа да набавуваат софтвер што ќе овозможи анализа и визуелизација на податоците што се однесуваат на здружувањата на работните места (на пример, geoSPatial Operating Console или SPOC). Покрај тоа, одделенијата за човечки ресурси ги

следеа мејлинг листите на вработените користени за цели на работничко здружување или групрање на вработените на социјалните медиуми.

Во случај на работа на одредена платформа, не е јасно дали влијанието на новите технологии врз здружувањето на вработените е позитивно или негативно. Апликациите што се користат за давање услуги може да го олеснат мобилизирањето на куририте и возачите - алатките за комуникација достапни во нивните системи им нудат на вработените во платформата (gig-workers) простор за размена на информации, а мрежите за масовно комуницирање можат да поврзат поединечни курири на ниво на градови, региони и дури и земји.

Во исто време, ефективноста на синдикатите на работниците на платформата често зависи од поддршката од страна на јавните власти за различни форми на самоорганизација. На пример, во Болоња, во соработка со синдикатите, беше создадена Повелба за основни права за дигитална работа во урбан контекст (италијански: *Carta dei diritti fondamentali del lavoro digitale nel Contesto Urbano*), која што воспоставува рамка на минимални стандарди што се однсеуваат на наградување, работно време и осигурување за работниците на платформата. Тоа што е поважно, сепак е тоа што самиот градоначалник на Болоња покажа голема поддршка за иницијативата и ги повика клиентите да ги бојкотираат платформите кај оние кои не ја потпишаа повелбата.

Во земјите каде што државата не обезбедува заштита за работниците на платформа, нивото на нивното синдикално здружување е многу пониско, а преговарачката моќ е послаба. Ова понекогаш се злоупотребува од платформи кои користат механизми во апликациите за подобро да ги контролираат куририте или возачите и да ги спречат обидите да се спротивставуваат на политиката на компанијата.

Штрајкот на полските курири кои доставуваат оброци од април 2021 година, кој беше стишен многу бргу, е пример тоа, како гигантите на економијата на споделување, со помош на технологијата ги ограничуваат иницијативите на вработените кои се борат за своите права. Причината за штрајкот беше неправедниот начин на распределување на нарачките и наградувањето со помош на алгоритам, а методот на спротивставување беше прекин на нарачките од курири, и покрај подготвеноста за работа декларирана во апликацијата. Возачите се надеваа дека ќе извршат притисок врз работодавачот и ќе го убедат да разговара со претставниците на заедницата. Сепак, компанијата користејќи ја апликацијата, без никаков обид за комуникација со куририте, ги блокираше штрајкувачите и им ги предаде нарачките на луѓе кои беа подготвени да работат и покрај неповолните услови.

3.3.2. Влијанието на дигитализацијата на пазарот на трудот - работа на платформа

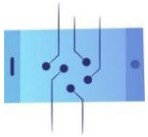
Работата на платформата е форма на вработување каде што вработениот користи дигитална платформа за да добие пристап до други организации или поединци со цел обезбедување на одредени услуги во замена за одреден надомест. Како платени задачи што се вршат преку дигитални платформи се вбројуваат такси и курирски услуги, испораки, сервис за поправки во домот, како и интелектуална работа, на пр. креативно пишување копии или сметководство. Иако апликациите како Uber или Bolt се развиваат во европскиот простор само една деценија, вработените кои обезбедуваат услуги на платформи од овој тип денес претставуваат значителен дел од работната сила (28,3 милиони вработени во 2022 година во Европската унија). Оваа бројка се споредува со бројот на луѓе вработени во секторите за индустриско производство (29 милиони работници). Уште повеќе, според Европската комисија, до 2025 година на платформите ќе бидат вработени уште 15 милиони луѓе. Најпопуларните платформи во ЕУ ги вклучуваат Uber, Deliveroo, Amazon Mechanical Turk, Fiverr, Upwork, Appjobs, Glovo и JustEat (во Полска познати како Pyszne.pl).

Бизнис моделот на платформите за работа се заснова на технологии кои користат алгоритми за ефективно усогласување на понудата и побарувачката за вработените и услугите што тие ги обезбедуваат. Дополнително, употребата на соодветно дизајнирани апликации овозможува бесконтактно, автоматизирано одлучување и следење на извршените задачи. Благодарение на системот за управување базиран на алгоритми, постои можност да се остави традиционалниот модел на менаџерски кадар. Ова, пак, ги поттикнува платформите да тврдат дека тие дејствуваат само како посредник кој нуди услуги за поврзување на самовработени лица со потенцијален клиент, а не како работодавач.

Кој најчесто бара вработување преку платформи за работа?

- Млади лица,
- мажи,
- Мигранти (особено од областа на физичка работа),
- лица со средно образование, за кои оваа работа е дополнителен извор на приход.

Покрај тоа, работниците на платформата можат да се поделат во две екстремни групи на пазарот на трудот. Првиот ги вклучува работниците од опсег на интелектуална работа, привилегирани во однос на своите компетенции, на пример, програмери кои можат да влијаат на условите за соработка со клиентите (хонорарство, обезбедување на ИТ услуги).



Во втората група има луѓе со ниски, лесно заменливи компетенции, чија преговарачка моќ на пазарот на трудот е мала (на пр. имигранти кои обезбедуваат услуги за такси превоз).

Предности и недостатоци на работата на платформата

Предностите на работа на платформа вклучуваат:

- флексибилно работно време и можност самостојно да се планира распоредот за работа,
- директен контакт со клиенти,
- поголема независност.

Меѓутоа, во сегашната форма на дигитални платформи, постојат бројни недостатоци на овој тип на вработување:

- Прашања за здравје и безбедност при работа:
    - недостаток на регулирани правила за заштита на здравјето и безбедноста при работа,
    - физички ризици,
    - стрес предизвикан од несигурност во работата;
- Услови за вработување:
    - 5,5 милиони работници што работат на платформи во ЕУ се погрешно класифицирани или се класифицирани како самовработени,
    - оние што неправилно се класифицирани како самовработени ги немаат истите права и бенефиции како оние кои се во работен однос;
- проблеми што произлегуваат од алгоритмизацијата на работата,
- Ограничени можности за здружување,
- непредвидена заработка и работно време (според Европската комисија, 41% од работното време на работниците на платформата вклучува неплатени задачи, како што се прелистување реклами или чекање нарачки).

Правото на ЕУ и работа на платформа

Некои земји-членки веќе спроведоа регулативи во своето национално законодавство од областа на работа на платформа. Дискусиите за овој конкретен тип на вработување се водат и на ниво на Заедницата. Концептот на работници на платформата е веќе воведен во

законодавството на ЕУ, на пример, преку Директивата за транспарентни и предвидливи работни услови во Европската Унија. Сепак, пробив во овој поглед треба да биде **Директивата за подобрување на условите за работа на платформите**, чиј нацрт беше претставен од Европската комисија на крајот на 2021 година.

Најважните одредби содржани во нацрт-директивата за подобрување на работните услови на платформата:

- Луѓето кои работат преку дигитални платформи ќе добијат работен статус, кој одговара на нивните реални работни услови, што ќе се проверува со утврдување на критериумите потребни за да се препознае платформата како работодавач.
- Платформата ќе се смета за работодавач доколку исполнува најмалку два од следниве критериуми:
    - го одредува нивото на наградување или максималната граница за надградување,
    - го надгледува извршувањето на работите по електронски пат,
    - ја ограничува слободата за избор на работно време или периоди на отсуство, слободата да се прифаќаат или одбиваат задачите или слободата да се користат подизведувачи или замени
    - воспоставува специфични обврзувачки правила за изглед и однесување кон примателот на услугата или клиентот,
    - ја ограничува можноста за проширување на базата на клиенти или извршување на работи за трети лица.
- Вработените на платформата треба да уживаат работни и социјални права што произлегуваат од статусот на вработено лице, како:
    - загарантирано време за одмор и платени одмори,
    - минимална плата,
    - можност за спроведување колективни преговори,
    - безбедност и заштита при работа,
    - надоместоци за невработеност и болест,
    - пензии по основ на придонеси.

- Платформата може да ја оспори класификацијата, но мора да докаже дека работниот однос не постои.
- Платформите ќе бидат обврзани за зголемување на транспарентноста на употребата на алгоритми и обезбедување на следење на работните услови од страна на човек.
- Вработените ќе имаат право да ги оспоруваат автоматизираните одлуки.

DIGITALIZZAZIONE DEL MERCATO DEL LAVORO

Modulo di formazione sviluppato nell'ambito del progetto
Avvio di attività per l'attuazione dell'Accordo quadro delle parti sociali europee sulla digitalizzazione
cofinanziato dall'Unione europea

IT

Co-funded by the European Union

NSZZ Solidarność Komisja Krajowa

CISL Confederazione Italiana Sindacati Lavoratori

NSZZ Solidarność Komisja Krajowa

CISL Confederazione Italiana Sindacati Lavoratori

Digitalizzazione del mercato del lavoro

Modulo di formazione sviluppato nell'ambito del progetto

Avvio di attività per l'attuazione dell'Accordo quadro delle parti sociali europee sulla digitalizzazione

cofinanziato dall'Unione europea

Co-funded by the European Union

Giugno 2023

Autrici:

Blanka Wawrzyniak

Marta Musidłowska

Supporto scientifico:

Hanna Sakowicz-Daszczyńska

Responsabile editoriale:

Julia Zaleska

Pubblicazione gratuita, finanziata dall'Unione europea nell'ambito del progetto n. 101051759 **"Avvio di attività per l'attuazione dell'Accordo quadro delle parti sociali europee sulla digitalizzazione (EFAD)".** Titolo originale: **"**Initiating activities to implement the European Social Partners Framework Agreement on Digitalisation (EFAD)".

Nota introduttiva

Questa pubblicazione è stata realizzata nell'ambito del progetto "Avvio delle attività di attuazione dell'accordo quadro delle parti sociali europee sulla digitalizzazione". Si tratta di un manuale che verrà utilizzato sia durante che dopo la formazione di progetto. Il modulo di formazione mira a preparare le parti sociali ai dinamici cambiamenti che avvengono nel mercato del lavoro a causa della trasformazione digitale. Si tratta di cambiamenti che riguardano, tra le altre cose, l'automazione della produzione, i nuovi modelli di business, lo smart working e i metodi di gestione innovativi nelle aziende. La pubblicazione comprende anche una discussione sui diritti dei dipendenti nell'era digitale. L'obiettivo è fornire ai dipendenti gli strumenti per staccare la spina e mantenere l'equilibrio tra vita professionale e vita privata.

Indice

Introduzione

Sebbene l'intelligenza artificiale (AI) sia un termine ampio che comprende un gruppo di algoritmi in grado di modificare i propri parametri e creare nuovi risultati, nei suoi termini più semplici può essere descritta come la capacità delle macchine di comprendere, apprendere, pianificare e dimostrare creatività.

Per molti esperti, il ritmo di sviluppo dell'intelligenza artificiale e il suo impatto sul mondo che ci circonda sembrano preoccupanti. Ciò è influenzato, tra le altre cose, dal fatto che i sistemi di IA vengono sviluppati dalle più grandi aziende tecnologiche statunitensi e cinesi, che in cima alle loro priorità mettono i propri profitti commerciali. La stessa industria tecnologica ha messo in guardia dai pericoli di uno sviluppo illimitato dell'IA. Una lettera aperta che chiede di fermare gli esperimenti sui sistemi di intelligenza artificiale e sui sistemi più potenti della Chat GPT-4 è stata firmata, tra gli altri, da Elon Musk (CEO di SpaceX, Tesla e Twitter), Steve Wozniak (co-fondatore di Apple) e Yuval Noah Harari (futurologo, professore all'Università Ebraica di Gerusalemme).

Controllare lo sviluppo dell'IA è essenziale per garantire che i sistemi di IA siano sicuri e che tengano conto dell'impatto sul benessere umano. Tuttavia, nell'ampio flusso di informazioni sull'IA, emergono le visioni più allarmistiche, non necessariamente fondate sulla realtà. Questo, a sua volta, porta a opinioni scettiche sulle nuove tecnologie, alla paura di una disoccupazione di massa e alla riluttanza a utilizzare gli strumenti digitali. Tuttavia è importante ricordare che le tecnologie digitali sono ormai parte integrante della vita quotidiana. Non sono solo fonte di intrattenimento, ma anche strumenti che facilitano lo svolgimento dei compiti domestici e professionali. Pertanto, la familiarizzazione con soluzioni innovative e l'educazione del pubblico a un uso corretto delle tecnologie digitali sono estremamente importanti.

Le attività di sensibilizzazione dovrebbero riguardare anche (o soprattutto) gli strumenti digitali utilizzati sul posto di lavoro. Come verrà sottolineato più avanti nel manuale, le nuove tecnologie sono utilizzate in molti settori e in diverse fasi dell'impiego (dall'assunzione alla valutazione dei dipendenti). Esse facilitano sia i processi di gestione aziendale che il lavoro quotidiano di molte persone (sia operai che impiegati). L'esempio migliore è la diffusione di traduttori automatici come Google Translator o Deepl, che migliorano la comunicazione transfrontaliera tra aziende o consentono di tradurre testi professionali senza dover ricorrere a un traduttore professionista.

Crescono anche le speranze di semplificare il lavoro con l'intelligenza artificiale generativa. Applicazioni come chat-GPT o DALL-E vengono già utilizzate per compiti creativi, come la scrittura di e-mail o l'analisi di dati. Ad esempio, con l'aiuto dell'intelligenza artificiale generativa è possibile analizzare più rapidamente il contenuto di un articolo o redigere il verbale di una riunione in un attimo. Dopo aver impartito un comando appropriato (ad esempio, "esponi

le principali conclusioni della discussione") e aver inserito i parametri di base nel sistema, si può prevedere che vengano generati i risultati attesi (conclusioni).

Allo stesso tempo, è importante tenere presente che i modelli *linguistici di grandi dimensioni* (LLM) come Chat GPT, pur producendo contenuti che sembrano naturali, li generano in modo automatico e non riflessivo. Questo, a sua volta, può portare a testi prodotti dagli algoritmi che, sebbene molto affidabili, contengono molti errori. È per questo che è così importante sviluppare negli utenti capacità di pensiero critico, la capacità di analizzare l'ambiente reale e di discernere ciò che non è vero (ad esempio, le *fake news*). Inoltre, nel lavoro nell'era digitale, oltre a preparare i dipendenti dei vari settori all'automazione e a dotarli di nuove competenze, è necessario insegnare ai dipendenti la convivenza con la tecnologia e la capacità di "staccare la spina". Questi sono i prerequisiti per un giusto equilibrio tra lavoro e vita privata.

Il presente elaborato è stato creato nel 2022/2023. Dato lo sviluppo dinamico dell'innovazione e, in particolare, degli strumenti di intelligenza artificiale (AI), le autricii del manuale desiderano sottolineare che alcuni contenuti potrebbero diventare obsoleti nei prossimi mesi e anni a causa dei progressi tecnologici.

Glossario

AI ACT / Legge sull'**intelligenza** artificiale

- Regolamento dell'UE che stabilisce norme armonizzate sull'intelligenza artificiale.

Algoritmo

- un insieme di istruzioni (formule computazionali) che prendono autonomamente decisioni basate su modelli statistici o regole decisionali senza l'intervento esplicito dell'uomo.

Anonimizzazione

- il processo di trasformazione dei dati personali in modo tale che non possano essere attribuiti a una persona fisica identificata o identificabile.

Automazione

- l'uso della tecnologia per controllare la produzione e creare prodotti e servizi utilizzando strumenti digitali.

Blockchain

- la cosiddetta "catena di blocchi", una tecnologia per il trasferimento e l'archiviazione di informazioni sulle transazioni online; un registro di dati decentralizzato che viene condiviso in modo sicuro. La tecnologia blockchain consente a un gruppo di partecipanti selezionati di condividere dati.

***Bring you own device (*BYOD) / Porta il tuo dispositivo**

- la tendenza a utilizzare dispositivi privati come laptop, smartphone e tablet per svolgere le proprie mansioni professionali.

Chat GPT

- uno strumento che utilizza l'intelligenza artificiale (chatbot) e che, in un formato simile al dialogo, consente di rispondere a domande poste in un linguaggio naturale dall'utente.

Dati personali

- qualsiasi informazione relativa a una persona fisica vivente identificata o identificabile (costituiscono dati personali anche le singole informazioni che, se considerate nel loro insieme, possono portare all'identificazione di una persona costituiscono anch'esse dati personali).

Deep Fake / Falso ***profondo***

- da due espressioni inglesi: *deep learning (apprendimento profondo)* e *fake (bufala, falso)*. Si tratta dell'elaborazione di suoni e immagini per creare un messaggio falso utilizzando tecniche di intelligenza artificiale. In questo modo è possibile produrre materiale che è difficile o impossibile da distinguere da filmati o fotografie creati con mezzi tradizionali e con persone reali.

Modelli linguistici di grandi dimensioni (LLM, Large Language Models)

- modelli di apprendimento automatico in grado di eseguire una serie di compiti di elaborazione del linguaggio naturale. L'addestramento di un sistema di questo tipo consiste nel fornirgli grandi quantità di dati (ad esempio libri, articoli, siti web) in modo che possa apprendere modelli e connessioni tra le parole per generare nuovi contenuti in futuro. Un esempio di LLM è Chat GPT, sviluppato da OpenAI e disponibile al pubblico dal novembre 2022. Questo modello è in grado di elaborare informazioni e generare testi simili a quelli umani in risposta alle richieste dell'utente.

Fake news / ***Notizie false***

- informazioni false o parzialmente false di natura sensazionale che inducono deliberatamente in errore il destinatario.

E*conomia della condivisione/su richiesta* (sharing *economy*; *on-demand economy*)

- un insieme di modelli di business basati sull'intermediazione di piattaforme collaborative, che creano un mercato ad accesso aperto per l'utilizzo temporaneo di beni o servizi spesso forniti da privati.

Competenze del futuro

- competenze specifiche per intraprendere e svolgere compiti in un ambiente di lavoro fondamentalmente flessibile, geograficamente disperso, soggetto a frequenti e rapidi cambiamenti e che comporta la necessità di utilizzare tecnologie digitali e collaborare con sistemi automatizzati e macchine che utilizzano l'intelligenza artificiale.

Mobbing

- azioni o comportamenti diretti a un lavoratore che consistono in molestie o intimidazioni persistenti e prolungate.

Lavoro tramite piattaforma

- una forma di impiego in cui un dipendente utilizza una piattaforma digitale per accedere ad altre organizzazioni o individui per fornire servizi specifici e in cambio di un compenso. Tra i compiti svolti a pagamento attraverso le piattaforme digitali vi sono i servizi di taxi e di corriere, le consegne, i servizi di riparazione a domicilio, nonché i lavori impiegatizi come il copywriting e la contabilità.

Lavoro assistito

- lavoro in cui alcune attività possono essere sostituite da robot, mentre altre richiedono l'intervento umano.

Diritto alla disconnessione

- Il diritto di non impegnarsi in compiti legati al lavoro al di fuori dell'orario di lavoro e di non partecipare alla comunicazione attraverso strumenti digitali.

Profilazione

- qualsiasi forma di trattamento automatizzato dei dati personali che comporti l'utilizzo degli stessi per valutare determinati fattori personali di un individuo. In particolare, la profilazione viene utilizzata per analizzare o prevedere le prestazioni di tale persona, la sua situazione economica, la sua salute, le sue preferenze personali, i suoi interessi, la sua affidabilità, il suo comportamento, la sua ubicazione o i suoi spostamenti.

Pseudonimizzazione

- trattare i dati personali in modo tale che non sia possibile identificare a chi appartengono senza accedere ad altre informazioni conservate in modo sicuro altrove.

GDPR

- *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla*

libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito: il Regolamento GDPR).

Robot collaborativi (co-bot)

- attrezzatura progettata per ridurre il carico di lavoro dei lavoratori in fabbrica, svolgendo parte delle loro mansioni.

Autoapprendimento (ML; *machine learning*)

- un'area dell'intelligenza artificiale dedicata agli algoritmi che migliorano continuamente le loro prestazioni attraverso l'esperienza o l'esposizione ai dati. Gli algoritmi di apprendimento automatico costruiscono un modello matematico a partire da dati campione (chiamati set di apprendimento) per fare previsioni o prendere decisioni senza la necessità di programmare un essere umano.

Spoofing

- un tipo di attacco in cui i criminali si fingono banche, istituzioni e uffici governativi, aziende o addirittura individui per estorcere dati o denaro alle loro vittime.

Start-up

- un'azienda di nuova costituzione o un'organizzazione temporanea alla ricerca di un modello di business per crescere in modo redditizio.

Intelligenza artificiale (AI)

- la capacità delle macchine di comprendere, apprendere, pianificare e dimostrare creatività. Secondo la definizione proposta dalla bozza di legge sull'intelligenza artificiale, per sistema di intelligenza artificiale si intende un software sviluppato utilizzando una o più delle tecniche e degli approcci descritti nel regolamento, in grado di generare, per un determinato insieme di scopi definiti dall'uomo, output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce. Questa definizione è molto ampia e vaga, ma è comprensibile nel contesto di una tecnologia in rapido sviluppo come l'intelligenza artificiale.

Crittografia dei dati

- un insieme di tecniche di codifica di informazioni sensibili o personali per garantirne la riservatezza.

Wearables / Dispositivi ***indossabili***

- Dispositivi elettronici "indossabili", cioè indossati vicino alla pelle. Possono monitorare e analizzare i parametri di salute o il comportamento di chi li indossa. I dispositivi più diffusi di questo tipo sono attualmente gli smartwatch, le fasce sportive (le cosiddette smartband) e gli orologi sportivi.

Equilibrio tra ***lavoro e vita privata***

- mantenere un equilibrio tra lavoro (sia retribuito che non), vita familiare e tempo libero.

Processo decisionale **automatizzato**

- Un'attività basata su calcoli avanzati e su mezzi esclusivamente tecnici di elaborazione delle informazioni. L'emissione di decisioni da parte di un computer senza il coinvolgimento dell'elemento umano.

1. Impatto della digitalizzazione sui processi lavorativi

1.1 Accordo quadro delle parti sociali europee sulla digitalizzazione - osservazioni generali

La trasformazione digitale dell'economia ha un enorme impatto sui datori di lavoro, sui lavoratori e sul corso stesso del lavoro. Per facilitare l'integrazione delle tecnologie digitali nei luoghi di lavoro, nel giugno 2020 è stato concluso l' Accordo quadro autonomo delle parti sociali europee (EFAD). Il suo obiettivo è prevenire e ridurre al minimo i rischi che i lavoratori e i datori di lavoro possono correre. L'accordo riguarda tutte le persone impiegate o che impiegano lavoratori nel settore pubblico e privato e in tutti i tipi di attività economica.

L'accordo EFAD è un'iniziativa autonoma ed è il risultato dei negoziati tra le parti sociali europee nell'ambito del Sesto programma di lavoro pluriennale 2019-2021. Alla luce dell'art. 155 del Trattato sul funzionamento dell'Unione europea (TFUE), questo accordo quadro europeo autonomo impegna i membri di BusinessEurope, SMEunited, CEEP e CES (e il comitato di collegamento EUROCADRES/CEC) a promuovere e attuare strumenti e misure (se necessario a livello nazionale, settoriale o aziendale) secondo le procedure e le prassi proprie delle parti sociali negli Stati membri e nei paesi dello Spazio economico europeo.

Esempi di altri accordi autonomi conclusi negli ultimi anni sono l'accordo quadro autonomo delle parti sociali europee sull'invecchiamento attivo e gli approcci intergenerazionali o l'accordo quadro europeo sullo stress legato al lavoro.

I. Principali obiettivi dell'accordo EFAD

1. Aumentare la consapevolezza e la comprensione tra i datori di lavoro, i lavoratori e i loro rappresentanti delle opportunità e delle sfide sul lavoro che derivano dalla trasformazione digitale.
2. Fornire assistenza ai lavoratori e ai loro rappresentanti e ai datori di lavoro nello sviluppo di misure e azioni per sfruttare le nuove opportunità digitali e quindi affrontare le sfide, tenendo conto delle iniziative, delle pratiche e dei contratti collettivi esistenti.
3. Incoraggiare un approccio di partenariato tra datori di lavoro e sindacati.

II. Fasi di creazione di partnership per facilitare il processo di trasformazione digitale in azienda

Ai rappresentanti dei lavoratori saranno fornite le strutture e le informazioni necessarie per un coinvolgimento efficace nelle varie fasi del processo.

Fase 1.

"Esplorazione/preparazione/sostegno congiunto", che si occupano di sensibilizzazione e di creare le condizioni e l'atmosfera di sostegno e fiducia. Queste attività mirano a consentire una discussione aperta sulle opportunità e sulle sfide/minacce della digitalizzazione e sul loro impatto sul luogo di lavoro, nonché a discutere di possibili azioni e soluzioni.

Fase 2.

La "mappatura/valutazione/analisi regolare congiunta" è un esercizio di mappatura delle aree tematiche in termini di benefici e opportunità, nonché di sfide e rischi che l'integrazione efficace delle tecnologie digitali può portare ai dipendenti e all'azienda.

Fase 3.

"Revisione congiunta della situazione e adozione di una strategia di trasformazione digitale", che è il risultato delle prime due fasi. Si tratta di una comprensione di base delle opportunità e delle sfide/rischi, dei diversi elementi che compongono la digitalizzazione dell'azienda e delle loro interrelazioni, e del concordare strategie digitali che fissino gli obiettivi dell'azienda per il futuro.

Fase 4.

"Adozione di misure/azioni appropriate" sulla base di un esame congiunto della situazione. Essa comprende: la possibilità di testare e pilotare le soluzioni previste, la definizione delle priorità, l'attuazione delle azioni in fasi temporali successive, il chiarimento e la definizione dei ruoli e delle responsabilità della direzione e del personale e dei loro rappresentanti, nonché le risorse e le misure di accompagnamento (ad esempio, supporto di esperti, monitoraggio).

Fase 5.

Il "regolare monitoraggio/follow-up, apprendimento, valutazione congiunti" è una valutazione congiunta dell'efficacia delle azioni e una discussione sulla necessità di ulteriori analisi, sensibilizzazione, supporto o altre azioni.

III. L'ambito di applicazione dell'accordo comprende:

1. Competenze digitali e occupazione

Le parti sociali dovrebbero essere interessate a facilitare l'accesso a una formazione di qualità e allo sviluppo delle competenze dei dipendenti. Una sfida fondamentale sarà quella di identificare le competenze digitali e i cambiamenti processuali da implementare in una determinata azienda.

Le misure da considerare includono:

- Impegno delle parti alla riqualificazione.
- Accesso e organizzazione della formazione, alta qualità ed efficacia della formazione, introduzione di opportunità part-time e assegnazione di tempo di lavoro specifico per la formazione.
- Condizioni di partecipazione chiaramente definite, tra cui: durata, aspetti finanziari, coinvolgimento dei dipendenti e compensazione se la formazione si svolge al di fuori dell'orario di lavoro.

2. Modalità di connessione e disconnessione

È dovere del datore di lavoro garantire la sicurezza e la salute dei lavoratori sotto ogni aspetto legato al lavoro. Pertanto, il diritto alla disconnessione è uno degli aspetti principali di questo manuale. Chiediamo ai sindacalisti di fare ragionevole chiarezza sulle aspettative del datore di lavoro nei confronti del lavoratore quanto all'uso dei dispositivi digitali anche con il sostegno della contrattazione collettiva ai livelli appropriati

Introdurre nuovi dispositivi digitali può assicurare flessibilità nell'organizzazione del lavoro con benefici sia per i lavoratori che i datori di lavoro. Al contempo questa può comportare un grave rischio legato ad una difficile separazione tra lavoro e vita privata. Per questo è opportuno concentrarsi sull'evitare fenomeni negativi che impattino la salute e la sicurezza dei lavoratori. Per far ciò è necessario definire bene i diritti, gli obblighi e le mansioni, nei quali il principio di precauzione è la più alta priorità.

Le misure da prendere in considerazione sono:

- Formazioni e altre attività di sensibilizzazione dei lavoratori.

- Creare una nuova cultura del lavoro tra i dirigenti che eviti il contatto con il dipendente al di fuori dell'orario di lavoro.
- Fornire una guida chiara sulla legislazione esistente in materia di orario di lavoro, telelavoro e lavoro mobile.
- Organizzazione efficiente del lavoro, compresa la garanzia che il numero di dipendenti non costringa a lavorare oltre l'orario di lavoro.
- Compenso adeguato per il tempo di lavoro supplementare.
- Procedure di allerta e sostegno che permettano di scollegarsi e che tutelino da sanzioni per la mancanza di contatto con il lavoratore dopo l'orario di lavoro.
- Prevenire l'isolamento sul lavoro.

3. Intelligenza artificiale e garanzia del principio del controllo umano

Non c'è dubbio che l'IA avrà un impatto crescente sul lavoro umano. Pertanto l'Accordo europeo autonomo stabilisce alcuni principi e indicazioni per la sua introduzione nel mercato del lavoro. Un elemento importante che dovrebbe essere garantito in ogni luogo di lavoro è il controllo umano sull'IA, che è la base per l'uso della robotica e delle applicazioni basate sull'IA. Il sistema dovrebbe essere legale ed equo e rispettare standard etici compatibili con i diritti umani. Da un punto di vista tecnico e sociale, invece, dovrebbe essere sicuro e trasparente.

4. Rispetto della dignità umana e della sorveglianza

A causa della significativa ingerenza delle moderne tecnologie nel processo lavorativo, sussiste il rischio di violare i valori fondamentali dell'essere umano che lavora (ad esempio, raccogliendo dati sensibili - si pensi all'accesso a locali o documenti attraverso un'impronta digitale o una scansione della pupilla o un chip impiantato). Tali tecnologie aumentano il rischio di violazione della dignità umana, soprattutto nel caso del monitoraggio personale. Ciò può portare
a un deterioramento delle condizioni di lavoro.

La minimizzazione e la trasparenza dei dati personali, insieme a regole chiare per il loro trattamento, riducono il rischio di un monitoraggio invasivo e di un uso improprio dei dati. Nel contesto lavorativo, le regole sul trattamento dei dati personali dei dipendenti sono stabilite dal regolamento GDPR. Inoltre, le parti sociali dell'accordo EFAD ricordano che l'articolo 88 del GDPR fa riferimento alla possibilità di stabilire, attraverso contratti collettivi, regole più dettagliate per la conservazione dei dati personali dei dipendenti. Ciò al fine di garantire la tutela

dei diritti e delle libertà dei lavoratori in relazione al trattamento dei loro dati personali nell'ambito del rapporto di lavoro.

Le misure da considerare includono:

- Consentire ai rappresentanti dei dipendenti di risolvere le questioni relative a dati, consenso, privacy e sorveglianza.
- Raccogliere dati per uno scopo specifico e trasparente. I dati non devono essere raccolti o conservati semplicemente perché è possibile o per uno scopo non definito.
- Informare i dipendenti che possono non acconsentire al trattamento di un particolare gruppo di dati personali o che possono revocare in qualsiasi momento il consenso precedentemente dato.
- Fornire ai rappresentanti del personale strutture e strumenti (digitali), ad esempio bacheche digitali, per svolgere i loro compiti.

5. Attuazione e follow-up

Le organizzazioni aderenti riferiranno al comitato di dialogo sociale in merito all'attuazione dell'accordo. Entro i primi tre anni dalla firma dell'accordo, il comitato di dialogo sociale è tenuto a preparare e adottare un pacchetto annuale che riassuma lo stato di attuazione in corso dell'accordo. Una relazione completa sulle attività di attuazione intraprese sarà preparata dal comitato e adottata dalle parti sociali europee negli anni successivi. L'accordo non pregiudica il diritto delle parti sociali di concludere accordi di adattamento e/o complementari in modo da tenere conto delle esigenze specifiche delle parti sociali interessate.

1.2 Le nuove tecnologie sul posto di lavoro - lavoro assistito dalle macchine e completamente automatizzato

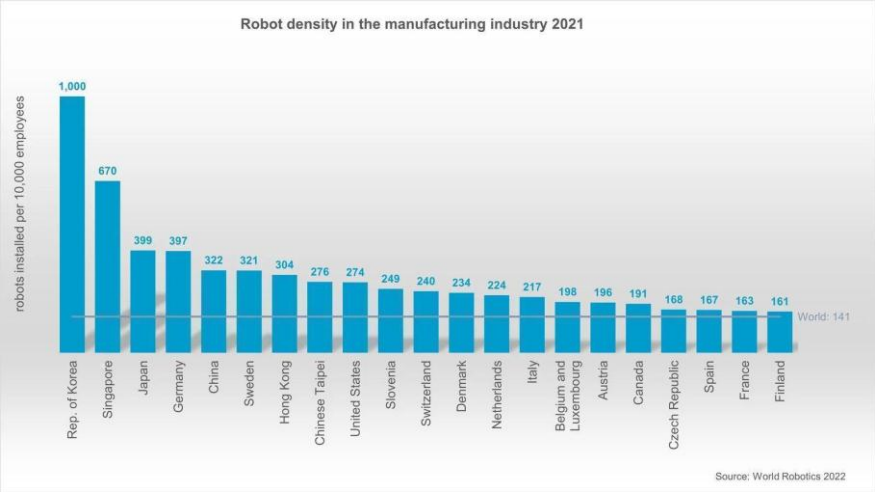
L'atteggiamento nei confronti della robotizzazione sta cambiando sia dal punto di vista delle imprese che dei lavoratori stessi. Il robot non rimane più solo un'immaginazione, ma appare come uno strumento di produzione che può alleggerire il peso dell'uomo e aiutarlo a risolvere problemi specifici. A seconda del settore e della fase di produzione, tuttavia, l'automazione può essere introdotta in diversa misura. Oltre a seconda del livello di coinvolgimento nelle varie mansioni, i robot possono essere suddivisi in quelli che svolgono un lavoro prevalentemente intellettuale (ad esempio tutti gli strumenti di intelligenza artificiale) e quelli che sollevano l'uomo da compiti ripetitivi (ad esempio nell'imballaggio dei prodotti).

Che cos'è un sistema di produzione automatizzato?

Per automazione della produzione si intende quella direzione di sviluppo delle aziende che comporti una significativa riduzione o la completa sostituzione del lavoro umano fisico e mentale con il lavoro delle macchine. Le origini di questo fenomeno possono essere fatte risalire al XX secolo, quando, nel 1913, Henry Ford cambiò per sempre il mondo con una catena di montaggio mobile gestita da operai specializzati. La premessa di questo lavoro era quella di aumentare la scala della produzione, abbassando al contempo il prezzo del prodotto finale.

Siamo ora di fronte alla prossima fase dell'evoluzione della produzione: la semplificazione dell'automazione attraverso la digitalizzazione. Grazie a tecnologie come i moduli di programmazione intuitivi, la creazione di istruzioni dettagliate per i robot sta diventando più semplice. I sensori avanzati consentono alle macchine di comprendere l'ambiente circostante e di essere più reattive. Secondo la Federazione Internazionale di Robotica, dal 2015 al 2020 la densità di robot[1] è quasi raddoppiata a livello mondiale, passando da 66 unità nel 2015 a 126 unità nel 2020.

Paesi con la produzione più automatizzata (2021)



Fonte: Federazione Internazionale di Robotica (*The Robot Report*, 2021).

[1] Una metrica utilizzata dalla Federazione Internazionale di Robotica che misura il numero di robot per 10.000 lavoratori in un settore.

Lavoro supportato

Per lavoro assistito si intendono quei casi in cui alcune attività della produzione possono essere sostituite da robot, mentre altre richiedono l'intervento umano. I *robot collaborativi* (i cosiddetti "co-bot") sono più spesso utilizzati per supportare i processi produttivi, con il compito di sgravare gli operai di una parte del carico di lavoro. Una caratteristica importante che distingue i cosiddetti co-bot dai sistemi industriali standard (che di solito sono separati dall'uomo) è che, nel caso della robotica collaborativa, i sistemi robotici controllati condividono lo stesso spazio di lavoro con gli esseri umani.

Modi in cui i robot interagiscono con gli esseri umani:

1. **Interazione umana limitata -** il robot si ferma completamente quando un uomo appare nell'area designata e riprende a funzionare in modo indipendente dopo che il lavoratore ha lasciato l'area.
2. **Collaborazione umana -** grazie ai sensori integrati, il co-bot rallenta le operazioni o interrompe il lavoro quando qualcuno si trova nelle sue vicinanze, consentendo un'interazione sicura tra uomo e macchina.
3. **Guida manuale** - il co-bot è sempre controllato dall'operatore. Ad esempio, il dispositivo trattiene il carico mentre un uomo ne guida il braccio.

Lavoro completamente automatizzato

L'automazione nell'industria è intesa come l'uso della tecnologia per controllare la produzione e creare prodotti e servizi utilizzando strumenti digitali. Nel caso dell'automazione completa, le persone e le macchine cessano di svolgere compiti complementari e iniziano a operare negli stessi ambiti. A causa della robotizzazione la partecipazione dei lavoratori ai processi produttivi diminuisce significativamente o scompare del tutto. Tutti i processi produttivi diventano completamente automatizzati e l'intervento umano si fa superfluo in ogni fase della creazione del prodotto.

Nonostante il diffuso timore causato dalla crescente automazione dei processi industriali, l'introduzione di questo tipo di tecnologia può portare benefici a vari livelli legati ai processi produttivi - anche quando il lavoro è rischioso per la vita e la salute umana.

Discussione - Il lavoro dei robot dovrebbe essere tassato?

Con la diminuzione dei costi di automazione dei processi produttivi, la scala della robotizzazione industriale sta aumentando. Le conseguenze previste comprendono sia aspetti positivi, come la crescita economica o l'aumento della produttività, sia aspetti negativi, come la riduzione dell'occupazione in vari comparti del settore manifatturiero.

La trasformazione dei modelli di business tradizionali sta suscitando molte polemiche e ci sono nuove sfide per i legislatori in quei paesi in cui l'automazione si è già sviluppata a un ritmo sorprendente.

Con la significativa riduzione del costo del lavoro e dei profitti causata dall'uso dei robot nell'industria, la **questione delle tasse imposte sul lavoro robotizzato** è diventata una delle questioni difficili da risolvere. Tuttavia, quando si tratta di acquistare nuovi macchinari e attrezzature, i singoli governi stanno utilizzando incentivi fiscali per incoraggiare la trasformazione digitale e la modernizzazione del settore industriale.
In Polonia, ad esempio, a partire dal 2022, gli imprenditori potranno detrarre fino al 150% del costo di acquisto di macchinari e attrezzature funzionalmente correlati per la sicurezza sul lavoro nelle postazioni in cui si verifica l'interazione uomo-robot.

Conseguenze positive e negative della robotizzazione

1. **Economia**

   a) **Positive:**

      i) Capacità di migliorare i prodotti e di immetterli sul mercato più rapidamente.

      ii) Sviluppo più rapido di nuove tecnologie.

      iii) Miglioramento della competitività delle aziende.

   b) **Negative:**

      i) Aumento della disoccupazione - secondo le stime degli autori del rapporto 2023 *Future of Jobs* (World Economic Forum), nel prossimo futuro le macchine svolgeranno una percentuale maggiore di compiti rispetto agli esseri umani. Se nel 2018, in media, il 71% del tempo di lavoro consisteva in compiti che coinvolgevano il fattore umano, questa proporzione è destinata a cambiare significativamente nel

2025. Gli esseri umani saranno responsabili di circa il 48% delle attività, mentre il restante 52% sarà completamente automatizzato.

ii) Aumento del consumo di energia e contributo all'aumento dell'inquinamento ambientale.

2. Datore di lavoro

a) Positive:

i) Riduzione dei costi di produzione.

ii) Riduzione del rischio di errori.

iii) Capacità di registrare meglio le prestazioni.

iv) Individuazione più rapida dei colli di bottiglia, che facilita l'ottimizzazione del lavoro.

v) In alcuni paesi (ad esempio la Polonia) - è possibile detrarre i costi di acquisto di robot industriali con uno scopo specifico.

b) Negative:

i) Elevati costi iniziali di installazione delle apparecchiature.

ii) *N*ecessità di inventario ed elevato costo di riparazione.

iii) Se i processi sono altamente automatizzati, i guasti alle apparecchiature causano interruzioni della produzione.

iv) Ridotta flessibilità di risposta a problemi o errori imprevisti rispetto alla risposta dei dipendenti.

v) Necessità di rispettare le normative più esigenti.

vi) Alti costi di consumo energetico.

3. Dipendente

a) Positive:

i) Semplificazione del processo produttivo.

ii) Supporto nelle attività più difficili o ripetitive.

iii) Maggiore efficienza produttiva con un minore coinvolgimento dei dipendenti.

iv) Possibilità di dedicare tempo ad altre attività di sviluppo grazie alla cessione di quelle ripetitive a strumenti automatizzati.

v) L'emergere di nuovi posti di lavoro legati alla creazione, al funzionamento o alla riparazione di macchinari.

b) Negative:

i) Potenziale perdita di posti di lavoro dovuta all'automazione del processo

ii) Maggiore probabilità di burnout lavorativo innescato dalla paura di perdere il lavoro

iii) Se i macchinari si rompono o non sono utilizzati correttamente - esposizione al deterioramento delle condizioni di salute/di pericolo di vita.

1.3 Come evitare un controllo sul luogo di lavoro sproporzionato ed eccessivo

La supervisione sul posto di lavoro - opportunità e rischi

Le aziende del settore tecnologico sono desiderose di rispondere alla crescente domanda da parte dei datori di lavoro in termini di nuove tecnologie. Al contrario, il trend riscontrabile negli strumenti di IA sta creando opportunità per mettere i dipendenti sotto pieno controllo, indipendentemente dalla loro conoscenza o dal loro consenso. Esiste anche una forte tendenza ad accettare il nuovo stato di cose come una conseguenza "naturale" dello sviluppo delle aziende.

Opportunità:

- Il monitoraggio utilizzato in situazioni di pericolo e in caso di incidente sul lavoro può andare a vantaggio del dipendente (ad esempio, quando è necessario dimostrare che il luogo di lavoro non era sufficientemente sicuro)
- in alcuni settori il monitoraggio è necessario per garantire la conformità (ad esempio, nel settore bancario può essere utilizzato per prevenire l'*insider trading*)
- *l*a sorveglianza utilizzata durante la formazione dei dipendenti può accelerare i processi di inserimento (ad esempio, nel settore edile, i *wearable* sono caschi intelligenti con sensori di vibrazione che avvertono i lavoratori della presenza di oggetti potenzialmente pericolosi nell'ambiente).

Esempio di Stellate

Stellate, una start-up di analisi dei dati con sede a San Francisco, ha un team di dipendenti sparsi in tutto il mondo. Oltre agli strumenti utilizzati per collaborare in remoto, l'azienda controlla lo sviluppo dei propri dipendenti attraverso programmi di formazione e mentoring. Piuttosto che sanzioni per prestazioni inadeguate o altri comportamenti scorretti, l'obiettivo

principale di queste iniziative è promuovere tra i dipendenti dell'azienda strumenti per migliorare l'efficienza del loro lavoro.

Minacce:

- l'uso eccessivo o scorretto delle tecnologie digitali può portare a violazioni della privacy e dei diritti di tutela dei dati dei dipendenti,
- rischi per la salute mentale e fisica dei lavoratori a causa dello stress dovuto all'eccessiva supervisione e agli standard di lavoro imposti,
- forme associative di dipendenti ostacolate- il monitoraggio dei dipendenti e l'identificazione del sentimento aziendale consentono di cogliere i movimenti a favore dell'associazione (ad esempio, nei grandi luoghi di lavoro, accade che i dati dei dipendenti vengano utilizzati per identificare gli atteggiamenti dei dipendenti nei confronti del datore di lavoro e determinare dove è più probabile che i dipendenti si oppongano alle politiche aziendali).

Principi fondamentali del monitoraggio del luogo di lavoro

È riconosciuto che i datori di lavoro devono essere in grado di sorvegliare i luoghi di lavoro e di valutare le prestazioni dei propri dipendenti per garantire una migliore gestione dell'azienda e per proteggere i segreti aziendali, imporre il rispetto della legge e prevenire la criminalità dei dipendenti. Allo stesso tempo, l'Unione europea e i singoli Stati membri attribuiscono grande importanza alla privacy dei dipendenti e al rispetto della loro vita privata.

Il monitoraggio del luogo di lavoro è legale, ma...[2]

- le finalità del trattamento delle informazioni (ad esempio, per garantire la sicurezza dei dipendenti) devono essere esplicitate in dettaglio prima di utilizzare la videosorveglianza,
- il datore di lavoro deve informare le persone potenzialmente soggette a monitoraggio che il monitoraggio è in atto e quale area è coperta.

[2] Norme sul monitoraggio dei luoghi di lavoro previste dal diritto comunitario (articolo 8 della Convenzione europea dei diritti dell'uomo, regolamento GDPR), decisioni di tribunali e corti, codici del lavoro dei singoli Stati membri.

Inoltre è importante che gli obiettivi, la portata e il metodo di applicazione del monitoraggio siano stabiliti in un contratto collettivo o in un regolamento di lavoro, ad esempio nell'ambito della contrattazione collettiva. Nelle situazioni in cui il datore di lavoro non è coperto da un contratto collettivo o non è obbligato a stabilire un regolamento di lavoro, le regole vanno sancite in un avviso.

La videosorveglianza occulta è consentita solo in misura limitata quando vi è il ragionevole sospetto che sia stato commesso un grave illecito o un reato penale che abbia causato un danno significativo al datore di lavoro.

Inoltre, il datore di lavoro può utilizzare altri tipi di monitoraggio. Ad esempio:

- GPS montato su un'auto aziendale,
- monitoraggio di Internet e della messaggistica istantanea utilizzata sulle apparecchiature aziendali,
- geolocalizzazione di un telefono cellulare o di un computer portatile aziendale.

Le disposizioni sulla videosorveglianza si applicano *mutatis mutandis* a tutte le forme di monitoraggio (ad esempio, un datore di lavoro può monitorare la posta elettronica di un dipendente solo dopo averne dato notifica preventiva al dipendente stesso).

Monitoraggio sul lavoro e legge - esempi dai paesi partner

Polonia

Secondo il Codice del lavoro polacco, il monitoraggio è una forma specificia di sorveglianza dei locali di un luogo di lavoro o dell'area circostante un luogo di lavoro, sotto forma di mezzi tecnici che consentono la registrazione di immagini.

Il monitoraggio in Polonia è consentito se è necessario per:

- garantire la sicurezza dei lavoratori,
- proteggere la proprietà o esercitare controllo sulla produzione,
- mantenere riservate le informazioni la cui divulgazione potrebbe esporre il datore di lavoro a danni
- il monitoraggio della posta elettronica (articolo 223 del Codice del lavoro) è consentito nella misura in cui questo si rende necessario per garantire un'organizzazione del lavoro che consenta il pieno utilizzo dell'orario di lavoro e il corretto uso degli strumenti di lavoro forniti al dipendente; il monitoraggio della posta elettronica non deve violare la segretezza della corrispondenza e altri diritti personali del dipendente.

Le registrazioni video possono essere utilizzate dal datore di lavoro solo allo scopo per cui sono state raccolte e conservate, per un periodo non superiore a tre mesi dalla data di registrazione.

Come condurre il monitoraggio in modo lecito? Procedura in sei fasi

Per condurre un monitoraggio legittimo, il datore di lavoro deve valutare l'impatto che le sue azioni possono avere sui dipendenti. Le fasi seguenti indicano su quali domande dovrebbe basarsi tale analisi.

Passi	Domanda	Azione
Fase 1	Se il monitoraggio è già stato introdotto, in cosa consiste in questo preciso momento?	Condurre un audit per determinare quali tipi di monitoraggio sono utilizzati sul posto di lavoro e chi, all'interno dell'organizzazione, ha l'autorità di monitorare i dipendenti.
Fase 2	Perché si fa o si dovrebbe fare monitoraggio?	• Comprendere lo scopo del monitoraggio dei dipendenti. • Definire precisamente la funzione del monitoraggio (i dati raccolti da un monitoraggio specifico possono essere utilizzati solo allo scopo per cui sono stati raccolti). **Eccezione**: se, nel corso del monitoraggio, un'organizzazione viene in possesso di informazioni su attività che non possono essere ignorate (ad esempio, potenziali attività criminali, bullismo), i dati raccolti possono essere utilizzati stabilire le responsabilità.
Fase 3	È possibile raggiungere questo obiettivo senza monitoraggio?	• Una volta individuato il motivo dell'introduzione del monitoraggio, è importante stabilire se lo stesso obiettivo può essere raggiunto senza il monitoraggio dei dipendenti. **Esempio:** l'introduzione del monitoraggio dei siti visitati dai dipendenti può essere sostituita dal blocco dei siti inappropriati o dalla possibilità per i dipendenti di caricare file solo da account specifici ed entro una certa dimensione.

Fase 4	Se un determinato obiettivo non può essere raggiunto senza monitoraggio, esiste un mezzo di controllo meno invasivo di quello attualmente in esame?	**Ad esempio,** il controllo che i dipendenti non violino la politica di riservatezza dell'azienda può essere effettuato sia controllando il contenuto delle e-mail inviate dai dipendenti, sia attraverso un monitoraggio automatico, come il controllo degli indirizzi e degli oggetti delle e-mail o il blocco delle e-mail con allegati di una certa dimensione.
Fase 5	Che effetto avrà il monitoraggio sui dipendenti?	• È necessario rispondere alle seguenti domande: ◦ Il monitoraggio può essere considerato svalutante o ingiusto? ◦ Il monitoraggio influirà sulla fiducia reciproca tra datore di lavoro e dipendenti? ◦ Le informazioni riservate o sensibili possono essere condivise con persone che non hanno necessità di conoscerle? **Esempio:** al team contabile può essere comunicato che una persona è stata assente dal lavoro per malattia (per consentire il pagamento dell'indennità di malattia), ma solo il responsabile delle risorse umane deve conoscere i motivi medici dell'assenza.
Fase 6	L'introduzione del monitoraggio è giustificata?	• Decidere se l'introduzione del monitoraggio è giustificata (un monitoraggio meno intrusivo è più facile da giustificare, di cui i dipendenti sono informati). • Il personale può essere consultato prima dell'introduzione del monitoraggio, sviluppare congiuntamente una logica per il monitoraggio

Supervisione dei dipendenti e lavoro a distanza

La sorveglianza dei lavoratori dipendenti può avvenire tramite l'installazione di applicazioni di controllo sui computer dei dipendenti, che spesso non vengono comunicate ai dipendenti stessi.

Il cosiddetto *bossware*[3] può registrare i tasti premuti, fare screenshot e persino attivare le webcam dei dipendenti che lavorano in remoto.

Vale la pena notare che il timore costante di essere osservati da un datore di lavoro può portare a un deterioramento dello stato mentale dei dipendenti. Secondo le ricerche, ben il 56% degli intervistati si sente stressato e ansioso per il fatto che il proprio datore di lavoro controlli le sue comunicazioni elettroniche, il 41% si chiede costantemente se sia osservato e il 32% è meno propenso a fare pause sul lavoro per questo motivo.

Come controllare efficacemente il lavoro senza compromettere il benessere dei dipendenti?

Suggerimenti per il datore di lavoro:

- informare il dipendente sugli strumenti di sorveglianza utilizzati,
- chiarire le regole sull'uso del monitoraggio e stabilirne i limiti (ad esempio sul tipo di dati trattati),
- invece di un'eccessiva supervisione e di un approfondimento delle attività quotidiane del dipendente, introdurre un sistema di responsabilità per i risultati (ad esempio, revisione e valutazione settimanale dei compiti),
- utilizzare applicazioni per monitorare e gestire i flussi di lavoro (ad esempio Connecteam) e migliorare la comunicazione inter-team a distanza e la pianificazione congiunta.

1.4 Differenza tra lavoro a distanza e telelavoro - effetto sulle relazioni di lavoro

Secondo una ricerca della Commissione europea, nell'anno precedente allo scoppio della pandemia COVID-19, solo il 5,4% degli occupati nell'UE-27 lavorava da casa, una percentuale che non è cambiata dal 2009. A seguito della pandemia, questa percentuale è più che raddoppiata, raggiungendo il 12,3%. In alcuni Stati membri, questa cifra ha superato fino a un quarto degli occupati, indipendentemente dall'industria o dal settore economico.

Nonostante le iniziali difficoltà di adattamento alla nuova realtà (causate soprattutto dalla mancanza di infrastrutture TIC adeguate o di formazione alla digitalizzazione dei processi lavorativi), i dipendenti oggi non riescono a immaginare un ritorno al al modo in cui lavoravano

[3] Il nome deriva dalle parole inglesi *boss e software e significa* software per il datore di lavoro.

prima della pandemia. Apprezzano la maggiore flessibilità sul lavoro, l'opportunità di trascorrere del tempo con le proprie famiglie e l'aumento dell'efficienza lavorativa.

Tuttavia, nonostante la popolarità del lavoro ibrido, sono ancora molti i datori di lavoro e i dipendenti che scelgono di tornare in ufficio, motivando questa decisione con il miglioramento dei rapporti di lavoro e della collaborazione, nonché con la possibilità di creare un ambiente favorevole all'innovazione collettiva e a una migliore produttività, separando nettamente la vita privata da quella professionale.

Lavoro a distanza - concetti di base

La crescente popolarità del lavoro con gli strumenti digitali e la moltitudine di possibilità che essi offrono ha reso necessario l'uso di una serie di nuovi termini. Per facilitare l'orientamento nel labirinto delle definizioni, è stata creata una tabella che mostra le differenze tra le varie modalità di lavoro.

Tipo di lavoro che utilizza strumenti digitali	Definizione
Lavoro a distanza	Per lavoro a distanza si intende qualsiasi attività svolta fuori dalla sede del datore di lavoro, indipendentemente dalla tecnologia utilizzata. Secondo gli emendamenti al Codice del Lavoro polacco si tratta di: lavoro svolto interamente o parzialmente in un luogo indicato dal lavoratore e concordato con il datore di lavoro di volta in volta
Telelavoro	Il telelavoro è qualsiasi forma di organizzazione e/o esecuzione del lavoro che utilizza le tecnologie dell'informazione, nel contesto di un contratto/rapporto di lavoro in cui il lavoro, che può anche essere svolto nei locali del datore di lavoro, viene regolarmente svolto fuori da tali locali.
Telelavoro a tempo parziale	Questa modalità di lavoro combina giorni di lavoro a distanza con giorni in ufficio ed è stata messa in pratica per la prima volta da Jack Nilles all'inizio degli anni '70 negli Stati Uniti.

Telelavoro e lavoro mobile basati sulle TIC (TICTM)	Il termine TICTM si riferisce all'uso di tecnologie dell'informazione e della comunicazione come smartphone, tablet, computer portatili e desktop per lavorare fuori dalla sede del datore di lavoro. Copre tutte le forme di telelavoro, ma cerca di distinguere tra il lavoro da casa o da una postazione fissa (telelavoro) e il lavoro mobile basato sulle TIC. Quest'ultimo termine è utilizzato in Germania per distinguere il telelavoro svolto a casa da una forma di lavoro più mobile.
Smart working/lavoro agile	Lo smart working si riferisce a un sistema di lavoro flessibile che consente ai dipendenti di lavorare in modo comodo ed efficiente senza vincoli di tempo e di spazio (sempre e ovunque) utilizzando le TIC in rete. Un termine simile ("lavoro agile") viene utilizzato in Italia.
Condizioni di lavoro flessibili	Gli accordi di lavoro flessibile sono opzioni di lavoro alternative che consentono di svolgere il lavoro al di fuori dei tradizionali confini temporali e/o spaziali della giornata lavorativa standard.
Lavoro virtuale	Il lavoro virtuale è un lavoro retribuito o non retribuito che viene svolto utilizzando una combinazione di tecnologie digitali e di telecomunicazioni o che produce contenuti per i media digitali
Lavoro ibrido	Si tratta di un accordo in cui il lavoro può essere svolto in parte presso la sede del datore di lavoro e in parte a casa o in altri luoghi.

Lavoro a distanza e telelavoro: cosa dice la legge?

Regolamenti a livello UE

Al momento manca una legislazione vincolante sul telelavoro, anche se diverse direttive e regolamenti affrontano questioni volte a garantire buone condizioni di lavoro per i telelavoratori. Esiste tuttavia l'*Accordo quadro europeo sul telelavoro* (2002). Questo documento è un accordo

autonomo tra le parti sociali europee (CES, UNICE, UEAPME e CEEP) e obbliga le organizzazioni nazionali affiliate ad attuarlo secondo le "procedure e le pratiche" specifiche di ogni Stato membro.

Lavoro a distanza/ telelavoro e legge - l'esempio della Polonia

La legge del 1° dicembre 2022 che modifica la legge sul codice del lavoro e alcuni altri atti ha introdotto il concetto di lavoro a distanza nel diritto del lavoro polacco, abrogando le disposizioni sul telelavoro. Secondo questa modifica, il lavoro a distanza **è un lavoro svolto in tutto o in parte in un luogo indicato dal dipendente e in ogni caso concordato con il datore di lavoro,** compreso l'indirizzo di casa del dipendente, tra l'altro utilizzando mezzi di comunicazione diretta a distanza.

Il telelavoro, invece, è una qualsiasi forma di organizzazione e/o esecuzione del lavoro con l'ausilio di tecnologie informatiche, nel contesto di un contratto/rapporto di lavoro, in cui il lavoro **che potrebbe essere svolto anche presso i locali del datore di lavoro viene regolarmente svolto fuori da tali locali**. Mentre il lavoro a distanza può essere temporaneo, il telelavoro si basa in linea di principio sullo svolgimento permanente delle mansioni da casa.

Le regole per il lavoro a distanza devono essere stabilite con l'accordo dei sindacati nel regolamento di lavoro o in un accordo individuale con il dipendente. Inoltre, il datore di lavoro non può rifiutare il lavoro a distanza ai genitori che allevano un bambino di età inferiore ai quattro anni, ai genitori o agli assistenti di persone con disabilità o alle donne in gravidanza (a meno che la natura delle mansioni svolte non lo consenta). Il datore di lavoro deve inoltre dotare il lavoratore delle attrezzature e degli strumenti necessari per svolgere il lavoro a distanza compensare, tra l'altro, i costi dell'elettricità o del consumo di Internet.

Il lavoro a distanza può essere effettuato su richiesta del dipendente o per ordine del datore di lavoro. Il datore di lavoro può anche ordinare il lavoro a distanza in caso di stato di emergenza, stato di minaccia epidemica o epidemia conclamata e per cause di forza maggiore, come la distruzione del luogo di lavoro a causa di incendi o inondazioni.

La riforma del Codice del Lavoro include anche una proposta per il cosiddetto lavoro a distanza occasionale, in base alla quale, su richiesta del dipendente, questi potrà svolgere lavoro a distanza per un periodo fino a 24 giorni per anno solare. La richiesta di lavoro a distanza occasionale da parte del lavoratore non è tuttavia vincolante e il datore di lavoro può rifiutarsi di accoglierla.

È importante notare che al datore di lavoro è vietato discriminare un dipendente per lo svolgimento di un lavoro a distanza, così come per il rifiuto di svolgere tale lavoro. Inoltre, il datore di lavoro è tenuto a consentire al dipendente che svolge lavoro a distanza di trovarsi nei locali del luogo di lavoro, di comunicare con gli altri dipendenti e di utilizzare i locali e le strutture del datore di lavoro, le strutture sociali dell'azienda e le attività sociali - alle stesse condizioni degli altri dipendenti.

1.5 Algoritmi e discriminazione sul posto di lavoro

In un mondo guidato dalle informazioni, sentiamo sempre più spesso parlare di *intelligenza artificiale* (IA), le cui applicazioni si trovano praticamente ovunque. Si può prevedere che sarà sempre più utilizzata anche in ambito lavorativo. Secondo uno studio di Forbes, circa quattro aziende su cinque considerano l'IA una priorità assoluta nella loro strategia aziendale. Tuttavia, le speranze di ottimizzazione dei costi e di maggiore efficienza nella produzione sono accompagnate dal timore dei dipendenti di perdere il posto di lavoro: secondo il rapporto Future of Jobs Forecast di Forrester, il numero di posti di lavoro persi per l'automazione raggiungerà 12 milioni solo in Europa entro il 2040.

Nonostante questa nuova tecnologia accenda gli animi, nel dibattito pubblico manca ancora una solida spiegazione di come funziona l'intelligenza artificiale e se qualsiasi tipo di automazione possa essere sicuramente classificata come IA. Per una piena comprensione del problema, è necessario anche considerare qual è la differenza tra un sistema di intelligenza artificiale e gli algoritmi, dato che questi termini sono spesso usati in modo intercambiabile.

AI è un termine estremamente ampio che comprende un gruppo di algoritmi in grado di modificare i propri parametri e creare nuovi algoritmi in risposta agli input appresi. Questa capacità di cambiare, adattarsi e crescere sulla base di nuovi dati è ciò che viene definito "intelligenza".

In termini più semplici, l'intelligenza artificiale può quindi essere definita come la **capacità delle macchine di comprendere, apprendere, pianificare e dimostrare creatività. Secondo la** definizione proposta dalla proposta di Regolamento sull'Intelligenza Artificiale (AI Act), invece, per sistema di intelligenza artificiale si intende un software sviluppato utilizzando una o più delle tecniche e degli approcci elencati nel regolamento[4] , in grado - per un determinato insieme di

[4] Tecniche e approcci di intelligenza artificiale elencati nella normativa:

(a) meccanismi di apprendimento automatico, tra cui l'apprendimento supervisionato, l'apprendimento automatico non supervisionato e l'apprendimento per rinforzo, utilizzando un'ampia gamma di metodi, tra cui l'apprendimento profondo;

(b) metodi logici e basati sulla conoscenza, tra cui la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenza, i motori di inferenza e deduzione, il ragionamento (simbolico) e i sistemi esperti;

(c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

scopi definiti dall'uomo - di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce.

Un algoritmo è un insieme di istruzioni, o più precisamente una formula computazionale, che prende autonomamente decisioni basate su modelli statistici o regole decisionali senza un esplicito intervento umano. Rappresenta una sequenza di istruzioni che indicano al computer cosa fare all'interno di un insieme di passi e regole precisamente definiti per eseguire un compito. Si tratta quindi di un corso d'azione predeterminato, rigido e codificato che si attiva quando si incontra un elemento specifico.

Un tema legato al campo dell'intelligenza artificiale è l'*autoapprendimento* (*machine learning*, ML). Il suo obiettivo principale è quello di creare un sistema operativo automatico che sia in grado di migliorarsi sulla base dell'esperienza sotto forma di dati e di acquisire nuove conoscenze su questa base. Il processo si basa sulla ricerca di uno schema nei dati forniti per rispondere a una domanda su un insieme sconosciuto. Si tratta quindi di una sorta di previsione del futuro che utilizza la probabilità e la statistica.

Non tutta l'intelligenza artificiale presenta capacità di autoapprendimento. Infatti, a volte un algoritmo può essere scritto in modo tale che il programma in cui è incorporato esegua i comandi senza apprendere da nuovi dati (come nel caso del ML).

Un esempio di algoritmo già correttamente programmato è quello del famoso supercomputer IBM Deep Blue. Questa macchina è diventata famosa dopo essere riuscita a vincere a scacchi contro il campione Garry Kasparov, 25 anni fa. Questo perché Deep Blue aveva memorizzato tutte le mosse possibili, a seconda del posizionamento dei pezzi sulla scacchiera e della strategia dell'avversario. Grazie a questo e alla sua elevata potenza di calcolo, poteva agire efficacemente in qualsiasi situazione.

L'opposto dell'algoritmo implementato in Deep Blue di IBM è stato il programma AlphaGo di DeepMind. Utilizzando meccanismi di autoapprendimento, questo sistema ha imparato a giocare a GO (un antico gioco da tavolo cinese in cui l'obiettivo è circondare il maggior numero possibile di territori con le proprie pietre su una scacchiera inizialmente vuota) e ha persino battuto un giocatore considerato il migliore al mondo.

L'intelligenza artificiale generale, invece, è un sistema autocosciente e dotato di conoscenze o capacità cognitive complete, in grado di pensare ed eseguire compiti in modo autonomo. La creazione dell'originalità tecnologica è stata per anni oggetto di molte controversie, ci si è soprattutto chiesto innanzitutto se sia possibile. Secondo uno dei principali critici dell'ascesa dell'intelligenza artificiale generale, il filosofo Hubert Dreyfus, i computer che non hanno un corpo, non attraversano l'infanzia e l'adolescenza e non partecipano a esperienze culturali, non possono assolutamente acquisire un'intelligenza in senso umano. Una delle argomentazioni

principali di Dreyfus era che lo sviluppo dell'intelligenza umana avviene in parte in modo inconscio e quindi non può essere articolato e incorporato in un programma informatico.

Algoritmi al lavoro

1. **Analisi del CV del candidato mediante un algoritmo prima dell'instaurazione del rapporto di lavoro**

L'assunzione algoritmica prevede l'utilizzo di sistemi di intelligenza artificiale e di *machine learning* per individuare i candidati, reclutare, fare colloqui e assumere per coprire dei posti di lavoro. Questa tecnica utilizza una serie di criteri per valutare un candidato, tra cui l'esperienza e la formazione, e spesso filtra i CV ricevuti utilizzando parole chiave. Gli algoritmi possono anche aiutare a valutare le competenze più *soft*, come la propensione del candidato ad apprendere rapidamente e a lavorare in team.

Utilizzando diversi strumenti di intelligenza artificiale durante il reclutamento, le aziende vogliono garantire che il processo sia condotto in modo equo. Questo perché, in teoria, non c'è spazio per il fattore umano e per eventuali discriminazioni nella prima valutazione automatizzata. Tuttavia, questi sistemi sono spesso criticati perché riflettono i pregiudizi delle persone che li hanno programmati.

È importante notare che gli algoritmi non prendono la decisione finale di assunzione. Il loro scopo principale è quello di restringere il campo dei candidati.

Metodi di analisi dei CV per algoritmo:

- **Punteggio del CV** - un algoritmo assegna punti in base a criteri predeterminati dal selezionatore,
- **Ranking** - ordinamento dei CV in base alla presenza di parole chiave,
- **Corrispondenza** - identificare le parole chiave che corrispondono a quelle dell'annuncio di lavoro,
- **Analisi** - l'algoritmo analizza la semantica del CV, estrae le informazioni principali e le suddivide in diverse categorie: esperienza, competenze, contatti.

2. **Caratteristiche e aree di utilizzo degli algoritmi sul posto di lavoro**

Tipi di algoritmi:

- **Descrittivi** - utilizzati per registrare eventi passati e analizzarne l'impatto sugli eventi presenti, come ad esempio gli algoritmi di valutazione delle prestazioni progettati per

raccogliere vari tipi di dati relativi alle prestazioni dei dipendenti e indicare una valutazione complessiva.

- **Predittivi** - mirano a prevedere il comportamento futuro o a stimare la probabilità che un evento si verifichi (ad esempio, prevedere un aumento della domanda di nuovi dipendenti).
- **Prescrittivo/raccomandativo**: il loro compito è selezionare lo scenario migliore tra varie possibilità e raccomandare un'azione specifica o semplicemente attuarla (ad esempio, decidere le risorse umane, l'assegnazione dei compiti o il calendario).

L'uso degli algoritmi nel mondo del lavoro comporta la cosiddetta **gestione algoritmica,** ovvero "un sistema di controllo in cui agli algoritmi viene affidata la responsabilità di prendere ed eseguire decisioni di prendere ed eseguire decisioni che riguardano il lavoro, riducendo così la partecipazione umana e la supervisione del processo di lavoro".

Sei funzioni chiave di gestione del flusso di lavoro per le quali sono stati utilizzati algoritmi:

1. monitoraggio/controllo dei dipendenti
2. definizione degli obiettivi
3. gestione delle prestazioni
4. programmazione

5 retribuzione

6. cessazione del rapporto di lavoro

Aumentare il controllo del datore di lavoro sui dipendenti con gli algoritmi

- **Raccomandazione algoritmica** - i datori di lavoro utilizzano algoritmi per valutare una determinata situazione e dare suggerimenti per far sì che il dipendente compia l'azione indicata dall'algoritmo.
- **Restrizione algoritmica** - l'uso di algoritmi per visualizzare solo determinate informazioni e consentire determinati comportamenti impedendone altri.

L'uso di algoritmi può aumentare la frustrazione dei dipendenti che, dovendo attenersi a raccomandazioni incomprensibili, possono sentire sminuita la loro voce in capitolo.

Algoritmi utilizzati per valutare il lavoro

- Registrazione **algoritmica** - l'uso di procedure computazionali per monitorare, aggregare e riportare, spesso in tempo reale, un'ampia gamma di dati selezionati con precisione da fonti interne ed esterne.
- **Tecnologie computazionali** - utilizzate per raccogliere valutazioni e classifiche per calcolare una qualche misura delle prestazioni dei dipendenti; anche analisi predittive per prevedere le loro prestazioni future.

La valutazione del lavoro tramite algoritmi può sollevare problemi specifici, non solo legati alla discriminazione, ma anche alla perdita del senso di privacy dei dipendenti, alla sicurezza delle informazioni, ecc.

Algoritmi utilizzati per la remunerazione

La remunerazione algoritmica può fornire premi in tempo reale per i comportamenti che seguono linee guida predefinite. Può anche utilizzare i principi della *gamification* per rendere l'esperienza lavorativa più positiva e divertente per i dipendenti.

Disciplina sul posto di lavoro

La sostituzione algoritmica consiste nel licenziamento rapido o addirittura automatico di dipendenti con scarse prestazioni dall'organizzazione e nella loro sostituzione con dipendenti più efficienti.

Processo decisionale automatizzato e profilazione

L'articolo 22 del GDPR stabilisce che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici o incida in modo analogo significativamente sulla persona.
Il diritto di una persona di contestare una decisione automatizzata riguardante la sua persona si basa sui due motivi della profilazione qualificata: il trattamento automatizzato e gli effetti giuridici o i fattori che incidono significativamente sulla persona.

Che cos'è il processo decisionale automatizzato?

Grazie alla conoscenza codificata e all'analisi precisa delle condizioni ambientali, un computer può impartire istruzioni senza l'intervento dell'uomo. Questa azione si basa su calcoli avanzati e su mezzi di elaborazione esclusivamente tecnici. In questo modo, il coinvolgimento umano nei processi decisionali è ridotto al minimo e i risultati vengono forniti in modo automatizzato.

Tuttavia, affinché il trattamento dei dati sia considerato completamente automatizzato, non deve esserci alcun intervento umano nel processo decisionale. Va notato che un apparente

coinvolgimento umano nel processo decisionale, consistente, ad esempio, nella mera approvazione di un verdetto indicato da un algoritmo, non costituirà un motivo di esclusione dall'ambito di applicazione del divieto di cui all'articolo 22 del GDPR. Tuttavia, se una persona, con il potere e l'autorità di cambiare il verdetto, agisse per modificare il verdetto, il processo decisionale automatizzato non avrebbe luogo.

Per quanto riguarda il catalogo delle situazioni coperte dall'articolo 22 del GDPR, questo è ampio e copre sia le situazioni in cui la decisione produce effetti giuridici (cioè incide sui diritti di un individuo ai sensi della legge; ad esempio, il diritto all'indennità di disoccupazione) sia quelle che hanno un "effetto altrettanto significativo" (ad esempio, relativo alla situazione finanziaria o alla salute del soggetto).

Che cos'è il profiling?

L'articolo 22 del GDPR comprende anche una categoria specifica di processo decisionale automatizzato, ossia quello basato sulla profilazione. Il termine "profilazione" (articolo 4 del GDPR) si riferisce a qualsiasi forma di trattamento automatizzato di dati personali che preveda l'uso di dati personali per valutare determinati fattori personali di una persona fisica. In particolare, si tratta dell'analisi o della previsione di aspetti relativi al **rendimento lavorativo**, alla situazione economica, alla salute, alle preferenze personali, agli interessi, all'affidabilità, al comportamento, all'ubicazione o agli spostamenti **di tale persona**[5] .

Esempi pratici di profilazione:

- **marketing** - creazione di profili di consumatori raccogliendo informazioni sulle preferenze di acquisto e facendo in modo che il sistema suggerisca prodotti personalizzati per il cliente,
- **prestiti e crediti** - profilando i candidati e prendendo una decisione di credito positiva subordinata all'analisi dei dati personali forniti all'algoritmo,
- **prestazioni di assistenza sociale** - utilizzo del profiling per allocare in modo equo le risorse dell'assistenza pubblica,
- **reclutamento e risorse umane** - i processi di reclutamento di massa sono spesso condotti utilizzando sistemi che analizzano i CV e altri dati dei candidati in modo indipendente e, sulla base di tale analisi, decidono se rifiutare o accettare il candidato (ad esempio, dopo

[5] Va notato che, nonostante le somiglianze, la profilazione e il processo decisionale automatizzato sono due attività diverse che possono essere o meno collegate.

aver cercato i CV per parole chiave). Nel campo delle risorse umane, la profilazione viene utilizzata anche per la valutazione delle offerte di lavoro.

Rischi associati alla profilazione

- **Ingerenza nella privacy e mancanza di trasparenza** - mentre molte persone sono consapevoli che alcuni tipi di dati (ad esempio quelli medici) sono particolarmente sensibili e dovrebbero essere protetti, una parte del pubblico non è consapevole di quante informazioni personali possano essere ricavate dai dati comportamentali utilizzati per una profilazione indesiderata. Inoltre, lo stesso processo di profilazione può essere spesso non trasparente e incomprensibile per le persone interessate.
- **Discriminazione** - gli algoritmi progettati dall'uomo possono portare con sé i pregiudizi dei loro creatori. Pertanto, il sistema potrebbe trattare in modo meno favorevole, ad esempio, persone con opinioni religiose, orientamento sessuale o colore della pelle diversi.
- **Riduzione della diversità** - la profilazione è progettata per valutare, caratterizzare e segmentare il pubblico di un determinato contenuto, al fine di adattare il materiale in base agli interessi o alle convinzioni (ad esempio, politiche) degli individui interessati. In questo modo, semplifica il catalogo delle informazioni fornite all'utente, limitando la diversità dei contenuti e creando le cosiddette bolle informative, restringendo l'orizzonte virtuale del destinatario.

Profilazione nel processo di lavoro - un *case study*

Dal 2020 il Centro per l'impiego austriaco (AMS) utilizza una profilazione algoritmica delle persone in cerca di lavoro per aumentare l'efficienza del processo di consulenza e adeguare i programmi attuali alle esigenze del mercato del lavoro. Il sistema mira a classificare le persone in cerca di lavoro in tre categorie:

- Gruppo A. Buone prospettive di trovare lavoro nel prossimo periodo.
- Gruppo B. Prospettive medie.
- Gruppo C. Basse prospettive a lungo termine.

Poi, a seconda della categoria assegnata, un algoritmo adatta il programma di assistenza alle esigenze del singolo.

Domanda di discussione: La profilazione algoritmica dei disoccupati per adattare i programmi di sostegno alle loro esigenze è giustificata?

Un esempio: a New York è stata annunciata una legge che limita l'uso di strumenti di intelligenza artificiale nei processi di assunzione. Come indicato, il problema principale che si verificava con le valutazioni realizzate dall'intelligenza artificiale era l'esclusione dal processo di gruppi che non rientravano nella chiave pre-programmata. Ad esempio, la squalifica delle persone con un difetto di pronuncia durante un colloquio video valutato dal computer, o il rifiuto di candidati con artrite o altre condizioni che limitano la loro idoneità fisica (per i test a tempo).

Domanda di discussione: Dovrebbero essere vietati tutti i tipi di valutazione algoritmica nel processo di assunzione?

Un esempio: un imprenditore stava lavorando allo sviluppo e all'implementazione di uno strumento di intelligenza artificiale nella sua azienda per aiutare ad assumere persone adatte al lavoro. Il lavoro è stato interrotto quando l'azienda si è resa conto che il sistema discriminava le donne. Il motivo del rifiuto più frequente dei profili femminili era che l'intelligenza artificiale si basava sui dati dei CV delle persone che avevano lavorato per l'azienda negli ultimi 10 anni (per lo più uomini). Di conseguenza, il computer ha valutato che avrebbe dovuto dare priorità agli uomini, riducendo automaticamente le possibilità di candidature con caratteristiche femminili.

Domanda di discussione: Potete identificare altri esempi di discriminazione che potrebbero verificarsi durante il reclutamento utilizzando algoritmi di profilazione?

Rischi e benefici dell'uso di algoritmi contro i dipendenti

Minacce:

- maggiore controllo da parte del datore di lavoro a scapito della privacy del dipendente (mancanza di un consenso adeguato da parte del dipendente)
- erosione dell'autonomia umana attraverso la sostituzione del contatto diretto tra i manager e i loro subordinati, ovvero la "disumanizzazione" dei sistemi di gestione
- pregiudizio e discriminazione algoritmica.

Vantaggi:

- aumento della produttività grazie al risparmio di tempo e a un processo decisionale più efficiente,
- pianificazione dei turni e un'assegnazione delle responsabilità più efficaci,
- possibilità di un reclutamento più rapido,

- *c*omprensione dei problemi che sorgono sul posto di lavoro grazie a una migliore conoscenza dell'ambiente di lavoro,
- meno frequenti favoritismi dei dipendenti e l'eliminazione dei pregiudizi che possono esistere nei rapporti diretti con i dipendenti,
- un processo decisionale automatizzato limita la possibilità di interferire con le decisioni della dirigenza in materia di retribuzione, approvazione delle ferie o assegnazione dei turni.

Algoritmizzazione del rapporto dipendente-datore di lavoro

L'algoritmizzazione dei processi lavorativi è già una realtà in molte aziende. Tuttavia, spesso si scontra con i dipendenti su questioni quali:

- **Licenziamento automatico dei dipendenti** (questione da discutere durante il workshop).
- **Liquidazione algoritmica dei salari:**
    - L'algoritmo dell'app per *rider* ordinava agli autisti di evadere gli ordini indipendentemente dalla distanza dal punto di ritiro. Gli autisti non venivano pagati per la distanza dal punto di ritiro. L'imprenditore copriva solo il costo del tragitto più breve, con il risultato che, dedotti i costi del carburante e l'ammortamento dell'auto, gli autisti non ricavavano alcun profitto.
    - L'azienda ha sostenuto che i guadagni dipendono dal numero di chilometri percorsi e che esiste una tariffa fissa per ogni ordine, chiamata "tariffa base", che può variare da città a città.
    - Tuttavia, anche l'incertezza dei lavoratori sulla tariffa oraria ha rappresentato un problema: durante il periodo della pandemia, i corrieri sono stati informati nel giro di un giorno che la tariffa era cambiata, con la conseguenza che spesso erano costretti a rimetterci piuttosto che guadagnare per il lavoro svolto.
    - In seguito allo sciopero, ai corrieri sono stati promessi diversi cambiamenti, tra cui la possibilità di rifiutare un ordine tre volte al giorno, anziché una sola. In questo modo, in caso di variazione sfavorevole del tasso di base, i corrieri hanno la possibilità di rifiutare un ordine. Tuttavia, non è stata dichiarata una maggiore stabilizzazione dei tassi.
- **Identificazione algoritmica dei dipendenti**
    - Le app di taxi utilizzano un software per verificare l'identità dei loro conducenti in base ai selfie che caricano. Nel 2018, questo tipo di software, utilizzato da

un'azienda, si è rivelato incline a commettere errori quando si tratta di persone con la pelle scura (vale la pena notare che la stragrande maggioranza dei conducenti che utilizzano le app per i taxi è di sesso maschile e molti provengono da ambienti BAME *(afroamericani, asiatici e di minoranze etniche)*.

- In relazione alla verifica dell'identità, più di una dozzina di corrieri hanno riferito che, a causa di problemi con l'algoritmo, sono stati minacciati di licenziamento, hanno subito il blocco dell'account o sono stati licenziati definitivamente dopo che un selfie scattato non ha superato il *Real Time ID Check*. Alcuni sono stati licenziati dopo che la funzione selfie si è rifiutata di funzionare. Questo processo non prevedeva il diritto di appello.

- **Valutazione algoritmica dei dipendenti (di performance e non)** (argomento che verrà discusso nel corso del workshop).

Algoritmizzazione e protezione dei dati

Come già detto, un algoritmo è una serie di istruzioni su come trasformare un insieme di fatti sul mondo in informazioni utili. Per dirla in modo ancora più semplice, i fatti sono trattati come dati, mentre le informazioni sono conoscenze che possono essere ulteriormente utilizzate dall'uomo o da altre macchine.

I dati sul posto di lavoro e la loro protezione

Per evitare conflitti in materia di privacy, i datori di lavoro devono attuare misure adeguate per proteggere i dati personali, in particolare quando tali dati vengono utilizzati per processi decisionali automatizzati con un impatto diretto sul dipendente. È quindi necessario bilanciare in modo appropriato l'interesse del datore di lavoro a implementare tecnologie basate sui dati e il benessere della persona interessata, agendo in conformità con i principi fondamentali della GDPR.

- **I datori di lavoro devono raccogliere dati sui dipendenti solo quando è necessario per la gestione del posto di lavoro e delle prestazioni dei dipendenti.**

Stando al principio della minimizzazione dei dati, i datori di lavoro dovrebbero limitare la raccolta dei dati dei dipendenti, ossia qualsiasi informazione relativa alla loro identità, salute e biometria, dati relativi alle attività sul posto di lavoro (ad esempio sulla produttività), ma anche informazioni derivanti dalle attività dei dipendenti sui social media. La raccolta di dati senza limiti espone inutilmente i dipendenti a rischi quali, ad esempio, l'uso improprio dei dati personali da parte dei datori di lavoro o la fuga incontrollata di notizie.

- **I dipendenti devono avere il diritto di ispezionare, correggere e recuperare i propri dati**

I dipendenti dovrebbero essere in grado di ricevere tutte le informazioni pertinenti sui loro dati, tra cui il motivo e il modo in cui i dati sono stati raccolti, cosa è stato dedotto sul dipendente dai dati e se i dati sono stati utilizzati per prendere una decisione relativa al loro impiego. I datori di lavoro dovrebbero invece essere responsabili di correggere eventuali dati inesatti.

- **I dati dei dipendenti devono essere protetti da un uso improprio**

In nessun caso un datore di lavoro dovrebbe consentire la vendita o la concessione in licenza dei dati dei dipendenti a terzi, senza questa riserva la promessa di profitto derivante dalla monetizzazione dei dati dei dipendenti creerebbe un rischio troppo grande di sfruttamento speculativo dei dati da parte dei datori di lavoro.

- **Consenso al trattamento dei dati personali**

Nei rapporti di lavoro, il consenso al trattamento dei dati personali è molto controverso perché, a causa dello squilibrio delle parti, è facile mettere in dubbio la facoltatività del consenso dato dal dipendente. Va notato che un datore di lavoro potrebbe facilmente costringere un dipendente a soddisfare le sue aspettative con la minaccia di conseguenze negative sul lavoro. Tuttavia, ai sensi dell'articolo 155 del GDPR, gli Stati membri possono introdurre norme specifiche relative al trattamento dei dati personali dei dipendenti nel contesto del lavoro e, in particolare, alle condizioni in cui i dati personali possono essere trattati con il consenso del dipendente.

Ad esempio, in Polonia, il datore di lavoro può raccogliere i dati personali elencati nel Codice del Lavoro se il dipendente è d'accordo. Tuttavia, va notato che il consenso deve essere dato volontariamente e quindi non sarà efficace se il dipendente non ha la possibilità di rifiutarlo per paura di subire conseguenze negative. Inoltre, può essere revocato in qualsiasi momento.

Tipi di dati utilizzati nelle diverse fasi di lavoro

Fase I. Ricerca di lavoro

Cosa può aspettarsi un datore di lavoro?

Il datore di lavoro può aspettarsi che il candidato gli fornisca i dati di base necessari per procedere alla stipula del contratto. Questi dati possono includere:

- identificazione (nome, cognome, data di nascita),
- contatto indicato da tale persona;

- istruzione, competenze, esperienza lavorativa (titoli scolastici e universitari, formazione e corsi frequentati, precedenti datori di lavoro, posizioni ricoperte e responsabilità professionali).

È importante notare che in caso di partecipazione al processo di reclutamento, nonostante l'invio di dati, non è necessario che alla fine si concluda un contratto.

Cosa può aspettarsi un candidato?

Già nella prima fase del processo di assunzione, un potenziale datore di lavoro che raccoglie dati dai candidati è obbligato a informarli:

- il nome completo e l'indirizzo legale dell'azienda,
- i dati di contatto del Responsabile della protezione dei dati (se nominato),
- la finalità del trattamento e la base giuridica del trattamento, i destinatari (intesi in senso lato) o le categorie di destinatari a lui noti al momento della raccolta,
- l'intenzione di un trattamento transfrontaliero dei dati (se presente),
- il periodo per il quale i dati saranno trattati o i criteri per determinare tale periodo,
- il diritto del candidato di richiedere l'accesso ai dati, compresa una copia degli stessi, nonché la rettifica, la cancellazione o la limitazione del trattamento,
- il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento effettuato sulla base del consenso prima della sua revoca (se i dati sono raccolti sulla base del consenso),
- il diritto di presentare un reclamo al Garante per la protezione dei dati
- la volontarietà o l'obbligo di fornire i dati e le conseguenze del mancato conferimento.

Fase II. Processo di reclutamento

Durante il colloquio, il selezionatore può fare molte domande dettagliate sulle informazioni che il candidato ha inserito nel suo CV. È importante, tuttavia, che queste si riferiscano solo a questioni relative alla posizione per la quale il candidato si sta candidando. Sono inaccettabili le domande che possono mettere in imbarazzo il candidato, violare il suo diritto alla privacy o i suoi interessi personali (per es. diritto alla privacy o interessi personali o riguardanti la vita privata, la religione, l'orientamento sessuale, le opinioni politiche, ecc.)

Tempo di archiviazione dei dati

Il periodo di conservazione dei dati del candidato deve essere conforme alle regole di trattamento dei dati predeterminate dal responsabile del trattamento. Come regola generale, il

datore di lavoro dovrebbe quindi cancellare definitivamente i dati personali di un candidato con il quale ha deciso di non concludere un contratto di lavoro subito dopo la conclusione del processo di assunzione, ossia dopo aver firmato un contratto di lavoro con il dipendente appena assunto (ad esempio, cancellando o restituendo i dati).

Fase III. Periodo di occupazione

Con l'instaurazione di un rapporto di lavoro, sorgono alcuni diritti e obblighi sia per il datore di lavoro che per il dipendente. L'attuazione di questi comporta chiaramente il trattamento dei dati personali del dipendente. La gestione dei dati personali, sebbene in linea di principio regolata dal GDPR, è ulteriormente chiarita nel caso del lavoro dalla legislazione nazionale.

Ad esempio, in Polonia, ai sensi dell'articolo 221, paragrafi 2 e 4, del Codice del Lavoro, un datore di lavoro ha il diritto di richiedere a un dipendente che ha deciso di assumere, di fornire (in aggiunta ai dati personali che può aver ottenuto da lui/lei nel corso dell'assunzione) anche i dati personali:

- indirizzo di residenza,
- numero PESEL[6]
- altri dati personali, compresi, tra l'altro, i nomi e le date di nascita dei figli, se il conferimento di tali dati è necessario per l'esercizio di prerogative speciali ai sensi del diritto del lavoro,
- istruzione e storia lavorativa precedente, se non c'erano i presupposti per richiederli al candidato all'assunzione,
- il numero di conto corrente per il pagamento se il dipendente non ha richiesto il pagamento in contanti

Obblighi di informazione del datore di lavoro nei confronti del lavoratore

Poiché il datore di lavoro tratterà i dati del dipendente per una finalità diversa da quella del candidato, il dipendente deve essere informato a questo proposito. Tale finalità può essere soddisfatta includendo tali informazioni nella clausola informativa fornita ai candidati nel corso del processo di assunzione, integrandola con informazioni sulle finalità del trattamento e indicando i destinatari dei dati in caso di assunzione del candidato, oppure integrando tali informazioni poco dopo l'assunzione del dipendente.

[6] In Polonia è il numero d'identità anagrafica, simile per uso al Codice Fiscale italiano.

Controllo degli algoritmi utilizzati nel lavoro (trasparenza degli algoritmi)

Gli esempi di utilizzo dell'intelligenza artificiale sul posto di lavoro citati di seguito dimostrano che l'uso incontrollato di strumenti di IA da parte delle aziende può portare a una maggiore insicurezza del lavoro e quindi avere un impatto negativo sulla vita dei dipendenti. Allo stesso tempo, secondo le stime del McKinsey Global Institute, entro il 2030 fino al 70% delle aziende avrà implementato una qualche forma di sistemi di intelligenza artificiale. Ecco perché è così importante valutare criticamente le nuove tecnologie e consentire alle autorità di regolamentazione e alle organizzazioni indipendenti di verificare l'IA.

- Nel Regno Unito, il software Horizon utilizzato dal National Post Office ha erroneamente sospettato singoli dipendenti di aver sottratto decine di migliaia di sterline. A causa dell'errore dell'intelligenza artificiale, ben 736 impiegati postali sono stati perseguiti e alcuni sono stati accusati e condannati.
- Nei Paesi Bassi, i conducenti di un'app per taxi hanno citato in giudizio la società dopo che un algoritmo aveva bloccato i loro account per presunte frodi. Il tribunale ha respinto le loro richieste perché ha ritenuto che le violazioni non rientrassero nella definizione di processo decisionale completamente automatizzato ai sensi del GDPR. Di conseguenza, i dipendenti sono rimasti senza alcuna tutela legale.
- In Italia, un tribunale ha ordinato a un'azienda di consegne di cibo a domicilio di rendere noto l'algoritmo dell'app e di eliminare gli elementi che, non avendo affrontato questioni regolamentate dal diritto del lavoro (come i congedi per malattia o il diritto di sciopero), la rendevano discriminatoria.

Algoritmo e segreto aziendale

Ai sensi della normativa europea, le informazioni sulla tecnologia o su qualsiasi altro aspetto di un'azienda possono essere protette come segreto aziendale. Tuttavia, devono soddisfare le seguenti condizioni:

- le informazioni sull'algoritmo non sono note al grande pubblico o agli esperti del settore,
- le informazioni sull'algoritmo hanno un valore commerciale,
- sono state adottate misure per garantire la riservatezza delle informazioni, ad esempio sono conservate in un luogo sicuro e tutti coloro che vi hanno accesso o che le condividono hanno firmato un accordo di riservatezza.

Nel caso delle nuove tecnologie utilizzate nei processi di lavoro, soddisfare questa logica non è difficile. Le aziende citano spesso i segreti commerciali, evidenziando le loro preoccupazioni per la perdita di competitività derivante dall'esposizione dei loro sistemi interni. Pertanto, la comprensione degli algoritmi e la verifica degli strumenti di IA nel settore privato sono

particolarmente problematici. Inoltre, ulteriori forme di tutela legale sotto forma di clausole di riservatezza impediscono agli *insider* (dipendenti attuali o ex) di condividere informazioni sui meccanismi che coordinano il loro lavoro.

Legge sull'intelligenza artificiale (AI Act)

Le ripetute accuse all'intelligenza artificiale di replicare pregiudizi, imprecisioni o discriminazioni da parte degli algoritmi hanno fatto sì che la Commissione europea si assumesse la responsabilità di introdurre una regolamentazione per controllare gli strumenti di intelligenza artificiale e prevenire gli effetti negativi del loro utilizzo.

12 aprile 2021 la Commissione europea ha presentato una bozza di regolamento UE sull'intelligenza artificiale, il primo atto legislativo completo sugli strumenti di intelligenza artificiale. L'obiettivo del regolamento è fornire un ambiente adatto allo sviluppo dell'intelligenza artificiale nell'Unione europea, tenendo conto dei rischi associati allo sviluppo delle tecnologie più recenti. Soprattutto, l'AI Act mira a rendere gli algoritmi utilizzati nell'UE sicuri, trasparenti, etici, imparziali e controllati dall'uomo.

Approccio basato sul rischio

L'obiettivo principale della legge è quello di identificare i rischi posti da un particolare sistema di IA e di porre come condizione gli obblighi e i requisiti normativi a cui saranno soggetti gli sviluppatori e gli implementatori di IA.

- **Rischi inaccettabili**: vietare l'IA

Divieto di applicazioni particolarmente dannose dell'intelligenza artificiale (IA), contrarie ai valori dell'UE, che rischiano di violare i diritti fondamentali dell'individuo, ad esempio: esecuzione di valutazioni dei cittadini (il cosiddetto *social scoring*), sfruttamento della vulnerabilità di un gruppo specifico di persone a causa dell'età, della disabilità motoria o di un disturbo mentale, uso di tecniche subliminali, uso dell'identificazione biometrica negli spazi pubblici e a fini di applicazione della legge (con alcune eccezioni).

- **Rischio elevato** - IA accettabile, ma a determinate condizioni.

Sono stati classificati come ad alto rischio gli strumenti che hanno un impatto negativo sulla sicurezza o sui diritti fondamentali delle persone, ovvero i sistemi che si trovano nelle seguenti aree:

  - identificazione biometrica e categorizzazione degli individui,
  - gestione delle infrastrutture critiche,

- istruzione o formazione professionale - la capacità di decidere l'accesso di un individuo all'istruzione e alla formazione professionale (ad esempio, la correzione degli esami),
- sicurezza dei prodotti (ad esempio, l'uso dell'intelligenza artificiale nella chirurgia assistita da robot),
- assunzione, gestione dei dipendenti e accesso al lavoro autonomo (ad esempio, software di analisi dei CV per le procedure di assunzione),
- servizi pubblici e privati di base (ad esempio, valutazione del credito, credit scoring),
- applicazione della legge - interferenza con i diritti fondamentali delle persone (ad esempio, verifica dell'autenticità dei documenti),
- gestione della migrazione, dell'asilo e del controllo delle frontiere (ad esempio, valutazione delle domande di asilo),
- amministrazione della giustizia e dei processi democratici (ad esempio, suggerendo il tipo di sanzioni e il livello di pena per una persona condannata per un reato).

Esempi di requisiti specifici per i sistemi ad alto rischio:

- **Requisiti di trasparenza** - il funzionamento dei sistemi di IA ad alto rischio deve essere sufficientemente trasparente da consentire agli utenti di interpretare i risultati che li riguardano. Per i sistemi di IA ad alto rischio devono essere sviluppate istruzioni per l'uso.
- **Supervisione umana obbligatoria** dei **sistemi ad alto rischio** - necessaria per fornire agli esseri umani una supervisione efficace delle IA ad alto rischio, compresa la comprensione delle capacità e dei limiti di un determinato sistema di IA. Le misure di supervisione appropriate possono includere la decisione di non utilizzare il sistema di IA in una determinata situazione, ignorare una decisione presa dal sistema di IA o interrompere il sistema con un pulsante di STOP.

Problemi di lavoro sollevati dalla legge sull'intelligenza artificiale

I sistemi ad alto rischio con un impatto sul mercato del lavoro e soggetti a sorveglianza specifica sono elencati nell'allegato III della proposta di legge sull'IA. Si tratta di sistemi di IA:

1. Utilizzati nel processo di reclutamento o di selezione di persone specifiche e, in particolare, quelli utilizzati per pubblicare offerte di lavoro, per pre-selezionare o filtrare le candidature, per valutare i candidati durante i colloqui o i test.
2. Decidere la promozione o il licenziamento di qualcuno, determinare la distribuzione dei compiti e monitorare le prestazioni e il comportamento dei dipendenti.

3. Decidere l'accesso alla formazione professionale o valutare i tirocinanti.

Come detto, i suddetti sistemi di intelligenza artificiale possono avere un impatto significativo sulle prospettive di lavoro delle persone di cui trattano i dati, incidendo così sul loro sostentamento e sul loro reddito. La Commissione europea ha anche sottolineato che i sistemi mal progettati e utilizzati possono perpetuare modelli discriminatori (ad esempio nei confronti di donne, anziani, persone con disabilità, orientamento razziale, etnico o sessuale). Inoltre, i sistemi di intelligenza artificiale utilizzati per verificare le prestazioni (in particolare quelli basati sulla biometria) possono avere un impatto sulla protezione dei dati personali e sul diritto alla privacy. Pertanto, dovrebbero essere soggetti a requisiti particolarmente severi e i dipendenti dovrebbero sempre avere una possibilità di ricorso contro le decisioni degli algoritmi.

Critiche alla legge sull'IA

Anche l'applicazione della legge sull'IA alle questioni occupazionali è stata oggetto di numerose critiche. Secondo gli esperti, il regolamento presta troppa poca attenzione alle questioni lavorative e il controllo della trasparenza degli algoritmi si riduce ai requisiti generali di trasparenza elencati nell'articolo 52 della bozza di regolamento. Inoltre, non è certo che il regolamento entrerà in vigore prima del 2025.

Paura di perdere il lavoro a causa dell'algoritmizzazione/robotizzazione

Secondo le stime di McKinsey, entro il 2030 l'automazione nei vari settori porterà alla necessità di riqualificare ben 375 milioni di lavoratori. Una previsione leggermente diversa, anche se altrettanto preoccupante, è stata fatta dal World Economic Forum nel suo rapporto, che ha indicato nella sua pubblicazione *Future of Jobs* che i progressi nelle aree dell'algoritmizzazione e delle tecniche di calcolo potrebbero portare le macchine a sostituire 75 milioni di posti di lavoro in tutto il mondo nei prossimi anni.

Per quanto riguarda gli effetti della robotizzazione, si può ipotizzare che i lavori manuali, soprattutto quelli basati su sequenze prevedibili, saranno i più colpiti. Tuttavia, anche alcuni professionisti potrebbero essere colpiti negativamente dall'automazione. Secondo il già citato rapporto *Future of Jobs,* tra le professioni soppiantate dall'IA, come il meccanico, il magazziniere e il direttore di produzione, ci sono anche avvocati e analisti finanziari. Inoltre, gli effetti dell'automazione saranno avvertiti da coloro le cui professioni consistono nel raccogliere e trattare dati, ossia mansioni realizzate in modo decisamente più rapido e preciso dalle macchine. Ben il 60% dei dipendenti vede automatizzato un terzo dei compiti del proprio lavoro. Non deve sorprendere, quindi, che gli occupati siano preoccupati per il loro attuale lavoro. Secondo il rapporto *Pandemic Automates Poland?* della Procontent Communication, quasi un intervistato su cinque (18,7%) teme l'automatizzazione del proprio lavoro, seguita dalla perdita del posto di

lavoro. Tuttavia, gli esperti stemperano i timori: guardando a livello globale, solo il 5% dei posti di lavoro rischia di scomparire completamente. Inoltre, anche se molti lavori saranno soppiantati dalle macchine, si può prevedere che al loro posto emergeranno nuove professioni grazie all'aumento della domanda di competenze trasversali che richiedono creatività, intelligenza emotiva e pensiero critico.

Inoltre, lo sviluppo della tecnologia contribuirà alla continua creazione di nuovi posti di lavoro ad alta remunerazione nel settore IT - a livello globale, si potrebbe arrivare a 50 milioni di posti di lavoro entro la fine del decennio. Questo approccio ottimistico sembra essere confermato dal già citato studio del World Economic Forum, che indica che con l'aumento dell'automazione verranno creati fino a 133 milioni di posti di lavoro. Sebbene sia difficile determinare con precisione la forma dei futuri livelli occupazionali a causa del dinamismo dei cambiamenti apportati dalla digitalizzazione, secondo le valutazioni degli esperti non è certo che nel prossimo futuro si verifichi una disoccupazione tecnologica strutturale.

La tecnologia al servizio dell'inclusività

La digitalizzazione dei posti di lavoro contribuisce a una più efficace integrazione nel mercato del lavoro di quei gruppi sociali che in precedenza ne erano temporaneamente o permanentemente esclusi.

Per le **persone con disabilità si** possono osservare i seguenti vantaggi:

- l'assenza delle difficoltà di trasporto verso il luogo di lavoro che in passato dovevano affrontare le persone con determinate limitazioni fisiche,
- una minore esposizione agli stimoli e una modalità di lavoro a distanza più tranquilla favoriscono un lavoro più efficace per le persone con disabilità intellettive, iperattività o difficoltà di concentrazione e apprendimento,
- l'uso di mezzi di telecomunicazione elettronici (e-mail, messaggistica istantanea) consente la partecipazione attiva alle discussioni da parte di persone con disturbi del linguaggio.

Esempi di vantaggi per i **genitori**:

- l'opportunità di trascorrere più tempo con i bambini,
- riduzione dell'esposizione di tutta la famiglia alle malattie infettive comuni (influenza, raffreddore, COVID-19),
- la possibilità per i giovani genitori di conciliare efficacemente vita privata e professionale.

Il lavoro a distanza ha anche un forte impatto sulla permanenza delle giovani madri nel mercato del lavoro (ben il 49% delle madri lavoratrici ammette di conoscere almeno una persona che ha lasciato il proprio lavoro o sta pensando di farlo a causa dell'obbligo di tornare in ufficio).

Esempi dei vantaggi dell'utilizzo delle **app per taxi**:

- lavorare per l'uguaglianza di genere (nella maggior parte delle città americane, le donne rappresentano finora meno del 5% dei tassisti, mentre nel caso delle applicazioni di sharing economy sono già circa il 20-30%), lavorare per l'uguaglianza di genere. 20-30%),
- facilitare l'ingresso degli immigrati (ad esempio dall'Ucraina) nel mercato del lavoro,
- offrire corse a prezzi più accessibili: ad esempio, a Los Angeles l'applicazione Uber è disponibile in 21 quartieri a basso reddito, dove offre corse significativamente più economiche rispetto alle compagnie di taxi tradizionali.

1.6 Effetto delle nuove tecnologie sulle relazioni contrattuali: una discussione sugli *smart contracts* e la loro futura applicazione nelle relazioni datore-lavoratore

La digitalizzazione si è ormai diffusa in quasi tutti gli ambiti della nostra vita quotidiana e privata. Ciò vale anche per i rapporti contrattuali precedentemente conclusi verbalmente o per iscritto, che ora vengono spesso rafforzati o integrati con strumenti digitali. Data la grande quantità di informazioni presenti sul web e la crescente conclusione di obbligazioni reciproche con un elemento digitale, gli strumenti basati sulla blockchain, come i *contratti intelligenti,* avranno sicuramente il maggiore impatto sui rapporti contrattuali nel prossimo futuro.

Che cos'è la blockchain?

La blockchain (*catena di blocchi*) è una tecnologia per il trasferimento e l'archiviazione di informazioni sulle transazioni effettuate su Internet. Le singole informazioni sono organizzate in blocchi successivi di dati. Una volta che un blocco è saturo di un certo numero di transazioni, le informazioni sulle transazioni vengono memorizzate nel blocco successivo. Grazie al riferimento al blocco precedente e al concatenamento delle informazioni in essi contenute, diventa impossibile modificare o cancellare la registrazione di una transazione senza che tale modifica venga registrata in tutti gli altri blocchi. Questa soluzione favorisce la trasparenza delle transazioni effettuate e contrasta la manipolazione fraudolenta delle informazioni.

Cosa sono i *contratti intelligenti*?

Uno smart contract è un programma "autoesecutivo" basato sulla logica *if-then (se...allora)*. È scritto interamente in un linguaggio di programmazione e può essere eseguito utilizzando la tecnologia DLT (distributed ledger technology, tecnologia del registro diffuso) o la blockchain. In quest'ultimo caso, il programma è memorizzato sulla blockchain e viene eseguito quando determinate condizioni innescano un'altra azione - ad esempio, può attivare un pagamento o fornire un determinato servizio. Si tratta quindi di una **fusione tra la realtà creata da un determinato contratto e il mondo reale attraverso la tecnologia.** Ciò rende il contratto più trasparente e affidabile, fornendo alle parti la fiducia nell'esecuzione dei suoi termini quando si verifica una determinata situazione.

Esempi di utilizzo dei contratti intelligenti:

- Acquisto di un immobile - grazie agli smart contract, il processo, solitamente molto complesso e che richiede il coinvolgimento di numerosi intermediari (notaio, agente immobiliare, consulente legale, istituto di credito), viene notevolmente semplificato e non richiede il coinvolgimento dei suddetti attori, rendendo possibile l'acquisizione del titolo di proprietà per via elettronica.
- Acquisti online - in questo caso, i contratti intelligenti garantiscono che il pagamento venga effettuato immediatamente e che quindi il prodotto venga inviato all'acquirente più rapidamente.
- Trattamento dei dati personali - poiché i dati personali e le ID digitali sono memorizzati sulla blockchain, il rischio di furto di identità è notevolmente ridotto.
- Registrazione dei risultati di elezioni o referendum - per ridurre al minimo il rischio di brogli elettorali. L'uso di smart contract a questo scopo può già essere osservato in pratica in Estonia, tra gli altri.
- Pagamento di compensazioni e premi - liquidazione automatica dei sinistri, calcolo dei premi.

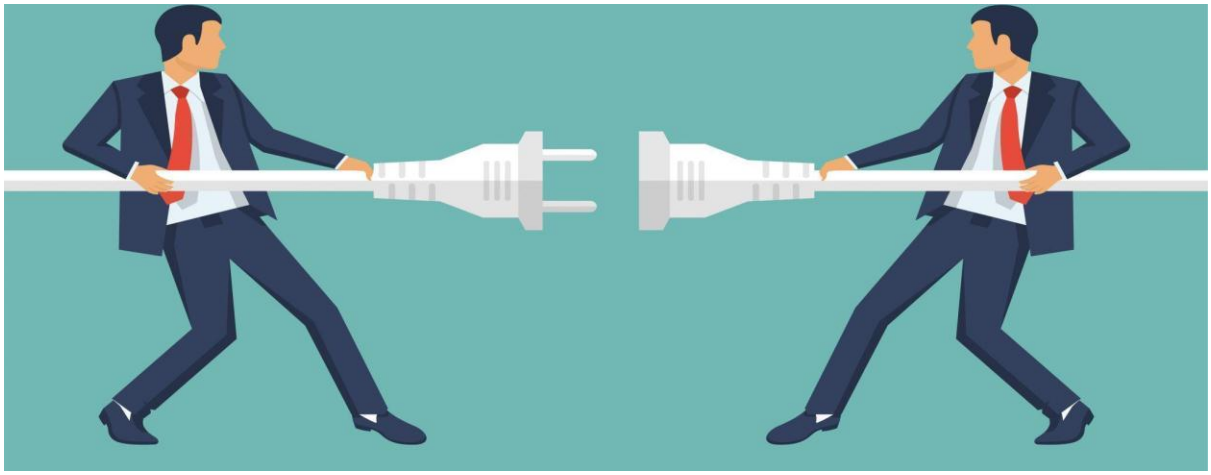
Effetti della digitalizzazione sulla vita privata dei lavoratori

2.1 Protezione del tempo di lavoro dei lavoratori nel lavoro a distanza. Lavoro a distanza e work-life balance

Secondo una ricerca di Eurofound, un terzo dei dipendenti dell'Unione Europea ha iniziato a lavorare da casa durante la pandemia e come risultato del passaggio al lavoro a distanza, fino al 27% ha dichiarato di svolgere le proprie mansioni lavorative nel tempo libero. Durante il lock-down, il confine tra vita privata e professionale ha iniziato a sfumare. I dipendenti hanno acquisito la capacità di organizzare il proprio tempo, ma sono stati anche esposti al rischio di essere sempre reperibili e di non potersi staccare completamente dai media elettronici al di fuori dell'orario di lavoro.

È importante notare che nella modalità basata sulle mansioni (non basata su orari di lavoro rigidi) si applicano le stesse regole del sistema tradizionale, ovvero il dipendente deve svolgere le proprie mansioni per 8 ore al giorno nell'arco di una settimana lavorativa di cinque giorni. I compiti svolti al di fuori di questo quadro dovrebbero essere considerati come straordinari. Tuttavia, sebbene l'orario di lavoro flessibile sia indubbiamente vantaggioso per i dipendenti, questi ultimi spesso credono erroneamente che, non essendo in ufficio a orari fissi, debbano dimostrare di essere disponibili in ogni momento della giornata.

2.1.1. Diritto alla disconnessione



Fonte: Shutterstock.

Come sancito dall'articolo 24 della Dichiarazione universale dei diritti dell'uomo, ogni individuo ha diritto al riposo e allo svago, compresa una ragionevole limitazione dell'orario di lavoro e ferie periodiche retribuite. Inoltre, secondo l'articolo 31 della Carta dei diritti fondamentali, ogni lavoratore ha diritto a condizioni di lavoro che rispettino la sua salute, la sua sicurezza e la sua dignità e ha diritto a periodi di riposo giornaliero e settimanale, a ferie annuali retribuite e, soprattutto, alla limitazione dell'orario di lavoro massimo.

La nuova realtà post-pandemica, in cui il confine tra vita privata e professionale è spesso labile, ha evidenziato la necessità di implementare una normativa che dia ai dipendenti la sicurezza di disconnettersi dal lavoro e di non rispondere alle e-mail dei superiori dopo l'orario di lavoro senza conseguenze negative. Per questo motivo, nel 2021, il Parlamento europeo ha adottato una risoluzione a favore del diritto alla disconnessione, invitando la Commissione europea a studiare l'elaborazione di una direttiva sul diritto a essere *offline*.

Vale la pena notare che le risoluzioni del Parlamento europeo non hanno carattere vincolante. Pertanto, la Commissione europea non è obbligata ad agire per l'attuazione della direttiva proposta dal Parlamento. Tuttavia, data la sostanza della questione, si può prevedere che la Commissione cercherà di regolamentare il diritto allo scollegarsi e di garantire un livello di protezione uniforme per i lavoratori in tutta l'Unione europea.

Come proposto dal Parlamento europeo, la direttiva sul diritto alla disconnessione intende garantire:

1) regole minime che garantiscano ai dipendenti che utilizzano mezzi di comunicazione a distanza nel loro lavoro quotidiano il diritto di essere *offline*,
2) Il divieto di discriminazione o di trattamento meno favorevole dei dipendenti (compresa la risoluzione dei contratti di lavoro) che esercitano il diritto alla disconnessione,

3) la parità di trattamento di tutti i dipendenti, sia del settore pubblico che di quello privato, dei dipendenti di livello inferiore o dei dirigenti (anche se in quest'ultimo caso può essere difficile, a causa delle normative specifiche per i dirigenti),

4) una procedura giudiziaria efficiente e la possibilità di chiedere riparazione per le violazioni dei diritti concessi (accesso alla protezione giudiziaria dalle ripercussioni).

Obblighi dei datori di lavoro in relazione al diritto dei dipendenti di essere *offline*

I nuovi diritti dei dipendenti comportano anche ulteriori obblighi da parte dei datori di lavoro. Tra questi, la necessità di dotarsi di un sistema interno che consenta di misurare con precisione l'orario di lavoro giornaliero del dipendente (nel rispetto del diritto alla privacy e alla protezione dei dati personali). Inoltre, è importante sostenere i dipendenti nell'essere *offline* - comunicando chiaramente la nuova legge nelle politiche aziendali, conducendo campagne di formazione e informazione in questo settore.

Tuttavia, in termini di sensibilizzazione, l'obbligo di informare per iscritto ciascun dipendente dei propri diritti sembra il più rilevante e promettente.

Inoltre i datori di lavoro dovrebbero evitare di promuovere una cultura di disponibilità continua e di premiare i dipendenti che non esercitano il diritto alla disconnessione. Anche la valutazione della salute e della sicurezza in relazione al diritto alla disconnessione (ad esempio in termini di rischi psicosociali) dovrebbe essere una considerazione importante.

2.1.2. Equilibrio tra la vita privata e professionale: il ruolo dello Stato

Fonte: Technology Headlines.

Lo Stato e le sue politiche del lavoro hanno un ruolo importante nel plasmare il rapporto tra lavoratore e datore di lavoro. In termini di equilibrio tra lavoro e vita privata, alcuni Paesi stanno adottando iniziative per promuovere buone prassi occupazionali. Da un lato ciò riguarda l'attuazione delle normative nazionali, dall'altro, gli strumenti legislativi che non hanno forza vincolante ma cercano di dare forma a determinati comportamenti.

Tali misure "soft" potrebbero consistere, ad esempio, nell'attuazione di codici di buona condotta o nel dare il buon esempio agli altri datori di lavoro promuovendo un approccio favorevole ai lavoratori all'interno delle strutture governative. Questa strada è stata scelta da Malta, che nel 2020 ha pubblicato un *Manuale sulle misure volte all'equilibrio tra lavoro e vita privata*. Questa pubblicazione raccoglie e descrive in dettaglio i diritti dei dipendenti, con istruzioni su come lavorare correttamente nell'era della digitalizzazione (ad esempio, come organizzare il proprio lavoro quando si svolgono mansioni a distanza). Tuttavia l'utilità del manuale non sta solo nella sua capacità di far conoscere meglio le prerogative dei dipendenti o nel campo della digitalizzazione. Tali codici di buone prassi, applicabili sul posto di lavoro (o in un determinato settore), possono anche essere una sorta di merce di scambio nelle trattative con il datore di lavoro.

Nel caso del manuale maltese, i promotori del progetto hanno dichiarato che il loro obiettivo principale era quello di garantire un equilibrio tra lavoro e vita privata per gli impiegati del settore pubblico, sensibilizzando i dipendenti. Vale la pena notare, tuttavia, che il manuale non amplia in alcun modo il catalogo dei diritti dei lavoratori, ma si limita a richiamare l'attenzione sulle corrette pratiche di impiego e a sensibilizzare i lavoratori sulla possibilità di negoziare le condizioni di lavoro in linea con le disposizioni del documento.

Esempi di promozione del diritto alla disconnessione nei paesi dell'UE

Sebbene al momento non esista ancora un quadro giuridico paneuropeo che disciplini il diritto alla disconnessione, esistono già alcuni esempi di azione legislativa in questo ambito nell'UE. A ciò si aggiunge la promozione del diritto alla disconnessione attraverso i contratti collettivi di lavoro. Inoltre, alcuni Stati membri hanno già attuato una legislazione proprioa sul diritto alla disconnessione.

Francia

La Francia è considerata un pioniere del diritto alla disconnessione. Già nel 2013 è stato adottato un accordo intersettoriale sulla qualità della vita sul lavoro, che incoraggiava le aziende a non interferire con la vita privata dei dipendenti e definiva il momento in cui i dispositivi di

contatto dei dipendenti dovevano essere spenti. Queste disposizioni sono state successivamente promulgate l'8 agosto 2016 e incorporate nel Codice del lavoro francese. Inoltre, da gennaio 2017, in Francia i datori di lavoro sono tenuti a negoziare accordi con i sindacati sul diritto alla disconnessione.

Italia

La Francia è stata seguita dall'Italia, che ha deciso di introdurre il diritto alla disconnessione nel 2017. La normativa si concentra sulle persone che svolgono un lavoro a distanza (*smart working*, *lavoro agile*) e stabilisce che i lavoratori a distanza hanno il diritto di disconnettersi dai dispositivi tecnologici e dalle piattaforme online senza subire alcuna conseguenza da parte dei loro datori di lavoro. Anche in Italia esistono contratti collettivi settoriali e aziendali che prevedono il diritto alla disconnessione.

Spagna

Un altro paese che ha adottato il diritto alla disconnessione nella legislazione nazionale è la Spagna. Nel 2018, con il recepimento del GDPR nella legislazione spagnola, è stato introdotto un nuovo pacchetto di diritti digitali. Con esso, ai dipendenti che lavorano sia nel settore privato che in quello pubblico è stato riconosciuto il diritto alla disconnessione, con l'obiettivo di mantenere un equilibrio tra lavoro e vita privata. Secondo il regolamento, i datori di lavoro, dopo aver ascoltato i rappresentanti dei lavoratori, devono stabilire politiche interne su come i dipendenti possono esercitare il loro diritto alla disconnessione e fornire formazione ai dipendenti sull'uso corretto delle nuove tecnologie.

Belgio

In Belgio, nel 2018, tutti i datori di lavoro con più di 50 dipendenti sono stati obbligati a discutere l'uso sicuro degli strumenti digitali e il diritto dei dipendenti alla disconnessione con il comitato per la salute e la sicurezza. Vale la pena notare che, con l'introduzione del diritto alla disconnessione, i dipendenti stessi non hanno acquisito nuovi poteri, ma solo maggiori opportunità di negoziazione con il datore di lavoro. Tuttavia, nel 2022 è stato adottato un nuovo regolamento che consente ai dipendenti pubblici di spegnere le e-mail di lavoro e di non rispondere a messaggi di testo e telefonate al di fuori dell'orario di lavoro senza temere ripercussioni. Sono in discussione anche piani per estendere le nuove norme ai dipendenti del settore privato.

Irlanda

Nell'aprile 2021, il governo irlandese ha promulgato un codice di condotta in base al quale tutti i dipendenti hanno il diritto di disconnettersi e di non rispondere immediatamente a e-mail, telefonate o altri messaggi provenienti dal proprio datore di lavoro dopo l'orario di lavoro. Il codice stabilisce inoltre che un dipendente, di regola generale, non deve essere costretto a lavorare al di fuori del suo orario di servizio standard e non deve subire conseguenze per aver rifiutato di occuparsi di questioni aziendali dopo l'orario di lavoro.

2.1.3 Esigenza della reperibilità continua da parte del datore di lavoro e mobbing

Fonte: jobs.ca.

Il mobbing è un'azione o un comportamento nei confronti di un dipendente che consiste in molestie o intimidazioni persistenti e prolungate. Si verifica quando le azioni in questione hanno lo scopo di umiliare o ridicolizzare il dipendente, ma anche quando mirano a indurlo a sottovalutare la propria idoneità professionale.

Poiché il mobbing può assumere diverse forme di aggressione, il catalogo dei comportamenti che si qualificano come questo tipo di violenza rimane aperto. Pretendere che un dipendente sia sempre disponibile sotto la minaccia di conseguenze negative può quindi essere considerato mobbing. Lo dimostrano, ad esempio, le sentenze in cui i tribunali hanno dato ragione ai dipendenti che sostenevano che la ricezione opprimente e ripetuta di messaggi contenenti istruzioni di lavoro dopo l'orario di lavoro o nei giorni di riposo dovrebbe essere considerato come mobbing.

Sentenza del Tribunale regionale di Lublino del 20 giugno 2018. (VIII Pa 86/18)

Un tribunale ha riconosciuto a una dipendente di un ufficio comunale un risarcimento di 25.000 zloty dal suo datore di lavoro per i danni alla salute causati dall'invio invadente di e-mail dopo l'orario di lavoro. Il caso riguardava una donna impiegata come dipendente pubblico a tempo pieno e indeterminato. Dopo il cambio di sindaco nel comune, il nuovo supervisore ha adottato l'invio di istruzioni ai dipendenti sotto forma di e-mail ai loro indirizzi di lavoro e privati come metodo principale di comunicazione con loro. Dal 1° gennaio 2015, la ricorrente aveva ricevuto circa 200 e-mail dal sindaco, di cui più di 100 sono state inviate dopo l'orario di lavoro, anche di notte e nei giorni festivi, durante le ferie annuali o i congedi per malattia. Il procedimento è sfociato in una sentenza del Tribunale regionale di Lublino, in cui la Corte ha ritenuto che incaricare un dipendente di compiti e inviare e-mail con ordini di lavoro in giorni non lavorativi, durante le assenze per malattia e ferie, e chiedergli di render conto in modo inadeguato delle sue prestazioni, possa essere considerato **mobbing.**

Violazione del diritto alla disconnessione - implicazioni per il datore di lavoro e meccanismi di reclamo

Le sanzioni per le violazioni del diritto alla disconnessione possono variare da un paese all'altro dell'UE. Ciò è dovuto al fatto che ogni Stato membro deve determinare individualmente il livello di sanzione imposto a un datore di lavoro per il mancato rispetto del tempo libero dei propri dipendenti.

In Polonia non è ancora stato introdotto un diritto separato del dipendente alla disconnessione, ma può essere dedotto dalle norme generali sull'orario di lavoro e dalla giurisprudenza dei tribunali. È quindi generalmente accettato che un dipendente non sia obbligato a rispondere al telefono o alle e-mail dopo l'orario di lavoro o durante le vacanze. Fa eccezione il caso in cui sia richiesto di essere reperibile, cioè di essere pronto a lavorare al di fuori dell'orario di lavoro.

I comportamenti scorretti più comuni da parte dei datori di lavoro in merito al rapporto di lavoro sono le irregolarità relative alla risoluzione dei contratti, le violazioni delle norme

sull'orario di lavoro, il pagamento improprio dei salari e la concessione impropria di congedi. In Polonia a seconda dell'entità e del tipo di infrazione, il datore di lavoro può incorrere in una multa che va da 1.000 a 30.000 zloty. Pertanto, si può prevedere che in Polonia il mancato rispetto del diritto alla disconnessione sarà sanzionato come qualsiasi altra violazione delle norme sull'orario di lavoro, ossia il datore di lavoro dovrà pagare una multa fino a 30.000 zloty. Inoltre, in caso di trattamento inferiore di un dipendente a causa della sua limitata disponibilità al di fuori dell'orario di lavoro designato, possono sorgere problemi di risarcimento per discriminazione (per un importo non inferiore al salario minimo applicabile).

Secondo un sondaggio d'opinione[7] , il 23,9% dei dipendenti in Polonia riceve e-mail, sms o altri messaggi dai superiori dopo l'orario di lavoro. Sebbene, come sottolineano gli esperti, ciò non sia vietato, tale azione può essere considerata come un'istruzione a lavorare oltre l'orario di lavoro (soprattutto quando il contatto obbliga il dipendente a eseguire un particolare compito). Se è necessario rispondere a un'e-mail o a una telefonata per questioni di lavoro, ai sensi degli articoli 151 (1) e 151 (2) del Codice del lavoro, tale azione deve essere compensata con una retribuzione aggiuntiva o con permessi.

Cosa deve fare un dipendente polacco i cui diritti sono stati violati?

a) Colloquio con il datore di lavoro

Prima di decidere di denunciare una violazione alle autorità esterne, è consigliabile che il dipendente cerchi di comunicare con il datore di lavoro. È importante che il direttore o il proprietario dell'azienda sia coinvolto nella conversazione, poiché può accadere che i dirigenti non siano a conoscenza di illeciti commessi da supervisori che agiscono a un livello inferiore.

b) Cercare il sostegno dei sindacati

Se il dialogo con il datore di lavoro non funziona, il dipendente può chiedere il sostegno del *sindacato*, se presente sul posto di lavoro. Il sindacato ha il compito di rappresentare i dipendenti e dovrebbe rinnovare il tentativo di raggiungere un accordo con il direttore/proprietario dell'azienda o con la sua direzione.

[7] Sondaggio condotto da UCE RESEARCH e da ePsycholodzy.it, https://uce-pl.com/news/blisko-24-proc-polakow-twierdzi-ze-pracodawca-kontaktuje-sie-z-nimi-w-czasie-wolnym-od-pracy.

c) Notifica delle violazioni all'Ispettorato statale del lavoro (PIP)

L'Ispettorato statale del lavoro (PIP) è l'istituzione più importante che si occupa di condizioni di lavoro e diritti dei lavoratori in Polonia. È ad esso che devono essere presentate, in prima istanza, le denunce formali di violazione dei diritti del lavoro. I contatti con il PIP sono disponibili all'indirizzo www.pip.gov.pl e le denunce possono essere presentate per iscritto, per telegrafo, fax, e-mail, tramite il modulo di denuncia elettronica o oralmente. I dati del dipendente che presenta il reclamo possono rimanere anonimi. Secondo la legge sull'ispettorato del lavoro[8], l'ispettore del lavoro è tenuto a non rivelare che un'ispezione è stata effettuata a seguito di un reclamo, a meno che il denunciante non acconsenta per iscritto. Tuttavia è importante ricordarsi di motivare adeguatamente le accuse mosse e di fornire prove solide, poiché sarà il PIP a decidere se la denuncia è credibile e se sarà verificata.

d) Portare il caso davanti al tribunale distrettuale

Il materiale presentato al PIP può anche costituire una prova nel caso in cui il caso venga sottoposto al
al tribunale distrettuale. Il ricorso al tribunale è tuttavia l'ultima risorsa, utilizzata solo quando le vie precedenti hanno fallito.

[8] Articolo 44, paragrafo 3, della *legge del 13 aprile 2007 sull'Ispettorato statale del lavoro* (Gazzetta ufficiale 2017, voce 786 e successive modifiche).

2.1.4. Work-life balance: cos'è l'equilibrio tra la vita privata e quella lavorativa?

Fonte: zapier.com.

Secondo il rapporto dell'OCSE *How's Life? Measuring Well-being*, il concetto di *work-life balance* si riferisce al mantenimento di un equilibrio tra lavoro (sia retribuito che non), vita familiare e tempo libero. Si riferisce alla capacità di un dipendente di organizzare le proprie responsabilità in modo tale da non interferire con il proprio tempo libero. Tuttavia, il giusto equilibrio tra le diverse aree della vita non dipende solo dal dipendente, ma anche dal datore di lavoro. È il datore di lavoro che di solito crea la cultura del lavoro in azienda e impone determinate norme.

Il rispetto del tempo libero dei dipendenti, siano essi fissi, remoti o ibridi, è di grande importanza.
Dopo tutto, il benessere di ogni dipendente (benessere; stato mentale) dipende da un buon equilibrio tra lavoro e vita privata. Secondo le ricerche, il sovraccarico e il lavoro continuo (compresi i lavori domestici e di assistenza alla persona) possono portare all'esaurimento e a problemi di salute, allo stress cronico e alla riduzione della produttività.

Prima della pandemia, il tempo dedicato al tempo libero e alla cura del proprio benessere da chi lavorava a tempo pieno variava da circa 14 a 16,5 ore al giorno. Gli uomini che lavorano a tempo pieno impiegavano 30 minuti in meno in tempo libero rispetto alle donne. Tuttavia, le statistiche sono diverse per il lavoro a distanza, che si è diffuso durante il blocco causato dalla pandemia COVID-19. Il tempo trascorso davanti al computer è aumentato in modo significativo (fino a due ore in più al giorno) e la qualità del riposo è diminuita. I lavoratori che svolgono le loro

mansioni da casa sono più propensi ad accettare di fare gli straordinari e di svolgere le mansioni la sera o nei fine settimana, rendendo così meno netta la linea di demarcazione tra vita privata e professionale.

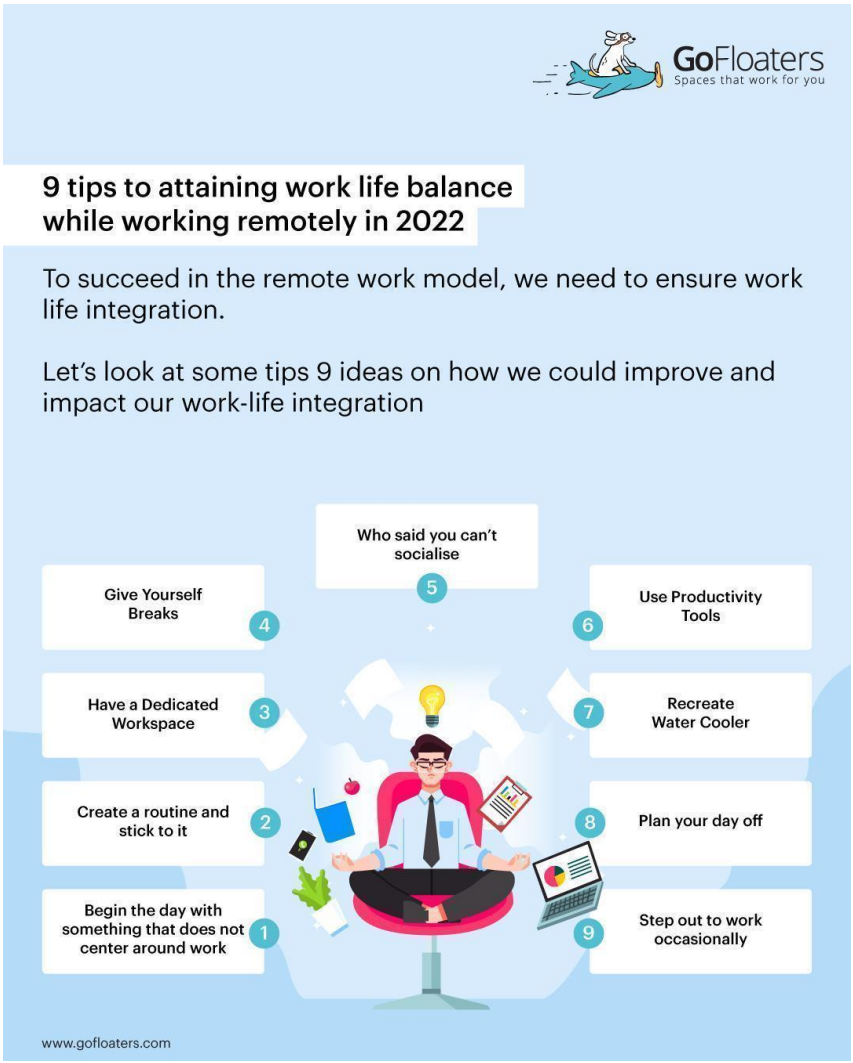
Eppure mantenere questo equilibrio è estremamente importante. Evita il *burnout* professionale, promuove una maggiore motivazione dei dipendenti e il loro impegno nei confronti dell'azienda. Contribuisce inoltre allo sviluppo personale e a una maggiore apertura a nuove sfide. In questo modo, nonostante il minor numero di ore lavorate, aumenta la produttività del personale e si riduce la necessità di cure mediche e di assenze per malattia.

Come possono i datori di lavoro migliorare l'*equilibrio tra lavoro e vita privata dei* loro dipendenti?

L'equilibrio tra lavoro e vita privata dei dipendenti dipende non di rado dai datori di lavoro e dai dirigenti. Sono loro che promuovono comportamenti specifici e a definire le politiche sul posto di lavoro. È quindi importante che sostengano le buone abitudini che consentono ai dipendenti di prendersi una pausa dalle responsabilità lavorative quotidiane. Ad esempio, i datori di lavoro possono incoraggiare i loro dipendenti a fare delle pause sul lavoro, a lavorare in orari flessibili e comodi per loro, a **esercitare il** loro diritto alla disconnessione, a comunicare chiaramente le loro esigenze (ad esempio, comunicando che sono sovraccarichi di responsabilità e hanno bisogno di rallentare).

È inoltre importante promuovere una cultura del lavoro sana, evitando il bonus di essere sempre disponibili o introducendo una politica di non rispondere a e-mail e messaggi dopo l'orario di lavoro. È anche una buona idea fornire ai dipendenti una formazione sull'*equilibrio tra lavoro e vita privata* e sul diritto alla disconnessione, e dare loro consigli su come ridurre facilmente l'uso eccessivo degli strumenti digitali.

2.1.5. Sicurezza e igiene sul posto di lavoro digitale, ovvero come limitare la reperibilità continua in modo autonomo



Suggerimenti per i dipendenti

1. **Disattivare le notifiche sul telefono**

Se il vostro telefono privato è dotato di messaggistica istantanea e di applicazioni utilizzate al lavoro o la casella di posta elettronica del lavoro è collegata a quella privata, disattivate tutte le notifiche che potrebbero disturbarvi durante il tempo libero. Può anche essere una buona idea impostare dei limiti di tempo per disattivare i messaggi dopo l'orario di lavoro standard.

2. **Utilizzare un computer aziendale durante il lavoro e un computer privato dopo l'orario di lavoro.**

Scegliere un computer aziendale piuttosto che un dispositivo privato per il lavoro è preferibile non solo per questioni di sicurezza informatica, ma anche per la possibilità di limitare l'esposizione ai messaggi e alle comunicazioni ricevute dai colleghi dopo l'orario di lavoro. Se la vostra azienda ha una politica BYOD (*bring your own device*), potete creare due account

(professionale e privato) sul vostro dispositivo e passare da uno all'altro a seconda del momento della giornata e delle vostre esigenze.

3. Mattina e sera analogiche

Le radiazioni di un telefono o di un computer portatile sono simili alla luce del sole e riducono la secrezione di melatonina nel cervello. Ciò rende più difficile addormentarsi, riduce la qualità del riposo e porta a ulteriori problemi di sonno. Per il vostro benessere, cercate di non utilizzare il telefono e il computer portatile almeno un'ora prima di andare a letto. Inoltre, non iniziate la mattina controllando nervosamente la casella di posta elettronica o i social media.

4. Indicare l'arco di tempo in cui si utilizzano gli strumenti digitali

Anche se lavorate con orari flessibili, informate i vostri supervisori e le persone con cui lavorate sugli orari ai quali potete essere contattati e quando la vostra disponibilità è limitata.

5. Introdurre un giorno intero di *digital detox*

Anche se la disintossicazione digitale non è un principio centrale dell'idea di *equilibrio tra lavoro e vita privata*, staccare completamente la spina dal web e dai social media per un periodo di tempo prolungato può avere enormi benefici per il benessere di un individuo. L'esperienza di staccare la spina dall'elettronica ci rende più consapevoli di quanto tempo effettivamente trascorriamo online. Ci aiuta a stabilire dei confini sani tra lavoro e vita privata. Inoltre, ci motiva a eliminare le cattive abitudini, come controllare compulsivamente la casella di posta elettronica o prendere il telefono appena svegli. Per questo motivo, si consiglia di attuare una disintossicazione ciclica (ad esempio, staccando completamente la spina nei fine settimana) e di dedicare il tempo libero al relax, agli incontri con la famiglia e gli amici o all'attività fisica piuttosto che alla navigazione sui social media.

2.2 Mercificazione obbligatoria e facoltativa delle risorse private

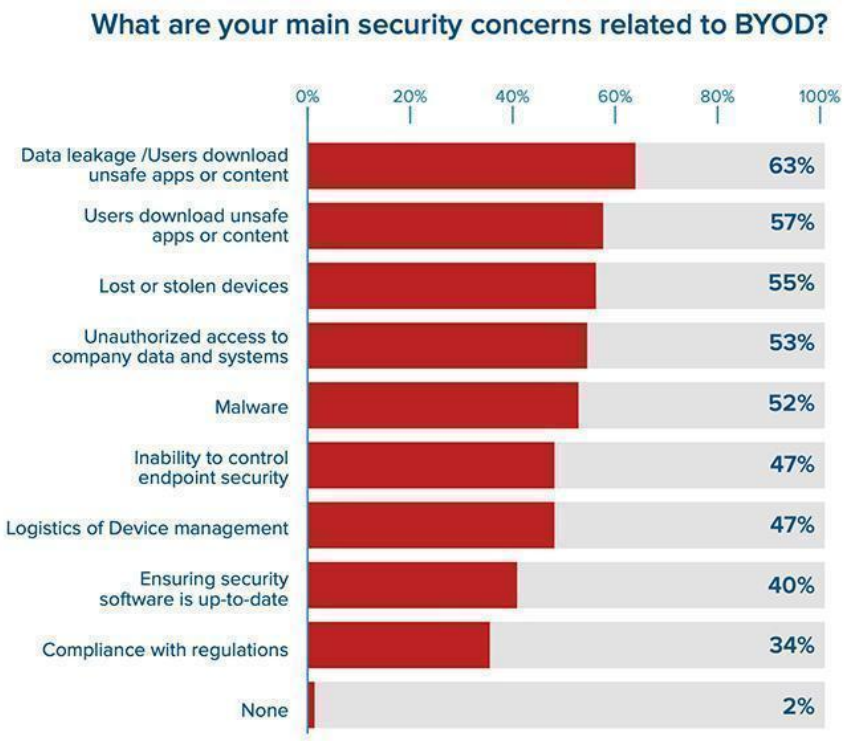
2.2.1. Che cos'è la politica BYOD (bring your own device)?

L'espressione *"bring your own device"* è nota anche con l'acronimo BYOD. Si tratta della tendenza a utilizzare dispositivi privati come laptop, smartphone o tablet per le mansioni lavorative. Questa tendenza è spesso il risultato della volontà dei dipendenti stessi (mercificazione volontaria di risorse private). Talvolta, tuttavia, le politiche BYOD sono preferite anche dai datori di lavoro (mercificazione forzata di risorse private). Sebbene questa tendenza presenti molti vantaggi, prima di implementarla in un'azienda è necessario considerare i rischi potenziali, come i problemi di sicurezza e di privacy.

Vale la pena di ricordare che il BYOD è l'esatto contrario dello stile di lavoro tradizionale, definito *"here's your own device"* (HYOD), in cui le aziende forniscono ai propri dipendenti i dispositivi elettronici di cui hanno bisogno per lavorare.

Vantaggi di una politica BYOD:

- **Flessibilità** - Il BYOD prevede che il datore di lavoro accetti di accedere ai documenti aziendali sui dispositivi privati del dipendente. In questo modo, lo svolgimento delle mansioni professionali diventa possibile ovunque e in qualsiasi momento. Inoltre, una maggiore flessibilità si manifesta nella possibilità di testare nuove soluzioni, software e strumenti digitali, poiché i dipendenti non sono limitati a utilizzare un solo tipo o marca di dispositivo.
- **Comfort**: uno dei vantaggi di una politica BYOD è che i dipendenti possono utilizzare dispositivi che conoscono bene e con cui si sentono a proprio agio.
- **Aumento della produttività** - l'uso del proprio computer portatile o smartphone può facilitare il processo di inserimento dei nuovi assunti, oltre ad aumentare la produttività dei dipendenti fissi.
- **Riduzione dei costi (vantaggio per il datore di lavoro)**: accettando una politica BYOD, i datori di lavoro spesso si sottraggono all'obbligo di fornire al dipendente le attrezzature di lavoro, evitando così costi aggiuntivi.
- **Decentramento dei dati (vantaggio per il datore di lavoro)**: tenere i documenti aziendali su un computer portatile privato (purché ben protetto) può essere vantaggioso per l'azienda grazie al maggior livello di decentramento dei dati. In caso di fuga di dati o di attacco malware al sistema aziendale, i file sui dispositivi dei dipendenti non saranno intercettati insieme al database centrale dell'azienda.



Fonte: helpnetsecurity.com, L'*adozione del BYOD sta crescendo rapidamente, ma la sicurezza è in ritardo*, https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/.

Svantaggi delle politiche BYOD:

- **Cyber(in)security** - oltre al vantaggio della decentralizzazione dei dati, i problemi di cyber security sono il più grande svantaggio delle politiche BYOD. Quando utilizzano dispositivi privati, i dipendenti tendono a conservare documenti riservati sulle loro unità, che tendono a essere meno sicure di quelle aziendali. Inoltre, quando lavorano in remoto da luoghi pubblici (ad esempio bar, biblioteche, mezzi di trasporto), spesso si collegano alla rete di qualcun altro, aumentando così la probabilità che i computer vengano violati e che vengano installati malware. Inoltre, c'è il rischio che il dispositivo di un dipendente venga rubato o perso.
- **Incompatibilità** - la flessibilità nella scelta degli strumenti di lavoro può tradursi in problemi di compatibilità con i sistemi utilizzati di default in azienda. Così, nel caso del BYOD, possono sorgere problemi dovuti all'incompatibilità dei formati e alla difficoltà di utilizzo dei documenti aziendali (ad esempio, a causa del diverso salvataggio dei file nel caso di Windows rispetto a macOS).
- **Recupero dei dati** - Le politiche BYOD possono causare problemi di recupero dei dati memorizzati sul dispositivo di un dipendente al termine del rapporto di lavoro. Questo perché i dipendenti hanno il pieno controllo dei loro dispositivi e possono smaltire autonomamente i file in essi memorizzati.

Diritti e obblighi BYOD

Se il lavoro viene svolto su attrezzature di proprietà privata, è necessario che queste soddisfino i requisiti di salute e sicurezza. Tuttavia, l'assicurazione di tali attrezzature non è obbligatoria: il dipendente e il datore di lavoro possono concordare la portata dell'assicurazione e le regole per l'utilizzo da parte del dipendente delle attrezzature necessarie per il lavoro e di sua proprietà.

Esempio della Polonia - Modifica del Codice del lavoro e nuove norme sul lavoro a distanza

Vale la pena notare che un dipendente con un contratto di lavoro ha il diritto di richiedere un computer aziendale e il datore di lavoro è obbligato a fornirglielo. Tuttavia, se per lo svolgimento del lavoro si utilizzano apparecchiature private, il dipendente ha diritto a un'indennità in denaro. Inoltre, il datore di lavoro deve coprire i costi dell'elettricità e dei servizi di telecomunicazione necessari per il lavoro a distanza. Il rimborso può essere in valore reale o sotto forma di somma forfettaria concordata tra le parti. Nel determinare l'importo dell'indennità e della somma forfettaria, il datore di lavoro deve tenere conto dei prezzi dei materiali e delle attrezzature, nonché dell'elettricità e dei servizi di telecomunicazione[9] .

A condizione che il lavoro venga svolto a domicilio, il datore di lavoro deve adempiere agli obblighi di salute e sicurezza nei confronti del lavoratore, ad eccezione di:

- dovere di curare le condizioni di sicurezza e igiene dei locali di lavoro,
- obblighi relativi alla costruzione o alla modifica dell'edificio in cui si trovano i locali di lavoro,
- obbligo di fornire strutture igieniche e sanitarie adeguate.

Tali obblighi del datore di lavoro di fornire condizioni di lavoro adeguate ai propri dipendenti hanno anche un impatto sulle questioni relative alla portata del termine "infortunio sul lavoro" e alla sicurezza sociale. Un lavoratore che subisce un infortunio sul lavoro, a prescindere dal luogo in cui svolge le proprie mansioni - a distanza o sul posto di lavoro - ha diritto alle **prestazioni di sicurezza sociale.**

[9] *Legge del 1° dicembre 2022 che modifica il Codice del lavoro e alcune altre leggi* (GU del 2022, voce 240).

Prima di essere autorizzato a lavorare a distanza, il dipendente conferma in una dichiarazione (presentata in forma cartacea o elettronica) di aver letto la valutazione dei rischi e le informazioni del datore di lavoro contenenti i principi del lavoro a distanza sano e sicuro e si impegna a rispettarli.

La valutazione dei rischi professionali deve tenere in particolare considerazione gli effetti del lavoro a distanza sulla vista e sull'apparato muscolo-scheletrico del lavoratore. Vengono prese in considerazione anche le condizioni psicosociali del lavoro in questione. Sulla base dei risultati della valutazione, il datore di lavoro elabora informazioni contenenti principi e modalità di organizzazione adeguata del luogo di lavoro a distanza. Questi devono tenere conto dei requisiti di ergonomia, dell'esecuzione sicura e igienica del lavoro a distanza, delle attività da svolgere al termine del lavoro a distanza, nonché delle regole per affrontare le situazioni di emergenza che rappresentano un rischio per la vita o la salute umana. Il datore di lavoro può anche redigere una valutazione universale dei rischi per gruppi specifici di posizioni di lavoro a distanza.

2.3 Tutela dei dati personali e sicurezza delle persone che lavorano on-line

2.3.1. Lavoro a distanza

A causa della crescente popolarità del lavoro a distanza ibrido o a tempo pieno, i legislatori di molti Stati membri hanno deciso di modificare di conseguenza il proprio diritto del lavoro. In particolare, è stato necessario adattare gli obblighi del lavoratore e del datore di lavoro alle nuove forme di lavoro. Questi obblighi derivano dalla necessità di garantire che l'infrastruttura informatica o lo spazio di lavoro presso il sito di lavoro remoto siano adeguati a soddisfare i requisiti di salute e sicurezza.

Lavoro a distanza e diritto del lavoro: l'esempio della Polonia

1. **Strumenti per il lavoro a distanza**

Secondo la proposta di modifica del Codice del lavoro, articolo 67 (24) § 1, il datore di lavoro è obbligato a fornire il lavoro a distanza al dipendente:

- **Materiali e strumenti di lavoro** - comprende l'attrezzatura tecnica necessaria per il lavoro a distanza (a seconda delle specificità del lavoro, a parte il computer, si possono includere i seguenti elementi ad esempio, cuffie adatte per le riunioni online, microfono, ecc.)
- **Installazione, assistenza e manutenzione degli strumenti di lavoro**, comprese le attrezzature tecniche, necessarie per il lavoro a distanza. In alternativa, il datore di lavoro può anche coprire i costi necessari per questi servizi.

- **Formazione e assistenza tecnica** necessarie per svolgere il lavoro a distanza.
- **Copertura dei costi dell'elettricità** - il datore di lavoro è tenuto a coprire anche i costi dell'energia e dei servizi di telecomunicazione necessari per il lavoro a distanza.

Un accordo tra il datore di lavoro e l'organizzazione sindacale aziendale o il regolamento del lavoro può obbligare il datore di lavoro a coprire altri costi direttamente connessi all'esecuzione del lavoro a distanza.

2. Disposizione dello spazio nel lavoro a distanza - controllo del datore di lavoro

Il dipendente è tenuto a organizzare la propria postazione di lavoro a distanza tenendo conto dei requisiti ergonomici. Ciò include, tra l'altro, la scelta di una sedia comoda, una scrivania di altezza adeguata, il posizionamento corretto del monitor rispetto agli occhi e un'illuminazione adeguata.

A condizione che il lavoro venga svolto presso il domicilio del lavoratore, il datore di lavoro deve adempiere ai doveri di salute e sicurezza nei confronti del lavoratore, ad eccezione di:

- dovere di curare le condizioni di sicurezza e igiene dei locali di lavoro,
- obbligo di cui al capitolo III della sezione 10 del Codice del lavoro (norme sulle strutture edilizie e sui locali di lavoro),
- obbligo di fornire strutture igieniche e sanitarie adeguate.

Tali obblighi del datore di lavoro di fornire condizioni di lavoro adeguate ai propri dipendenti hanno anche un impatto sulle questioni relative alla portata del termine "infortunio sul lavoro" e all'assicurazione sociale. Un dipendente che subisce un infortunio sul lavoro, indipendentemente dal luogo in cui svolge le proprie mansioni (a distanza o sul posto di lavoro), ha diritto alle **prestazioni di sicurezza sociale.**

Visti gli obblighi del datore di lavoro in materia di:

- applicazione di misure adeguate per prevenire gli infortuni nel lavoro a distanza,
- adozione le misure necessarie per eliminare o ridurre il rischio che si verifichi tale incidente,
- prestazione di primo soccorso alle persone infortunate e le circostanze e le cause dell'infortunio in conformità all'accordo stipulato con l'organizzazione sindacale dell'azienda o nei regolamenti;

i**l datore di lavoro ha il diritto di effettuare un'ispezione per quanto riguarda**:

- salute e sicurezza sul lavoro,
- **rispetto della sicurezza e della protezione delle informazioni**, comprese le procedure per la protezione dei dati personali.

Secondo le nuove norme del Codice del Lavoro, un datore di lavoro potrà introdurre controlli di sobrietà per i dipendenti solo se ciò è necessario per garantire la protezione della vita e della salute dei dipendenti, di altre persone o la protezione dei beni.

Ogni controllo di sobrietà dovrebbe essere:

- effettuato in consultazione con il dipendente,
- svolto presso la sede di lavoro remota e durante l'orario di lavoro del dipendente,
- adattato al luogo e al tipo di lavoro a distanza,
- di non ostacolo all'uso dei locali domestici in modo coerente con la loro destinazione d'uso,
- in caso di lavoro occasionale a distanza, i controlli di sobrietà devono essere effettuati su base concordata con il dipendente,
- nel rispetto della privacy del dipendente e degli altri (ad esempio, altri membri della famiglia o inquilini).

Se durante un'ispezione il datore di lavoro riscontra carenze in materia di salute e sicurezza, e sicurezza e protezione delle informazioni, compresa la protezione dei dati, ha due possibilità. Può dare al dipendente un termine per correggere le carenze o ritirare il consenso a svolgere il lavoro a distanza.

3. Protezione dei dati personali nel lavoro a distanza secondo le modifiche al Codice del Lavoro

Dato l'aumento del rischio di fuga di dati personali e di altre violazioni in questo settore, il datore di lavoro deve stabilire delle procedure per la protezione dei dati personali. All'interno dell'organizzazione dovrà essere fornita una formazione adeguata. Un dipendente che svolge un lavoro a distanza, d'altra parte, dovrebbe confermare di aver familiarizzato con gli standard stabiliti dal datore di lavoro in forma scritta o elettronica.

Sia il dipendente che il datore di lavoro devono anche stabilire come e con quali strumenti comunicheranno a distanza e trasmetteranno le informazioni relative allo svolgimento del lavoro.

2.3.2. Come applicare il GDPR per la difesa dei dati personali nel caso del lavoro a distanza?

L'aumento della popolarità del lavoro a distanza ha aumentato il rischio di fuga di informazioni aziendali sensibili. Questo perché può essere difficile, sia per il dipendente che per il datore di lavoro, stabilire con esattezza in quali condizioni siano state violate le norme sulla protezione delle informazioni, sulla sicurezza e sulla protezione dei dati. Dato che il lavoro a distanza (almeno in parte) è destinato a rimanere tra noi per molto tempo, è necessario ricordare le norme sulla protezione dei dati più frequentemente violate. Vale anche la pena di esaminare i rischi in agguato per chi lavora a distanza e come mitigare il rischio che si verifichino.

RICORDA!

Ai sensi dell'articolo 32 del Regolamento GDPR, il datore di lavoro, in qualità di responsabile del trattamento dei vostri dati personali, deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al grado di rischio di violazione dei diritti o delle libertà delle persone fisiche di varia probabilità e gravità.

A tal fine, il datore di lavoro può intraprendere le seguenti azioni:

(a) pseudonimizzare e crittografare i dati personali,

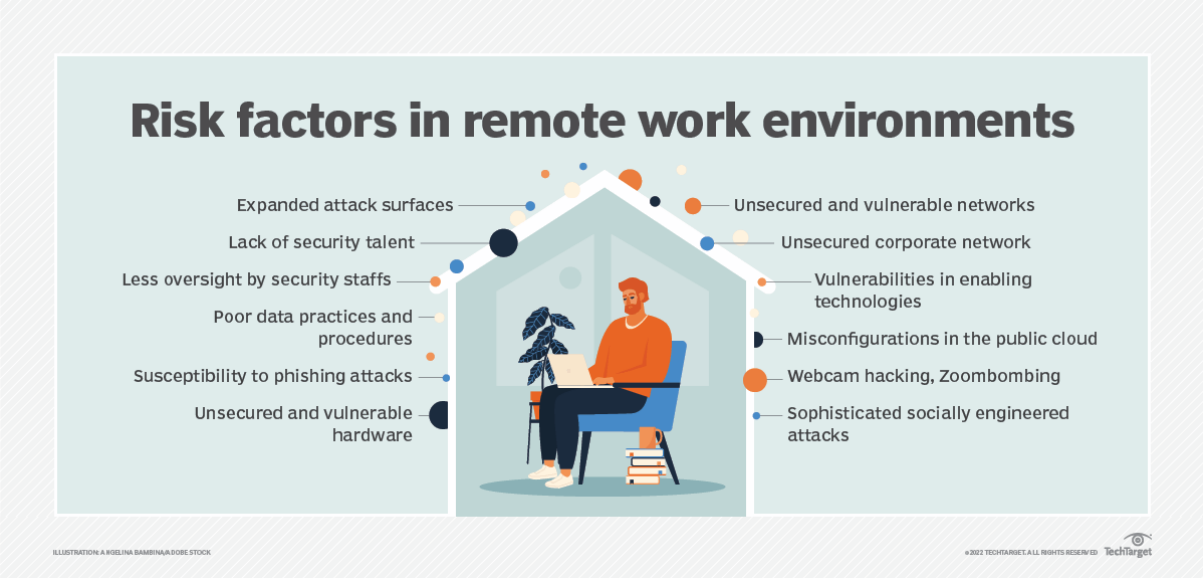
(b) garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione dati,

(c) garantire che la disponibilità e l'accesso ai dati personali possano essere ripristinati rapidamente in caso di incidente fisico o tecnico,

(d) garantire che l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento dei dati personali possa essere testata, misurata e valutata regolarmente.

Come spiegato dalla Commissione europea, i dipendenti che elaborano i dati nell'ambito del loro lavoro all'interno dell'organizzazione svolgono i compiti di un responsabile del trattamento dei dati. In quanto tali, anch'essi hanno la responsabilità di garantire la sicurezza dei dati personali.

2.3.3. Minacce online e lavoro a distanza



Sebbene la sicurezza informatica sia una delle sfide più importanti che le istituzioni statali si trovino ad affrontare oggi, la consapevolezza del pubblico al riguardo rimane limitata. Quasi tutti hanno sentito parlare di sicurezza informatica e della sua importanza, ma il comportamento dei cittadini non sempre riflette un alto livello di conoscenza dell'argomento. Secondo un sondaggio del sito web polacco ChronPESEL.pl e del Registro nazionale dei debiti condotto nel 2022, un polacco su tre teme la fuga di dati personali, ma meno della metà degli intervistati saprebbe cosa fare in una situazione del genere.

Sebbene sia impossibile garantire la protezione dei dati e la sicurezza delle informazioni al 100%, esistono una serie di misure preventive che possono ridurre adeguatamente il rischio di fuga di dati e altri pericoli.

Le minacce che si nascondono nell'ambiente di lavoro remoto non sono molto diverse da quelle di cui ogni utente di Internet dovrebbe diffidare. Il loro obiettivo è molto spesso quello di rubare informazioni protette o dati relativi a una persona o a un'azienda specifica, consentendo all'aggressore di ottenere un vantaggio finanziario, un vantaggio competitivo o altri scopi. Secondo un rapporto dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA), le minacce informatiche più comuni e pericolose sono:

1. **Software malevoli** (*malware*) - è un codice o un'applicazione dannosa che ostacola o impedisce completamente il normale utilizzo di un dispositivo finale (ad esempio, un computer o una stampante). Infettando il dispositivo in questione con il malware, i criminali possono ottenere l'accesso ai dati o ad altre funzioni del dispositivo. Possono

anche puntare a bloccare completamente il dispositivo, a patto che venga pagato un riscatto dall'utente o da un'altra persona parzialmente colpita dall'attacco.

2. ***Ransomware*** - un tipo di malware con il quale un criminale blocca l'accesso degli utenti ai propri sistemi o ai propri file personali, chiedendo poi un compenso in cambio del loro ripristino.
3. **Attacchi attraverso siti web** - un metodo con cui gli hacker ingannano le vittime dei loro attacchi utilizzando i sistemi e i servizi Internet come canale per preparare e portare a termine un attacco. In particolare, si distingue la fornitura o l'agevolazione di URL o script dannosi per indirizzare l'utente verso un sito web desiderato o scaricare contenuti dannosi. Il risultato è l'attuazione di codice maligno su un vero sito web esistente al fine di rubare informazioni e ottenere vantaggi finanziari.
4. ***Phishing*** **-** come per altri attacchi informatici, l'obiettivo dei criminali informatici è quello di ottenere informazioni preziose, principalmente login, password, codici fiscali o numeri di carte di credito. Il nome deriva dal fatto che i criminali utilizzano un'esca personalizzata per la persona specifica di cui vogliono rubare i dati. A tal fine, di solito utilizzano e-mail o SMS falsi, nonché canali di comunicazione sui social network. Per creare fiducia, i criminali informatici si spacciano per società di telecomunicazioni, servizi di corriere, banche, siti di aste e persino agenzie governative. Facendo leva sulle emozioni della vittima, cercano di convincerla a cliccare su un link che hanno preparato per raggiungere un sito web che, sebbene simile a quello autentico, è stato creato dal criminale e rappresenta il suo canale per commettere frodi.
5. **DDoS** - (*distributed denial of service*) è un tipo di attacco che prende di mira servizi di rete o sistemi informatici. Il loro compito è quello di sequestrare tutte le risorse disponibili e libere per impedire all'intero servizio di funzionare su Internet. L'attacco può colpire il sito web di un'azienda, la posta elettronica di un dipendente, ecc. Viene effettuato da diversi dispositivi informatici contemporaneamente, soprattutto da quelli su cui è stato preso il controllo tramite virus speciali - bot o trojan. Il pericolo di questo tipo di attacco è che l'utente dell'apparecchiatura in questione possa non rendersi conto che il suo computer viene utilizzato per effettuare un DDoS.
6. **Furto d'identità** - utilizzando il numero codice fiscale, i dati personali o la carta d'identità di una persona, un criminale si spaccia per tale persona al fine di ottenere, ad esempio, un credito o utilizzare in altro modo la sua identità a proprio vantaggio.
7. **Violazione della sicurezza dei dati** - è un tipo di incidente di sicurezza informatica in cui si accede alle informazioni (o a parte di un sistema informativo) senza un'autorizzazione adeguata, di solito con intento malevolo. Ciò comporta la potenziale perdita o l'uso improprio di tali informazioni. Il motivo per cui si verifica questo tipo di minaccia è spesso dovuto al cosiddetto errore umano, che può verificarsi durante la configurazione e

l'implementazione di alcuni servizi e sistemi, con conseguente esposizione involontaria dei dati.

8. **Perdita di informazioni**: una conseguenza comune delle violazioni della sicurezza dei dati, che riguarda un'ampia gamma di informazioni a rischio, dalle informazioni di identificazione personale (IIP) ai dati finanziari memorizzati nell'infrastruttura IT, fino ai dati sanitari personali memorizzati negli archivi dei fornitori di servizi sanitari.
9. **Minaccia interna** (abuso di potere) - è un'azione intrapresa da un individuo o da un gruppo di individui legati alla vittima di un attacco da un rapporto professionale o di altro tipo, in cui sia l'aggressore che la vittima si trovano sulla stessa rete o infrastruttura o hanno la possibilità di ottenere informazioni grazie all'interconnessione. Esistono diversi modelli associati a questi tipi di minacce. Possono verificarsi anche quando gli esterni collaborano con gli interni per ottenere un accesso non autorizzato alle risorse. Gli insider possono anche causare danni inavvertitamente per disattenzione o mancanza di conoscenza. Poiché gli insider godono spesso della fiducia dei colleghi e conoscono i processi e le procedure dell'organizzazione, può essere difficile distinguere tra l'accesso legittimo a dati e sistemi e le azioni in malafede.
10. **Botnet** - una rete di dispositivi interconnessi infettati da malware bot. Sono tipicamente utilizzate per lanciare attacchi DDoS. Le reti bot possono essere controllate da remoto da un criminale per agire in modo sincronizzato e ottenere un risultato specifico.

2.3.4. Igiene informatica: come difendersi in rete ogni giorno?

1. **Se potete, lavorate in uno spazio sicuro e privato.**

La fuga di dati può avvenire non solo in seguito a un attacco di hacking, ma anche attraverso metodi meno sofisticati e convenzionali, come ad esempio uno screen shot (fotografia dello schermo con lo stesso dispositivo). Va da sé che, a parte uno spazio di lavoro predisposto dal datore di lavoro, lo spazio più sicuro per il lavoro a distanza sembra essere il proprio spazio di lavoro domestico. L'ideale sarebbe una stanza chiusa a chiave dove potersi separare tranquillamente dal resto della famiglia.

Se non è possibile lavorare in una stanza isolata (ad esempio, durante un viaggio di lavoro), la questione della sicurezza si complica notevolmente. In particolare, fate attenzione agli spazi aperti (bar, treni, aeroporti) dove le persone intorno a voi sono costantemente nel vostro ambiente e cambiano in continuazione. Inoltre, in molti luoghi di questo tipo sono installate telecamere a circuito chiuso, che possono registrare non solo le azioni di chi si trova nel suo

raggio d'azione, ma anche ogni sorta di altro elemento dell'ambiente, compresi gli schermi dei computer.

Soluzione: dotarsi di un filtro/copertura per la privacy

Con questo strumento, il contenuto dello schermo è visibile solo alla persona che utilizza il computer/telefono. La tecnologia funziona in modo simile alle micro-tende: il filtro è costituito da canali microscopici rivolti verso la persona che utilizza lo schermo del monitor. Chi guarda lo schermo da un'angolazione diversa non vedrà lo stesso contenuto.

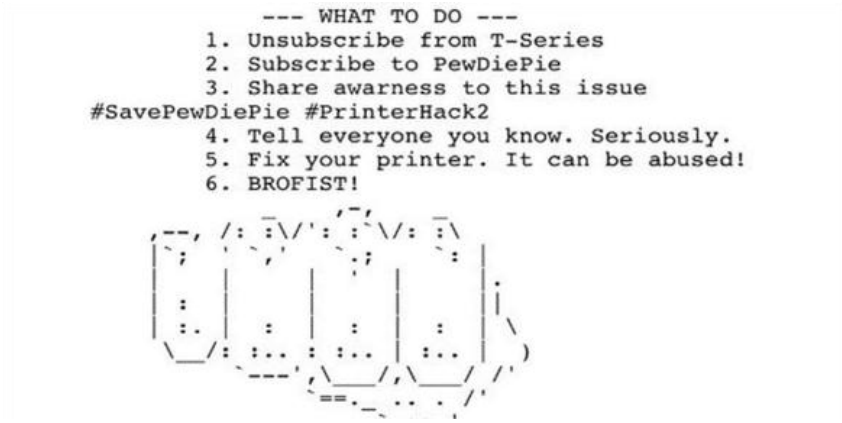
2. **Conservare i documenti in un'area sicura e chiudibile a chiave presso la sede di lavoro remota.**

La cosiddetta politica della scrivania pulita o dello schermo pulito, in vigore in molti luoghi di lavoro, dovrebbe essere applicata anche alla sede di lavoro remota. Anche se abbiamo fiducia nei membri della famiglia o nei coinquilini, nessun documento contenente informazioni personali dovrebbe essere lasciato in nostra assenza. Inoltre, non bisogna tenere in bella vista le password dei dispositivi di lavoro.

Soluzione: attrezzate il vostro spazio di lavoro remoto con un cassetto o un armadietto chiudibile a chiave.

Questo sarà il luogo in cui potrete riporre in modo sicuro tutti i vostri materiali durante il lavoro. Se possibile, tenete la chiave sempre con voi o nascondetela in un posto che conoscete solo voi.

3. **Se non è necessario, non stampate documenti a casa o nei punti di fotocopiatura pubblici.**



Da tempo gli esperti di cybersecurity avvertono che il dispositivo più trascurato in termini di necessità di implementare una sicurezza adeguata è... la stampante. Secondo una ricerca di InfoSecurity Magazine, circa il 66% dei lavoratori remoti intervistati ha stampato una media di cinque documenti a settimana. Un quarto di loro non ha ancora smaltito i documenti stampati, spiegando che intende riportarli in ufficio. Solo il 24% utilizza un distruggidocumenti domestico, ma ammette anche di gettare i documenti nel cestino di casa. Il 12% degli intervistati dichiara inoltre di non essere a conoscenza della normativa GDPR.

Le stampanti di oggi assomigliano sempre di più a computer piuttosto che a semplici dispositivi monouso: spesso fanno parte dell'*Internet delle cose (*IoT) e sono strumenti di lavoro multifunzionali. Uno degli attacchi di più alto profilo alle stampanti domestiche, che ha messo in luce il problema dell'inadeguatezza della sicurezza di questi dispositivi, è stato quello legato al noto youtuber PewDiePie. Nel 2018, un hacker (o un gruppo di molti fan di PewDiePie) ha attaccato decine di migliaia di stampanti in tutto il mondo. Senza alcuna interferenza da parte dei proprietari, i dispositivi hanno iniziato a stampare una brochure che promuoveva i contenuti pubblicati da PewDiePie e a incoraggiare il sostegno alle sue attività.

Le stampanti odierne, sempre più sofisticate, dispongono di una *cache* in cui i documenti vengono stampati. Le stampanti moderne funzionano anche in modalità wireless, il che significa che chiunque abbia i driver giusti sul proprio computer e l'accesso alla rete in cui si trova la stampante può collegarsi ad essa.
Se un hacker prende il controllo della stampante (ad esempio in un'azienda), può accedere sia ai documenti già stampati sia ad altre risorse memorizzate sul computer o persino alle password dei dispositivi che hanno utilizzato i servizi della stampante.

Soluzione: stampate i documenti solo sul posto di lavoro e, se dovete farlo a casa, assicuratevi che le vostre apparecchiature siano protette adeguatamente.

A tal fine è possibile impostare una password sicura per il wi-fi della stampante (se possibile). Se i documenti stampati non vi servono più, non gettateli nel cestino di casa, ma portateli in

azienda dove dovrebbe esserci un distruggidocumenti. Se questo non è possibile, chiedete al vostro datore di lavoro o all'ufficio risorse umane quali sono le procedure di distruzione dei documenti dell'azienda.

4. Sovrapposizione della webcam

Lavorare da casa significa di solito partecipare a teleconferenze e videochiamate che richiedono l'uso di una webcam. Purtroppo, gli hacker possono facilmente accedere alla vostra webcam, compromettendo la vostra privacy. Inoltre, se sul posto di lavoro fisico sono presenti documenti riservati che possono essere catturati da una webcam, i criminali potranno accedervi.

Soluzione: limitare la visualizzazione agli elementi contenenti dati personali

Quando la webcam è accesa, la possibilità di visualizzare oggetti contenenti informazioni personali nelle vicinanze deve essere limitata. Inoltre, se la webcam è separata dal dispositivo, deve essere scollegata quando non viene utilizzata. Se la webcam è incorporata, è opportuno adottare ulteriori misure di protezione, come ad esempio un cappuccio per la fotocamera. Nei negozi si trovano facilmente copri webcam scorrevoli di vari tipi. Di solito sono facili da installare, in quanto la maggior parte di esse è dotata di uno strato adesivo che aderisce alla telecamera. Utilizzando software e applicazioni per videoconferenze, è possibile utilizzare anche funzioni come la **sfocatura dello sfondo**.

5. Partecipare attivamente alla formazione aziendale sulla sicurezza informatica e alle modifiche della politica del datore di lavoro in materia di protezione dei dati e delle informazioni.

Secondo il GDPR, se vengono emanate nuove procedure di protezione dei dati in azienda, il datore di lavoro deve consentire ai propri dipendenti di familiarizzare con esse prima di applicarle.

Se il datore di lavoro non ha fornito una formazione adeguata sull'uso dei dispositivi, sull'uso degli strumenti di comunicazione interna ed esterna o sui principi di base relativi alla protezione dei dati in azienda, il dipendente ha il diritto di chiedergliela. Se, anche dopo la formazione, il dipendente non è ancora sicuro delle procedure da seguire in una determinata situazione, deve segnalarlo al proprio datore di lavoro o alla persona designata all'interno dell'azienda responsabile della gestione informatica, del reparto risorse umane, ecc.

Igiene informatica quando si lavora da remoto

Cos'altro potete fare per proteggere il vostro computer?

Crittografia dei dati personali

Soprattutto se si tratta di dati sensibili o se li inviate all'esterno dell'organizzazione. Come già detto, i dipendenti che trattano i dati nell'ambito delle loro mansioni lavorative svolgono quindi i compiti del responsabile del trattamento dei dati, che è il datore di lavoro. In conformità con l'articolo 32 del GDPR, il responsabile del trattamento e l'incaricato del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza dei dati appropriato all'ambito, al contesto e alle finalità del trattamento e al rischio di interferenza con i diritti o le libertà delle persone fisiche. Il regolamento GDPR cita tra le misure di sicurezza la pseudonimizzazione e la cifratura dei dati personali.

Sebbene il GDPR non contenga requisiti espliciti sul metodo di sicurezza più efficace, il regolamento sottolinea ripetutamente che la **crittografia e la pseudonimizzazione** sono misure tecniche e organizzative adeguate per mantenere la sicurezza dei dati personali.

La crittografia mira a codificare un determinato contenuto in modo tale che possa essere compreso solo da un destinatario in possesso della chiave giusta. In termini più semplici, l'idea è, ad esempio, quella di trasformare una stringa di lettere in una stringa di altre lettere o numeri, di aggiungere altre stringhe di lettere o numeri e così via.

La pseudonimizzazione, invece, è il trattamento dei dati personali in modo tale che non sia possibile identificarne l'identità senza accedere alle informazioni, conservate in modo sicuro altrove. Si tratta quindi di mascherare i dati sostituendo le informazioni su una persona con identificatori immaginari.

Qual è la differenza tra i due metodi?

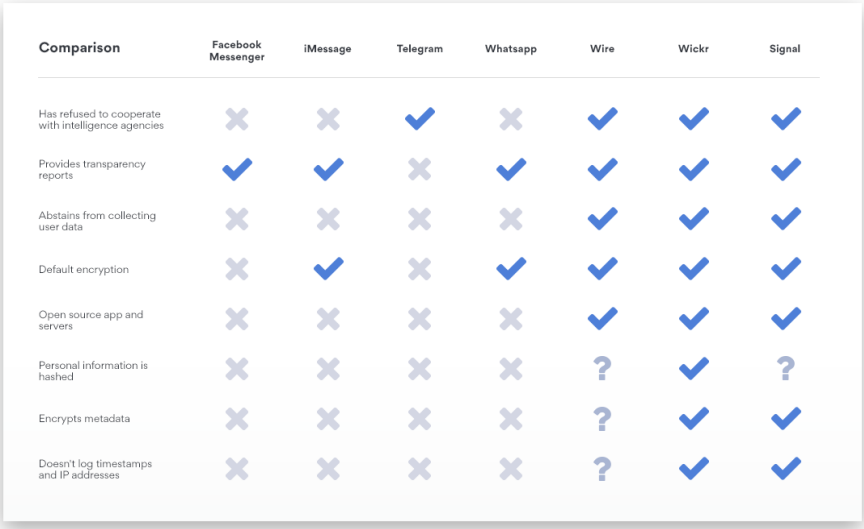
Come la pseudonimizzazione, la crittografia nasconde le informazioni sostituendo gli identificatori con qualcos'altro. Tuttavia, mentre la pseudonimizzazione consente a chiunque abbia accesso ai dati di vedere una parte del dataset, la crittografia permette solo agli utenti autorizzati di accedere all'intero dataset. La pseudonimizzazione e la crittografia possono essere utilizzate contemporaneamente o separatamente.

Metodi per proteggere/criptare i dati nelle comunicazioni interne e con l'esterno.

a. **Comunicazione interna: utilizzo di messaggistica criptata e piattaforme sicure.**

Sebbene l'e-mail rimanga ancora uno dei metodi di comunicazione aziendale più diffusi (316,9 miliardi di e-mail inviate e ricevute ogni giorno nel 2021 e si prevede che questo numero salirà a 376,4 miliardi entro il 2025), non è nemmeno il sistema più sicuro per lo scambio di informazioni riservate. A causa della sua elevata popolarità, l'e-mail è anche un importante canale per gli attacchi di hacking. Deloitte ha rilevato che il 91% di tutti gli attacchi informatici proviene da e-mail *di phishing*. Il costo di un attacco di questo tipo per le organizzazioni può essere molto elevato.

Per le comunicazioni interne, dove spesso vengono scambiate informazioni riservate sull'azienda, sui dipendenti o sui clienti, si possono utilizzare altri strumenti più sicuri.



Comparison	Facebook Messenger	iMessage	Telegram	Whatsapp	Wire	Wickr	Signal
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓
Open source app and servers	✗	✗	✗	✗	✓	✓	✓
Personal information is hashed	✗	✗	✗	✗	?	✓	?
Encrypts metadata	✗	✗	✗	✗	?	✓	✓
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	?	✓	✓

Whatsapp e Messenger: i messenger più popolari e le loro caratteristiche

1. **WhatsApp:**
   - utilizza la crittografia Signal,
   - la maggior parte delle persone in Europa probabilmente utilizzerà questa applicazione,
   - un'applicazione di facile utilizzo che offre funzionalità aggiuntive,
   - è di proprietà di Facebook,
   - in precedenza si sono verificate gravi violazioni della protezione dei dati nell'applicazione.
2. **Messenger:**

- ampia portata - grazie al collegamento con Facebook, la maggior parte delle persone possiede questo programma di messaggistica,
- può essere utilizzato anche dopo la disattivazione dell'account Facebook,
- la crittografia non è quella predefinita,
- il comunicatore non cripta le conversazioni passate,
- l'applicazione tiene traccia del comportamento dell'utente.

Le migliori applicazioni in termini di sicurezza dei dati:

1. **Signal:**
   - supporta chat di gruppo, SMS, messaggistica vocale e video e consente il trasferimento di documenti e foto,
   - offre messaggi che scompaiono (con un timer),
   - utilizza un protocollo di segnalazione - un protocollo crittografico non federato che può essere utilizzato per crittografare chiamate vocali e conversazioni di messaggistica istantanea, dove i messaggi in chiaro possono essere letti solo dai comunicanti,
   - software *open source* (cioè il cui codice sorgente è reso disponibile gratuitamente e può essere distribuito e modificato senza alcun pagamento),
   - non memorizza dati o metadati dell'utente,
   - promosso da Edward Snowden,
   - richiede un numero di telefono per la registrazione.

Piattaforme software e workspace sicure:

1. Microsoft Teams.
2. Google Workspace.
3. Slack.
4. Asana.
5. Trello.

b. Comunicazione esterna - crittografia di file contenenti dati personali ed elenchi di destinatari di posta elettronica

Si raccomanda che, ogni volta che i dati vengono trasferiti da una sede a un'altra, siano pseudonimizzati o criptati per proteggersi da eventuali fughe di notizie.

Conferimento dei dati personali nella mailing list

Utilizzare il campo UDW (hidden to message, BCC). Il campo UDW consente di inviare i messaggi in modo che i destinatari non vedano gli indirizzi degli altri. Questa opzione si trova in ogni e-mail.

Trasmissione di dati personali in file inviati per posta elettronica

Nei documenti inviati via e-mail possono essere nascosti molti dati personali o altre informazioni protette dalla legge, per cui è necessario proteggerli ulteriormente. I metodi di crittografia dei file possono variare a seconda del formato in cui sono archiviati. Tuttavia, tutti hanno un principio di base in comune: trasmettere la password del documento crittografato attraverso un mezzo di comunicazione diverso dalla posta elettronica.

Per criptare correttamente un file, i programmi più comunemente scelti sono **WinRAR** e **7-zip**. Con ciascuno di essi, dopo aver selezionato l'opzione "aggiungi all'archivio", si apre una finestra che consente, tra l'altro, di impostare una password per accedere al documento.

Eseguite regolarmente il backup dei vostri dati e memorizzateli su unità esterne.

Nel caso in cui l'hardware venga infettato da un virus o da altri eventi che possono portare alla cancellazione dei dati dal computer e all'impossibilità di ripristinarli, la soluzione migliore è quella di effettuare regolarmente dei backup.
cancellare i dati dal computer e non poterli ripristinare, la soluzione migliore è quella di effettuare regolarmente dei **backup.**

I backup, noti anche come copie di sicurezza, sono copie di informazioni che vengono archiviate in un luogo diverso dall'originale. Il primo passo da fare è decidere se si vuole fare un backup:

1. Dati specifici che sono importanti per qualche motivo.
2. L'intero sistema operativo.

La maggior parte degli strumenti di backup sono configurati di default per il primo scopo e copiano i dati in base ai documenti utilizzati più spesso. Se non si è sicuri di quali file copiare, si consiglia di archiviarli tutti.

Con quale frequenza effettuare i backup?

La risposta dipende dalle preferenze individuali e dalla frequenza dei cambi. Alcuni lo fanno ogni ora, altri una volta al giorno e altri ancora una volta alla settimana. Tuttavia, è consigliabile eseguire il backup dei documenti quotidianamente.

Come faccio a fare il backup dei miei documenti?

A seconda del sistema operativo del computer, esistono programmi consigliati che consentono di impostare un periodo ogni volta che viene eseguito automaticamente un backup. Tra questi vi sono Microsoft Windows Backup and Restore o Time Machine di Apple. Questi programmi funzionano sia quando il dispositivo è in uso sia quando è inattivo.

Dati su supporti esterni o dati nel cloud?

Preferibilmente entrambi. I supporti di memorizzazione esterni possono essere, tra l'altro, una chiavetta di memoria, un'unità esterna portatile o altri dispositivi a cui ci si può collegare tramite wi-fi. Il vantaggio di questi dispositivi è sicuramente quello di poter archiviare grandi quantità di dati in un periodo di tempo piuttosto breve. Purtroppo, trattandosi di un metodo di backup fisico, può subire gli stessi guasti o danni di un computer. Un backup su supporti esterni può essere rubato, perso, allagato, surriscaldato e così via. Inoltre, se il dispositivo da cui provengono i dati è stato precedentemente infettato da malware, c'è purtroppo il rischio che anche il supporto, e di conseguenza il backup stesso, venga infettato.

Il backup in cloud, invece, consiste nel collocare copie di documenti o altri file su Internet. Più precisamente, si tratta di collezioni di server e centri dati dispersi a livello globale in cui vengono archiviati i dati. Ciò avviene automaticamente, di solito tramite uno strumento predefinito di una piattaforma di elaborazione testi (ad esempio Google Docs), che crea un backup ogni periodo di tempo stabilito o dopo ogni modifica di un file. Un indubbio vantaggio dell'archiviazione di copie di file nel cloud è la loro permanenza e la possibilità di accedere al backup da qualsiasi altro dispositivo (a condizione, ovviamente, che si disponga della password dell'account all'interno del quale si trova il cloud). Tuttavia questa soluzione non è del tutto priva di inconvenienti: se si desidera eseguire rapidamente il backup di una grande quantità di dati, la soluzione può essere molto più lenta di un backup fisico su un'unità esterna. Inoltre, è possibile che il cloud esaurisca lo spazio per archiviare i nuovi dati e che si debba eliminare parte di essi o acquistare risorse aggiuntive dal provider cloud.

Accesso sicuro al computer, al telefono e persino alle riunioni online

Così come la crittografia dei dati stessi è necessaria per garantire la sicurezza dei dati personali, è estremamente importante che anche le apparecchiature che utilizziamo siano adeguatamente protette. L'uso di password o di altri tipi di crittografia garantisce che solo le persone autorizzate abbiano accesso a determinate risorse.

Esistono diversi metodi per fissare le apparecchiature:

- **Una password forte, cioè:**
    - **lunga** - contenente almeno otto caratteri (più lungo è, meglio è),
    - **complessa -** contenente almeno un carattere di ogni categoria: lettere maiuscole, lettere minuscole, caratteri speciali (ad es. !, ?), numeri,
    - **difficile da indovinare** - se volete scegliere una frase, una citazione o un modo di dire, assicuratevi che non sia direttamente collegata a voi, al vostro lavoro o al vostro ambiente; tuttavia, se sapete che non ricorderete la password senza facili associazioni - sostituite le parole con simboli o numeri appropriati della tastiera, ad esempio "Ala ha un gatto" **può essere** scritto come "4Lah@1g@tT0",
    - **diversa dalla password precedente per il dispositivo in questione** - se si cambia la password per un account esistente, non deve essere uguale a quella precedente; né si deve cambiare la password solo leggermente aggiungendo, ad esempio, una cifra alla fine o all'inizio.

Suggerimento: utilizzate uno strumento di gestione delle password per memorizzare le password crittografate online - vi permetterà di creare password complesse contenenti lettere maiuscole e minuscole, numeri, vari caratteri speciali ecc. In questo modo si creerà una stringa di caratteri senza senso che sarà difficile da decifrare.

RICORDATE!

- non utilizzate una password che sia anche un nome o che sia simile a un nome utente, al nome di una società, ecc..,
- non utilizzate una sequenza di lettere o numeri della tastiera o dell'alfabeto,
- non utilizzate più di due lettere o numeri ripetutamente (ad esempio, abba),
- non utilizzate i dati personali di nessuno per creare una password,
- non utilizzate versioni di parole scritte al contrario (ad esempio, janek1 come 1kenaj),
- non inserite la password in presenza di altre persone,
- non scrivete la vostra password su carta - se dovete scriverla, utilizzate uno strumento di gestione delle password su una chiavetta USB e portatelo con voi
- non utilizzate la stessa password per tutti i dispositivi o siti,
- non accedete a un dispositivo non vostro,
- non inviate la password via e-mail,

- non condividete le password online - se dovete condividere le informazioni di accesso con un collega, chiamatelo per comunicargli i dettagli e non inviategli la password via e-mail, SMS o altri messaggi,
- se il vostro computer/sito è stato violato, cambiate immediatamente la password.

Antipattern - un elenco delle password meno sicure[10] :

1. password
2. 123456
3. 123456789
4. ospite
5. qwerty
6. 12345678
7. 111111
8. 12345
9. col123456
10. 123123
11. 1234567
12. 1234
13. 1234567890
14. 000000
15. 555555
16. 666666
17. 123321
18. 654321
19. 7777777
20. 123

---

[10] Secondo uno studio di NordPass, Top 200 delle password più comuni, https://nordpass.com/most-common-passwords-list/.

Autenticazione multicomponente

L'autenticazione a più fattori (MFA o 2FA) è un metodo di sicurezza che richiede l'uso di almeno due componenti indipendenti per autenticare un'azione (ad esempio, l'inserimento della password di un account e la successiva immissione di un codice SMS). Questo metodo impedisce la maggior parte degli attacchi basati sulle credenziali di identità.

Molte applicazioni o piattaforme offrono già la possibilità di abilitare questo tipo di sicurezza (ad esempio Apple ID, Microsoft, Google, Twitter o Facebook). Il secondo componente di autenticazione può essere un codice SMS, un codice una tantum da un'applicazione (Google Authenticator o Microsoft Authenticator) o un codice permanente proposto dal fornitore dello strumento in questione e scelto dall'utente.

Chiavi U2F

Secondo gli esperti di sicurezza informatica, la chiave U2F è l'unico metodo di autenticazione in due fasi che protegge al 100% dagli attacchi *di phishing (*ma non da altri attacchi, come il *malware*). Infatti, se una persona in possesso della chiave U2F viene ingannata dai criminali informatici e inserisce login e password su un sito web falso, l'aggressore non riuscirà a impossessarsi dei dati dell'account dell'utente.

Ciò è dovuto a un *elemento sicuro* (un cosiddetto piccolo computer) integrato nella chiave U2F. Funziona in modo tale che, quando la chiavetta viene inserita in una porta USB (o quando viene avvicinata a un lettore su uno smartphone), questa si avvia e può eseguire operazioni crittografiche sul suo sistema interno anziché sul dispositivo dell'utente. Inoltre, è bene procurarsi due chiavette: anche se la stessa può essere collegata a diversi servizi,

vale la pena averne una di riserva. Una volta acquistata, la chiave deve essere configurata. Molti servizi offrono la possibilità di aggiungere una chiave come forma di autenticazione multilivello. Anche diversi social media, Amazon, GitHub o account di posta elettronica raccomandano questa soluzione. Se si decide di utilizzare la chiave U2F, gli altri metodi di autenticazione a due livelli devono essere rimossi dal servizio in questione.

Protezione delle riunioni online

Non è solo l'hardware a dover essere protetto, ma anche le riunioni in rete e le videoconferenze. Lavorare in remoto significa spesso affidarsi a un software di videoconferenza, che a sua volta crea potenziali rischi per la sicurezza del dispositivo. A seguito di una serie di attacchi alla piattaforma Zoom, in cui persone non invitate si sono introdotte nelle videoconferenze per intimidire o molestare i partecipanti (*zoom bombing*), l'azienda è stata costretta a correggere le falle di sicurezza. Nonostante il nome, lo *zoom bombing* può verificarsi anche su altre piattaforme. Questo tipo di attacco può provocare la fuga di informazioni riservate sull'azienda, sui clienti, sugli altri dipendenti o sull'utente stesso.

In risposta agli attentati di Zoom, l'FBI ha pubblicato dei consigli per aiutare gli utenti a proteggersi quando utilizzano un software di videoconferenza:

1. Verificare che la riunione sia privata, richiedendo una password per partecipare alla riunione o controllando l'accesso degli ospiti dalla sala d'attesa.
2. Considerare i requisiti di sicurezza nella scelta dei fornitori. La crittografia *end-to-end* (che nasconde il messaggio al mittente e lo decifra solo al destinatario) garantisce privacy e sicurezza, quindi verificate se il software di videoconferenza che state utilizzando è dotato di questa funzione.
3. Assicuratevi che il vostro software sia aggiornato installando le patch e gli aggiornamenti più recenti.

La piattaforma più sicura per le videoconferenze è attualmente Microsoft Teams. La perfetta integrazione di tutte le applicazioni di Office consente anche ulteriori impostazioni di sicurezza, in modo che tutti i membri dell'organizzazione possano lavorare insieme rimanendo al sicuro anche nell'ufficio di casa.

Installare e tenere aggiornato il software antivirus e la protezione contro il malware.

L'aggiornamento di sistemi, applicazioni e browser viene spesso trascurato e rimandato a un secondo momento. In realtà, farlo al momento giusto può prevenire gran parte degli attacchi. Assicuratevi quindi di utilizzare un software antivirus aggiornato e moderno. Gli aggiornamenti

contengono importanti modifiche che migliorano le prestazioni e la sicurezza dei dispositivi. Oggi gli aggiornamenti vengono rilasciati addirittura mensilmente, ma vale la pena attivare la modalità di backup giornaliero. Questo aumenta significativamente la sicurezza, in quanto gli sviluppatori possono applicare rapidamente le patch alle vulnerabilità di sicurezza individuate, proteggendo ulteriormente i dispositivi dalle minacce informatiche.

Un semplice passo da compiere è anche quello di assicurarsi che il software di protezione da *malware* sia installato e utilizzato in aggiunta al software antivirus standard. Questo strumento può non solo fornire una protezione contro gli attacchi, ma anche avvisare l'utente quando viene tentato un attacco.

Evitate di collegare i vostri dispositivi a reti pubbliche

L'utilizzo di una rete pubblica, cioè una rete a cui chiunque può connettersi, per il fatto stesso di essere completamente aperta può essere un canale per numerosi attacchi e comporta il rischio di perdita di dati. Se dovete lavorare in uno spazio pubblico, assicuratevi di collegarvi solo a reti fidate e sempre con una VPN o una connessione dal vostro telefono (tramite un cosiddetto hotspot).

Che cos'è una VPN?

Si tratta di reti private virtuali che forniscono connessioni sicure e dirette alla rete informatica di un'organizzazione. Possono essere essenziali quando si accede a file, si lavora con informazioni riservate o per l'utilizzo di determinati siti web.

La VPN cripta le connessioni degli utenti ai suoi server, consentendo un accesso sicuro alla rete dell'organizzazione. Un tunnel VPN aziendale crittografato contribuisce inoltre a garantire la sicurezza dei dati trasmessi. Inoltre, impedirà agli aggressori che non dispongono di una VPN aziendale, di accedere ai server.

La sicurezza delle VPN può essere migliorata utilizzando un metodo di autenticazione solido. Molte VPN utilizzano un nome utente e una password, ma si può anche pensare all'aggiornamento e all'utilizzo di *smart card per* proteggere il processo di login degli utenti e controllare meglio l'accesso agli account.

Naturalmente, non importa quanto sia forte la VPN. Se la password viene violata, gli hacker saranno in grado di accedervi facilmente. È quindi opportuno aggiornarla regolarmente. È una buona idea limitare l'uso di una VPN alle sole situazioni in cui è necessario. Se i dispositivi aziendali per uso personale vengono utilizzati la sera o nei fine settimana (se ciò è in linea con la politica aziendale), è meglio spegnere la VPN.

Quali altre opzioni oltre alla VPN?

Un'altra opzione è quella di utilizzare una rete 5G. Offre una migliore connettività e promette una maggiore sicurezza rispetto all'utilizzo di connessioni wi-fi o addirittura VPN. L'annunciata minore latenza del 5G potrebbe renderlo una valida alternativa al wi-fi. La tecnologia è dotata di crittografia incorporata attraverso strumenti che impediscono il tracciamento o *spoofing*.

Quando si lavora da casa, è essenziale proteggere anche il router domestico. Dovrebbe essere aggiornato e protetto con una password lunga e unica, diversa da quella automatica di cui sono dotati tutti i router. A tal fine, è possibile accedere alla pagina delle impostazioni del router digitando la frase appropriata nel browser e modificare la password. Nella stessa pagina, di solito è possibile modificare anche l'SSID, ossia il nome della rete wireless, per rendere più difficile a terzi l'identificazione e l'accesso alla rete wi-fi domestica. Non utilizzate il vostro nome, l'indirizzo di casa o qualsiasi altro elemento che possa essere utilizzato per l'identificazione.

È inoltre necessario assicurarsi che la crittografia di rete sia abilitata nelle impostazioni di sicurezza della pagina di configurazione wireless. È possibile scegliere tra diversi metodi di sicurezza, come WEP, WPA e WPA2. Il più potente è il WPA2, che richiede un hardware più recente del 2006.

3. Effetto della digitalizzazione sul mercato del lavoro

3.1 Trattamento discriminatorio in fase di selezione del personale

In un mondo antecedente alla tecnologia, tutte le decisioni riguardanti l'assunzione e la valutazione di un dipendente venivano prese dalle persone. Queste decisioni tenevano solitamente conto del contesto locale, di considerazioni etiche, di aspetti legali in termini di trasparenza del processo e di validità delle scelte manageriali. Oggi, invece, molte aziende utilizzano sistemi informatici che offrono una maggiore efficienza e riducono il noioso esame dei documenti alla ricerca di informazioni specifiche.

Questi sistemi, noti come ADS (*sistemi decisionali algoritmici*), si basano sull'analisi di grandi quantità di dati elaborati per produrre risultati che costituiscono la base del processo decisionale. L'intervento umano in questo processo è solitamente assai limitato e, in alcuni casi, può essere

completamente eliminato. Tuttavia l'impatto di una particolare decisione su una determinata persona può essere di grande importanza, in quanto ne condiziona la situazione di vita.

Affidarsi totalmente agli ADS nel processo decisionale solleva quindi una serie di problemi etici, politici o legali. A causa del rischio che i sistemi algoritmici trasmettano i pregiudizi dei loro creatori, un affidamento illimitato alla tecnologia è controverso in particolare in settori come l'occupazione o l'accesso a servizi pubblici e privati (ad esempio, assistenza sanitaria, sistemi di valutazione del credito).

3.1.1. Cosa può fare una persona colpita da discriminazione algoritmica

Si presume che le disposizioni sulla parità di trattamento in materia di occupazione (in Polonia questo tema è coperto dall'articolo 18 [3a] e seguenti del Codice del lavoro) e il divieto di discriminazione (articolo 11 [3] del Codice del lavoro) debbano essere applicati nel processo di assunzione. Ciò significa che qualsiasi discriminazione sul lavoro (in particolare per motivi di sesso, età, disabilità, razza, religione, nazionalità, credo politico, appartenenza sindacale, origine etnica, religione, orientamento sessuale) è inaccettabile.

Tuttavia i casi di comportamento discriminatorio nel processo di assunzione esistono. Tra questi, la preferenza per i candidati di sesso maschile, il rifiuto di assumere giovani donne sposate o con figli o l'inserimento di clausole discriminatorie nei confronti degli stranieri. I criteri di esclusione possono essere tanto più diffusi quanto più un'azienda utilizza l'e-recruitment basato su sistemi decisionali automatizzati. Non solo si possono verificare discriminazioni involontarie contro i candidati a causa di un'intelligenza artificiale condizionata, ma la direzione di un'azienda può introdurre deliberatamente nel sistema criteri di esclusione.

In caso di discriminazione nel processo di assunzione, manifestata dal contenuto non inclusivo di un annuncio o da domande indiscrete sulla vita privata e familiare, la persona lesa può perseguire la tutela dei propri interessi in tribunale. L'onere della prova in questi procedimenti spetta al datore di lavoro, mentre il potenziale candidato deve solo rendere plausibile l'esistenza di una discriminazione (articolo 18 [3b] del Codice del lavoro). Se il tribunale conferma la violazione, il datore di lavoro sarà obbligato a pagare alla persona discriminata un risarcimento di importo non inferiore al salario minimo.

Con il processo decisionale algoritmico, tuttavia, dimostrare e rivendicare un rifiuto ingiustificato nel processo di assunzione è molto più difficile. Ciò è legato al cosiddetto *problema della scatola nera*, ovvero la mancanza di trasparenza nel funzionamento degli strumenti di intelligenza artificiale. Ciò significa che spesso anche gli stessi sviluppatori, e quindi anche i datori di lavoro che implementano uno strumento di intelligenza artificiale, non sono consapevoli del suo funzionamento indesiderato, ma ciò non significa che siano esenti da responsabilità in caso di violazioni. Una persona che sospetta di essere stata ingiustamente respinta da un algoritmo può

intraprendere azioni concrete per tutelare i propri interessi e modificare la decisione presa dal sistema.

L'articolo 22 del GDPR rimane fondamentale a questo proposito. Questa disposizione impone al responsabile del trattamento di attuare misure adeguate per proteggere i diritti, le libertà e gli interessi legittimi degli interessati (e quindi delle decisioni), nonché meccanismi che consentano a una persona specifica di contestare una decisione basata esclusivamente su un trattamento automatizzato.

Se, a vostro avviso, la vostra candidatura è stata erroneamente respinta nel processo di e-recruitment:

1. Verificate che la decisione sia stata completamente automatizzata. A tal fine, leggete attentamente i termini e le condizioni di assunzione o contattate l'ufficio risorse umane dell'azienda e stabilite come funziona l'algoritmo nel contesto del processo di candidatura.
2. Chiedete all'azienda (responsabile del trattamento dei dati) di darvi l'opportunità di fornire il vostro punto di vista e di spiegare perché ritenete che il rifiuto sia stato sbagliato.
3. Richiedete una spiegazione della decisione presa dall'azienda e chiedete che la domanda venga riesaminata nuovamente, ma questa volta da un essere umano. L'amministratore deve rispondere quanto prima a tale richiesta (entro un mese al massimo). Entro un mese, l'amministratore deve anche informare l'utente che la richiesta non è stata soddisfatta e le relative motivazioni.
4. Tuttavia, se il responsabile del trattamento ignora la richiesta o la risposta non è soddisfacente, è possibile rivolgersi alle autorità di protezione dei dati e presentare un reclamo.
5. Inoltre, indipendentemente dal procedimento dinanzi all'autorità di protezione dei dati, avete il diritto di tutelare i vostri diritti dinanzi a un tribunale civile. Se ritenete che il trattamento dei vostri dati violi la legge, potete citare in giudizio il responsabile del trattamento o l'incaricato del trattamento. Davanti al tribunale, potete chiedere il risarcimento dei danni per le violazioni della legislazione sulla protezione dei dati, nonché sollevare questioni di discriminazione che hanno causato danni patrimoniali o non patrimoniali.
6.

3.1.2. Norme UE in materia di AI e selezione del personale

Come già accennato, nella bozza di regolamento sull'intelligenza artificiale (AI Act), le questioni relative all'occupazione e alla gestione delle risorse umane sono state inserite

nell'elenco dei sistemi ad alto rischio. Ciò significa che gli strumenti per la valutazione automatizzata di un candidato a una posizione dovranno passare attraverso un percorso speciale per essere autorizzati.

Molti obblighi ricadranno sui fornitori di sistemi di IA, che saranno soggetti a requisiti rigorosi per la progettazione, il collaudo, l'audit e la certificazione dei sistemi di IA. Inoltre, coloro che utilizzano i sistemi di IA proposti dai fornitori (ad esempio le aziende) saranno tenuti a utilizzarli in conformità alla legge e alle istruzioni operative e a garantire l'adeguatezza dei dati inseriti nei sistemi, il loro monitoraggio e la conservazione dei registri degli eventi in caso di incidenti.

Le nuove disposizioni dovrebbero fornire ulteriori garanzie contro le decisioni discriminatorie prive di fattore umano. Allo stesso tempo, la legge sull'IA non concede ulteriori poteri alle entità interessate da tali decisioni. Il quadro dell'UE sarà tuttavia integrato dalla prevista *direttiva sulla responsabilità dell'intelligenza artificiale*, che introdurrà per la prima volta disposizioni sui danni causati dai sistemi di intelligenza artificiale. L'obiettivo è stabilire una protezione più ampia per coloro che sono stati danneggiati dall'IA applicata e rendere più facile per loro chiedere un risarcimento. I regolamenti proposti rappresentano quindi un passo avanti nel fornire un accesso effettivo ai rimedi anche nei casi di discriminazione nell'uso dei sistemi di impiego. Infatti, presuppongono che sia il datore di lavoro a non aver adempiuto al proprio dovere di diligenza utilizzando un sistema di impiego che discrimina determinate categorie di persone.

I lavori sulla bozza di regolamento sull'intelligenza artificiale (AI Act), e sulla direttiva sulla responsabilità dell'intelligenza artificiale sono già in fase avanzata. Tuttavia, secondo l'attuale formulazione dei nuovi regolamenti, le loro disposizioni non saranno applicabili in tutti gli Stati membri dell'UE prima di due anni dalla loro adozione.

3.2 Il futuro del lavoro

3.2.1. Professioni in via di estinzione, competenze del futuro e responsabilità del datore di lavoro per adattare le competenze dei lavoratori all'automazione

Secondo una recente ricerca del Centre for Economic Policy Research (CEPR), il 40% degli intervistati dichiara di avere più del 50% di probabilità di essere sostituito da macchine, robot o algoritmi nel prossimo decennio. I timori di una disoccupazione tecnologica non sono del tutto infondati. Secondo il rapporto *Future Jobs*, si registra un aumento significativo della quota di nuove tecnologie nelle mansioni svolte. Nel 2018, in media, il 71% del tempo di lavoro era rappresentato da attività umane e il 29% da quelle svolte da macchine. Si prevede che queste proporzioni cambieranno in modo significativo entro il 2025. Gli esseri umani saranno responsabili di circa il 48% delle attività, mentre il restante 52% dei compiti sarà completamente automatizzato.

Per quanto riguarda l'impatto dell'automazione, si può ipotizzare che i lavori manuali, che possono essere facilmente sostituiti dai robot (cioè basati su sequenze prevedibili), saranno i più colpiti. Tuttavia, la digitalizzazione può riguardare anche alcuni professionisti. Secondo il rapporto *Future of Jobs,* tra le professioni in esubero, come il meccanico, il magazziniere e il direttore di produzione, troveremo anche l'analista finanziario o l'impiegato. Tuttavia, gli esperti del McKinsey Global Institute stemperano questi timori, poiché si stima che a livello globale solo il 5% delle professioni sarà completamente eliminato.

Ciò che cambierà senza dubbio è il modo in cui vengono svolte le mansioni lavorative (una quota maggiore di sistemi informatici e macchine nelle mansioni svolte) e le competenze desiderate dai dipendenti. Dato che molti compiti saranno svolti dalle macchine, aumenterà la richiesta di competenze che i computer non possono riprodurre con precisione. Stiamo parlando di competenze soft, cioè quelle che richiedono creatività, intelligenza emotiva, pensiero critico. La digitalizzazione aumenterà anche la domanda di competenze tecniche e creerà posti di lavoro per colletti bianchi ben qualificati in grado di far funzionare i nuovi sistemi. D'altro canto, ciò può sollevare preoccupazioni circa una crescente polarizzazione del mercato (inferiorità dei colletti blu e crescente importanza di quelli più istruiti). Queste preoccupazioni sembrano essere confermate dai risultati di uno studio del Centro europeo per lo sviluppo della formazione professionale (Cedefop), secondo cui oltre il 70% degli occupati ha bisogno di competenze informatiche almeno di base per orientarsi nell'attuale mercato del lavoro, ma ben il 30% rischia di non poter acquisire in modo permanente le competenze desiderate (e quindi di perdere il posto di lavoro).

3.2.2. Competenze del futuro e professioni superflue nell'era digitale

L'uso crescente della tecnologia farà sì che le competenze richieste dal mercato del lavoro cambieranno in modo significativo nei prossimi anni. Si prevede che con l'automazione e l'algoritmizzazione la domanda di competenze facilmente sostituibili dalle macchine diminuirà. Si tratta sia delle competenze manuali (nel caso di lavoratori manuali e di produzione) sia di quelle relative al lavoro mentale (ad esempio, calcolo o scrittura creativa). D'altro canto, aumenterà la richiesta di **competenze del futuro**, come definite nel rapporto DELab (*Competences of the future. How to shape them in a flexible educational ecosystem*?) come: *abilità specifiche per svolgere compiti in un ambiente di lavoro fondamentalmente flessibile, geograficamente disperso, soggetto a frequenti e rapidi cambiamenti, che comporta la necessità di utilizzare le tecnologie digitali e di cooperare con sistemi automatizzati e macchine che utilizzano l'intelligenza artificiale*.

McKinsey ha suddiviso queste competenze in tre gruppi: tecniche e digitali, sociali e cognitive.

Le competenze del futuro	
Tecnico e digitale	• Secondo le indicazioni, la domanda di competenze digitali **di base** aumenterà del 65%. Stiamo parlando della capacità di utilizzare la tecnologia nel lavoro di tutti i giorni, soprattutto per quanto riguarda la risoluzione di problemi e il reperimento di informazioni. • Entro il 2030, i lavoratori europei dedicheranno più del 40% del tempo ad attività che utilizzano competenze digitali avanzate. Inoltre, la domanda di competenze di programmazione e IT aumenterà del 90%.
Sociale	• Entro il 2030, la domanda di competenze sociali da parte del mercato del lavoro europeo, in particolare di imprenditorialità e capacità di prendere iniziative, aumenterà del 22%.
Cognitivo (superiore): pensiero critico, creatività, capacità di gestire le persone	• La richiesta di competenze cognitive superiori aumenterà del 14% entro il 2030. Allo stesso tempo, l'importanza delle competenze cognitive di base come la lettura, la scrittura e l'elaborazione di base diminuirà del 23%.

Kompetencje przyszłości w podziale na trzy grupy umiejętności: poznawcze, społeczne i techniczne

Il World Economic Forum (WFE) indica che nei prossimi anni futuro queste saranno le competenze più importanti:

- **gestione delle persone (HR)** - costruire la forza lavoro trovando le persone migliori per compiti specifici; motivare e gestire le persone mentre lavorano,
- *c***apacità di negoziazione**: capacità di risolvere i conflitti e di superare le divergenze di opinione, dimostrando capacità di persuasione,
- *i***ntelligenza emotiva** - la capacità di identificare e dare un nome alle proprie emozioni e le emozioni altrui; la capacità di gestire e utilizzare le emozioni nel prendere giudizi e decisioni; la comprensione dei bisogni degli altri (dipendenti e clienti),
- **cooperazione con gli altri** - capacità di lavorare in gruppo,
- **flessibilità cognitiva**: la capacità di "passare" da un compito all'altro,
- **risolvere problemi complessi** - capacità di trovare soluzioni non ovvie in contesti diversi,
- **pensiero critico** - usare la logica e il ragionamento per identificare i punti di forza e di debolezza di soluzioni e le debolezze di soluzioni, conclusioni o approcci alternativi ai problemi,
- **creatività** - la capacità di pensare fuori dagli schemi, di proporre idee innovative, di risolvere i problemi in modi non ovvi.

Inoltre, nel suo rapporto il Forum economico mondiale elenca anche le **professioni che perderanno importanza nell'era della digitalizzazione**. Si tratta di professioni quali: addetto all'inserimento dati, addetto alla contabilità e alle buste paga, segretario amministrativo ed esecutivo, addetto all'assemblaggio e alla produzione, addetto all'informazione e al servizio clienti, responsabile dei servizi amministrativi e commerciali, contabile e revisore dei conti, magazziniere, direttore generale e operativo, impiegato postale, analista finanziario, cassiere e controllore di biglietti, meccanico, addetto al telemarketing, installatore di elettronica e telecomunicazioni, banchiere, autista, broker e agente di vendita, venditore porta a porta e venditore ambulante, addetto alle assicurazioni, statistiche e finanza, avvocato.

Zawody – prognoza na 2020 r.

Źródło: World Economic Forum (2018) The Future of Jobs Report 2018, s. 9. Zawody oznaczone * występują w więcej niż jednej kolumnie tabeli, co spowodowane jest różnicami między poszczególnymi sektorami.

3.2.3. Digitalizzazione e tendenze nell'ambito della gestione aziendale - il ruolo dei datori di lavoro

Per sfruttare appieno la digitalizzazione e i vantaggi derivanti dall'implementazione delle nuove tecnologie, le aziende dovranno riorganizzare le proprie strutture e cambiare l'attuale approccio al lavoro. A tal fine sarà necessario ridisegnare l'organizzazione formale dell'azienda, aggiungere personale con nuove competenze, riqualificare o sviluppare i talenti esistenti. Secondo McKinsey, a causa del cambiamento delle professioni desiderate e delle competenze più ricercate le organizzazioni saranno costrette a **aggiornarsi in cinque aree chiave** - mentalità, struttura organizzativa, assegnazione del lavoro, composizione della forza lavoro e responsabilità del management e delle risorse umane.

In termini di mentalità aziendale, la chiave per il successo futuro dell'organizzazione sarà promuovere la tendenza del cosiddetto *apprendimento permanente*, ossia offrire ai dipendenti l'opportunità di acquisire nuove competenze e conoscenze durante tutto il percorso di carriera, non solo all'inizio. In termini di struttura organizzativa, l'introduzione di modalità di gestione più

dinamiche e innovative, nonché una più frequente collaborazione tra i team e la condivisione di conoscenze e funzioni tra i dipendenti sono indicate come priorità per i prossimi anni.

Le aziende che implementano l'automazione su larga scala prevedono anche di trasferire le mansioni attualmente svolte da lavoratori altamente qualificati a lavoratori meno qualificati (con il supporto di macchine e computer). In termini di risorse umane si prevede un maggiore ricorso a vari tipi di freelance e lavoratori temporanei. Ciò deriverà dalla crescita della cosiddetta *sharing economy/economia on-demand*, ovvero modelli di business basati sull'intermediazione di piattaforme collaborative, che creano un mercato ad accesso libero per l'utilizzo temporaneo di beni o servizi, spesso forniti da privati.

Preservare la competitività dell'azienda sostenendo i dipendenti nel processo di digitalizzazione

Nel rapporto *Beyond Hiring. How companies are re-skilling to address talent shortages,* McKinsey ha delineato diverse tattiche per mantenere le aziende competitive e colmare il divario tra le competenze desiderate e quelle disponibili dei dipendenti del settore privato. Tra le pratiche che i datori di lavoro che cercano di far crescere la propria attività e di costruire una forza lavoro competente dovrebbero prendere in considerazione vi sono:

- **Riqualificazione** - incoraggiare l'acquisizione di nuove competenze e l'aggiornamento di quelle esistenti da parte dei dipendenti esistenti, nonché l'implementazione e la formazione dei nuovi assunti nelle capacità desiderate. Una questione fondamentale per le aziende sarà decidere le modalità di erogazione della formazione: internamente (utilizzando le risorse e i programmi disponibili) o esternamente (in collaborazione con un istituto di istruzione o un centro di formazione). Per quanto riguarda le aree in cui gli imprenditori intendono investire, il più delle volte riguardano la costruzione di competenze strategiche per la loro azienda, ad esempio competenze informatiche avanzate, capacità di scrittura creativa, pensiero critico, capacità di risolvere problemi. D'altro canto, per le competenze meno complesse, i datori di lavoro dichiarano la possibilità di assumere persone esterne all'organizzazione.

- **Trasferimenti all'interno dell'azienda** - spostamento dei dipendenti con competenze specifiche in reparti/team dove possono sfruttare meglio le loro capacità. In un sondaggio McKinsey condotto nel febbraio 2018 tra i dirigenti d'azienda. Il 55% degli intervistati ha dichiarato che preferirebbe ricollocare alcuni dipendenti in ruoli diversi o completamente nuovi piuttosto che licenziarli completamente.

- **Assunzione** - ricerca di individui o interi team con le competenze specifiche richieste (anche se l'offerta di esperti sul mercato potrebbe non essere sufficiente per tutte le

aziende per perseguire questa strategia). Da un lato, il costo dell'assunzione può essere inferiore a quello della riqualificazione, ma dall'altro l'approvvigionamento di nuovi membri del team comporta un rischio per le prestazioni del singolo. Per riuscire ad attrarre nuovi talenti chiave, le aziende dovrebbero quindi innovare il modo in cui reclutano i candidati, oltre a offrire una cultura del lavoro attraente e benefici non salariali.

- **Creare nuove forme di collaborazione** - le aziende possono beneficiare delle competenze apportate da persone esterne all'organizzazione (liberi professionisti, esperti, agenti temporanei di agenzie di reclutamento). L'aspetto negativo di questo modello, tuttavia, è il rischio di trasferire segreti commerciali (ad esempio, know-how, opere coperte da diritti di proprietà intellettuale) a persone esterne, nonché la difficoltà di inserirsi nella cultura e nelle modalità di lavoro dell'azienda. Per questo motivo, i datori di lavoro dichiarano di occupare posizioni non correlate alle attività principali dell'azienda o che richiedono basse qualifiche con appaltatori indipendenti.

- **Possibili esuberi** - In alcune aziende possono essere necessari degli esuberi, in particolare nei settori che non crescono abbastanza rapidamente e in cui l'automazione sostituirà in modo significativo la forza lavoro. Una strategia di esuberi può essere attuata riducendo o interrompendo l'assunzione di nuovi dipendenti, consentendo al contempo di continuare il normale processo di pensionamento e di uscita di quelli già impiegati.

Sebbene siano possibili licenziamenti dovuti al maggiore utilizzo delle macchine, è difficile pensare che i dipendenti di tutti i settori debbano temere per il proprio posto di lavoro. Tuttavia ci saranno indubbiamente nuove tecnologie, sistemi e programmi che richiederanno l'acquisizione di ulteriori competenze informatiche.

Come possono i datori di lavoro sostenere i propri dipendenti nella digitalizzazione dell'impresa? Innanzitutto possono:

- familiarizzare i dipendenti con i nuovi strumenti - eliminare la paura e il conservatorismo nei confronti delle nuove tecnologie e mostrare come gli strumenti digitali possono essere utilizzati nel lavoro quotidiano,
- sensibilizzare i dipendenti - spiegare perché e come l'azienda utilizza la tecnologia; con informazioni in questo ambito, i dipendenti comprenderanno meglio i nuovi strumenti di lavoro e saranno motivati a utilizzarli,

- preparare bene i manager ai cambiamenti imminenti - i manager devono conoscere le risposte alle domande di base sui nuovi strumenti di lavoro e mostrare agli altri membri del team come utilizzare le tecnologie implementate,
- fornire formazione sui nuovi sistemi - anche i dipendenti esperti di tecnologia hanno bisogno di tempo per familiarizzare con nuovi software e strumenti digitali che non hanno mai usato prima; l'azienda dovrebbe fornire una formazione professionale a tutti i dipendenti.

3.2.4. Altri soggetti che svolgono un ruolo chiave nella processi di digitalizzazione del lavoro e nella riqualificazione dei lavoratori

Istituzioni educative

Il ruolo dell'istruzione nel processo di digitalizzazione è già riconosciuto dagli organismi dell'Unione Europea. Le conclusioni del Consiglio europeo hanno sottolineato che l'accesso a un'istruzione di alta qualità supportata dalle tecnologie digitali è un prerequisito per la trasformazione di singoli settori e per un'ulteriore crescita economica.

Inoltre, la Commissione europea ha incluso la creazione di un piano d'azione per l'istruzione digitale per il periodo 2021-2027 che definisce una visione per l'istruzione digitale in Europa. L'obiettivo di entrambe le iniziative era quello di incoraggiare le università, le scuole e il personale docente a svolgere un ruolo più attivo nella costruzione di competenze digitali e nel soddisfare le esigenze del mercato del lavoro. Il ruolo di queste istituzioni nella trasformazione digitale sembra essere confermato anche da pubblicazioni economiche, come il rapporto di PwC e WFE *Raising Skills for Shared Prosperity* (2021), che sottolinea come gli istituti di istruzione superiore abbiano il potenziale per guidare il cambiamento - per aumentare le conoscenze, le abilità e le competenze complessive degli studenti e della società.

Autorità pubblica

Il ruolo dello Stato è quello di sostenere sia gli imprenditori che i dipendenti nel processo di digitalizzazione. È quindi importante che i responsabili politici attuino politiche che incoraggino l'acquisizione di competenze digitali o la riqualificazione dei dipendenti (ad esempio, attraverso programmi di sussidi alla formazione per le piccole e medie imprese). Inoltre, è importante stimolare il mercato del lavoro ed evitare la disoccupazione attraverso politiche attive per l'occupazione: invece di affidarsi ai sussidi di disoccupazione, lo Stato dovrebbe investire in agenzie per l'impiego che diventino centri di collocamento e facilitino la riqualificazione dei disoccupati.

ONG

Le ONG e i think tank spesso fungono da incubatori di soluzioni socialmente utili. Tendono ad avere maggiore libertà d'azione rispetto alle istituzioni statali e possono proporre soluzioni diverse ai problemi. Per questo motivo, alcune aziende intraprendono iniziative filantropiche o collaborano con fondazioni in settori legati all'acquisizione di nuove competenze da parte dei dipendenti. Un esempio è l'iniziativa Generation, che lavora per combattere la disoccupazione colmando il divario di competenze tra i giovani e sostenendo gli adulti nella ricerca di un lavoro adatto a loro attraverso il reclutamento, la formazione e il tutoraggio.

Sindacati e organizzazioni professionali

In qualità di parti sociali, le associazioni industriali e i sindacati svolgono un ruolo importante nella digitalizzazione del mercato del lavoro. In Svezia, ad esempio, sono stati istituiti dei consigli per la tutela del lavoro finanziati dalle aziende e dai sindacati. Questi enti formano le persone che hanno perso il lavoro, fornendo loro un sostegno finanziario temporaneo e facilitando il processo di riqualificazione in modo che i disoccupati rientrino più rapidamente nel mercato del lavoro.

3.3 Nuovi business model e loro impatto sul mercato del lavoro

3.3.1. Erosione del la forza negozianel dei lavoratori - in che modo le tecnologie ostacolano la sindacalizzazione dei lavoratori

Le nuove tecnologie facilitano la comunicazione e mettono in contatto gli utenti tra loro, nonostante la distanza che li separa. Allo stesso tempo, però, stanno portando a una maggiore alienazione e a una sempre minore interazione umana. Questo fenomeno non riguarda solo la sfera privata, ma anche quella professionale. La digitalizzazione e lo spostamento del lavoro nel mondo online hanno fatto sì che i dipendenti sporadicamente instaurino relazioni durature e che si incontrino e discutano dei problemi sul posto di lavoro meno frequentemente.

Le nuove tecnologie favoriscono l'isolamento, non solo a causa del lavoro a distanza. Gli strumenti di intelligenza artificiale utilizzati dalle aziende per controllare i dipendenti e misurare la loro produttività sono spesso usati anche per sorvegliarli e impedire l'associazione dei lavoratori.

Talvolta i modelli di business delle grandi imprese si basano su un controllo estensivo dei lavoratori e su una costante accelerazione dei ritmi di lavoro. La sindacalizzazione dei lavoratori per rappresentare i loro diritti e interessi collettivi e individuali rappresenta quindi un rischio

reale per un sistema che si preoccupa solo di massimizzare i profitti aziendali. Per questo motivo, le imprese adottano misure per impedire ai lavoratori di sindacalizzarsi. Questa pratica si è intensificata durante la pandemia da COVID-19, quando le raccomandazioni in materia di salute e sicurezza introdotte in quel periodo hanno iniziato a essere utilizzate per implementare nei luoghi di lavoro strumenti per misurare la distanza tra le persone nei magazzini, vietando loro di stare troppo vicine. Le aziende hanno iniziato a dotarsi di software che consentivano di analizzare e visualizzare i dati sulle relazioni all'interno dei luoghi di lavoro (ad esempio, la geoSPatial Operating Console o SPOC). Inoltre, i dipartimenti delle risorse umane hanno monitorato le mailing list dei dipendenti utilizzate per scopi attivistici o i gruppi di dipendenti sui social media.

Nel caso del lavoro su piattaforma, l'impatto delle nuove tecnologie sull'associazione dei lavoratori non è nettamente solo positivo o negativo. Le app utilizzate per fornire servizi possono facilitare la mobilitazione di corrieri e autisti - le chat room interne disponibili nei loro sistemi offrono ai lavoratori delle piattaforme (*gig-worker*) uno spazio per scambiare informazioni, mentre le reti di comunicazione di massa possono collegare i singoli corrieri a livello di città, regioni e persino Paesi.

Allo stesso tempo, l'efficacia dei sindacati dei lavoratori delle piattaforme dipende spesso dal sostegno delle autorità pubbliche a varie forme di auto-organizzazione. A Bologna, ad esempio, è stata creata, in collaborazione con i sindacalisti, una *Carta dei diritti fondamentali del lavoro digitale nel contesto urbano*, che stabilisce un quadro di standard minimi per i salari, l'orario di lavoro e la protezione assicurativa dei lavoratori delle piattaforme. È significativo, tuttavia, che lo stesso sindaco di Bologna abbia mostrato grande sostegno per l'iniziativa e abbia invitato i clienti a boicottare le piattaforme che non avessero firmato la Carta.

Nei Paesi in cui lo Stato non estende l'assistenza ai lavoratori delle piattaforme, il loro livello di sindacalizzazione è molto più basso e il loro potere contrattuale più debole. Di questo aspetto abusano talvolta le piattaforme, che utilizzano i meccanismi delle app per controllare meglio i corrieri o gli autisti e vanificare i tentativi di opporsi alle politiche aziendali.

Un esempio di come i giganti della sharing economy stiano usando la tecnologia per limitare le iniziative dei lavoratori che lottano per i loro diritti è stato lo sciopero nell'aprile 2021, rapidamente messo a tacere, dei rider polacchi che consegnano i pasti. Lo sciopero è stato motivato dall'iniquità con cui l'algoritmo distribuiva gli ordini e fissava la retribuzione. Il metodo di protesta è stato che i corrieri avevano smesso di evadere gli ordini, nonostante la loro dichiarata disponibilità a lavorare nell'app. Gli autisti speravano di fare pressione sull'azienda e di convincerla a parlare con i rappresentanti della comunità. Tuttavia, l'azienda, utilizzando l'app, senza alcun tentativo di comunicare con i corrieri, ha bloccato gli scioperanti e ha passato gli ordini a persone disposte a svolgere il lavoro nonostante le condizioni avverse.

3.3.2. Effetto della digitalizzazione sul mercato del lavoro - il lavoro tramite piattaforma

Il lavoro su piattaforma è una forma di occupazione in cui un lavoratore utilizza una piattaforma digitale per accedere ad altre organizzazioni o individui per fornire determinati servizi in cambio di un determinato stipendio. I compiti svolti a pagamento attraverso le piattaforme digitali includono servizi di taxi e corriere, consegne, servizi di riparazione a domicilio, nonché lavori impiegatizi come il copywriting e la contabilità. Sebbene app come Uber e Bolt si siano sviluppate nello spazio europeo solo da un decennio, i lavoratori che forniscono servizi attraverso piattaforme di questo tipo costituiscono oggi una parte significativa della forza lavoro (28,3 milioni di lavoratori nel 2022 nell'Unione Europea). Questo dato è paragonabile al numero di persone impiegate nei settori produttivi industriali (29 milioni di lavoratori). Inoltre, secondo la Commissione europea, le piattaforme dovrebbero aggiungere altri 15 milioni di dipendenti entro il 2025. Le piattaforme più popolari nell'UE includono Uber, Deliveroo, Amazon Mechanical Turk, Fiverr, Upwork, Appjobs, Glovo o JustEat.

Il modello di business delle piattaforme di lavoro si basa su tecnologie che utilizzano algoritmi per far incontrare efficacemente la domanda e l'offerta di lavoratori e i servizi che essi forniscono. Inoltre, l'uso di applicazioni opportunamente progettate consente di prendere decisioni automatiche senza contatto e di monitorare le mansioni svolte. Con un sistema di gestione basato su algoritmi, è possibile fare a meno del personale dirigente tradizionale. Questo, a sua volta, fa sì che le piattaforme sostengano di agire semplicemente come un intermediario che offre servizi per mettere in contatto i lavoratori autonomi con i potenziali clienti, piuttosto che come un datore di lavoro.

Chi è più propenso a cercare lavoro attraverso le piattaforme di lavoro?

- giovani
- uomini
- immigrati (soprattutto per quanto riguarda i lavori manuali),
- persone con istruzione post-secondaria, per le quali questo lavoro rappresenta una fonte di reddito aggiuntiva.

Inoltre, i lavoratori delle piattaforme possono essere suddivisi in due gruppi agli antipodi nel mercato del lavoro. Il primo gruppo comprende i colletti bianchi, privilegiati in termini di competenze, ad esempio i programmatori che possono influenzare i termini e le condizioni di collaborazione con i clienti (freelance, fornitura di servizi informatici). Il secondo gruppo, invece, comprende persone con competenze basse e facilmente sostituibili, il cui potere negoziale sul mercato del lavoro è basso (ad esempio, gli immigrati che forniscono servizi di taxi).

Vantaggi e svantaggi del lavoro su piattaforma

I vantaggi del lavoro su piattaforma includono:

- orari di lavoro flessibili e la possibilità di pianificare il proprio programma di lavoro,
- contatto diretto con i committenti,
- maggiore indipendenza.

Allo stato attuale delle piattaforme digitali, tuttavia, questo tipo di impiego presenta una serie di svantaggi:

- problemi di salute e sicurezza:
    - mancanza di norme regolamentate in materia di salute e sicurezza,
    - rischi fisici,
    - stress causato dall'insicurezza del lavoro;
- termini e condizioni di impiego:
    - 5,5 milioni di persone che lavorano attraverso piattaforme di lavoro nell'UE sono erroneamente classificate come lavoratori autonomi,
    - le persone classificate erroneamente come lavoratori autonomi non hanno diritto agli stessi diritti e benefici dei lavoratori dipendenti;
- problemi derivanti dall'algoritmizzazione del lavoro,
- opportunità limitate di associazione,
- salari e orari di lavoro imprevedibili (secondo la Commissione europea, il 41% dell'orario di lavoro dei lavoratori delle piattaforme consiste in attività non retribuite, come la consultazione di annunci o l'attesa di ordini).

Diritto dell'UE e lavoro su piattaforma

Alcuni Stati membri hanno già introdotto norme per il lavoro su piattaforme nella legislazione nazionale. Anche a livello comunitario si sta discutendo di questo particolare tipo di occupazione. Il concetto di lavoratore su piattaforma è già stato introdotto nella legislazione dell'UE, ad esempio attraverso la direttiva sulle condizioni di lavoro trasparenti e prevedibili nell'Unione europea. Tuttavia il punto di svolta è rappresentato dalla **Direttiva sul miglioramento delle condizioni di lavoro dei lavoratori delle piattaforme**, la cui bozza è stata presentata dalla Commissione europea alla fine del 2021.

Alcune disposizioni chiave incluse nella proposta di direttiva sul miglioramento delle condizioni di lavoro dei lavoratori tramite piattaforme:

- Coloro che lavorano attraverso le piattaforme digitali otterranno uno status occupazionale che corrisponde alle loro effettive condizioni di lavoro, che saranno verificate stabilendo i criteri necessari per riconoscere la piattaforma come datore di lavoro.
- Una piattaforma sarà considerata un datore di lavoro se soddisfa almeno due dei seguenti criteri:
    - determina il livello di remunerazione o fissa un tetto massimo,
    - supervisiona per via elettronica l'esecuzione del lavoro,
    - limita la libertà di scegliere l'orario di lavoro o i periodi di assenza, la libertà di accettare o rifiutare incarichi o la libertà di ricorrere a subappaltatori o sostituti,
    - stabilisce regole specifiche e vincolanti sull'aspetto e sul comportamento nei confronti del destinatario del servizio o del committente dell'opera,
    - limita la capacità di espandere la base di clienti o di eseguire lavori per conto di terzi.
- Ai lavoratori delle piattaforme dovrebbero spettare i diritti lavorativi e sociali in base al loro status occupazionale:
    - tempi di riposo garantiti e ferie pagate,
    - salario minimo,
    - la possibilità di contrattazione collettiva,
    - sicurezza e protezione della salute,
    - indennità di disoccupazione e di malattia,
    - pensioni basate sui contributi.
- La piattaforma può contestare la classificazione, ma deve dimostrare che non esiste un rapporto di lavoro.
- Le piattaforme dovranno aumentare la trasparenza nell'uso degli algoritmi e garantire il monitoraggio umano delle condizioni di lavoro.
- I dipendenti avranno il diritto di contestare le decisioni automatizzate.

DIGITALIZAREA PIEȚEI MUNCII

Modul de instruire elaborat în cadrul proiectului
Inițierea de activități pentru punerea în aplicare a Acordului-cadru al partenerilor sociali europeni privind digitalizarea,
cofinanțat de Uniunea Europeană

RO

Co-funded by the European Union

NSZZ Solidarność Komisja Krajowa

Blocul Național Sindical

Digitalizarea pieței muncii

Modul de instruire elaborat în cadrul proiectului

Inițierea de activități pentru punerea în aplicare a Acordului-cadru al partenerilor sociali europeni privind digitalizarea,

cofinanțat de Uniunea Europeană

Co-funded by the European Union

Iunie 2023

Autori:

Blanka Wawrzyniak

Marta Musidłowska

Consultant de specialitate:

Hanna Sakowicz-Daszczyńska

Redactor:

Julia Zaleska

Publicație gratuită, finanțată de Uniunea Europeană în cadrul proiectului nr. 101051759

„Inițierea de activități pentru implementarea Acordului-cadru al partenerilor sociali europeni privind digitalizarea (EFAD)”. Titlul original: „Initiating activities to implement the European Social Partners Framework Agreement on Digitalisation (EFAD)”.

Notă introductivă

Această publicație a fost elaborată în cadrul proiectului „Inițierea de activități pentru implementarea Acordului-cadru al partenerilor sociali europeni privind digitalizarea”. Acesta este un manual ce urmează a fi utilizat atât în timpul, cât și după instruirea din cadrul proiectului. Modulul de instruire urmărește să pregătească partenerii sociali pentru schimbările dinamice care au loc pe piața muncii ca urmare a transformării digitale. Este vorba de schimbări care privesc, printre altele, automatizarea producției, noile modele de afaceri, munca la distanță și metodele inovatoare de administrare a firmelor. Publicația include, de asemenea, o parte consacrată drepturilor angajaților în era digitală. Scopul acesteia este să le ofere angajaților instrumente care să le permită să se deconecteze și să păstreze un echilibru între viața profesională și cea privată.

Cuprins

Introducere

Deși inteligența artificială (AI) este un termen larg care acoperă un grup de algoritmi care își pot modifica parametrii și pot crea noi rezultate, în termenii cei mai simpli, aceasta poate fi descrisă ca fiind capacitatea mașinilor de a înțelege, învăța, planifica și demonstra creativitate.

Pentru mulți experți, ritmul în care se dezvoltă inteligența artificială și impactul acesteia asupra lumii din jurul nostru pare îngrijorător. Acest lucru este influențat, printre altele, de faptul că sistemele de inteligență artificială sunt dezvoltate de cele mai mari companii de tehnologie din SUA și China, pentru care cel mai important este profitul. Asupra pericolelor unei dezvoltări fără nici o limitare a AI avertizează chiar reprezentanții din domeniu. O scrisoare deschisă în care se cere sistarea experimentelor cu sisteme de inteligență artificială și a sistemelor mai puternice decât Chat GPT-4 a fost semnată, printre alții, de Elon Musk (CEO al SpaceX, Tesla și Twitter), Steve Wozniak (cofondator al Apple) și Yuval Noah Harari (futurist, profesor la Universitatea Ebraică din Ierusalim).

Este esențial controlul dezvoltării inteligenței artificiale pentru a garanta că sistemele de inteligență artificială sunt sigure și că țin cont de impactul asupra bunăstării umane. Cu toate acestea, în avalanșa de informații despre AI, cele mai vizibile sunt viziunile alarmiste, care nu sunt neapărat bazate pe realitate. Acest lucru, la rândul său, conduce la opinii sceptice cu privire la noile tehnologii, la teama de șomaj în masă și la reticență privind utilizarea instrumentelor digitale. Cu toate acestea, este important să ne amintim că tehnologia este în prezent parte integrantă din viața de zi cu zi. Și nu doar ca sursă de divertisment, ci și prin unelte care ușurează îndeplinirea sarcinilor casnice și profesionale. De aceea este extrem de importantă adoptarea de soluții inovatoare și educarea publicului cu privire la utilizarea corectă a acestora.

Activitățile de conștientizare ar trebui să abordeze, de asemenea (sau mai ales) soluțiile digitale de la locul de muncă. După cum se va arăta mai târziu în manual, noile tehnologii sunt utilizate în multe sectoare și în diferite etape ale angajării (de la recrutare la evaluarea angajaților). Ele ușurează atât procesele de gestionare a afacerilor, cât și activitatea de zi cu zi a multor persoane (atât a celor care lucrează fizic cât și celor care prestează muncă intelectuală). Cel mai bun exemplu în acest sens este utilizarea pe scară largă a programelor de traducere automată precum Google Translator sau Deepl, care îmbunătățesc comunicarea transfrontalieră între firme sau permit traducerea de texte de specialitate fără a fi nevoie să se apeleze la un traducător profesionist.

Există, de asemenea, speranțe din ce în ce mai mari de eficientizare a muncii cu ajutorul inteligenței artificiale generative. Aplicații precum GPT Chat sau DALL-E sunt deja utilizate pentru sarcini creative, cum ar fi scrierea de e-mailuri sau efectuarea de analize de date. De exemplu, cu ajutorul inteligenței artificiale generative, este posibilă o analiză mai rapidă a conținutul unui

articol sau redactarea minutei unei întâlniri într-o clipă. După comunicarea comenzii potrivite (de exemplu, „spune principalele concluzii ale discuției”) și introducerea în sistem a principalilor parametri, ne putem aștepta să fie generat rezultatul dorit (concluziile).

În același timp, trebuie reținut faptul că modelele lingvistice mari (LLM, din eng. *Large Language Model*), precum Chat GPT, deși produc un conținut care sună natural, îl generează în mod automat și fără a reflecta. Acest lucru, la rândul său, poate face ca textele produse de algoritmi, deși foarte credibile, să conțină multe erori. De aceea este atât de important să se dezvolte în rândul utilizatorilor abilitățile de gândire critică, capacitatea de a analiza mediul real și de a selecta ceea ce nu este adevărat (de exemplu, *fake news*). În plus, lucrând în era digitală, pe lângă pregătirea angajaților din diverse sectoare în perspectiva automatizării și echiparea lor cu noi competențe, este necesar să îi învățăm pe angajați cum să coexiste cu tehnologia dar și cum să se „deconecteze”. Acestea sunt condițiile unui echilibru corespunzător între viața profesională și cea privată.

Această lucrare a fost elaborată la sfârșitul anului 2022/începutul lui 2023. Având în vedere dinamica rapidă a dezvoltării inovației și, în special, a instrumentelor inteligenței artificiale (AI), autoarele manualului doresc să sublinieze că unele părți din conținutul acestuia ar putea să-și piardă din actualitate în următoarele luni și ani ca urmare a progresului tehnologiei.

Glosar de termeni

AI Act /Documentul privind inteligența artificială

- Regulamentul UE de stabilire a unor norme armonizate privind inteligența artificială.

Algoritm

- un set de instrucțiuni (formula de calcul) care iau decizii în mod autonom, pe baza unor modele statistice sau a unor reguli de decizie, fără intervenție umană clară.

Anonimizare

- procesul de transformare a datelor cu caracter personal într-un mod care împiedică asocierea acestora cu o persoană fizică identificată sau identificabilă.

Automatizare

- utilizarea tehnologiei pentru a controla producția și a crea produse și servicii cu ajutorul instrumentelor digitale.

Blockchain

- tehnologie de transfer și stocare a informațiilor despre tranzacțiile online; registru de date descentralizate partajate în siguranță. Tehnologia blockchain permite partajarea datelor într-un grup de participanți selectați.

*Bring your own device (*BYOD)

- tendința ce constă în folosirea dispozitivelor personale, precum laptopurile, smartphone-urile și tabletele, pentru îndeplinirea sarcinilor de serviciu.

Chat GPT

- instrument care utilizează inteligența artificială (chatbot) și care, într-o formă asemănătoare dialogului, permite primirea unui răspuns la întrebările adresate în limbaj natural de utilizator.

Date cu caracter personal

- orice informație referitoare la o persoană fizică în viață identificată sau identificabilă (informațiile individuale care, împreună, pot conduce la identificarea unei persoane constituie, de asemenea, date cu caracter personal).

Deep fake

- din două expresii englezești: *deep learning* (învățare profundă) și *fake* (fals). Este vorba de procesarea sunetului și a imaginilor cu scopul de a crea un mesaj fals folosind tehnici din domeniul inteligenței artificiale. Astfel este posibilă producerea de materiale pe care este greu sau imposibil să le deosebim de filmele sau fotografiile create prin mijloace tradiționale și cu persoane reale.

Modele lingvistice mari (LLM, din eng. *Large Language Models***)**

- modele de învățare automată capabile să realizeze diverse sarcini de procesare a limbajului natural. Antrenarea unui astfel de sistem constă din aceea că i se furnizează cantități mari de date (de exemplu, cărți, articole, site-uri web) din care poate învăța modele și conexiuni de cuvinte pentru a genera conținut nou în viitor. Un exemplu de LLM este Chat GPT, care a fost dezvoltat de OpenAI și pus la dispoziția publicului în noiembrie 2022. Acest model este capabil să proceseze informații și să genereze texte asemănătoare celor create de om, ca răspuns la indicațiile utilizatorului.

Fake news

- informații false sau parțial false, cu caracter senzațional, care îi induc în mod deliberat în eroare pe cei cărora le sunt destinate.

Economie colaborativă / economie la cerere (*sharing economy*; *on-demand economy*)

- set de modele de afaceri bazate pe intermedierea unor platforme de colaborare, care creează o piață accesibilă de utilizare temporară a bunurilor sau serviciilor furnizate, adeseori, de persoane particulare.

Competențele viitorului

- acele competențe care permit asumarea și îndeplinirea sarcinilor într-un mediu de lucru care este fundamental flexibil, dispersat geografic, predispus la schimbări frecvente și rapide și care implică nevoia de a folosi tehnologii digitale și de a colabora cu sisteme automate și mașini care utilizează inteligența artificială.

Mobbing

- acțiuni sau comportamente față de un angajat, constând din hărțuire sau intimidare insistentă și prelungită.

Munca prin intermediul platformelor

- o formă de angajare în cadrul căreia angajatul folosește o platformă digitală pentru a avea acces la alte organizații sau persoane, cu scopul de a furniza servicii specifice și în schimbul unei remunerații. Printre sarcinile efectuate contra cost prin intermediul platformelor digitale se numără serviciile de taxi și de curierat, livrările, service-urile de reparații la domiciliu, precum și activități intelectuale precum copywriting sau contabilitatea.

Munca asistată

- muncă în care unele activități pot fi efectuate de roboți, în timp ce pentru altele este nevoie de intervenție umană.

Dreptul la deconectare

- dreptul de a nu se angaja în sarcini legate de muncă în afara timpului de lucru și de a nu participa la comunicarea prin intermediul instrumentelor digitale.

Profilare

- orice formă de prelucrare automată a datelor cu caracter personal care constă din utilizarea acestora pentru a evalua anumiți factori personali ai unei persoane fizice. În special, profilarea se folosește pentru a analiza sau a prognoza efectele muncii acelei persoane, situația sa economică, sănătatea, preferințele personale, interesele, credibilitatea, comportamentele, locația sau deplasarea acesteia.

Pseudonimizarea

- prelucrarea datelor cu caracter personal în așa fel încât să nu fie posibilă identificarea celui la care se referă fără a accesa alte informații stocate în siguranță în altă parte.

GDPR

- *Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE* (denumit în continuare: Regulamentul GDPR).

Roboți colaborativi (*collaborative robots*; coboți)

- echipamente concepute cu scopul de a reduce volumul de muncă pentru lucrătorii din fabrici prin preluarea unei părți a sarcinilor acestora.

Autoînvățare (ML; *machine learning*)

- domeniu al inteligenței artificiale dedicat algoritmilor care, prin experiență, respectiv prin expunerea la date, își îmbunătățesc continuu performanțele. Algoritmii de învățare automată construiesc un model matematic din date de eșantionare (numit set de învățare) pentru a prognoza sau a lua decizii fără a fi nevoie să fie programați în acest sens de om.

Spoofing

- un tip de atac în care infractorii pretind că sunt bănci, instituții sau oficii ale statului, companii sau chiar persoane fizice pentru a extorca date sau bani de la victimele lor.

Start-up

- o companie nou înființată sau o organizație temporară care caută un model de afaceri pentru a crește în mod profitabil.

Inteligența artificială (IA, AI)

- capacitatea mașinilor de a înțelege, de a învăța, de a planifica și de a da dovadă de creativitate. Potrivit definiției propuse de proiectul de lege privind inteligența artificială (AI Act), un sistem de inteligență artificială înseamnă un software dezvoltat cu ajutorul uneia sau mai multor tehnici și abordări dintre cele prezentate în detaliu în regulament care poate, pentru un anumit set de scopuri definite de om, să genereze rezultate precum conținut, predicții, recomandări sau decizii

care afectează mediile cu care interacționează. Această definiție este foarte largă și vagă, dar acest lucru este de înțeles în contextul unei tehnologii în dezvoltare rapidă precum inteligența artificială.

Criptarea datelor

- un set de tehnici de codificare a informațiilor sensibile sau personale pentru a asigura confidențialitatea acestora.

Wearables

- Dispozitive electronice „purtabile”, adică purtate aproape de piele. Acestea pot monitoriza și analiza parametrii de sănătate sau comportamentul purtătorului. Cele mai populare dispozitive de acest tip includ în prezent ceasurile inteligente (smartwatch), brățările de fitness (așa-numitele smartbands) și ceasurile sport.

Work-life balance

- menținerea unui echilibru între muncă (atât cea remunerată cât și neremunerată) și viața de familie sau timpul liber.

Proces decizional automatizat

- activitate bazată pe calcule avansate și pe mijloace exclusiv tehnice de prelucrare a informațiilor. Emiterea de decizii de către calculator, fără implicarea elementului uman.

1. Impactul digitalizării asupra proceselor de lucru

1.1 Acordul-cadru al partenerilor sociali europeni privind digitalizarea – observații generale

Transformarea digitală a economiei are un impact uriaș asupra angajatorilor, angajaților și asupra modului în care se desfășoară activitatea profesională. Pentru a facilita integrarea tehnologiilor digitale la locul de muncă, în iunie 2020 a fost încheiat Acordul-cadru autonom al partenerilor sociali europeni (EFAD). Scopul acestuia este de a preveni și de a minimiza riscurile cu care se pot confrunta angajații și angajatorii. Acordul se referă la toate persoanele angajate sau care angajează lucrători în sectorul public și privat și în toate tipurile de activități economice.

Acordul EFAD este o inițiativă independentă și rezultatul negocierilor dintre partenerii sociali europeni în cadrul celui de-al șaselea program de lucru multianual 2019-2021. Având în vedere articolul 155 din Tratatul privind funcționarea Uniunii Europene (TFUE), acest acord-cadru european autonom obligă membrii BusinessEurope, SMEunited, CEEP și CES (și comitetul de legătură EUROCADRES/CEC) să promoveze și să pună în aplicare instrumente și măsuri (dacă este necesar la nivel național, sectorial sau de întreprindere) în conformitate cu procedurile și practicile specifice partenerilor sociali din statele membre și din țările din Spațiul Economic European.

Printre exemplele de alte acorduri autonome încheiate în ultimii ani se numără acordul-cadru autonom al partenerilor sociali europeni privind îmbătrânirea activă și abordările intergeneraționale sau acordul-cadru european privind stresul legat de muncă.

I. Principalele obiective ale acordului EFAD

1. Creșterea gradului de conștientizare și o mai bună înțelegere în rândul angajatorilor, al angajaților și al reprezentanților acestora cu privire la oportunitățile și provocările la locul de muncă care decurg din transformarea digitală.
2. Oferirea de asistență lucrătorilor și reprezentanților acestora, precum și angajatorilor, în elaborarea de măsuri și acțiuni pentru a profita de noile oportunități digitale și pentru a face față provocărilor, ținând cont de inițiativele, practicile și contractele colective existente.

3. Încurajarea unei abordări din perspectivă partenerială a angajatorilor și sindicatelor.

II. Etapele pentru crearea de parteneriate care să faciliteze procesul de transformare digitală în cadrul companiei

Reprezentanților lucrătorilor li se vor pune la dispoziție facilitățile și informațiile necesare pentru o implicare eficientă în diferitele etape ale procesului.

Etapa 1

„Explorare/pregătire/sprijin împreună", care se referă la creșterea gradului de conștientizare și la crearea condițiilor și a unei atmosfere de sprijin și încredere. Aceste activități au scopul de a permite o discuție deschisă cu privire la oportunitățile și provocările/riscurile digitalizării, precum și la impactul acestora asupra locului de muncă, precum și discuții despre posibile acțiuni și soluții.

Etapa 2

„Cartografierea comună/evaluare periodică /analiză" este un exercițiu de cartografiere a domeniilor tematice în ceea ce privește beneficiile și oportunitățile, precum și provocările și riscurile pe care integrarea eficientă a tehnologiilor digitale le poate aduce angajaților și companiei.

Etapa 3

„Analiza în comun a situației și adoptarea unei strategii de transformare digitală", care reprezintă rezultatul primelor două etape. Este vorba despre o înțelegere de bază a oportunităților
și a provocărilor/riscurilor, a diferitelor elemente care alcătuiesc digitalizarea companiei și a interrelațiilor dintre acestea, precum și despre convenirea unor strategii digitale care să stabilească obiectivele companiei pentru viitor.

Etapa 4

„Adoptarea de măsuri/acțiuni adecvate" pe baza unei analizei în comun a situației. Aceasta include: posibilitatea de a testa și de a pilota soluțiile avute în vedere, stabilirea priorităților, punerea în aplicare a acțiunilor în etapele ulterioare, clarificarea și definirea rolurilor și responsabilităților atât ale conducerii cât și ale angajaților și reprezentanților acestora, precum și a resurselor și a măsurilor de însoțire (de exemplu, sprijin de specialitate, monitorizare).

Etapa 5

„Monitorizarea/urmărirea comună periodică, învățarea și evaluarea" reprezintă evaluarea împreună a eficienței acțiunilor și o discuție din care să reiasă dacă mai este nevoie de analize, creșterea gradului de conștientizare, de sprijin sau alte acțiuni suplimentare.

III. Domeniul de aplicare al acordului include:

1. Competențele digitale și asigurarea unui loc de muncă

Partenerii sociali ar trebui să fie interesați să faciliteze accesul angajaților la instruiri de calitate și la dezvoltarea competențelor. O provocare esențială în acest sens va fi identificarea competențelor digitale și schimbărilor de proces concrete ce trebuie implementate într-o anumită companie.

Printre măsurile care trebuie luate în considerare se numără:

- Angajamentul părților în ceea ce privește reconversia profesională.
- Accesul la instruiri și organizarea acestora, calitatea ridicată și eficacitatea formării, introducerea de oportunități de lucru cu fracțiune de normă și alocarea de timp pentru instruire.
- Condiții de participare clar definite, inclusiv: durata, aspectele financiare, implicarea angajaților și compensarea în cazul în care instruirea are loc în afara timpului de lucru.

2. Modalități de conectare și deconectare

Angajatorul are obligația de a asigura securitatea și sănătatea lucrătorilor în toate aspectele legate de muncă. Prin urmare, dreptul la deconectare este unul dintre aspectele principale ale acestui manual. Îndemnăm sindicaliștii să susțină precizarea cu o claritate deplină și rezonabilă a așteptărilor angajatorului față de angajat atunci când lucrează cu dispozitive digitale, prin negocieri colective la nivelurile corespunzătoare.

Introducerea noilor dispozitive digitale poate oferi posibilitatea unor aranjamente de lucru flexibile, benefice atât pentru angajați cât și pentru angajatori. În același timp, poate genera riscuri serioase legate de dificultatea separării vieții profesionale de cea personală. Prin urmare, ar trebui să se pună accent pe prevenirea fenomenelor negative care afectează sănătatea și securitatea lucrătorilor. Pentru aceasta este necesară o definire clară a drepturilor, responsabilităților și sarcinilor, în care prioritatea absolută este reprezentată de principiul prevenirii.

Printre măsurile care trebuie luate în considerare se numără:

- Activități de instruire și alte activități de creștere a gradului de conștientizare al angajaților.

- Crearea unei noi culturi de lucru în rândul membrilor conducerii care să ducă la evitarea contactării angajatului în afara orelor de lucru.
- Furnizarea de orientări clare cu privire la legislația existentă în materie de timp de lucru, tele-muncă și munca mobilă.
- Organizarea eficientă a muncii, inclusiv asigurarea unui număr de angajați suficient astfel încât angajații să nu trebuiască să lucreze după orele de program.
- Compensații adecvate pentru timpul suplimentar lucrat.
- Proceduri de avertizare și de sprijin care să permită deconectarea și să protejeze împotriva sancțiunilor în cazul în care angajatul nu poate fi contactat în afara orelor de lucru.
- Prevenirea izolării la locul de muncă.

3. Inteligența artificială și garantarea principiului controlului uman

Nu există nicio îndoială că inteligența artificială va avea un impact din ce în ce mai mare asupra muncii umane. Prin urmare, Acordul european privind autonomia stabilește câteva principii și direcții privind introducerea acesteia *pe* piața muncii. Un element important care ar trebui să fie garantat la fiecare loc de muncă este controlul uman asupra IA, care reprezintă baza pentru utilizarea roboticii și a aplicațiilor bazate pe inteligența artificială. Sistemul ar trebui să fie legal și echitabil și să respecte standardele etice conforme cu drepturile omului. Pe de altă parte, din punct de vedere tehnic și social, acesta ar trebui să fie sigur și transparent.

4. Respectul pentru demnitatea umană și urmărirea

Datorită ingerinței importante a tehnologiilor moderne în procesul de lucru, există riscul că vor fi încălcate valorile fundamentale ale persoanei care lucrează (de exemplu, prin colectarea de date sensibile – accesul la spații sau documente pe baza scanării amprentelor, pupilei sau a unui cip implantat). Astfel de tehnologii cresc riscul de încălcare a demnității umane, în special în cazul monitorizării personale. Aceasta poate duce la deteriorarea condițiilor de muncă.

Reducerea la minimum și transparența datelor cu caracter personal, împreună cu reguli clare de prelucrare a acestora, reduc riscul de monitorizare intruzivă și de utilizare abuzivă a datelor. În contextul ocupării forței de muncă, normele privind prelucrarea datelor cu caracter personal ale angajaților sunt stabilite în regulamentul GDPR. De asemenea, partenerii sociali din cadrul acordului EFAD reamintesc că articolul 88 din GDPR se referă la posibilitatea de a stabili, prin acorduri colective, norme mai detaliate pentru stocarea datelor cu caracter personal ale

angajaților. Aceasta pentru a asigura protecția drepturilor și libertăților angajaților în ceea ce privește prelucrarea datelor lor cu caracter personal în contextul relației de muncă.

Printre măsurile care trebuie luate în considerare se numără:

- Permisiunea ca reprezentanții angajaților să rezolve problemele legate de date, consimțământ pentru prelucrarea datelor personale, confidențialitate și supraveghere.
- Colectarea datelor într-un scop specific și transparent. Datele nu trebuie colectate sau stocate doar pentru că acest lucru este posibil sau pentru un scop nedefinit.
- Informarea angajaților că pot să nu își dea consimțământul pentru prelucrarea unui anumit grup de date cu caracter personal sau că își pot retrage în orice moment consimțământul dat anterior.
- Punerea la dispoziția reprezentanților personalului de facilități și instrumente (digitale), de
  exemplu panouri de afișaj digitale, pentru a-și îndeplini sarcinile.

5. Punerea în aplicare și activități ulterioare

Organizațiile membre vor raporta comitetului pentru dialog social cu privire la punerea în aplicare a acordului. Comitetul pentru dialog social a fost obligat ca, în primii trei ani de la semnarea acestui acord, să pregătească și să adopte pachete anuale care să sintetizeze punerea în aplicare a acordului. Un raport complet privind activitățile de punere în aplicare întreprinse va fi pregătit de comitet și adoptat de partenerii sociali europeni în anii următori. Acordul nu aduce atingere dreptului partenerilor sociali de a încheia acorduri de adaptare și/sau acorduri complementare într-un mod care să țină seama de nevoile specifice ale partenerilor sociali în cauză.

1.2 Noile tehnologii la locul de muncă – munca asistată de tehnologie (colaboratoare) și munca complet automatizată

Atitudinea față de robotizare se schimbă atât din perspectiva întreprinderilor, cât și a lucrătorilor înșiși. Robotul nu mai rămâne doar în sfera imaginației, ci apare ca un instrument de producție care poate ușura povara oamenilor și îi poate ajuta să rezolve probleme specifice. Cu toate acestea, în funcție de sector și de etapa de producție, automatizarea poate fi introdusă în grade diferite. Pe lângă nivelul de implicare în sarcini, roboții pot fi împărțiți în roboți care desfășoară în principal activități intelectuale (de exemplu, toate instrumentele de inteligență

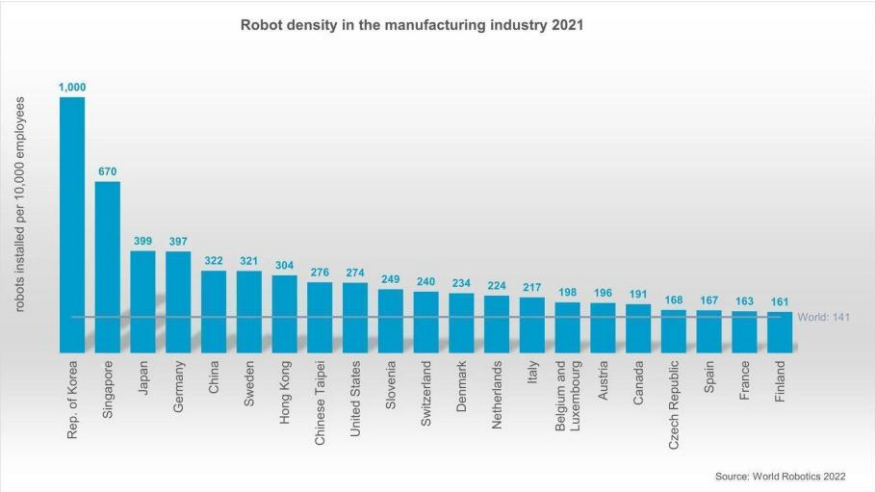
artificială) și cei care îi ajută pe oameni la îndeplinirea sarcinilor repetitive (de exemplu, ambalarea produselor).

Ce este un sistem de producție automatizat?

Automatizarea producției se referă la direcția de dezvoltare a întreprinderilor care implică o reducere semnificativă sau o înlocuire completă a muncii fizice și psihice umane cu munca mecanică. Originile acestui fenomen pot fi găsite în secolul al XX-lea când, în 1913, Henry Ford a schimbat lumea pentru totdeauna cu o linie de asamblare mobilă operată de muncitori specializați. Premisa muncii în acest mod era de a crește capacitatea de producție, reducând în același timp prețul produsului final.

În prezent, ne confruntăm cu următoarea etapă în evoluția producției – eficientizarea automatizării prin digitalizare. Datorită unor tehnologii precum modulele de programare intuitive, crearea de instrucțiuni detaliate pentru roboți devine mai ușoară. Senzorii avansați permit mașinilor să înțeleagă mediul înconjurător și să fie mai receptive. Potrivit Federației Internaționale de Robotică (International Federation of Robotics), între 2015 și 2020, densitatea roboților[1] aproape că s-a dublat la nivel mondial, crescând de la 66 de unități în 2015 la 126 de unități în 2020.

Țările cu cea mai automatizată producție (2021)



Sursa: Federația Internațională de Robotică (*The Robot Report*, 2021).

[1] Un parametru utilizat de Federația Internațională de Robotică care măsoară numărul de roboți la 10 000 de lucrători dintr-o industrie.

Munca asistată

Munca asistată are loc acolo unde anumite activități din producție pot fi înlocuite de roboți, în timp ce altele necesită intervenția umană. De cele mai multe ori, pentru sprijinirea proceselor de producție, sunt utilizați roboții colaborativi *(collaborative robots*; așa-numiții „coboți"), sarcina lor fiind aceea de a-i scuti pe lucrătorii din fabrică de o parte din volumul de muncă. O caracteristică importantă care distinge așa-numiții coboți de sistemele industriale standard (care sunt, de obicei, separate de oameni) este că, în cazul roboticii colaborative, sistemele robotizate controlate împart același spațiu de lucru cu oamenii.

Modalități prin care roboții interacționează cu oamenii:

1. **Interacțiune umană limitată –** robotul se oprește complet atunci când apare un om în zona desemnată și își reia funcționarea în mod independent după ce lucrătorul părăsește spațiul.
2. **Colaborarea umană** – datorită senzorilor încorporați, cobotul încetinește operațiunile sau întrerupe activitatea atunci când cineva se află în apropierea sa, permițând o interacțiune sigură între om și mașină.
3. **Ghidare manuală –** cobotul este controlat în permanență de către operator. De exemplu, echipamentul ține încărcătura în timp ce un om îi dirijează brațul.

Munca complet automatizată

Automatizarea în industrie este înțeleasă ca fiind utilizarea tehnologiei pentru a controla producția și a crea produse și servicii folosind instrumente digitale. În cazul automatizării complete, oamenii și mașinile încetează să mai îndeplinească sarcini complementare și încep să opereze în aceleași domenii. Ca urmare a robotizării, participarea lucrătorilor la procesele de producție scade semnificativ sau dispare cu totul. Diverse procese de producție devin complet automatizate, iar intervenția umană nu este necesară în nicio etapă a realizării produsului.

În ciuda temerilor generalizate cauzate de automatizarea tot mai mare a proceselor industriale, introducerea acestui tip de tehnologie poate aduce beneficii la diferite niveluri legate de procesele de producție – printre altele acolo unde activitatea este riscantă pentru viața și sănătatea oamenilor.

Discuție – ar trebui impozitată munca roboților?

Pe măsură ce costurile de automatizare a proceselor de producție scad, amploarea robotizării industriale crește. Consecințele așteptate ale acestui fapt includ atât aspecte pozitive, cum ar fi creșterea economică sau creșterea productivității, cât și aspecte negative, cum ar fi reducerea numărului de locuri de muncă în diferite ramuri ale sectorului de producție.

Transformarea modelelor de afaceri tradiționale provoacă numeroase controverse și există noi provocări pentru legiuitori în țările în care automatizarea s-a dezvoltat deja într-un ritm uimitor.

Odată cu reducerea semnificativă a costurilor forței de muncă și cu obținerea de profituri în urma utilizării roboților în industrie, una dintre problemele dificil de rezolvat s-a dovedit a fi **aceea a impozitelor impuse pe forța de muncă robotizată**. În schimb, în privința achiziționării de noi mașini și echipamente, guvernele diverselor state recurg la stimulente fiscale pentru a încuraja transformarea digitală și modernizarea sectorului industrial. De exemplu, în Polonia, începând cu anul 2022, antreprenorii pot deduce până la 150% din costul achiziționării de utilaje și echipamente legate funcțional de acestea, care asigură securitatea la posturile de lucru în care are loc interacțiunea om-robot.

Consecințele pozitive și negative ale robotizării

1. **Economia**

   a) **Pozitive:**

      i) Capacitatea de a îmbunătăți mai rapid produsele și de a le introduce pe piață.

      ii) Dezvoltarea mai rapidă a noilor tehnologii.

      iii) Îmbunătățirea competitivității întreprinderilor.

   b) **Negative:**

      i) Creșterea șomajului – potrivit estimărilor autorilor raportului *Future of Jobs,* din 2023 (World Economic Forum), în viitorul apropiat, mașinile vor îndeplini un procent mai mare de sarcini decât oamenii. În timp ce în 2018, în medie, 71% din timpul de lucru a constat în sarcini care implică factorul uman, această proporție se va schimba

semnificativ în 2025. Oamenii vor fi responsabili pentru aproximativ 48% din activități, în timp ce restul de 52% vor fi complet automatizate.

ii) Creșterea consumului de energie, precum și contribuția la creșterea poluării mediului.

2. Angajator

a) **Pozitive:**

i) Reducerea costurilor de producție.

ii) Reducerea riscului de comitere de erori.

iii) Posibilitatea de a evidenția mai bine capacitatea de producție.

iv) Descoperirea mai rapidă a blocajelor („gâtuielilor”), ceea ce facilitează optimizarea activității.

v) În unele țări (de exemplu, în Polonia) – este posibilă deducerea costurilor de achiziționare a roboților industriali cu un scop specific.

b) **Negative:**

i) Costuri inițiale ridicate de instalare a echipamentelor.

ii) Nevoia de inventariere și costul ridicat al reparațiilor.

iii) În cazul în care procesele sunt foarte automatizate, defecțiunile echipamentelor cauzează întreruperi ale producției.

iv) Flexibilitatea redusă a răspunsului la probleme sau erori neașteptate, în comparație cu reacțiile unui angajat.

v) Necesitatea de a se conforma unor reglementări exigente.

vi) Costuri ridicate ale consumului de energie.

3. **Angajat**

a) **Pozitive:**

i) Simplificarea deservirii procesului de producție.

ii) Sprijin în activități mai dificile sau repetitive.

iii) Eficiență crescută a producției cu o implicare mai mică a angajaților.

iv) Capacitatea de a dedica timp unor activități mai interesante datorită cedării activităților repetitive uneltelor automate.

v) Apariția de noi locuri de muncă legate de producerea, exploatarea sau repararea mașinilor.

b) **Negative:**

i) Potențiala pierdere a locurilor de muncă din cauza automatizării procesului.

ii) Probabilitate mai mare de epuizare profesională declanșată de teama de pierdere a locului de muncă.

iii) În cazul în care utilajele se defectează sau nu sunt utilizate în mod corespunzător – expunere la deteriorarea stării de sănătate/punerea vieții în pericol.

1.3 Prevenirea supravegherii disproporționate și excesive la locul de muncă

Supravegherea la locul de muncă – oportunități și riscuri

Companiile de tehnologie sunt dornice să răspundă cererii tot mai mari de tehnologii noi venite din partea angajatorilor. În schimb, direcția în care se dezvoltă instrumentele AI dă posibilitatea unui control total asupra angajaților – indiferent dacă aceștia sunt conștienți sau nu și independent de consimțământul lor. Există, de asemenea, tendințe puternice de acceptare a noii stări de lucruri drept o consecință „naturală" a dezvoltării companiilor.

Oportunități:

- monitorizarea utilizată în situații periculoase și în cazul unui accident de muncă poate fi în avantajul angajatului (de exemplu, atunci când este necesar să se demonstreze că locul de muncă nu era suficient de sigur),
- în anumite sectoare, monitorizarea este necesară pentru a asigura respectarea normelor (de exemplu, în sectorul bancar, poate fi utilizată pentru a preveni folosirea informațiilor confidențiale),
- supravegherea utilizată în timpul instruirii angajaților poate accelera procesele de obișnuire cu procesele din firmă (de exemplu, în industria construcțiilor, există *wearables* sub forma unor căștile inteligente cu senzori de vibrații care îi avertizează pe lucrători cu privire la obiectele potențial periculoase din jurul lor).

Exemplul Stellate

Stellate, un start-up din San Francisco care se ocupă cu analiza datelor, are angajații răspândiți în întreaga lume. Pe lângă instrumentele folosite pentru a putea lucra împreună de la distanță, compania monitorizează dezvoltarea angajaților săi cu ajutorul unor programe de instruire și mentorat. Scopul principal al acestor inițiative nu este însă de a sancționa

comportamentul necorespunzător sau performanțele nesatisfăcătoare ale angajaților ci, mai degrabă, de a promova în rândul angajaților companiei instrumentele ce urmează să le îmbunătățească eficiența muncii.

Riscuri:

- utilizarea excesivă sau necorespunzătoare a tehnologiilor digitale poate duce la încălcări ale
  dreptului angajaților la confidențialitate și la protecția datelor,
- riscuri pentru sănătatea mentală și fizică a lucrătorilor din cauza stresului provocat de supravegherea excesivă și de normele de lucru impuse,
- îngreunarea procesului de asociere a angajaților – urmărirea angajaților și identificarea atmosferei din firmă permite identificarea oricăror tentative de asociere (de exemplu, în fabricile mari, se întâmplă ca datele angajaților să fie folosite pentru a identifica atitudinea acestora față de angajator și pentru a determina unde *este cel* mai probabil ca angajații să se opună politicilor companiei).

Principiile de bază în ceea ce privește monitorizarea la locul de muncă

Este recunoscut că angajatorii ar trebui să aibă posibilitatea de a supraveghea locurile de muncă și de a evalua performanțele angajaților lor pentru a asigura o mai bună administrare a firmei și a proteja secretele întreprinderii, pentru a impune respectarea legii și pentru a preveni comiterea de fapte ilicite de către angajat. În același timp, Uniunea Europeană și fiecare stat membru în parte pun un mare accent pe viața privată a angajaților și pe respectul pentru viața lor personală.

Monitorizarea locului de muncă este legală, însă...[2]

- înainte de a începe utilizarea echipamentelor de supraveghere video, trebuie să fie specificate foarte clar scopurile prelucrării informațiilor (de exemplu, pentru a asigura siguranța angajaților),
- angajatorul trebuie să informeze persoanele care ar putea fi supuse monitorizării că există o monitorizare și care este acoperirea acestuia.

[2] Norme referitoare la monitorizarea locului de muncă în temeiul dreptului comunitar (articolul 8 din Convenția Europeană a Drepturilor Omului, regulamentul GDPR), decizii ale instanțelor judecătorești și ale tribunalelor, codurile muncii din fiecare stat membru.

De asemenea, este important ca scopul și acoperirea monitorizării cât și metoda de monitorizare să fie stipulate în contractul colectiv de muncă sau în regulamentul intern, de exemplu, ca parte a negocierilor colective. În situațiile în care angajatorul nu este supus unui contract colectiv sau nu are obligația de a avea regulament intern, aceste condiții se vor consemna într-o notificare.

Monitorizarea video necomunicată este permisă doar într-o măsură limitată în cazul în care există o suspiciune rezonabilă că a fost comisă o abatere gravă sau o infracțiune care a cauzat pierderi importante angajatorului.

În plus, angajatorul poate utiliza și alte tipuri de monitorizare. De exemplu, acestea pot include:

- GPS montat pe mașina de serviciu,
- monitorizarea internetului și a aplicațiilor de mesagerie utilizate pe echipamentele companiei,
- geolocalizarea telefonului mobil sau a laptopului de la firmă.

Dispozițiile privind monitorizarea video se aplică în mod corespunzător tuturor formelor de monitorizare (de exemplu, un angajator poate monitoriza e-mailul unui angajat numai după înștiințarea prealabilă a acestuia).

Monitorizarea la locul de muncă și legislația – exemple din țările partenere

Polonia

În conformitate cu Codul muncii polonez, monitorizarea reprezintă supravegherea specială a spațiilor de la locul de muncă sau a zonei din jurul locului de muncă cu mijloace tehnice care permit înregistrarea de imagini.

Monitorizarea este permisă în Polonia dacă este necesară pentru:

- asigurarea siguranței lucrătorilor,
- paza bunurilor sau controlul producției,
- păstrarea confidențialității informațiilor a căror divulgare ar putea expune angajatorul la prejudicii,
- monitorizarea poștei electronice (articolul 223 din Codul muncii), care este permisă în măsura în care este necesară pentru a asigura o organizare a muncii care să permită folosirea corectă a timpului de lucru și utilizarea adecvată a instrumentelor de lucru puse la dispoziția angajatului; monitorizarea poștei electronice nu poate să afecteze secretul corespondenței și alte bunuri personale ale angajatului.

Înregistrările video pot fi utilizate de către angajator numai în scopul pentru care au fost colectate și păstrate pentru o perioadă care nu depășește trei luni de la data înregistrării.

Cum se poate face monitorizarea în limitele legii? Procedura în șase pași

O monitorizare legală presupune ca angajatorul să evalueze impactul pe care acțiunile sale îl pot avea asupra angajaților. Pașii prezentați mai jos indică pe ce întrebări ar trebui să se bazeze o astfel de analiză.

Pașii	Întrebarea	Acțiunea
Pasul 1	În cazul în care monitorizarea a fost deja introdusă, în ce constă ea în acest moment?	Efectuarea unui audit pentru a determina ce tipuri de monitorizare sunt utilizate la locul de muncă și cine din cadrul organizației are autoritatea de a monitoriza angajații
Pasul 2	De ce s-a introdus sau ar trebui să fie introdusă monitorizarea?	• Înțelegerea scopului monitorizării angajaților. • Definirea precisă a funcției monitorizării (datele colectate în cadrul unei monitorizări anume pot fi utilizate numai în scopul pentru care au fost colectate). **Excepție**: în cazul în care, în cursul monitorizării, organizația intră în posesia unor informații despre o activitate care nu poate fi ignorată (de exemplu, o potențială activitate infracțională, mobbing), datele colectate pot fi utilizate pentru a-i trage la răspundere pe cei responsabili.
Pasul 3	Se poate atinge acest scop și fără monitorizare?	• Odată ce a fost identificat motivul introducerii monitorizării, este important să se stabilească dacă același scop poate fi atins fără monitorizarea angajaților. **Exemplu:** introducerea monitorizării paginilor accesate de angajați poate fi înlocuită cu blocarea paginilor nepotrivite sau permițând angajaților să trimită fișiere doar de pe anumite conturi și cu dimensiuni limitate.

Pasul 4	În cazul în care un anumit scop nu poate fi atins fără monitorizare, există un mijloc de control mai puțin intruziv decât cel avut în vedere în prezent?	**De exemplu**: verificarea dacă angajații nu încalcă politica de confidențialitate a companiei poate fi monitorizată atât prin controlul conținutului e-mailurilor trimise de angajați, cât și prin monitorizare automată, cum ar fi verificarea adreselor de e-mail și a subiectelor e-mail-urilor sau blocarea e-mailurilor cu atașamente de dimensiuni prea mari.
Pasul 5	Cum va afecta monitorizarea angajații?	• Trebuie să se răspundă la următoarele întrebări: ○ Poate fi considerată monitorizarea ca fiind depreciativă sau nedreaptă? ○ Va afecta monitorizarea încrederea reciprocă dintre angajator și angajați? ○ Pot fi transmise informații confidențiale sau sensibile către persoane care nu au nevoie să le cunoască? **Exemplu:** angajații de la contabilitate pot primi informația că o persoană anume a lipsit de la serviciu pe motive medicale (pentru a fi posibilă plata indemnizației de boală), dar numai managerul departamentului resurse umane trebuie să cunoască motivele medicale ale absenței.
Pasul 6	Este justificată introducerea monitorizării?	• Decizia dacă introducerea monitorizării este justificată (este mai ușor de justificat o monitorizare mai puțin intruzivă, despre care angajații sunt informați). • Personalul poate fi consultat înainte de introducerea monitorizării, pentru a gândi împreună justificarea pentru monitorizare

Supravegherea angajaților și lucrul la distanță

Supravegherea persoanelor angajate se poate face prin instalarea de aplicații de control pe calculatoarele angajaților, fapt care adesea nu este comunicat angajaților. Așa-numitele bossware[3] pot înregistra apăsările tastelor, pot face capturi de ecran și pot chiar activa camerele web ale angajaților în timp ce aceștia lucrează de la distanță.

Este demn de remarcat faptul că teama constantă de a fi supravegheat de un angajator poate duce la o deteriorare a stării psihice a angajaților. Potrivit cercetărilor, 56% dintre respondenți se

[3] Denumirea provine din cuvintele englezești "*boss*" și "*software*" și înseamnă software pentru angajatori.

simt stresați și anxioși din cauză că angajatorul le monitorizează comunicațiile electronice, 41% se întreabă în mod constant dacă sunt supravegheați și 32% iau mai rar pauze în timpul lucrului din această cauză.

Cum se poate controla eficient munca fără a aduce atingere angajaților?

Recomandări pentru angajator:

- informează-ți angajatul cu privire la instrumentele de supraveghere utilizate,
- explică regulile de utilizare a monitorizării și stabilește limitele acesteia (de exemplu, în ceea ce privește tipul de date prelucrate),
- în locul unei supravegheri excesive și a unei urmăriri a activităților zilnice ale angajatului, introduceți un sistem de responsabilitate pentru rezultate (de exemplu, trecerea în revistă și evaluarea săptămânală a sarcinilor),
- folosește aplicații de monitorizare și gestionare a fluxurilor de lucru (de exemplu, Connecteam) și îmbunătățește comunicarea la distanță între membrii echipelor și planificarea comună.

1.4 Diferența dintre munca la distanță și telemuncă – impactul asupra relațiilor de la locul de muncă

Potrivit unui studiu realizat de Comisia Europeană, în anul dinaintea izbucnirii pandemiei COVID-19, doar 5,4 % dintre angajații din UE-27 lucrau de acasă – proporție care nu se schimbase din 2009. Ca urmare a pandemiei, această proporție a crescut de mai mult de două ori, ajungând la 12,3%. În unele state membre, cifra totală a depășit chiar un sfert din persoanele angajate, indiferent de industrie sau de sectorul economic.

În ciuda dificultăților inițiale de adaptare la noua realitate (cauzate în primul rând de lipsa unei infrastructuri de tehnologia informației și comunicațiilor adecvate sau a instruirii în domeniul digitalizării proceselor de lucru), angajații nu își pot imagina astăzi întoarcerea la modul în care lucrau înainte de pandemie. Aceștia apreciază flexibilitatea mai mare la locul de muncă, posibilitatea de a petrece timp cu familiile lor și creșterea eficienței muncii.

Cu toate acestea, în ciuda popularității muncii hibride, există încă mulți angajatori și angajați care aleg să se întoarcă la birou. Aceștia argumentează această decizie printr-o colaborare și relații de muncă mai bune, precum și prin posibilitatea de a crea un mediu care favorizează inovarea colectivă și o mai bună productivitate, separând clar viața privată de cea profesională.

Munca la distanță – noțiuni de bază

Popularitatea tot mai mare a lucrului cu instrumente digitale și multitudinea de posibilități pe care acestea le oferă a necesitat utilizarea unei serii de termeni noi. Pentru o mai bună orientare în labirintul de definiții, tabelul de mai jos prezintă diferențele dintre diferitele moduri de lucru.

Tipul de activitate care utilizează instrumente digitale	Definiție
Munca la distanță	Munca la distanță se referă la orice activitate desfășurată în afara sediului angajatorului, indiferent de tehnologia utilizată. Conform modificărilor aduse Codului muncii polonez, aceasta este: munca prestată în întregime sau parțial într-un loc indicat de angajat și convenit de fiecare dată cu angajatorul.
Telemunca	Telemuncă este orice formă de organizare și/sau de desfășurare a activității cu ajutorul tehnologiei informației, în cadrul unui contract/relație de muncă în care munca, care poate fi efectuată și la sediul angajatorului, este efectuată în mod regulat în afara sediului.
Telemuncă parțială	Acest aranjament de lucru combină zilele de lucru la distanță cu cele petrecute la birou și a fost pus în practică pentru prima dată de Jack Nilles la începutul anilor 1970, în SUA.
Telemunca și munca mobilă bazate pe tehnologia informației și comunicațiilor (TICTM)	TICTM se referă la utilizarea tehnologiilor informației și comunicațiilor, cum ar fi telefoanele inteligente, tabletele, laptopurile și calculatoarele de birou, pentru a lucra în afara sediului angajatorului. Aceasta acoperă toate formele de telemuncă, dar încearcă să facă o distincție între munca de la domiciliu sau dintr-un loc fix (telemuncă) și munca mobilă bazată pe tehnologia informației și comunicațiilor. Acest din urmă termen este utilizat în Germania pentru a face distincția între munca la domiciliu și o formă de muncă mai mobilă.

Munca inteligentă/munca agilă	Munca inteligentă se referă la un sistem de lucru flexibil care permite angajaților să lucreze confortabil și eficient, fără constrângeri de timp și spațiu (oricând și de oriunde), utilizând tehnologia informației și comunicațiilor în rețea. Un termen similar („munca agilă”) este utilizat în Italia
Condiții de lucru flexibile	Organizarea flexibilă a lucrului înseamnă opțiuni de lucru alternative care permit desfășurarea activității în afara limitelor tradiționale de timp și/sau spațiu ale zilei de lucru standard.
Muncă virtuală	Munca virtuală este o muncă remunerată sau neremunerată care se desfășoară cu ajutorul unei combinații de tehnologii digitale și de telecomunicații sau care produce conținut pentru mediile digitale.
Munca hibridă	Acesta este un aranjament în care munca poate fi efectuată parțial de la sediul angajatorului și parțial de la domiciliu sau din alte locații.

Munca la distanță și telemunca – ce spune legea în această privință?

Reglementarea la nivelul UE

În prezent, nu există o legislație cu caracter obligatoriu care să se concentreze asupra telemuncii, deși mai multe directive și regulamente abordează aspecte care să asigure condiții bune de lucru pentru telelucrători. Totuși, există *Acordul-cadru* european *privind telemunca* (2002). Acest document este un acord autonom între partenerii sociali europeni (CES, UNICE, UEAPME și CEEP) și obligă organizațiile naționale afiliate să îl pună în aplicare în conformitate cu „procedurile și practicile” specifice fiecărui stat membru.

Munca la distanță/ telemunca și legea – exemplul Poloniei

Legea din 1 decembrie 2022 de modificare a Legii privind Codul Muncii și a altor legi a introdus conceptul de muncă la distanță în legislația poloneză a muncii, abrogând totodată dispozițiile privind telemunca. Conform acestei modificări, munca la distanță **este munca efectuată integral sau parțial într-un loc indicat de angajat și convenit cu angajatorul de fiecare**

dată, inclusiv la adresa de domiciliu a angajatului, printre altele, cu utilizarea mijloacelor de comunicare directă la distanță.

Pe de altă parte, **telemunca** reprezintă orice formă de organizare și/sau de efectuare a muncii cu ajutorul tehnologiei informației, în contextul unui contract/relație de muncă, în care munca **care ar putea fi efectuată și la sediul angajatorului este efectuată în mod regulat în afara acestuia**. În timp ce munca la distanță poate avea, prin urmare, caracter temporar, telemunca se bazează, în principiu, pe îndeplinirea permanentă a sarcinilor de la domiciliu.

Condițiile de desfășurare a muncii la distanță trebuie să fie convenite cu sindicatele și stipulate în regulamentul de muncă sau într-un acord individual încheiat cu angajatul. În plus, angajatorul nu poate refuza munca la distanță părinților care au copii cu vârsta sub patru ani, părinților sau îngrijitorilor persoanelor cu dizabilități sau femeilor însărcinate (cu excepția cazului în care natura sarcinilor îndeplinite nu permite acest lucru). De asemenea, angajatorul este obligat să doteze angajatul cu echipamentul și instrumentele necesare pentru efectuarea muncii la distanță și să compenseze, printre altele, costurile legate de consumul de energie electrică sau costurile cu internetul.

Munca la distanță poate fi efectuată la cererea angajatului sau din dispoziția angajatorului. Angajatorul poate, de asemenea, să dispună munca la distanță în cazul declarării stării de urgență, al unei stări de urgență epidemică sau al unei epidemii cât și în caz de forță majoră, cum ar fi distrugerea locului de muncă din cauza unui incendiu sau a unei inundații.

Modificarea Codului Muncii include, de asemenea, o propunere pentru așa-numita muncă ocazională la distanță, potrivit căreia, la cererea angajatului, acesta va putea efectua muncă la distanță pentru până la 24 de zile pe an calendaristic. Angajatorul nu este totuși ținut de cererea angajatului privind munca ocazională la distanță putând refuza să își dea acordul pentru aceasta.

Este important de menționat faptul că unui angajator îi este interzis să discrimineze un angajat pe motiv că efectuează muncă la distanță, precum și dacă refuză să efectueze o astfel de muncă. În plus, angajatorul este obligat să permită unui angajat care efectuează muncă la distanță să se afle în incinta locului de muncă, să comunice cu ceilalți angajați și să utilizeze spațiile și facilitățile angajatorului, facilitățile sociale ale companiei și activitățile sociale derulate –în aceleași condiții ca și pentru restul angajaților.

1.5 Algoritmii și discriminarea la locul de muncă

Într-o lume bazată pe informație, auzim tot mai des despre inteligența artificială ***(****artificial intelligence* **–** AI), ale cărei aplicații pot fi găsite aproape peste tot. Este de așteptat ca aceasta să fie utilizată din ce în ce mai mult și în sfera muncii. Potrivit unui studiu Forbes, aproximativ patru din cinci firme consideră că AI este o prioritate de top în strategia lor de afaceri. Cu toate acestea,

speranțele de optimizare a costurilor și de creștere a eficienței în producție sunt însoțite de teama angajaților privind pierderea locurilor de muncă – potrivit raportului Forrester's Future of Jobs Forecast, numărul locurilor de muncă pierdute din cauza automatizării va ajunge la 12 milioane numai în Europa până în 2040.

În ciuda faptului că a stârnit multe sentimente, dezbaterea publică încă nu are o explicație solidă cu privire la modul în care funcționează inteligența artificială și dacă este sigur că orice tip de automatizare poate fi clasificat drept AI. Pentru o înțelegere deplină a problemei, este necesar să se ia în considerare și care este diferența dintre un sistem de inteligență artificială și algoritmi, deoarece acești termeni sunt adesea utilizați în mod interschimbabil.

AI (inteligența artificială) este un termen extrem de larg care denumește un grup de algoritmi care își pot modifica parametrii și pot crea noi algoritmi ca răspuns la datele învățate. Această capacitate de a se schimba, de a se adapta și de a se dezvolta pe baza noilor date este ceea ce se numește „inteligență".

În termenii cei mai simpli, inteligența artificială poate fi definită ca fiind **capacitatea mașinilor de a înțelege, învăța, planifica și demonstra creativitate.** În schimb, conform definiției propuse de proiectul de regulament privind inteligența artificială (AI Act), un sistem de inteligență artificială înseamnă un software dezvoltat folosind una sau mai multe dintre tehnicile și abordările enumerate în regulament[4] , care poate – pentru un anumit set de scopuri definite de om – să genereze rezultate – cum ar fi conținut, predicții, recomandări sau decizii – care afectează mediile cu care interacționează.

Un algoritm este un set de instrucțiuni sau, mai precis, o formulă de calcul care ia decizii în mod autonom, pe baza unor modele statistice sau a unor reguli de decizie, fără intervenție umană clară. Acesta reprezintă o secvență de instrucțiuni care îi spun calculatorului ce trebuie să facă
în cadrul unui set de etape și reguli precis definite, concepute pentru a îndeplini o sarcină. Este, prin urmare, un curs de acțiune predeterminat, rigid, codificat, care este declanșat atunci când se întâlnește un anumit element.

[4] Tehnici și abordări de inteligență artificială enumerate în regulament:

(a) mecanisme de învățare automată, inclusiv învățarea supravegheată, învățarea automată nesupravegheată și învățarea prin consolidare, utilizând o gamă largă de metode, inclusiv învățarea profundă,

(b) metode bazate pe logică și cunoaștere, inclusiv reprezentarea cunoștințelor, programarea inductivă (logică), bazele de cunoștințe, motoarele de inferență și deducție, raționamentul (simbolic) și sistemele expert,

(c) abordări statistice, estimare bayesiană, metode de căutare și optimizare.

Un subiect din domeniul inteligenței artificiale este **autoînvățarea** (*machine learning*, ML). Principalul său obiectiv este crearea unui sistem care să funcționeze automat și care să fie capabil să se îmbunătățească pe baza experienței acumulate sub formă de date și să dobândească noi cunoștințe pe această bază. Procesul se bazează pe găsirea unui model în datele furnizate pentru a răspunde la o întrebare despre un set necunoscut. Este, prin urmare, un fel de predicție a viitorului folosind probabilitatea și statistica.

Nu toate inteligențele artificiale prezintă capacități de autoînvățare. Într-adevăr, uneori, un algoritm poate fi scris astfel încât programul în care este încorporat să execute comenzi fără a învăța din date noi (ca în cazul ML).

Un exemplu de algoritm care era deja programat corespunzător a fost cel al celebrului supercomputer IBM Deep Blue. Această mașină a devenit celebră după ce a reușit să câștige la șah împotriva maestrului Garry Kasparov acum 25 de ani. Aceasta datorită faptului că Deep Blue avea înregistrate toate mutările posibile, în funcție de poziționarea pieselor pe tabla de șah și de strategia adversarului. Datorită acestui fapt și a puterii sale mari de calcul, putea acționa eficient în orice situație.

Opusul algoritmului implementat în programul Deep Blue al IBM a fost programul AlphaGo de la DeepMind. Folosind mecanisme de autoînvățare, acest sistem a învățat să joace GO (un joc de societate chinezesc antic în care scopul este de a înconjura cât mai mult teritoriu posibil cu propriile pietre pe o tablă inițial goală) și chiar l-a învins pe jucătorul considerat cel mai bun din lume.

Pe de altă parte, **inteligența artificială generală** este un sistem care este conștient de sine și are cunoștințe sau abilități cognitive cuprinzătoare, care este capabil să gândească și să îndeplinească sarcini în mod autonom. Crearea unei astfel de curiozități tehnologice a fost un subiect controversat de-a lungul multor ani – punându-se în special întrebarea dacă aceasta este măcar posibilă. Potrivit unuia dintre cei mai importanți critici ai apariției inteligenței artificiale generale, filosoful Hubert Dreyfus, computerele care nu au un corp, nu trec prin copilărie și adolescență și nu participă la experiențe culturale nu pot dobândi deloc inteligență în sensul uman. Unul dintre principalele argumente ale lui Dreyfus a fost acela că dezvoltarea inteligenței umane are loc parțial în mod inconștient și, prin urmare, nu poate fi articulată și încorporată
într-un program de calculator.

Algoritmi la lucru

1. Analiza CV-ului candidatului cu ajutorul unui algoritm înainte de angajare

Angajarea algoritmică presupune utilizarea inteligenței artificiale și a sistemelor de învățare automată pentru a găsi candidați, a recruta, a intervieva și a angaja pentru un loc de muncă. Tehnica utilizează o serie de criterii pentru a evalua un candidat, inclusiv experiența și educația acestuia, și adesea filtrează CV-urile primite folosind cuvinte-cheie. Algoritmii pot ajuta, de asemenea, la evaluarea competențelor mai soft, cum ar fi înclinația unui candidat de a învăța rapid și de a lucra în echipă.

Prin utilizarea diferitelor instrumente de inteligență artificială în timpul recrutării, companiile doresc să se asigure că procesul se desfășoară în mod echitabil. Acest lucru se datorează faptului că, în teorie, în prima evaluare, automată, nu există loc pentru factorul uman și pentru o posibilă discriminare. Cu toate acestea, aceste sisteme sunt adesea criticate pentru că reflectă prejudecățile persoanelor care le-au programat.

Este important de menționat că algoritmii nu iau decizia finală de angajare. Aceștia au în primul rând rolul de a reduce numărul de candidați.

Metode de analiză a CV-urilor prin algoritm:

- **punctarea CV-urilor –** algoritmul acordă puncte în funcție de criterii prestabilite de către recrutor,
- **clasificare –** ordonarea CV-urilor pe baza apariției cuvintelor-cheie,
- **potrivire –** identificarea cuvintelor cheie care se potrivesc cu cele din anunțul de angajare,
- **analiză –** algoritmul analizează semantica CV-ului, extrage informațiile principale și le împarte în diferite categorii: experiență, competențe, date de contact.

2. Caracteristici și domenii de utilizare a algoritmilor la locul de muncă

Tipuri de algoritmi:

- **Descriptivi –** utilizați pentru a înregistra evenimente trecute și a analiza impactul acestora asupra evenimentelor prezente, cum ar fi algoritmii de evaluare a performanțelor, concepuți pentru a colecta diverse tipuri de date legate de performanța angajaților și a indica un rating general.
- **Predictivi** – scopul lor este să prezică un comportament viitor sau să estimeze probabilitatea de apariție a unui eveniment (de exemplu, prezicerea unei creșteri a cererii de noi angajați).
- **Prescriptivi/de recomandare –** sarcina lor este de a selecta cel mai bun scenariu din diferite posibilități și de a recomanda o acțiune anume sau pur și simplu de a o pune în aplicare (de exemplu, luarea de decizii privind resursele umane, alocarea sarcinilor sau programul).

Utilizarea algoritmilor la locul de muncă implică ceea ce se numește **management algoritmic**. Acesta se referă la „un sistem de control în care algoritmilor li se atribuie responsabilități pentru luarea și punerea în executare a deciziilor care afectează activitatea, reducând astfel participarea și supravegherea umană a procesului de lucru”.

Cele șase funcții esențiale în ceea ce privește gestionarea proceselor de lucru pentru care au fost utilizați algoritmi:

1. monitorizarea/controlul angajaților
2. stabilirea obiectivelor
3. managementul performanței
4. programarea
5. remunerarea
6. încetarea raportului de muncă.

Creșterea controlului angajatorului asupra angajaților cu ajutorul algoritmilor

- **Recomandarea algoritmică –** angajatorii folosesc algoritmi pentru a evalua o anumită situație și a emite sugestii menite să determine angajatul să facă activitățile indicate de algoritm.
- **Limitare algoritmică –** utilizarea algoritmilor pentru a afișa doar anumite informații și a permite anumite comportamente, în același timp împiedicând altele.

Această utilizare a algoritmilor poate crește frustrarea angajaților care, din cauza faptului că trebuie să se conformeze unor recomandări pe care nu le înțeleg, pot simți că vocea lor nu este ascultată.

Algoritmi utilizați pentru evaluarea muncii

- **Evidența algoritmică –** utilizarea procedurilor de calcul pentru monitorizarea, agregarea și raportarea, adesea în timp real, a unei game largi de date selectate cu precizie din surse interne și externe.
- **Tehnologii computaționale –** utilizate pentru a colecta evaluări și clasamente cu scopul de a calcula o anumită măsură a performanțelor angajaților; de asemenea, analiza predictivă pentru a prezice performanțele viitoare ale acestora.

Evaluarea muncii de către algoritmi poate ridica probleme specifice – nu numai legate de discriminare, ci și de pierderea sentimentului de intimitate al angajaților, de securitatea informațiilor etc.

Algoritmi utilizați pentru recompensare

Premierea algoritmică poate oferi recompense în timp real pentru comportamente care urmează recomandările anterioare, predefinite. De asemenea, poate face uz de reguli de gamificare, pentru a face experiența de lucru mai pozitivă și mai distractivă pentru angajați.

Disciplina la locul de muncă

Înlocuirea algoritmică (*algorithmic replacing*) constă din concedierea rapidă sau chiar automată din organizație a angajaților cu performanțe scăzute și înlocuirea acestora cu alți angajați, mai eficienți.

Procesul decizional automatizat și crearea de profiluri

Articolul 22 din regulamentul GDPR prevede că o persoană vizată are dreptul de a nu face obiectul unei decizii care se bazează exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice sau o afectează în mod similar într-o măsură semnificativă. Dreptul unei persoane de a contesta o decizie automatizată privind persoana sa se bazează pe cele două motive ale profilării calificate: prelucrarea automatizată și efectele juridice sau factorii care afectează în mod semnificativ persoana respectivă.

Ce este procesul decizional automatizat?

Datorită cunoștințelor codificate și a analizei precise a condițiilor de mediu, un computer poate emite instrucțiuni fără ajutorul elementului uman. Această acțiune se bazează pe calcule avansate și pe mijloace de prelucrare exclusiv tehnice. Astfel, implicarea omului în procesele decizionale este redusă la minimum, iar rezultatele sunt oferite în mod automat.

Cu toate acestea, pentru ca prelucrarea datelor să fie considerată complet automatizată, nu trebuie să existe nicio intervenție umană în procesul de luare a deciziilor. Trebuie remarcat faptul că o implicare aparentă a factorului uman în procesul decizional, constând, de exemplu, doar în aprobarea unui verdict indicat de un algoritm, nu va constitui un motiv de excludere din domeniul de aplicare a interdicției prevăzute la articolul 22 din GDPR. Cu toate acestea, în cazul în care o persoană, având puterea și autoritatea de a modifica verdictul, a luat măsuri pentru a modifica verdictul, nu ar avea loc un proces decizional automatizat.

În ceea ce privește catalogul situațiilor reglementate de articolul 22 din regulamentul GDPR, acesta este larg și acoperă atât situațiile în care decizia produce efecte juridice (adică afectează drepturile unei persoane în temeiul legii; de exemplu, dreptul la indemnizația de șomaj), cât și

situațiile în care are un „efect semnificativ similar” (de exemplu, în legătură cu situația financiară sau cu sănătatea persoanei vizate).

Ce este profilarea?

Articolul 22 din GDPR include, de asemenea, o categorie specifică de luare automată a deciziilor, și anume pe baza profilării. Termenul „crearea de profiluri” (articolul 4 din GDPR) se referă la orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind **performanța la locul de muncă**, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află **persoana fizică** respectivă sau deplasările acesteia[5] .

Exemple practice de profilare:

- **marketing –** crearea de profiluri de consumator prin colectarea de informații privind preferințele de cumpărare și sugerarea de către sistem a unor produse adaptate individual clientului,
- **împrumuturi și credite –** crearea de profiluri ale candidaților și condiționarea luării unei decizii pozitive privind creditarea de analiza datelor cu caracter personal furnizate algoritmului,
- **prestații de asistență socială –** utilizarea profilării pentru alocarea echitabilă a resurselor de asistență publică,
- **recrutare și resurse umane –** procesele de recrutare în masă se desfășoară adesea cu ajutorul unor sisteme care analizează în mod independent CV-urile și alte date despre candidați și care, pe baza acestei analize, decid dacă resping sau acceptă candidatul (de exemplu, după ce caută CV-urile în funcție de cuvinte cheie). În domeniul resurselor umane, crearea de profiluri este utilizată, de asemenea, pentru evaluarea muncii.

Riscuri asociate cu crearea de profiluri

- **Invadarea vieții private și lipsa de transparență –** deși mulți oameni sunt conștienți că anumite tipuri de date (de exemplu, cele medicale) sunt deosebit de sensibile și ar trebui protejate, o parte a publicului nu este conștientă de cât de multe informații despre ei pot fi obținute din datele comportamentale utilizate pentru crearea de profiluri

[5] Trebuie remarcat faptul că, în ciuda asemănărilor, crearea de profiluri și luarea automată a deciziilor sunt două activități diferite care pot fi sau nu legate între ele.

nedorite. În plus, procesul de creare a profilului în sine poate fi adesea netransparent și de neînțeles pentru cei afectați.

- **Discriminare –** algoritmii concepuți de oameni pot prelua prejudecățile creatorilor lor. Astfel, este posibil ca sistemul să trateze mai puțin favorabil, de exemplu, persoanele cu opinii religioase, orientare sexuală sau culoare a pielii diferite.
- **Reducerea diversității –** crearea de profiluri are ca scop evaluarea, caracterizarea și segmentarea publicului unui conținut specific în vederea adaptării materialului în funcție de interesele sau convingerile (de exemplu, politice) ale persoanelor în cauză. Astfel, se simplifică catalogul de informații furnizate utilizatorului, limitând diversitatea conținutului și creând așa-numitele „bule de informații" , îngustând totodată orizontul virtual al destinatarului.

Profilarea în procesele de muncă – studiu de caz

Din 2020, Serviciul public de ocupare a forței de muncă din Austria (AMS) utilizează profilarea algoritmică a persoanelor aflate în căutarea unui loc de muncă pentru a crește eficiența procesului de consiliere și pentru a adapta programele actuale la nevoile pieței muncii. Sistemul are ca scop clasificarea persoanelor aflate în căutarea unui loc de muncă în trei categorii:

- Grupa A. Perspective bune de a găsi un loc de muncă în perioada următoare.

- Grupa B. Perspective medii.

- Grupa C. Perspective scăzute pe termen lung.

Apoi, în funcție de categoria atribuită, un algoritm adaptează programul de asistență la nevoile individului.

Întrebare pentru discuție: Este justificată crearea de profiluri algoritmice ale șomerilor pentru a adapta programele de sprijin la nevoile acestora?

Exemplu: în New York, au fost anunțate prevederi care restricționează utilizarea instrumentelor de inteligență artificială în procesele de recrutare. După cum s-a arătat, principala problemă care apare în cazul evaluărilor făcute de inteligența artificială a fost excluderea din proces a grupurilor care nu se încadrau în cheia preprogramată. Ca exemplu, descalificarea persoanelor cu dificultăți de vorbire în timpul unui interviu video evaluat de computer, sau respingerea candidaților care suferă de artrită sau alte afecțiuni care le limitează performanțele fizice (în cazul testelor cu timp limitat).

Întrebare pentru discuție: Ar trebui interzise toate tipurile de evaluare algoritmică în procesul de recrutare?

Exemplu: un antreprenor lucra la dezvoltarea și implementarea unui instrument de inteligență artificială în cadrul companiei sale pentru a ajuta la angajarea de persoane potrivite pentru locul de muncă. Activitatea a fost întreruptă atunci când compania și-a dat seama că sistemul discrimina femeile. Motivul pentru care profilurile feminine erau respinse mai frecvent era faptul că inteligența artificială se baza pe datele din CV-urile persoanelor care lucraseră pentru companie în ultimii 10 ani (majoritatea bărbați). Ca urmare, computerul a evaluat că ar trebui să acorde prioritate bărbaților, ceea ce a redus automat șansele de apariție a candidaturilor care manifestau caracteristici feminine.

Întrebare de discuție: Puteți identifica alte exemple de discriminare care ar putea apărea în timpul recrutării care folosește algoritmi de profilare?

Riscurile și beneficiile utilizării algoritmilor împotriva angajaților

Riscuri:

- un control mai mare din partea angajatorului cu prețul vieții private a angajatului (lipsa unui consimțământ corespunzător din parte angajatului),
- erodarea autonomiei umane prin înlocuirea contactului direct dintre manageri și subordonații lor, adică „dezumanizarea" sistemelor de management,
- prejudecăți și discriminări algoritmice.

Beneficii:

- creșterea productivității prin economisirea de timp și luarea mai eficientă a deciziilor,
- o planificare mai eficientă a schimburilor și o repartizare mai eficientă a responsabilităților,
- posibilitatea unei recrutări mai rapide,
- înțelegerea problemelor care apar la locul de muncă printr-o mai bună înțelegere a mediului de lucru,
- mai puține cazuri de favorizare a anumitor angajați și eliminarea prejudecăților care pot exista în relațiile directe de muncă,
- procesul decizional automatizat limitează capacitatea de a interveni în deciziile conducerii privind salarizarea, aprobarea concediilor sau alocarea turelor.

Algoritmizarea relației angajat-angajator

Algoritmizarea proceselor de lucru este deja o realitate în multe companii. Cu toate acestea, ea acționează adesea în defavoarea angajaților în probleme precum:

- **Concedierea automată a angajaților** (aspect de discutat în cadrul atelierelor).
- **Calcularea algoritmică a remunerației:**
    - Algoritmul unei aplicații de curierat le încredința șoferilor livratori comenzi pe care trebuiau să le preia indiferent de distanța de parcurs până la punctul de preluare a comenzii. Șoferii nu erau plătiți pentru distanța parcursă până la punctul de preluare. Firma acoperea doar costul de parcurgere a unei distanțe mai scurte, astfel încât, scăzând costurile cu combustibilul și uzura mașinii, șoferii nu generau niciun profit.
    - Firma afirma că veniturile sunt în funcție de numărul de kilometri parcurși și că pentru fiecare comandă există o sumă fixă, numită „tarif de bază", care poate fi diferită de la un oraș la altul.
    - O altă problemă a fost reprezentată, în timpul pandemiei, de faptul că angajații nu erau siguri nici de tariful orar – curierii erau anunțați în timpul zilei că se modifică tariful, consecința fiind că, de multe ori, trebuiau să „aducă bani de acasă" în loc să câștige din munca depusă.
    - După ce au făcut grevă, curierilor li s-au promis mai multe schimbări, inclusiv că vor avea posibilitatea să refuze comanda de trei ori într-o zi, nu doar o singură dată. Astfel, în cazul unei modificări a tarifului de bază care nu îi avantajează, curierii au opțiunea de a refuza comanda. Totuși, nu s-a promis o stabilizare mai mare a tarifelor.
- **Identificarea algoritmică a angajaților**
    - Aplicațiile de taxi folosesc un software pentru a verifica identitatea șoferilor lor pe *baza* selfie-urilor pe care aceștia le încarcă. În 2018, s-a constatat că software-ul de tipul acesta, utilizat de o astfel de companie, era predispus la erori în cazul persoanelor cu pielea închisă la culoare (merită menționat faptul că majoritatea șoferilor care utilizează aplicațiile de taxi sunt bărbați și mulți dintre ei provin din medii BAME *(Black, Asian and minority ethnic))*.
    - În ceea ce privește verificarea identității, mai mult de o duzină de curieri au raportat că, din cauza unor probleme cu algoritmul, au fost amenințați cu rezilierea, li s-au înghețat conturile sau au fost concediați definitiv după ce un selfie pe care și-l făcuseră nu a trecut de testul *Real Time ID Check*. Unele

persoane au fost chiar concediate atunci când funcția selfie nu a mai funcționat deloc. Acest proces nu prevedea nici o modalitate de a ataca decizia luată.

- **Evaluarea algoritmică a angajaților (de performanță și nu numai)** (subiect de discutat în cadrul atelierelor).

Algoritmizarea și protecția datelor

După cum s-a menționat deja, un algoritm reprezintă o serie de instrucțiuni privind modul de transformare a unui set de date despre lume în informații utile. Pentru a simplifica și mai mult, faptele sunt tratate ca date, în timp ce informațiile sunt cunoștințe care pot fi utilizate ulterior de către oameni sau alte mașini.

Datele la locul de muncă și protecția acestora

Pentru a evita conflictele legate de viața privată, angajatorii ar trebui să pună în aplicare măsuri adecvate pentru a proteja datele cu caracter personal, în special atunci când aceste date sunt utilizate pentru luarea automată a deciziilor cu impact direct asupra angajatului. Prin urmare, este necesar să se echilibreze în mod corespunzător interesul angajatorului de a pune în aplicare tehnologii bazate pe date, pe de o parte, și binele persoanei vizate, pe de altă parte, și să se acționeze în conformitate cu principiile de bază prevăzute de GDPR.

- **Angajatorii ar trebui să colecteze date despre angajați doar atunci când acest lucru este necesar pentru gestionarea locului de muncă și pentru îndeplinirea sarcinilor de către angajați.**

În conformitate cu principiul reducerii la minimum a datelor, angajatorii ar trebui să limiteze colectarea datelor angajaților, și anume orice informații legate de identitatea, sănătatea și datele biometrice ale acestora, datele legate de activitățile la locul de muncă (de exemplu, privind productivitatea), dar și informațiile rezultate din activitățile angajaților în rețelele de socializare. Colectarea nerestricționată a datelor expune în mod inutil angajații la riscuri, cum ar fi, de exemplu, utilizarea abuzivă a datelor cu caracter personal de către angajatori sau scurgeri necontrolate.

- **Angajații ar trebui să aibă dreptul de a consulta, corecta și recupera datele proprii**

Angajații ar trebui să aibă posibilitatea de a primi toate informațiile relevante cu privire la datele lor – inclusiv de ce și cum au fost colectate datele, ce s-a dedus despre angajat din datele respective și dacă datele au fost folosite pentru a lua o decizie legată de angajare. În schimb, angajatorii ar trebui să fie responsabili pentru corectarea oricăror date inexacte.

- **Datele angajaților trebuie protejate împotriva utilizării abuzive**

Angajatorul nu ar trebui să permită în niciun caz vânzarea sau acordarea de licențe pentru folosirea datelor angajaților de către terți. Dacă nu ar fi existat această rezervă, promisiunea de profit din monetizarea datelor angajaților ar fi creat un risc prea mare ca angajatorii să folosească datele în mod necorespunzător pentru câștiguri suplimentare.

- **Consimțământul pentru prelucrarea datelor cu caracter personal**

În relațiile de muncă, consimțământul pentru prelucrarea datelor cu caracter personal este foarte controversat, deoarece, din cauza dezechilibrului dintre părți, este ușor de pus la îndoială caracterul voluntar al consimțământului dat de angajat. Trebuie remarcat faptul că un angajator ar putea cu ușurință să forțeze un angajat să se conformeze așteptărilor sale sub amenințarea unor consecințe negative asupra angajării. Cu toate acestea, în temeiul articolului 155 din GDPR, statele membre pot introduce reglementări specifice privind prelucrarea datelor cu caracter personal ale angajaților în contextul angajării și, în special, condițiile în care datele cu caracter personal pot fi prelucrate cu consimțământul angajatului.

De exemplu, în Polonia, un angajator poate colecta datele cu caracter personal enumerate în Codul muncii dacă angajatul este de acord. Cu toate acestea, trebuie remarcat faptul că consimțământul ar trebui să fie dat în mod voluntar și, prin urmare, nu va fi eficient dacă angajatul nu are posibilitatea de a-l refuza de teama de a se confrunta cu consecințe negative. În plus, acesta poate fi revocat în orice moment.

Tipuri de date utilizate în diferite etape de lucru

Etapa I. Căutarea unui loc de muncă

La ce se poate aștepta un angajator?

Angajatorul se poate aștepta de la candidat să îi furnizeze datele de bază necesare pentru a face demersuri în vederea încheierii unui contract. Aceste date pot include:

- datele de identificare (prenumele, numele, prenumele părinților, data nașterii),
- datele de contact indicate de o astfel de persoană;
- datele referitoare la educație, competențe, experiență profesională (despre școlile și facultățile absolvite, instruiri și cursuri urmate, angajatori anteriori, funcții deținute și responsabilități profesionale).

Este important de menționat faptul că, în cazul unui proces de recrutare, chiar dacă datele sunt transmise, este posibil ca nici măcar să nu se încheie un contract până la urmă.

La ce se poate aștepta un candidat?

Încă din prima etapă a procesului de recrutare, un potențial angajator care colectează date de la candidați este obligat să informeze aceste persoane cu privire la:

- denumirea completă și adresa sediului societății,
- datele de contact ale responsabilului cu protecția datelor (în cazul în care acesta a desemnat un responsabil),
- scopul prelucrării și temeiul juridic al prelucrării, destinatarii (înțeleși în sens larg) sau categoriile de destinatari pe care îi cunoaște la momentul colectării,
- intenția de prelucrare transfrontalieră a datelor (dacă este cazul),
- perioada pentru care vor fi prelucrate datele sau criteriile de stabilire a acestei perioade,
- dreptul candidatului de a solicita accesul la date, inclusiv o copie a acestora, precum și rectificarea, ștergerea sau restricționarea prelucrării,
- dreptul de a retrage acordul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza acordului înainte de retragerea acestuia (în cazul în care datele sunt colectate pe baza acordului),
- dreptul de a depune o plângere la președintele Autorității pentru protecția datelor,
- caracterul voluntar sau obligația de a furniza datele și consecințele în cazul în care nu sunt furnizate.

Etapa II. Procesul de recrutare

În timpul interviului, recrutorul poate pune multe întrebări detaliate cu privire la informațiile pe care candidatul la angajare le-a furnizat în CV. Este important, însă, ca acestea să se refere doar la aspecte legate de postul pentru care candidează. Nu sunt acceptabile întrebări care îl pot stânjeni pe candidat, care îi încalcă dreptul la viață privată sau interese personale (de exemplu, cu privire la viața privată, religie, orientare sexuală, opinii politice etc.).

Perioada de păstrare a datelor

Perioada de păstrare a datelor candidatului ar trebui să fie în conformitate cu normele de prelucrare a datelor prestabilite de către operator. Ca regulă generală, angajatorul ar trebui, prin urmare, să șteargă definitiv datele cu caracter personal ale unui candidat cu care a decis să nu încheie un contract de muncă imediat după încheierea procesului de recrutare, și anume după

semnarea unui contract de muncă cu persoana nou-angajată (de exemplu, prin ștergerea sau returnarea datelor).

Etapa III. Perioada de angajare

Odată cu stabilirea unei relații de muncă, apar anumite drepturi și obligații atât din partea angajatorului, cât și a angajatului. Punerea în aplicare a acestora implică în mod clar prelucrarea datelor cu caracter personal ale angajatului. Administrarea datelor cu caracter personal, deși reglementată în principiu de regulamentul GDPR, în cazul muncii este clarificată suplimentar de legislația națională.

De exemplu, în Polonia, în conformitate cu articolul 221 alineatele (2) și (4) din Codul muncii, un angajator are dreptul de a solicita unui angajat pe care a decis să îl angajeze să furnizeze (pe lângă datele cu caracter personal pe care le-ar fi putut obține de la acesta în cursul recrutării) și:

- adresa de reședință,
- numărul CNP,
- alte date cu caracter personal, inclusiv, printre altele, numele și datele de naștere ale copiilor săi, în cazul în care furnizarea acestor date este necesară pentru exercitarea drepturilor sale specifice în temeiul dreptului muncii,
- educația și istoricul angajărilor anterioare, dacă nu au existat motive pentru a le solicita solicitantului de angajare,
- numărul contului în care să se facă plata salariului, în cazul în care angajatul nu a solicitat ca salariul să fie plătit în umerar.

Obligațiile de informare ale angajatorului față de angajat

Deoarece angajatorul va prelucra datele angajatului într-un scop diferit decât pe timpul când era candidat, angajatul trebuie informat în acest sens. Acest scop poate fi îndeplinit prin includerea unor astfel de informații în clauza de informare furnizată candidaților în cursul procesului de recrutare, prin completarea acesteia cu informații privind scopul prelucrării și indicarea destinatarilor datelor, în cazul în care candidatul este angajat, sau prin completarea acestor informații la scurt timp după angajarea angajatului.

Controlul algoritmilor utilizați la locul de muncă (transparența algoritmilor)

Exemplele de utilizare a inteligenței artificiale la locul de muncă, prezentate mai jos, arată că utilizarea necontrolată a instrumentelor de inteligență artificială de către companii poate duce la creșterea nesiguranței locului de muncă și, prin urmare, poate avea un impact negativ asupra vieții angajaților. În același timp, conform estimărilor McKinsey Global Institute, până la 70 %

dintre companii vor fi implementat o formă de sisteme de inteligență artificială până în 2030. De aceea este atât de important să se evalueze critic noile tehnologii și să se permită autorităților de reglementare și organizațiilor independente să auditeze AI.

- În Marea Britanie, software-ul Horizon, utilizat de National Post Office, a suspectat în mod eronat anumiți angajați că au furat până la zeci de mii de lire sterline. Ca urmare a erorii a inteligenței artificiale, nu mai puțin de 736 de lucrători poștali au fost urmăriți penal, iar unii au fost acuzați și condamnați.
- În Olanda, șoferii înscriși la o aplicație de taxi au dat în judecată compania după ce un algoritm le-a blocat conturile pentru că ar fi comis fraude. Instanța le-a respins cererile deoarece a constatat că încălcările nu se încadrează în definiția procesului decizional complet automatizat în conformitate cu GDPR. Prin urmare, angajații au rămas fără nicio protecție juridică.
- În Italia, instanța a obligat una dintre companiile care livrau mâncare să dezvăluie algoritmul aplicației și să elimine elementele care, deoarece nu țineau cont de aspecte reglementate de legislația muncii (cum ar fi concediul medical sau dreptul la grevă), o făceau discriminatorie.

Algoritmii și secretul întreprinderii

În conformitate cu legislația UE, informațiile privind tehnologia sau orice alt aspect al unei firme pot fi protejate ca secret al întreprinderii. Totuși, ele trebuie să îndeplinească următoarele condiții:

- informațiile despre algoritm nu sunt cunoscute de publicul larg sau de experții din domeniu,
- informațiile privind algoritmii au valoare comercială,
- au fost luate măsuri pentru a asigura confidențialitatea informațiilor, de exemplu, acestea sunt păstrate într-un loc sigur și toți cei care au acces la ele sau cărora le sunt comunicate au semnat un acord de confidențialitate.

În cazul noilor tehnologii utilizate în procesele de lucru, nu este dificil să se respecte acest raționament. Companiile invocă adesea secretele comerciale, subliniind preocupările lor legate de pierderea competitivității ca urmare a dezvăluirii sistemelor lor interne. Prin urmare, cunoașterea algoritmilor și verificarea instrumentelor AI în sectorul privat sunt deosebit de problematice. În plus, forme suplimentare de protecție juridică sub forma unor clauze de confidențialitate împiedică persoanele din interior (actuali sau foști angajați) să împărtășească informații despre mecanismele care le coordonează activitatea.

Legea privind inteligența artificială (AI Act)

Acuzațiile repetate privind replicarea de către inteligența artificială a unor prejudecăți, inexactități sau discriminări din partea algoritmilor au determinat Comisia Europeană să își asume sarcina de a introduce reglementări pentru a controla instrumentele de inteligență artificială și a preveni efectele negative ale utilizării acestora.

La 12 aprilie 2021 CE a prezentat un proiect de regulament al UE privind inteligența artificială – primul act legislativ cuprinzător de acest tip privind instrumentele AI. Scopul regulamentului este de a oferi un mediu adecvat pentru dezvoltarea inteligenței artificiale în Uniunea Europeană, ținând seama în același timp de riscurile asociate cu dezvoltarea celor mai recente tehnologii. Mai presus de toate, AI Act urmărește ca algoritmii implementați în UE să fie siguri, transparenți, etici, imparțiali și controlați de oameni.

Abordarea bazată pe risc

Principalul obiectiv al legii este de a identifica riscurile pe care le prezintă un anumit sistem de inteligență artificială și de a condiționa obligațiile și cerințele de reglementare la care vor fi supuși atât dezvoltatorii, cât și implementatorii de AI.

- **Riscuri inacceptabile –** interzicerea AI

Interzicerea aplicațiilor deosebit de dăunătoare ale inteligenței artificiale,contrare valorilor UE, care dau naștere riscului de încălcare a drepturilor fundamentale ale persoanei, de exemplu: efectuarea de evaluări ale cetățenilor (așa-numitul *social scoring*), exploatarea vulnerabilității unui anumit grup de persoane din cauza vârstei, a dificultăților de mobilitate sau a tulburărilor mintale, utilizarea tehnicilor subliminale, utilizarea identificării biometrice în spațiile publice și în scopuri de aplicare a legii (cu câteva excepții).

- **Risc ridicat –** AI acceptabilă, dar în anumite condiții

Au fost clasificate ca fiind de risc ridicat instrumentele care au un impact negativ asupra siguranței persoanelor sau asupra drepturilor fundamentale, și anume sistemele din următoarele domenii:

  - identificarea și clasificarea biometrică a persoanelor,
  - gestionarea infrastructurii critice,
  - educație sau instruire profesională – posibilitatea de a decide în privința accesului unei persoane la educație și instruire profesională (de exemplu, corectarea examenelor),
  - siguranța produselor (de exemplu, utilizarea inteligenței artificiale în chirurgia asistată de roboți),

- angajarea, gestionarea angajaților și accesul la activități independente (de exemplu, software de analiză a CV-urilor pentru procedurile de recrutare),
- servicii publice și private de bază (de exemplu, evaluarea bonității, scoring de credit),
- aplicarea legii – conflict cu drepturile fundamentale ale persoanelor (de exemplu, verificarea autenticității documentelor),
- gestionarea migrației, a azilului și a controlului la frontiere (de exemplu, evaluarea cererilor de azil),
- administrarea justiției și procesele democratice (de exemplu, sugerarea tipului de pedeapsă și a nivelului pedepsei pentru o persoană condamnată pentru o infracțiune).

Exemple de cerințe specifice pentru sistemele cu risc ridicat:

- **Cerințe de transparență –** funcționarea sistemelor de inteligență artificială cu risc ridicat ar trebui să fie suficient de transparentă pentru a permite utilizatorilor să interpreteze rezultatele care îi privesc. Ar trebui elaborate instrucțiuni de utilizare pentru sistemele de AI cu risc ridicat.
- **Supravegherea umană obligatorie a sistemelor cu risc ridicat** – necesară pentru a oferi oamenilor o supraveghere eficientă a AI cu risc ridicat, inclusiv înțelegerea capacităților și a limitelor unui anumit sistem de AI. Măsurile de supraveghere adecvate pot include decizia de a nu utiliza sistemul de AI într-o anumită situație, ignorarea unei decizii luate de sistemul de AI sau întreruperea sistemului cu ajutorul butonului STOP.

Probleme de muncă ridicate în legea privind inteligența artificială (AI Act)

Sistemele cu risc ridicat care au un impact asupra pieței muncii și care fac obiectul unei supravegheri specifice sunt enumerate în anexa III la proiectul de lege privind AI. Este vorba despre sistemele de AI:

1. utilizate în procesul de recrutare sau de selecție a anumitor persoane și, în special, cele utilizate pentru a publica ofertele de angajare, pentru a preselecta sau filtra cererile, pentru a evalua candidații în timpul interviurilor sau al testelor.
2. care decid cu privire la promovarea sau concedierea unei persoane, stabilirea distribuției sarcinilor și monitorizarea performanțelor și a comportamentului angajaților.
3. care decid cu privire la accesul la instruirea profesională sau evaluarea cursanților.

După cum s-a spus, sistemele de inteligență artificială menționate mai sus pot avea un impact semnificativ asupra perspectivelor profesionale ale persoanelor ale căror date sunt prelucrate și, prin urmare, pot afecta mijloacele de trai și veniturile acestora. Comisia Europeană a atras, de asemenea, atenția că sistemele care sunt concepute și utilizate în mod necorespunzător pot

perpetua modele discriminatorii (de exemplu, față de femei, persoane în vârstă, persoane cu handicap, rasiale, etnice sau de altă orientare sexuală). În plus, sistemele de inteligență artificială utilizate pentru a verifica performanța (în special cele bazate pe date biometrice) pot avea un impact asupra protecției datelor cu caracter personal și a dreptului la viață privată. Prin urmare, acestea ar trebui să facă obiectul unor cerințe deosebit de stricte, iar angajații ar trebui să aibă întotdeauna o cale de atac împotriva deciziilor algoritmilor.

Critici la adresa AI Act

În ceea ce privește aplicarea AI Act la aspectele legate de ocuparea forței de muncă, au existat, de asemenea, multe critici. Potrivit experților, regulamentul acordă prea puțină atenție aspectelor legate de muncă, iar controlul transparenței algoritmilor este redus la cerințele generale de transparență enumerate la articolul 52 din proiectul de regulament. În plus, este îndoielnic că regulamentul va intra în vigoare înainte de 2025.

Teama de pierderea locului de muncă din cauza algoritmizării/robotizării

Potrivit estimărilor McKinsey, până în 2030, automatizarea în toate industriile va duce la necesitatea de a recalifica până la 375 de milioane de lucrători. O prognoză ușor diferită, deși la fel de îngrijorătoare, a fost făcută de Forumul Economic Mondial în raportul său, care a indicat în publicația *„Future of Jobs”* că progresele în domeniul algoritmizării și al tehnicilor de calcul ar putea duce la înlocuirea de către mașini a 75 de milioane de locuri de muncă la nivel mondial în următorii ani.

În ceea ce privește efectele robotizării, se poate presupune că cei care fac muncă manuală, în special munca bazată pe secvențe previzibile, vor fi cei mai afectați. Totuși, și unii profesioniști pot fi, de asemenea, afectați negativ de automatizare. Potrivit raportului *Future of Jobs* menționat anterior, printre profesiile desființate de AI, precum cea de mecanic, magazioner și manager de producție, se numără și avocații și analiștii financiari. Mai mult, efectele automatizării vor fi resimțite și de cei ale căror profesii implică colectarea și prelucrarea datelor, sarcini care sunt îndeplinite mult mai rapid și mai precis de către mașini.

Nu mai puțin de 60% dintre angajați sunt martorii automatizării unei treimi din sarcinile de la locul lor de muncă actual. Prin urmare, nu ar trebui să fie o surpriză faptul că cei angajați sunt îngrijorați de locurile lor de muncă actuale. După cum rezultă din raportul Procontent Communication's *Pandemia Automatizează Polonia?*, aproape unul din cinci respondenți (18,7%) se teme că locurile lor de muncă vor fi automatizate, urmând pierderea locului de muncă. Cu toate acestea, experții temperează temerile – dacă privim la nivel global, doar 5% dintre locurile de muncă sunt susceptibile de a dispărea complet. Mai mult, deși multe locuri de muncă vor fi

înlocuite de mașini, este de așteptat ca în locul lor să apară noi profesii, datorită creșterii cererii de competențe soft care necesită creativitate, inteligență emoțională și gândire critică.

În plus, dezvoltarea tehnologiei va contribui la crearea în continuare de noi locuri de muncă bine plătite în sectorul IT – la nivel global, acestea ar putea reprezenta până la 50 de milioane de locuri de muncă până la sfârșitul deceniului. Această abordare optimistă pare să fie confirmată de studiul Forumului Economic Mondial menționat mai sus, care indică faptul că, odată cu creșterea automatizării, vor fi create până la 133 de milioane de locuri de muncă. Deși este dificil de determinat cu precizie forma viitoarelor niveluri de ocupare a forței de muncă din cauza dinamismului schimbărilor aduse de digitalizare, este îndoielnic, conform evaluărilor experților, că în viitorul apropiat va apărea șomajul structural tehnologic.

Tehnologia în slujba incluziunii

Digitalizarea locurilor de muncă contribuie la o integrare mai eficientă pe piața forței de muncă a acelor grupuri sociale care anterior erau excluse temporar sau permanent de pe aceasta.

Pentru **persoanele cu dizabilități,** pot fi observate următoarele beneficii:

- absența dificultăților legate de transportul la locul de muncă cu care se confruntau anterior persoanele cu anumite limitări fizice,
- o expunere mai redusă la stimuli și un mod de lucru mai liniștit la distanță favorizează o muncă mai eficientă pentru persoanele cu dizabilități intelectuale, hiperactivitate sau dificultăți de concentrare și de învățare,
- utilizarea mijloacelor electronice de telecomunicații (e-mail, mesagerie instantanee) permite participarea activă la discuții a persoanelor cu deficiențe de vorbire.

Exemple de beneficii pentru **părinți**:

- posibilitatea de a petrece mai mult timp cu copiii,
- reducerea expunerii întregii familii la boli infecțioase comune (gripă, răceală, COVID-19),
- posibilitatea de a reconcilia în mod eficient viața privată cu cea profesională pentru tinerii părinți.

Munca la distanță are, de asemenea, un impact major asupra rămânerii tinerelor mame pe piața muncii (49% dintre mamele care lucrează recunosc că știu cel puțin o persoană care a renunțat la locul de muncă sau intenționează să facă acest lucru din cauza obligației de a se întoarce la birou).

Exemple de beneficii ale utilizării **aplicațiilor de taxi**:

- acționarea în direcția egalității de gen (în majoritatea orașelor americane, femeile au reprezentat până acum mai puțin de 5% din șoferii de taxi, în cazul aplicațiilor de sharing economy acest procent este deja de aproximativ 20-30%),
- facilitarea intrării imigranților (de exemplu, din Ucraina) pe piața muncii,
- oferirea de curse mai accesibile – de exemplu, aplicația Uber din Los Angeles este disponibilă în 21 de cartiere cu venituri mici, unde oferă curse mult mai ieftine decât companiile de taxi tradiționale.

1.6 Impactul noilor tehnologii asupra relațiilor contractuale – discuția din jurul smart contracts și aplicarea lor viitoare în relația angajat-angajator

Digitalizarea s-a răspândit în prezent în aproape toate domeniile vieții noastre cotidiene și private. Acest lucru este valabil și pentru relațiile contractuale încheiate anterior verbal sau în scris, care sunt acum adesea consolidate sau completate cu ajutorul instrumentelor digitale. Având în vedere cantitatea mare de informații de pe internet și încheierea tot mai frecventă de obligații reciproce cu un element digital, instrumentele bazate pe blockchain, cum ar fi contractele inteligente *(smart contracts),* vor avea cu siguranță cel mai mare impact asupra relațiilor contractuale în viitorul apropiat.

Ce este blockchain?

Blockchain (lanțul de blocuri) este o tehnologie de transfer și stocare a informațiilor privind tranzacțiile efectuate pe internet. Informațiile separate sunt aranjate în blocuri succesive de date. Odată ce un bloc este saturat cu un anumit număr de tranzacții, alte informații despre tranzacții sunt stocate în blocul următor. Datorită trimiterii la blocul anterior și înlănțuirii informațiilor din acestea, devine imposibil să se modifice sau să se șteargă înregistrarea unei tranzacții fără ca o astfel de modificare să fie înregistrată în toate celelalte blocuri. Această soluție promovează transparența tranzacțiilor efectuate și combate manipularea frauduloasă a informațiilor.

Ce sunt *smart contracts*?

Un contract inteligent este un program „autoexecutabil” bazat pe logica *„if-then”*. Acesta este scris în întregime într-un limbaj de programare și poate fi executat cu ajutorul tehnologiei registrului distribuit (DLT) sau al blockchain. În acest din urmă caz, programul este stocat pe blockchain și se execută atunci când anumite condiții declanșează o altă acțiune – de exemplu, poate declanșa o plată sau poate furniza un anumit serviciu. Prin urmare, este vorba de o **fuziune**

a realității create de un anumit contract cu lumea reală prin intermediul tehnologiei. Acest lucru face contractul mai transparent și mai demn de încredere, oferind părților încredere în îndeplinirea condițiilor sale atunci când apare o anumită situație.

Exemple de utilizare a contractelor inteligente:

- Achiziționarea unei proprietăți – datorită contractelor inteligente, procesul, care este de obicei foarte complex și necesită implicarea multor intermediari (notar, agent imobiliar, consilier juridic, instituție de creditare), este mult simplificat și nu necesită implicarea actorilor menționați mai sus, făcând posibilă dobândirea titlului de proprietate în format electronic.
- Cumpărături online – în acest caz, contractele inteligente asigură efectuarea imediată a plății și, prin urmare, expedierea mai rapidă a produsului către cumpărător.
- Prelucrarea datelor cu caracter personal – deoarece datele cu caracter personal și ID-urile digitale sunt stocate pe blockchain, riscul de furt de identitate este redus semnificativ.
- Înregistrarea rezultatelor alegerilor sau ale referendumurilor – reducerea la minimum a riscului de fraudă electorală. Utilizarea contractelor inteligente în acest scop poate fi observată în practică, printre altele, în Estonia.
- Plata despăgubirilor și a primelor – decontarea automată a cererilor de despăgubire, calcularea primelor.

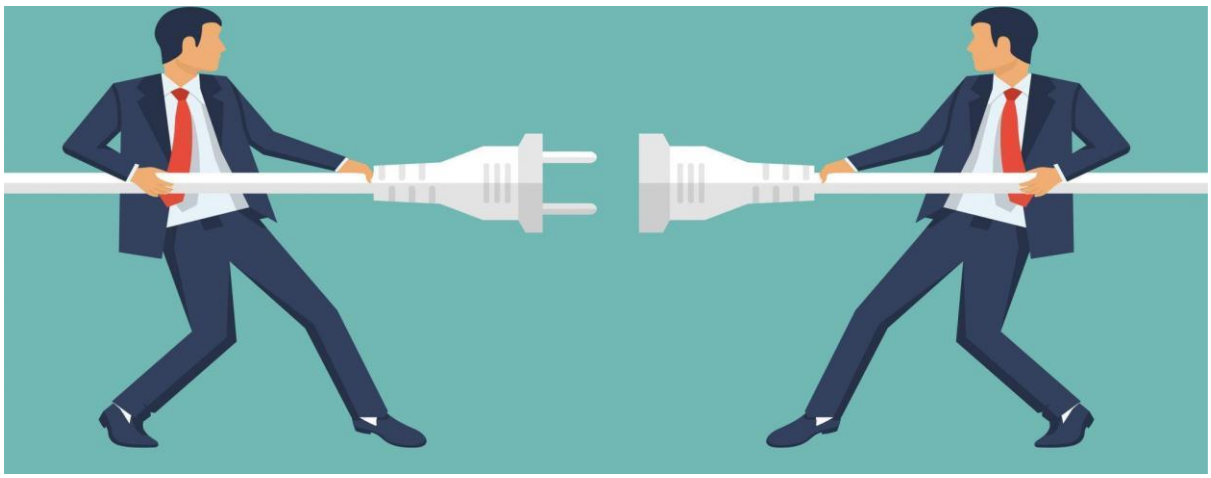
2. Impactul digitalizării asupra vieții private a angajaților

2.1 Respectarea timpului de lucru al angajaților în cazul muncii la distanță. Munca la distanță versus work-life balance

Potrivit unui studiu realizat de Eurofound, o treime dintre angajații din Uniunea Europeană au început să lucreze de acasă în timpul pandemiei, iar ca urmare a trecerii la munca la distanță, nu mai puțin de 27% au declarat că îndeplinesc sarcini de serviciu în timpul liber. În lockdown, granița dintre viața privată și cea profesională a început să se estompeze. Angajații au câștigat capacitatea de a-și organiza singuri timpul, dar au fost, de asemenea, expuși riscului de a fi permanent disponibili și de a nu se putea deconecta complet de la mediile electronice în afara orelor de lucru.

Este important de menționat faptul că în modul bazat pe sarcini (care nu se bazează pe un program de lucru rigid) se aplică aceleași reguli ca în sistemul tradițional, adică angajatul ar trebui să își îndeplinească sarcinile timp de 8 ore pe zi în cadrul unei săptămâni de lucru de cinci zile. Sarcinile efectuate în afara acestui cadru ar trebui considerate ore suplimentare. Cu toate acestea, deși orele de lucru flexibile sunt fără îndoială benefice pentru angajați, aceștia cred adesea, în mod eronat, că din moment ce nu se află la birou la ore fixe, ar trebui să arate că sunt disponibili în orice moment al zilei.

2.1.1. Dreptul la deconectare



Sursa: Shutterstock.

După cum se prevede la articolul 24 din Declarația universală a drepturilor omului, orice persoană are dreptul la odihnă și la petrecerea timpului liber, inclusiv la limite rezonabile ale timpului de lucru și la concedii periodice plătite. În plus, în conformitate cu articolul 31 din Carta drepturilor fundamentale, orice lucrător are dreptul la condiții de muncă care să îi respecte sănătatea, siguranța și demnitatea și are dreptul la perioade de repaus zilnic și săptămânal, la concediu anual plătit și, mai ales, la limitarea duratei maxime a timpului de lucru.

Noua realitate post-pandemică, în care granița dintre viața privată și cea profesională este adesea neclară, a evidențiat necesitatea de a pune în aplicare un regulament care să le ofere angajaților încrederea că se pot deconecta de la muncă și să nu răspundă la e-mailurile șefilor în afara orelor de program fără consecințe negative. Din acest motiv, în 2021, Parlamentul European a adoptat o rezoluție în favoarea dreptului la deconectare, solicitând astfel Comisiei Europene să analizeze pregătirea unei directive privind dreptul de a fi offline.

Este de remarcat faptul că rezoluțiile Parlamentului European nu au forță obligatorie. Astfel, Comisia Europeană nu este obligată să acționeze cu privire la punerea în aplicare a directivei propuse de Parlament. Cu toate acestea, având în vedere fondul problemei, este de așteptat ca Comisia să încerce să reglementeze dreptul la deconectare și să asigure un nivel uniform de protecție pentru lucrătorii din întreaga Uniune Europeană.

Așa cum a fost propusă de Parlamentul European, scopul directivei privind dreptul de a fi offline este de a garanta:

1) norme minime care să garanteze angajaților care utilizează mijloace de comunicare la distanță în munca lor zilnică dreptul de a fi offline,
2) interzicerea discriminării sau a unui tratament mai puțin favorabil (inclusiv a rezilierii contractelor de muncă) față de angajații care își exercită dreptul de deconectare,
3) tratamentul egal al tuturor angajaților, fie că sunt din sectorul public sau privat, fie că sunt angajați de nivel inferior sau manageri (deși, în acest din urmă caz, acest lucru poate fi dificil, din cauza reglementărilor specifice pentru manageri),
4) o procedură judiciară eficientă și posibilitatea de a solicita despăgubiri în cazul încălcării drepturilor acordate (acces la protecție judiciară împotriva repercusiunilor).

Obligațiile angajatorilor în ceea ce privește dreptul angajaților de a fi offline

Noile drepturi ale angajaților presupun, de asemenea, obligații suplimentare pentru angajatori. Printre acestea – nevoia de a asigura un sistem intern care să permită măsurarea cu exactitate a timpului lucrat în fiecare zi de către angajat (respectând în același timp dreptul la viață privată și la protecția datelor cu caracter personal). În plus, este important sprijinul pentru ca angajații să poată fi offline – prin comunicate clare privind noile reglementări în politicile

companiei, organizarea de campanii de instruire și informare în acest domeniu. Cu toate acestea, în ceea ce privește creșterea gradului de conștientizare, cea mai relevantă și promițătoare pare a fi obligația de a informa în scris fiecare angajat cu privire la drepturile sale.

În plus, angajatorii ar trebui să evite promovarea unei culturi a disponibilității continue și recompensarea angajaților care nu își exercită dreptul de a se deconecta. Evaluarea sănătății și a siguranței în legătură cu dreptul la deconectare (de exemplu, în ceea ce privește riscurile psihosociale) ar trebui să fie, de asemenea, un aspect important.

2.1.2. Echilibrul dintre viața profesională și cea privată – rolul statului

Sursa: Technology Headlines.

Statul și politicile sale de muncă au un rol important în modelarea relației angajat-angajator. În ceea ce privește echilibrul dintre viața profesională și cea privată, unele țări iau inițiative pentru a promova bunele practici de angajare. Pe de o parte, aceasta se referă la punerea în aplicare a reglementărilor naționale, iar pe de altă parte, la instrumente legate de lege care nu au forță juridică obligatorie, dar care încearcă să modeleze anumite comportamente.

Astfel de măsuri „soft” ar putea consta, de exemplu, în punerea în aplicare a unor coduri de bună conduită sau în oferirea unui exemplu bun pentru alți angajatori prin promovarea unei abordări favorabile lucrătorilor în cadrul structurilor guvernamentale. Această cale a fost aleasă de Malta, care a publicat în 2020 un *Manual de măsuri care vizează un echilibru între viața profesională și cea privată*. Această publicație compilează și descrie în detaliu drepturile angajaților, cu instrucțiuni privind modul în care se poate munci în mod corespunzător în era

digitalizării (de exemplu, cum să-ți organizezi munca atunci când îți îndeplinești sarcinile de la distanță). Totuși, utilitatea manualului nu constă doar într-o mai bună cunoaștere a privilegiilor angajaților sau în cunoștințe suplimentare în domeniul digitalizării. Astfel de coduri de bune practici, aplicabile la locul de muncă (sau într-un anumit sector), pot fi, de asemenea, un fel de monedă de schimb în negocierile cu angajatorul.

În cazul manualului maltez, inițiatorii proiectului au indicat că scopul lor principal a fost acela de a asigura un echilibru între viața profesională și cea privată pentru cei angajați în sectorul public prin creșterea gradului de conștientizare în rândul angajaților. Cu toate acestea, este demn de remarcat faptul că manualul nu extinde în niciun fel catalogul drepturilor lucrătorilor, ci doar atrage atenția asupra practicilor adecvate de pe piața muncii și îi face pe lucrători să conștientizeze posibilitatea de a negocia condițiile de muncă în conformitate cu dispozițiile documentului.

Exemple de promovare a dreptului la deconectare în țările UE

Deși în acest moment nu există încă un cadru juridic paneuropean care să reglementeze dreptul la deconectare, există deja câteva exemple de acțiuni legislative în acest domeniu pe scena UE. Acest lucru este dublat de promovarea dreptului la deconectare prin intermediul contractelor colective de muncă. În plus, unele state membre au implementat deja reglementări proprii privind dreptul de a fi deconectat.

Franța

Franța este considerată un pionier în ceea ce privește dreptul la deconectare. Încă din 2013, acolo a fost adoptat un acord intersectorial privind calitatea vieții la locul de muncă, care a încurajat companiile să evite să intervină în viața privată a angajaților și a definit momentul în care dispozitivele de contact ale angajaților ar trebui să fie deconectate. Aceste dispoziții au fost ulterior adoptate la 8 august 2016 și încorporate în Codul francez al muncii. În plus, din ianuarie 2017, în Franța este obligatoriu din punct de vedere legal ca angajatorii să negocieze cu sindicatele acorduri privind dreptul la deconectare.

Italia

Franța a fost urmată de Italia, care a decis să introducă dreptul la deconectare în 2017. Regulementarea se concentrează asupra persoanelor care lucrează la distanță (*smart working*, italiană: *lavoro agile*) și stabilește că lucrătorii la distanță au dreptul de a se deconecta de la dispozitivele tehnologice și de la platformele online fără a suferi consecințe din partea

angajatorilor lor. În Italia există, de asemenea, contracte colective sectoriale și de întreprindere care prevăd dreptul la deconectare.

Spania

O altă țară care a adoptat dreptul la deconectare în legislația națională a fost Spania. În 2018, odată cu transpunerea GDPR în legislația spaniolă, a fost introdus un nou pachet de drepturi digitale. Odată cu acesta, angajații care lucrează atât în sectorul privat, cât și în cel public au primit dreptul de a se deconecta, cu scopul de a menține un echilibru între viața profesională și cea privată. Conform regulamentului, angajatorii ar trebui, după ce au ascultat reprezentanții angajaților, să stabilească politici interne privind modul în care angajații își pot exercita dreptul la deconectare și să le ofere angajaților cursuri de instruire privind utilizarea corectă a noilor tehnologii.

Belgia

În Belgia, în 2018, toți angajatorii cu mai mult de 50 de angajați au fost obligați să discute cu comitetul de sănătate și securitate despre utilizarea în siguranță a instrumentelor digitale și despre dreptul angajaților de a se deconecta. Este demn de remarcat faptul că, odată cu introducerea dreptului la deconectare, angajații înșiși nu au dobândit noi competențe, ci doar oportunități sporite de a negocia cu angajatorul lor. Cu toate acestea, în 2022 a fost adoptat un nou regulament care le permite funcționarilor publici să deconecteze e-mailurile de serviciu și să nu răspundă la mesaje text și apeluri telefonice în afara orelor de program fără teama de represalii. Sunt, de asemenea, în discuție planuri de extindere a noilor reglementări și la angajații din sectorul privat.

Irlanda

În aprilie 2021, guvernul irlandez a adoptat un cod de conduită conform căruia toți angajații au dreptul de a se deconecta și de a nu răspunde imediat la e-mailuri, apeluri telefonice sau alte mesaje de la angajatorul lor după orele de lucru. De asemenea, codul a stabilit, că un angajat, ca regulă generală, nu ar trebui să fie obligat să lucreze în afara orelor de program standard și nu ar trebui să suporte consecințe dacă refuză să se ocupe de chestiuni de serviciu după orele de program.

2.1.3. Impunerea disponibilității continue de către angajator și mobbing-ul

Sursa: jobs.ca.

Mobbing-ul este o acțiune sau un comportament față de un angajat care constă în hărțuire sau intimidare persistentă și prelungită. Acesta apare atunci când acțiunile în cauză au ca scop să îl umilească sau să îl ridiculizeze pe angajat, dar și atunci când sunt menite să îl determine pe angajat să aibă o părere proastă despre aptitudinile sale profesionale.

Deoarece mobbing-ul poate lua diferite forme de agresiune, catalogul comportamentelor care se califică drept acest tip de violență rămâne deschis. Așteptarea ca un angajat să fie disponibil în orice moment sub amenințarea unor consecințe negative poate fi, prin urmare, considerată un tip de mobbing. Acest lucru este evidențiat, de exemplu, de hotărârile în care instanțele au dat dreptate angajaților care au arătat că primirea de mesaje insistente și repetate cu instrucțiuni de serviciu după orele de program sau în zilele libere ar trebui să fie tratate ca mobbing.

Hotărârea Tribunalului Regional Lublin din 20 iunie 2018. (VIII Pa 86/18)

Instanța a acordat unei angajate a unui birou municipal o despăgubire de 25.000 PLN de la angajatorul său pentru afectarea sănătății sale cauzată de trimiterea de e-mailuri insistente după orele de program. Cauza a vizat o femeie angajată ca funcționar public permanent cu normă întreagă. După schimbarea primarului, noul șef a recurs la trimiterea de instrucțiuni angajaților sub formă de e-mailuri pe adresele de serviciu și private ale acestora ca principal mod de comunicare cu aceștia. De la 1 ianuarie 2015, reclamanta a primit aproximativ

200 de e-mailuri din partea primarului, dintre care peste 100 au fost trimise după orele de lucru, inclusiv noaptea și în zilele de sărbători legale, în timpul concediului anual sau al concediului medical. Procedurile s-au finalizat cu o hotărâre a Tribunalului Regional din Lublin, în care instanța a apreciat că încărcarea unui angajat cu sarcini și trimiterea de e-mailuri cu instrucțiuni de lucru în zilele nelucrătoare, în timpul concediilor medicale și al sărbătorilor legale, precum și evaluarea inadecvată a respectării acestora poate fi considerată **mobbing.**

Încălcarea dreptului la deconectare – implicațiile pentru angajator și mecanismele de transmitere a plângerilor

Sancțiunile pentru încălcarea dreptului la deconectare pot varia de la o țară din UE la alta. Acest lucru se datorează faptului că fiecare stat membru ar trebui să stabilească în mod individual nivelul de sancțiune impus unui angajator pentru nerespectarea timpului liber al angajaților săi.

În Polonia nu a fost încă introdus un act de lege specială privind dreptul angajatului la deconectare, dar acesta poate fi dedus din reglementările generale privind timpul de lucru și din jurisprudența instanțelor. Prin urmare, este în general acceptat faptul că un angajat nu este obligat să răspundă la telefon sau să răspundă la e-mailuri după orele de lucru sau în timpul concediilor. Excepție de la această regulă este cazul în care are obligația de serviciu de a face gardă, adică să fie în stand-by, pregătit pentru a lucra în afara orelor de program.

Cele mai frecvente abateri din partea angajatorilor în ceea ce privește raportul de muncă sunt neregulile legate de încetarea contractelor, încălcarea reglementărilor privind timpul de lucru, plata necorespunzătoare a salariilor și acordarea necorespunzătoare a concediilor. În funcție de amploarea și de tipul abaterii, angajatorul poate fi sancționat cu o amendă cuprinsă între 1.000 și 30.000 PLN (zloți polonezi).

Astfel, este de așteptat ca, în Polonia, nerespectarea dreptului la deconectare să fie sancționată ca orice altă încălcare a reglementărilor privind timpul de lucru, adică angajatorul veste pasibil de amendă de până la 30 000 PLN. În plus, în cazul în care se aplică un tratament mai prost unui angajat din cauza disponibilității limitate a acestuia în afara timpului de lucru, pot apărea probleme legate de despăgubiri pentru discriminare (într-o sumă care să nu fie mai mică decât salariul minim în vigoare).

Conform unui sondaj de opinie[6] , 23,9% dintre angajații din Polonia primesc e-mailuri, mesaje text sau alte mesaje de la șefi după orele de lucru. Deși, după cum notează experții, acest lucru nu este interzis, o astfel de acțiune poate fi considerată ca o sarcină de a

[6] Sondaj realizat de UCE RESEARCH și ePsycholodzy.co.uk, https://uce-pl.com/news/blisko-24-proc-polakow-twierdzi-ze-pracodawca-kontaktuje-sie-z-nimi-w-czasie-wolnym-od-pracy.

lucra
ore suplimentare (mai ales atunci când contactul îl obligă pe angajat să îndeplinească acea sarcină). În cazul în care este necesar să se răspundă la un e-mail sau la un apel telefonic pe teme de serviciu, în conformitate cu articolul 151 alineatul (1) și 151 alineatul (2) din Codul muncii, o astfel de acțiune trebuie compensată cu o remunerație suplimentară sau cu timp liber.

Ce ar trebui să facă un angajat polonez ale cărui drepturi sunt încălcate?

a) Discuție cu angajatorul

Înainte de a decide să sesizeze instituțiile externe cu privire la o încălcare, este recomandabil ca angajatul să încerce să comunice cu angajatorul. Este important ca directorul sau proprietarul companiei să fie implicat în conversație, deoarece se poate întâmpla ca cei din conducere să nu fie conștienți de abaterile comise de șefii de la un nivel inferior.

b) Căutarea sprijinului din partea sindicatelor

Dacă discuția cu angajatorul nu are rezultat, angajatul poate căuta sprijin din partea sindicatului, dacă există unul la locul de muncă. Sindicatul are rolul de a reprezenta angajații și ar trebui să încerce din nou să ajungă la un acord cu directorul/proprietarul companiei sau cu conducerea acesteia.

c) Sesizarea asupra încălcărilor a Inspectoratul de Stat pentru Muncă (PIP)

Inspectoratul de Stat pentru Muncă (PIP) este cea mai importantă instituție care se ocupă de problemele legate de condițiile de muncă și de drepturile lucrătorilor în Polonia. Acesta este cel căruia ar trebui să i se transmită, în primul rând, sesizările oficiale privind încălcarea drepturilor

lucrătorilor. Detaliile de contact ale PIP pot fi găsite la adresa www.pip.gov.pl, iar plângerea poate fi depusă în scris, prin telegraf, telefax, e-mail, formular de plângere electronică sau oral cu consemnare într-un proces-verbal. Detaliile angajatului care depune plângerea pot rămâne anonime. În conformitate cu Legea privind Inspectoratul de Stat pentru Muncă [7] , inspectorul de muncă este obligat să nu divulge faptul că se efectuează o inspecție ca urmare a unei plângeri, cu excepția cazului în care reclamantul este de acord în scris cu acest lucru. Cu toate acestea, este important să nu uitați să argumentați în mod adecvat acuzațiile formulate și să furnizați dovezi solide, deoarece PIP va decide dacă sesizarea este credibilă și dacă va fi verificat.

d) Acționarea în instanță, la instanța districtuală

Materialele transmise către PIP pot constitui, de asemenea, probe în cazul în care cauza va fi judecată la instanța districtuală. Totuși, sesizarea instanței de judecată este o ultimă soluție, utilizată doar atunci când căile anterioare au eșuat.

2.1.4.
Work-life balance – ce este echilibrul între viața profesională și cea privată ?

Sursa: zapier.com.

Potrivit raportului OCDE How's Life? Measuring Well-being, conceptul de *work-life balance* se referă la menținerea unui echilibru între muncă (remunerată și neremunerată), viața de familie și timpul liber. Acesta se referă la capacitatea unui angajat de a-și organiza responsabilitățile astfel

[7] Articolul 44 alineatul (3) din *Legea din 13 aprilie 2007 privind Inspecția de Stat pentru Muncă* (Monitorul Oficial 2017, poziția 786, cu modificările ulterioare).

încât acestea să nu interfereze cu timpul liber. Cu toate acestea, echilibrul corect între diferitele domenii ale vieții nu depinde doar de angajat, ci și de angajator. Angajatorul este cel care, de obicei, creează cultura de lucru în cadrul companiei și impune anumite norme.

Respectarea timpului liber al angajaților, indiferent dacă efectuează muncă la sediu, muncă la distanță sau hibridă, are o importanță foarte mare. La urma urmei, starea de bine a fiecărui angajat (dispoziția; starea mentală) depinde de un echilibru bun între viața profesională și cea privată. Conform cercetărilor, o supraîncărcare cu responsabilități și lucrul tot timpul (inclusiv pentru activitățile casnice sau de îngrijire a altor persoane) poate duce la epuizare și probleme de sănătate, stres cronic și productivitate redusă.

Înainte de pandemie, timpul petrecut pentru petrecerea timpului liber și pentru propria stare de bine de către persoanele care aveau un loc de muncă cu normă întreagă era cuprins între 14 și 16,5 ore pe zi. Bărbații care lucrau cu normă întreagă foloseau cu 30 de minute mai puțin timp liber în comparație cu femeile. Statisticile arată însă diferit în cazul muncii la distanță, care a devenit larg răspândită în timpul lockdown-ului cauzat de pandemia COVID-19. Timpul petrecut în fața calculatorului a crescut atunci în mod semnificativ (până la două ore suplimentare pe zi), iar calitatea odihnei a scăzut. Lucrătorii care își îndeplinesc sarcinile de la domiciliu sunt mai predispuși să accepte să facă ore suplimentare și să îndeplinească sarcini seara sau în weekend, estompând astfel granița dintre viața privată și cea profesională.

Menținerea acestui echilibru este totuși extrem de importantă. Se evită astfel epuizarea profesională, crește motivația angajaților și implicarea în funcționarea companiei. Contribuie, de asemenea, la dezvoltarea personală și la o mai mare deschidere față de noi provocări. Astfel, în ciuda numărului mai mic de ore lucrate, productivitatea personalului crește și se reduce nevoia de asistență medicală și de concediu medical.

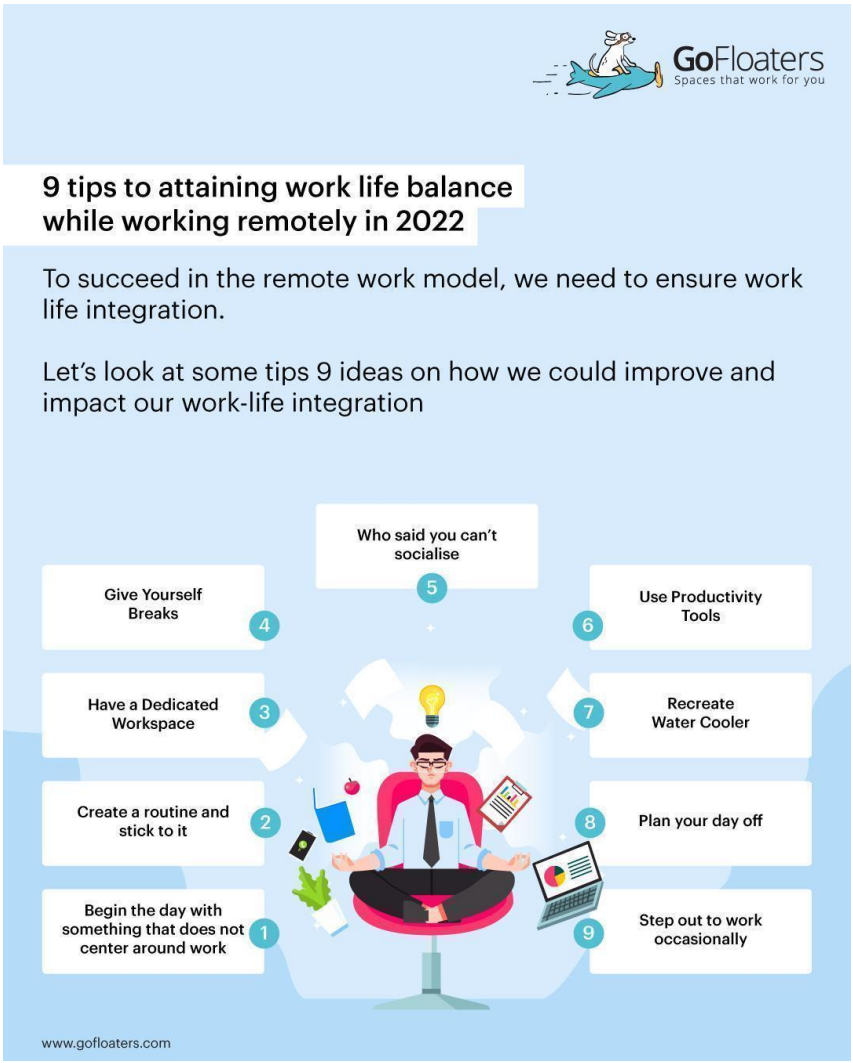
Cum poate angajatorul să îmbunătățească *work-life balance* pentru angajații săi?

Echilibrul dintre viața profesională și cea privată a angajaților depinde nu de puține ori de angajatori și manageri. Aceștia sunt cei care promovează comportamente specifice și modelează politicile la locul de muncă. Prin urmare, este important ca aceștia să sprijine bunele obiceiuri care le permit angajaților să ia o pauză de la responsabilitățile zilnice de la locul de muncă. De exemplu, angajatorii își pot încuraja angajații să facă pauze la locul de muncă, să lucreze cu un program flexibil care să le convină, să își exercite dreptul la deconectare, să își comunice clar nevoile **(**de exemplu, comunicând că sunt supraîncărcați de responsabilități și că au nevoie să o ia mai încet).

De asemenea, este important să se promoveze o cultură de lucru sănătoasă prin evitarea recompensării disponibilității permanente sau prin introducerea regulii că nu se răspunde la e-mailuri și mesaje după orele de lucru. De asemenea, este o idee bună să se ofere angajaților

cursuri de instruire privind *work-life balance* și dreptul de a se deconecta cât și recomandări despre
cum să reducă ușor utilizarea excesivă a instrumentelor digitale.

2.1.5. Sănătatea și securitatea digitală sau cum să faci să nu fii conectat non-stop la internet



Recomandări pentru angajat

1. **Dezactivați notificările de pe telefon**

Dacă telefonul personal are instalate aplicațiile de mesagerie și aplicațiile utilizate la serviciu sau căsuța de e-mail de la serviciu este legată de una privată, dezactivați toate notificările care vă pot deranja în timpul liber. De asemenea, poate fi o idee bună să stabiliți limite de timp pentru a dezactiva orice mesaj după orele standard de lucru.

2. **Utilizați un computer de la firmă în timpul lucrului și un computer privat după orele de lucru**

Alegerea unui computer al firmei pentru muncă în locul unui dispozitiv privat este de preferat nu numai din cauza problemelor de securitate cibernetică, ci și dată fiind posibilitatea de a vă limita expunerea la mesajele și comunicările primite de la serviciu după orele de program. În cazul în care compania dvs. are o politică BYOD (*bring your own device*), puteți crea două conturi (profesional și privat) pe dispozitivul dvs. și puteți trece de la unul la altul în funcție de momentul zilei și de nevoile dvs.

3. **Dimineți și seri analogice**

Radiațiile unui telefon sau laptop sunt similare cu cele ale luminii solare, reducând astfel secreția de melatonină din creier. Acest lucru, la rândul său, face mai dificilă adormirea, reduce calitatea odihnei și duce la alte probleme de somn. În interesul bunăstării dumneavoastră, încercați să nu folosiți telefonul și laptopul cu cel puțin o oră înainte de a merge la culcare. De asemenea, nu vă începeți dimineața verificându-vă nervos căsuța de e-mail sau rețelele de socializare.

4. **Introduceți intervale de timp în care utilizați instrumentele digitale**

Chiar dacă lucrați cu program flexibil, informați-i pe șefii dvs. și pe persoanele cu care lucrați despre orele la care puteți fi contactat și despre situațiile în care disponibilitatea dvs. va fi limitată.

5. **Introduceți o detoxifiere de o zi întreagă**

Deși detoxifierea digitală nu este un principiu central al ideii de *work-life balance,* deconectarea completă de la internet și de la rețelele de socializare pentru o perioadă extinsă de timp poate avea beneficii uriașe pentru starea de bine a unei persoane. Experiența desprinderii de electronice ne face mai conștienți de cât timp petrecem de fapt online. Ajută la stabilirea unor limite sănătoase între viața profesională și cea privată. De asemenea, ne motivează să scăpăm de obiceiurile proaste, cum ar fi verificarea compulsivă a căsuței de e-mail sau să punem mâna pe telefon imediat ce ne trezim. Prin urmare, se recomandă să se implementeze o detoxifiere ciclică (de exemplu, deconectarea completă la sfârșit de săptămână) iar timpul liber să fie petrecut în relaxare, la întâlniri cu familia și prietenii sau făcând activități fizice, mai degrabă decât navigând pe rețelele sociale.

2.2 Utilizarea resurselor private – forțată și voluntară

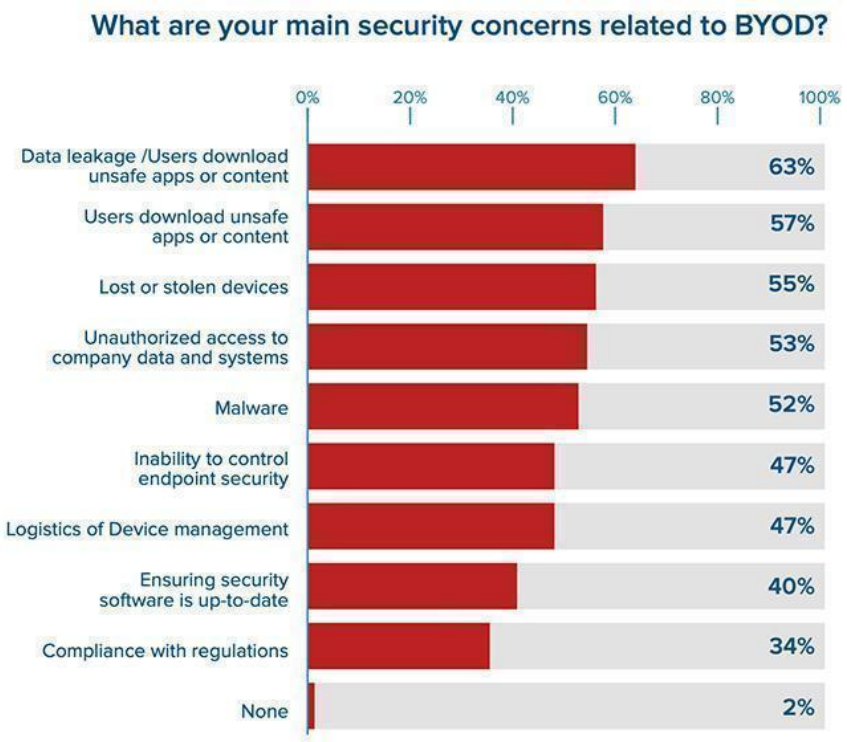
2.2.1. Ce este politica BYOD (bring your own device)?

Expresia *bring your own device este* cunoscută și sub acronimul BYOD. Aceasta reprezintă tendința de a utiliza dispozitive private, cum ar fi laptopuri, smartphone-uri sau tablete, pentru sarcinile de serviciu. Urmarea acestei tendințe este adesea rezultatul voinței angajaților înșiși (utilizarea voluntară a resurselor private). Uneori, însă, politicile BYOD sunt preferate și de către angajatori (utilizarea forțată a resurselor private). Deși această tendință are multe avantaje, înainte de a o pune în aplicare într-o companie ar trebui să se ia în considerare riscurile potențiale, cum ar fi problemele de securitate și de confidențialitate.

Merită menționat faptul că BYOD este complet opus stilului tradițional de lucru denumit *„here's your own device" (*HYOD), în care companiile le oferă angajaților orice dispozitiv electronic de care au nevoie pentru muncă.

Avantajele politicii BYOD:

- **Flexibilitate –** BYOD presupune acordul angajatorului de a accesa documentele companiei de pe dispozitivele private ale angajatului. Astfel, îndeplinirea sarcinilor profesionale devine posibilă oriunde și oricând. În plus, o mai mare flexibilitate se manifestă prin posibilitatea de a testa noi soluții, software, instrumente digitale, deoarece angajații nu sunt limitați la utilizarea unui singur tip sau marcă de dispozitiv.
- **Confort –** unul dintre avantajele politicii BYOD este că angajații pot folosi dispozitive pe care le cunosc bine și pe care se simt confortabil să le folosească.
- **Creșterea productivității** – utilizarea propriului laptop sau smartphone poate facilita procesul de integrare a noilor angajați, precum și creșterea productivității angajaților permanenți.
- **Costuri mai mici (avantajul angajatorului) –** prin acceptarea unei politici BYOD, angajatorii se sustrag adesea de la obligația de a pune la dispoziția angajatului echipament de lucru, evitând astfel costuri suplimentare.
- **Descentralizarea datelor (avantajul angajatorului) –** păstrarea documentelor de serviciu pe un laptop privat (atâta timp cât acestea sunt bine protejate) poate fi benefică pentru companie datorită nivelului mai ridicat de descentralizare a datelor. În cazul unei scurgeri de date sau al unui atac malware asupra sistemului companiei, fișierele de pe dispozitivele angajaților nu vor fi interceptate împreună cu baza de date centrală a companiei.



Sursa: helpnetsecurity.com, *BYOD adoption is growing rapidly, but security is lagging*, https://www.helpnetsecurity.com/2020/07/09/byod-adoption-is-growing-rapidly-but-security-is-lagging/.

Dezavantajele politicilor BYOD:

- **(in)securitate** cibernetică – pe lângă beneficiul descentralizării datelor, problemele de securitate cibernetică reprezintă cel mai mare dezavantaj al politicilor BYOD. Atunci când folosesc dispozitive private, angajații au tendința de a păstra documente confidențiale pe unitățile lor, care tind să fie mai puțin sigure decât cele ale companiei. În plus, atunci când lucrează de la distanță din locuri publice (de exemplu, cafenele, biblioteci, mijloace de transport), aceștia se conectează adesea la rețeaua altcuiva, crescând astfel probabilitatea să le fie sparte calculatoarele și să fie instalate programe malware. În plus, există riscul ca dispozitivul unui angajat să fie furat sau pierdut.
- **Incompatibilitate –** flexibilitatea în alegerea instrumentelor de lucru se poate traduce prin probleme de compatibilitate cu sistemele utilizate în mod implicit în cadrul companiei. Astfel, în cazul BYOD, pot apărea probleme legate de incompatibilitatea formatelor și de utilizarea deficitară a documentelor de serviciu (de exemplu, pentru că fișierele sunt salvate diferit pe Windows și diferit pe MacOS).
- **Recuperarea datelor –** politica BYOD poate cauza probleme în ceea ce privește recuperarea datelor stocate pe dispozitivul unui angajat atunci când încetează relația de muncă. Acest lucru se datorează faptului că angajații au control deplin asupra dispozitivelor lor și pot dispune în mod independent de fișierele stocate pe acestea.

Drepturile și obligațiile în cazul lucrului în modelul BYOD

În cazul în care se efectuează lucrări pe echipamente aflate în proprietate privată, este necesar ca acestea să fie conforme cu cerințele de sănătate și siguranță. Cu toate acestea, asigurarea acestor echipamente nu este obligatorie – angajatul și angajatorul pot conveni asupra domeniului de aplicare a asigurării și asupra regulilor de utilizare de către angajat a echipamentelor necesare pentru muncă și aflate în proprietatea acestuia.

Exemplul Poloniei – modificarea Codului muncii și noi reglementări privind munca la distanță

Este demn de remarcat faptul că un angajat cu contract de muncă are dreptul de a solicita un computer al companiei, iar angajatorul este obligat să i-l pună la dispoziție. Cu toate acestea, dacă pentru prestarea muncii este utilizat echipament privat, atunci angajatul are dreptul la o indemnizație în bani. În plus, angajatorul ar trebui să acopere costurile la electricitate și de servicii de telecomunicații necesare pentru munca la distanță. Rambursarea poate fi în valoare reală sau sub forma unei sume forfetare convenite între părți. La stabilirea valorii indemnizației și a sumei forfetare, angajatorul trebuie să țină seama de prețurile materialelor și echipamentelor, precum și de cele ale energiei electrice și ale serviciilor de telecomunicații[8] .

În cazul în care munca se desfășoară la domiciliu, angajatorul își îndeplinește obligațiile de sănătate și securitate față de angajat, cu excepția:

- obligația de a se îngriji de starea de siguranță și de igienă a spațiilor de lucru,
- obligații legate de construcția sau modificarea clădirii în care se află spațiile de lucru,
- obligația de a asigura condiții adecvate de igienă și instalații sanitare.

Astfel de obligații ale angajatorului de a asigura condiții de muncă adecvate pentru angajații săi au, de asemenea, un impact asupra aspectelor legate de domeniul de aplicare al termenului „accident de muncă” și de securitatea socială. Un angajat care suferă un accident de muncă, indiferent de indiferent de locul în care acesta își îndeplinește sarcinile – lucrând la distanță sau la locul de muncă – are dreptul la **prestații de securitate socială.**

Înainte de a i se permite să lucreze la distanță, angajatul confirmă printr-o declarație (transmisă pe suport de hârtie sau electronic) că a citit evaluarea riscurilor și informațiile angajatorului care conțin principiile de lucru la distanță în condiții de siguranță și sănătate și că se angajează să le respecte.

Evaluarea riscurilor profesionale ia în considerare în special efectele muncii la distanță asupra vederii și a sistemului musculo-scheletal al lucrătorului. De asemenea, se iau în

[8] *Legea din 1 decembrie 2022 de modificare a Legii - Codul muncii și a altor acte* (DZ.U. din 2022, poziția 240).

considerare condițiile psihosociale ale locului de muncă în cauză. Pe baza rezultatelor evaluării, angajatorul elaborează informații care conțin principii și modalități de organizare adecvată a locului de muncă la distanță. Acestea ar trebui să țină seama de cerințele ergonomiei, de desfășurarea în condiții de siguranță și igienă a muncii la distanță, de activitățile care trebuie desfășurate după terminarea muncii la distanță, precum și de regulile de abordare a situațiilor de urgență care prezintă un risc pentru viața sau sănătatea umană. Angajatorul poate, de asemenea, să întocmească o evaluare universală a riscurilor pentru grupuri specifice de posturi de lucru la distanță.

2.3 Confidențialitatea datelor personale și securitatea persoanelor care lucrează în rețea

2.3.1. Lucrul la distanță

Datorită popularității tot mai mari a muncii la distanță hibride sau cu normă întreagă, legiuitorii din multe state membre au decis să își modifice legislația muncii în consecință. În special, obligațiile angajatului și ale angajatorului trebuiau să fie adaptate la noile forme de muncă. Acestea decurg din necesitatea de a se asigura că infrastructura IT sau spațiul de lucru de la locul de muncă la distanță sunt adecvate pentru a îndeplini cerințele de sănătate și siguranță.

Munca la distanță și dreptul muncii – exemplul Poloniei

1. **Instrumente de lucru la distanță**

În conformitate cu propunerea de modificare a Codului muncii, articolul 67 alineatul (24) § 1, angajatorul este obligat să ofere salariatului care lucrează la distanță:

- **Materiale și instrumente de lucru –** aceasta include echipamentul tehnic necesar pentru lucrul la distanță (în funcție de specificul postului, în afară de calculator, acestea pot include, de exemplu, căști adecvate pentru întâlniri online, microfon etc.).
- **Instalarea, repararea și întreținerea instrumentelor de lucru –** inclusiv a echipamentelor tehnice necesare pentru lucrul la distanță. Alternativ, angajatorul poate, de asemenea, să acopere costurile necesare legate de aceste servicii.
- **Instruirea și asistența tehnică** necesare pentru desfășurarea activității la distanță.
- **Acoperirea costului energiei electrice –** angajatorul trebuie, de asemenea, să acopere costul energiei și al serviciilor de telecomunicații necesare pentru munca la distanță.

Un acord între angajator și organizația sindicală a întreprinderii sau regulamentul de muncă poate obliga angajatorul să acopere și alte costuri legate direct de desfășurarea activității la distanță.

2. Amenajarea spațiului în munca la distanță – controlul angajatorului

Angajatul este obligat să își organizeze postul de lucru la distanță ținând cont de cerințele ergonomiei. Aceasta include, printre altele, alegerea unui scaun confortabil, a unui birou de înălțime corespunzătoare, poziționarea corectă a monitorului în raport cu ochii și o iluminare adecvată.

În cazul în care activitatea se desfășoară la domiciliul angajatului, angajatorul își îndeplinește obligațiile de sănătate și securitate față de angajat, mai puțin:

- obligația de a se îngriji de siguranța și igiena spațiilor de lucru,
- obligația prevăzută în capitolul III din secțiunea a zecea a Codului muncii (reglementări privind obiectivele de construcții și spațiile de lucru),
- obligația de a asigura echipamente adecvate de igienă și sanitare.

Astfel de obligații ale angajatorului de a asigura condiții de muncă adecvate pentru angajații săi au, de asemenea, un impact asupra aspectelor legate de domeniul de aplicare al termenului „accident de muncă” și de asigurarea socială. Un angajat care suferă un accident la locul de muncă, indiferent de locul în care își îndeplinește sarcinile (lucru la distanță sau la locul de muncă), are dreptul la **prestații din asigurările sociale.**

Date fiind obligațiile angajatorului în ceea ce privește:

- aplicarea de măsuri adecvate pentru a preveni accidentele în cazul muncii la distanță,
- luarea măsurilor necesare pentru a elimina sau a reduce riscul producerii unui astfel de accident,
- acordarea primului ajutor persoanelor rănite, precum și circumstanțele și cauzele accidentului, în conformitate cu acordul încheiat cu organizația sindicală a întreprinderii sau în regulamente;

angajatorul are dreptul de a efectua o inspecție cu privire la:

- sănătatea și siguranța la locul de muncă,
- **respectarea securității și protecției informațiilor**, inclusiv a procedurilor de protecție a datelor cu caracter personal.

În conformitate cu noile reglementări din Codul muncii, un angajator va putea introduce controale de sobrietate pentru angajați doar dacă acest lucru este necesar pentru a asigura protecția vieții și sănătății angajaților, a altor persoane sau a bunurilor.

Fiecare control de sobrietate ar trebui să fie:

- derulat de comun acord cu angajatul,
- derulat la locul de muncă la distanță și în timpul orelor de lucru ale angajatului,
- adaptat la locul și tipul de muncă la distanță,
- să nu împiedice utilizarea spațiilor domestice într-o manieră conformă cu destinația lor,
- în cazul muncii ocazionale la distanță, controalele de sobrietate ar trebui să aibă loc pe baza unor condiții agreate cu angajatul,
- derulat cu respectarea intimității angajatului și a altor persoane (de exemplu, alți membri ai gospodăriei sau chiriași).

În cazul în care, în timpul unei inspecții, angajatorul constată deficiențe în ceea ce privește sănătatea și siguranța, securitatea și protecția informațiilor, inclusiv protecția datelor, acesta are două opțiuni. Acesta poate fie să îi acorde angajatului un termen limită pentru a remedia deficiențele, fie să își retragă consimțământul pentru ca angajatul să desfășoare activități la distanță.

3. Protecția datelor cu caracter personal în munca la distanță conform modificărilor aduse Codului Muncii

Având în vedere riscul crescut de scurgere de date cu caracter personal și alte încălcări în acest domeniu, angajatorul ar trebui să stabilească proceduri pentru protecția datelor cu caracter personal. De asemenea, va trebui să se asigure o instruire adecvată în cadrul organizației. Pe de altă parte, un angajat care efectuează muncă la distanță ar trebui să confirme că s-a familiarizat cu standardele stabilite de angajator în scris sau în format electronic.

Atât angajatul, cât și angajatorul ar trebui să stabilească, de asemenea, cum și cu ce instrumente vor comunica de la distanță și vor transmite informații privind desfășurarea activității.

2.3.2. Cum se aplică GDPR-ul pentru protejarea datelor cu caracter personal atunci când se lucrează de la distanță?

Popularitatea tot mai mare a muncii la distanță a crescut riscul de scurgere a informațiilor sensibile ale companiei. Acest lucru se datorează faptului că poate fi dificil atât pentru angajat, cât și pentru angajator să stabilească cu exactitate în ce condiții au fost încălcate normele de protecție a informațiilor, de securitate și de protecție a datelor. Întrucât este probabil ca munca la distanță (cel puțin parțial) să rămână cu noi pentru o perioadă lungă de timp, este necesar să ne amintim care sunt cele mai frecvent încălcate norme de protecție a datelor. Merită, de asemenea, să analizăm riscurile care îi pândesc pe cei care lucrează la distanță și modul în care se poate diminua riscul de apariție a acestora.

AMINTEȘTE-ȚI!

În conformitate cu articolul 32 din regulamentul GDPR, angajatorul, în calitate de operator al datelor dumneavoastră cu caracter personal, ar trebui să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un grad de securitate corespunzător gradului de risc de încălcare a drepturilor sau libertăților persoanelor fizice, cu probabilitate și gravitate diferite.

În acest scop, angajatorul poate lua următoarele măsuri:

a) pseudonimizarea și criptarea datelor cu caracter personal,

b) asigurarea confidențialității, integrității, disponibilității și rezilienței sistemelor și serviciilor de prelucrare a datelor,

c) asigurarea că disponibilitatea datelor cu caracter personal și accesul la acestea pot fi restabilite rapid în cazul unui incident fizic sau tehnic,

d) asigurarea că eficacitatea măsurilor tehnice și organizatorice de asigurare a securității prelucrării datelor cu caracter personal poate fi testată, măsurată și evaluată în mod regulat.

După cum a explicat Comisia Europeană, angajații care prelucrează date în cadrul activității lor
în cadrul organizației îndeplinesc astfel sarcinile unui operator de date. Ca atare, și aceștia sunt responsabili de asigurarea securității datelor cu caracter personal.

Deși securitatea cibernetică este una dintre cele mai importante provocări cu care se confruntă în prezent instituțiile statului, gradul de conștientizare a publicului cu privire la aceasta rămâne limitat. Aproape toată lumea a auzit de securitatea cibernetică și de importanța acesteia, însă comportamentul cetățenilor nu reflectă întotdeauna un nivel ridicat de cunoștințe pe această temă. Potrivit unui sondaj realizat în 2022 pe site-ul ChronPESEL.pl și în cadrul Registrului național al datoriilor, unul din trei polonezi se teme de scurgerea de date personale, dar mai puțin de jumătate dintre cei chestionați ar ști ce să facă într-o astfel de situație.

Deși este imposibil să se asigure protecția datelor și securitatea informațiilor în proporție de 100%, există o serie de măsuri preventive care pot reduce în mod adecvat riscul de scurgere a datelor și alte pericole.

Amenințările care se ascund în mediul de lucru la distanță nu sunt cu mult diferite de cele de care ar trebui să se ferească orice utilizator de internet. Scopul lor este cel mai adesea de a fura informații protejate sau date despre o anumită persoană sau companie, permițând atacatorului să obțină un avantaj financiar, un avantaj competitiv sau alte obiective. Potrivit unui raport al Agenției pentru Securitate Cibernetică a Uniunii Europene (ENISA), cele mai frecvente și mai periculoase amenințări cibernetice sunt:

1. **Software rău intenționat** (*malware*) – reprezintă coduri sau aplicații rău intenționate care îngreunează sau împiedică complet utilizarea normală a unui terminal (de exemplu, un computer sau o imprimantă). Prin infectarea echipamentului în cauză cu malware, infractorii pot obține acces la date sau la alte funcții ale dispozitivului. De asemenea, aceștia pot avea ca scop blocarea completă a dispozitivului, cu condiția ca utilizatorul sau o altă persoană afectată parțial de atac să plătească o răscumpărare.

2. ***Ransomware* –** un tip de malware cu ajutorul căruia un infractor blochează accesul utilizatorilor la sistemele lor sau la fișierele personale și apoi solicită o taxă în schimbul restaurării acestora.
3. **Atacurile prin intermediul site-urilor web –** o metodă prin care hackerii înșală victimele atacurilor lor, folosind sistemele și serviciile de internet ca un canal pentru a pregăti și a efectua un atac. În special, se poate distinge aici furnizarea sau facilitarea de URL-uri sau scripturi rău intenționate pentru a direcționa utilizatorul către un site web dorit sau pentru a descărca conținut rău intenționat. Rezultatul este implementarea de coduri rău intenționate într-un site web autentic existent, în scopul de a fura informații și de a obține beneficii financiare.
4. ***Phishing* –** la fel ca în cazul altor atacuri cibernetice, scopul infractorilor cibernetici este de a obține informații valoroase, în special nume de utilizator, parole, numere CNP sau numere de carduri de credit. Denumirea provine de la faptul că infractorii folosesc o momeală adaptată la persoana specifică ale cărei date vor să le fure. Pentru aceasta, ei folosesc de obicei e-mailuri sau SMS-uri false, precum și canale de comunicare pe rețelele de socializare. Pentru a crea încredere, infractorii cibernetici se dau drept companii de telecomunicații, servicii de curierat, bănci, site-uri de licitații și chiar instituții ale statului. Acționând pe baza emoțiilor victimei, ei încearcă să o determine să acceseze un link pregătit de ei către un site web care, deși este similar cu cel autentic, a fost creat de infractor și reprezintă canalul său de fraudare.
5. **DDoS –** (*distributed denial of service*) este un tip de atac care vizează serviciile de rețea sau sistemele informatice. Sarcina lor este de a acapara toate resursele disponibile și libere pentru a împiedica funcționarea întregului serviciu pe internet. Atacul poate afecta site-ul web al unei companii, poșta electronică găzduită a unui angajat etc. Se desfășoară de pe diferite dispozitive informatice în același timp – în principal de pe cele asupra cărora s-a preluat controlul cu ajutorul unor viruși speciali – boți sau troieni. Pericolul acestui tip de atac constă în faptul că utilizatorul echipamentului în cauză poate să nu știe că computerul său este folosit pentru a efectua un DDoS.
6. **Furtul de identitate –** folosind numărul CNP, detaliile personale sau cartea de identitate a unei persoane, un infractor se dă drept persoana respectivă pentru a obține, de exemplu, un credit sau pentru a folosi identitatea acesteia în interes propriu.
7. **Încălcarea securității datelor –** este un tip de incident de securitate cibernetică în care informațiile (sau o parte a unui sistem informatic) sunt accesate fără autorizația corespunzătoare, de obicei cu rele intenții. Acest lucru duce la o potențială pierdere sau utilizare abuzivă a informațiilor respective. Motivul apariției acestui tip de amenințare se datorează adesea la ceea ce se numește eroare umană, care poate apărea în timpul

configurării și implementării anumitor servicii și sisteme, ceea ce duce la expunerea neintenționată a datelor.

8. **Scurgerea de informații –** o consecință frecventă a breșelor de securitate a datelor, care acoperă o gamă largă de informații aflate în pericol – de la informații de identificare personală, la date financiare stocate în infrastructura IT și până la date personale de sănătate stocate în sistemele furnizorilor de servicii medicale.
9. **O amenințare din interior** (abuz de putere) – este o acțiune întreprinsă de o persoană sau de un grup de persoane legate de victima unui atac printr-o relație profesională sau de altă natură, în care atât atacatorul, cât și victima rămân în aceeași rețea sau infrastructură sau au capacitatea de a obține informații prin interconectare. Există mai multe modele asociate cu aceste tipuri de amenințări. Ele pot apărea, de asemenea, atunci când persoane din exterior colaborează cu persoane din interior pentru a obține acces neautorizat la resurse. De asemenea, persoanele din interior pot provoca prejudicii în mod involuntar, din neatenție sau din lipsă de cunoștințe. Întrucât persoanele din interior au adesea încredere în colegii lor și cunosc procesele și procedurile organizației, poate fi dificil să se facă distincția între accesul legitim la date și sisteme și acțiunile de rea-credință.
10. **Botnet –** o rețea de dispozitive interconectate infectate cu programe malware de tip bot. Acestea sunt utilizate de obicei pentru a lansa atacuri de tip DDoS. Botnet-urile pot fi controlate de la distanță de către un infractor pentru a acționa în mod sincronizat în vederea obținerii unui anumit rezultat.

2.3.4. Igiena cibernetică – cum să fii în siguranță online în fiecare zi?

1. **Dacă puteți, lucrați într-un spațiu sigur și privat.**

Scurgerea de date poate avea loc nu numai ca urmare a unui atac de hacking, ci și prin metode mai puțin sofisticate, convenționale – cum ar fi o privire ce surprinde conținutului ecranului calculatorului și fotografierea monitorului nostru. Este de la sine înțeles că, în afară de un spațiu de lucru pregătit de angajator, cel mai sigur spațiu pentru a lucra de la distanță pare a fi propriul spațiu de lucru de acasă. În mod ideal, acesta ar trebui să fie o cameră care se poate încuia și în care vă puteți separa în liniște de restul persoanelor din casă.

În cazul în care nu este posibil să lucrați într-o cameră izolată (de exemplu, în timpul unei călătorii de afaceri), problema siguranței devine mult mai complicată. În special, feriți-vă de spațiile deschise (cafenele, trenuri, aeroporturi), unde oamenii din jurul nostru se schimbă tot timpul. În plus, în multe locuri de acest tip sunt instalate camere de supraveghere, care pot

înregistra nu numai acțiunile celor aflați în raza de acțiune, ci și tot felul de alte elemente din mediul înconjurător, inclusiv ecrane de calculator.

Soluție: Obțineți un filtru de confidențialitate/folie pe ecran

Cu acest instrument, conținutul ecranului este vizibil doar pentru persoana care utilizează calculatorul/telefonul. Tehnologia funcționează într-un mod similar cu micro-blindurile – filtrul este format din canale microscopice orientate spre persoana care utilizează ecranul monitorului. Persoanele care privesc ecranul dintr-un unghi diferit nu vor vedea același conținut.

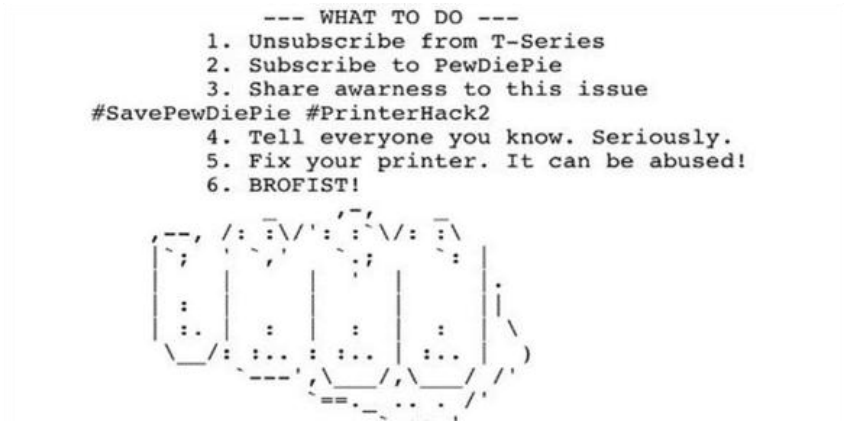
2. **Păstrați documentele într-o zonă securizată, care poate fi încuiată, la locul de muncă la distanță.**

Așa-numita politică a biroului curat sau a ecranului curat, care este în vigoare în multe locuri de muncă, ar trebui să fie aplicată și la locul de muncă la distanță. Chiar dacă avem încredere în membrii gospodăriei sau în colegii de cameră, niciun document care conține date personale nu ar trebui să fie lăsat la vedere în absența noastră. De asemenea, nu ar trebui să păstrați parolele dispozitivelor de lucru la vedere.

Soluție: echipați-vă spațiul de lucru la distanță cu un sertar sau un dulap care se poate încuia.

Acesta va fi locul în care veți putea depozita în siguranță toate materialele de lucru în timpul lucrului. Dacă este posibil, țineți cheia la dumneavoastră în permanență sau păstrați-o într-un loc pe care numai dumneavoastră îl cunoașteți.

3. **Dacă nu este neapărat necesar, nu imprimați documente acasă sau la puncte publice de fotocopiere.**



Experții în securitate cibernetică au tras de mult timp un semnal de alarmă asupra faptului că cel mai neglijat dispozitiv în ceea ce privește necesitatea de a implementa o securitate adecvată este... imprimanta. Potrivit studiilor realizate de InfoSecurity Magazine, aproximativ 66% dintre lucrătorii la distanță intervievați au tipărit în medie cinci documente pe săptămână. Un sfert dintre aceștia încă mai au documentele tipărite, explicând că intenționează să le ducă înapoi la birou. Doar 24% folosesc un distrugător de documente acasă, dar recunosc, de asemenea, că aruncă documentele în coșul de gunoi de acasă. Nu mai puțin de 12% dintre cei intervievați declară, de asemenea, că nu cunosc regulamentul GDPR.

Imprimantele de astăzi seamănă din ce în ce mai mult cu computerele decât cu dispozitive simple, cu o singură destinație – ele fac adesea parte din *Internetul obiectelor (Internet of Things,* IoT) și sunt instrumente de lucru multifuncționale. Unul dintre cele mai mediatizate atacuri asupra imprimantelor de uz casnic, care a evidențiat problema securității inadecvate pentru aceste dispozitive, a fost cel legat de bine-cunoscutul creator al YouTube – PewDiePie. În 2018, un hacker (sau un grup de mai mulți fani ai lui PewDiePie) a atacat zeci de mii de imprimante din întreaga lume. Fără intervenția proprietarilor lor, dispozitivele au început să tipărească o broșură de promovare a conținutului publicat de PewDiePie care îndemna la sprijinirea activităților derulate de acesta.

Imprimantele din ce în ce mai sofisticate tehnologic din ziua de azi au o memorie cache în care documentele sunt trimise pentru a fi tipărite. Imprimantele moderne funcționează, de asemenea, fără fir, ceea ce înseamnă că oricine are driverele potrivite pe computer și acces la rețeaua în care se află imprimanta se poate conecta la aceasta. Dacă un hacker preia controlul asupra imprimantei (de exemplu, într-o companie), poate obține acces atât la documentele care

au fost deja tipărite, cât și la alte resurse stocate pe computer sau chiar la parolele dispozitivelor care au utilizat serviciile imprimantei.

Soluție: imprimați documentele doar la locul de muncă, iar dacă trebuie să o faceți acasă, asigurați-vă că echipamentul este protejat corespunzător

Acest lucru se poate face prin setarea unei parole securizate pentru rețeaua Wi-Fi a imprimantei (dacă este posibil). Dacă nu mai aveți nevoie de documentele tipărite, nu le aruncați la coșul de gunoi de acasă, ci duceți-le la firmă, unde ar trebui să existe un distrugător. Dacă aceasta nu este o opțiune, întrebați angajatorul sau departamentul de resurse umane despre procedura de distrugere a documentelor din cadrul companiei.

4. Acoperirea camerei web

Lucrul de acasă înseamnă, de obicei, participarea la teleconferințe și apeluri video care necesită utilizarea unei camere web. Din nefericire, hackerii pot accesa cu ușurință camera dvs. web, compromițându-vă confidențialitatea. În plus, dacă la locul de muncă fizic există documente confidențiale care pot fi captate de o cameră web, infractorii vor putea avea acces la ele.

Soluție: Restricționarea vizibilității asupra elementelor care conțin date cu caracter personal

Atunci când camera web este pornită, ar trebui să se limiteze posibilitatea de a vizualiza elemente care conțin informații personale în apropierea acesteia. În plus, în cazul în care camera web este separată de dispozitiv, aceasta trebuie deconectată atunci când nu este utilizată. În cazul în care camera web este încorporată, merită să luați măsuri de protecție suplimentare, cum ar fi achiziționarea unui capac pentru cameră. Capace glisante pentru camere web de diferite tipuri pot fi găsite cu ușurință în magazine. De obicei, acestea sunt ușor de instalat, deoarece majoritatea au un strat adeziv care aderă la cameră. Utilizând programele și aplicațiile de videoconferință, puteți folosi, de asemenea, funcții precum **blurarea fundalului**.

5. Participați activ la instruirile din cadrul companiei cu privire la securitatea cibernetică și la modificările politicilor angajatorului privind protecția datelor și informațiilor

Conform GDPR, în cazul în care sunt adoptate noi proceduri de protecție a datelor în cadrul firmei, angajatorul ar trebui să le permită angajaților săi să se familiarizeze cu acestea înainte de a le pune în aplicare.

În cazul în care angajatorul nu a asigurat o instruire adecvată privind utilizarea dispozitivelor, utilizarea instrumentelor de comunicare internă și externă sau a principiilor de bază legate de

protecția datelor în cadrul întreprinderii, angajatul are dreptul de a solicita acest lucru. În cazul în care, chiar și după instruire, angajatul este în continuare nesigur cu privire la procedurile care trebuie urmate într-o anumită situație, acesta ar trebui să raporteze acest lucru angajatorului său sau persoanei desemnate din cadrul firmei ca fiind responsabilă cu administrarea infrastructurii IT, departamentului de resurse umane etc.

Igiena cibernetică atunci când se lucrează de la distanță

Ce altceva puteți face pentru a vă securiza computerul?

Criptarea datelor cu caracter personal

Mai ales dacă este vorba de date sensibile sau dacă le trimiteți în afara organizației. După cum s-a menționat mai sus, angajații care prelucrează date în cadrul sarcinilor lor de serviciu îndeplinesc astfel sarcinile operatorului de date, care este angajatorul. În conformitate cu articolul 32 din GDPR, operatorul și persoana împuternicită de către operator implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate a datelor corespunzător domeniului de aplicare, contextului și scopurilor prelucrării și riscului de atingere a drepturilor sau libertăților persoanelor fizice. Ca măsuri de securitate, Regulamentul GDPR menționează, printre altele, pseudonimizarea și criptarea datelor cu caracter personal.

Deși nu există cerințe explicite în GDPR cu privire la cea mai eficientă metodă de securitate, regulamentul subliniază în mod repetat că **criptarea și pseudonimizarea** sunt măsuri tehnice și organizatorice adecvate pentru a păstra securitatea datelor cu caracter personal.

Criptarea are ca scop codificarea unui anumit conținut în așa fel încât acesta să poată fi înțeles doar de către un destinatar care deține cheia corectă. În termenii cei mai simpli, ideea este, de exemplu, de a transforma un șir de litere într-un șir de alte litere sau numere, de a adăuga șiruri suplimentare de litere sau numere și așa mai departe.

Pseudonimizarea, pe de altă parte, reprezintă prelucrarea datelor cu caracter personal astfel încât să nu fie posibilă identificarea persoanei căreia îi aparțin fără a avea acces la informațiile stocate în siguranță în altă parte. Astfel, aceasta presupune mascarea datelor prin înlocuirea informațiilor despre o persoană cu identificatori imaginari.

Care este diferența dintre cele două metode?

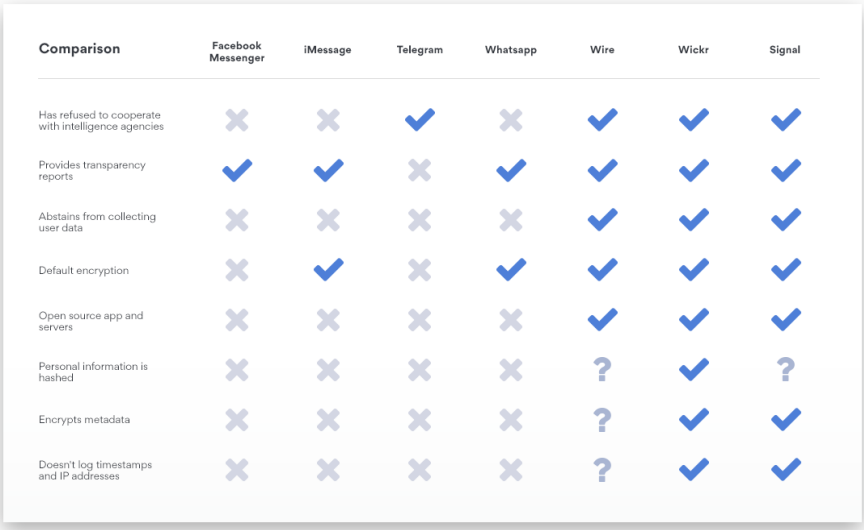
Ca și pseudonimizarea, criptarea ascunde informațiile prin înlocuirea identificatorilor cu altceva. Totuși, în timp ce pseudonimizarea permite oricărei persoane cu acces la date să vadă o parte din setul de date, criptarea permite doar utilizatorilor autorizați să acceseze întregul set de date. Pseudonimizarea și criptarea pot fi utilizate simultan sau separat.

Metode de securizare/criptare a datelor în comunicarea internă, precum și în comunicarea cu părțile externe

a. Comunicarea internă – utilizarea mesageriei criptate și a platformelor securizate

În timp ce e-mailul rămâne încă una dintre cele mai populare metode de comunicare la serviciu (316,9 miliarde de e-mailuri au fost trimise și primite în fiecare zi în 2021, iar acest număr se așteaptă să crească la 376,4 miliarde până în 2025), acesta nu este cel mai sigur sistem pentru schimbul de informații confidențiale. Datorită popularității sale ridicate, e-mailul este, de asemenea, un canal important pentru atacurile de hacking. Deloitte a constatat că 91% din toate atacurile cibernetice provin din e-mailuri de *phishing*. Costurile pe care le implică un astfel de atac pentru organizații pot fi foarte mari.

Pentru comunicările interne, în cazul în care se schimbă adesea informații confidențiale despre companie, angajați sau clienți, pot fi utilizate alte instrumente mai sigure.



Comparison	Facebook Messenger	iMessage	Telegram	Whatsapp	Wire	Wickr	Signal
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓
Open source app and servers	✗	✗	✗	✗	✓	✓	✓
Personal information is hashed	✗	✗	✗	✗	?	✓	?
Encrypts metadata	✗	✗	✗	✗	?	✓	✓
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	?	✓	✓

Whatsapp și Messenger – cele mai populare mesagerii și caracteristicile lor

1. **WhatsApp:**
   - utilizează criptarea semnalului,
   - probabil această aplicație este folosită de majoritatea persoanelor din Europa,
   - o aplicație ușor de utilizat care oferă funcționalități suplimentare,
   - este deținută de Facebook,
   - au avut loc anterior încălcări grave ale protecției datelor în cadrul aplicației.

2. **Messenger:**

   - acoperire largă – datorită legăturii cu Facebook, majoritatea oamenilor au acest comunicator,
   - Acesta poate fi utilizat chiar și după dezactivarea contului de Facebook,
   - criptarea nu este implicită,
   - comunicatorul nu criptează conversațiile anterioare,
   - aplicația urmărește comportamentul utilizatorului.

Cele mai bune aplicații în ceea ce privește securitatea datelor:

1. **Signal:**

   - suportă chat-uri de grup, mesaje SMS, mesaje vocale și video și permite transferul de documente și fotografii,
   - oferă ștergerea mesajelor (cu un cronometru),
   - utilizează un protocol de semnalizare – un protocol criptografic nefederalizat care poate fi utilizat pentru criptarea apelurilor vocale și a conversațiilor de mesagerie instantanee, în care mesajele în text clar pot fi citite doar de către cei care comunică,
   - software de tip *open source* (adică al cărui cod sursă este pus la dispoziție în mod gratuit și care poate fi distribuit și modificat fără plată),
   - nu stochează date de utilizator sau metadate,
   - promovat de Edward Snowden,
   - necesită un număr de telefon pentru înregistrare.

Platforme software și spații de lucru securizate:

1. Microsoft Teams.
2. Google Workspace.
3. Slack.
4. Asana.
5. Trello.

b. Comunicarea externă – criptarea fișierelor care conțin date cu caracter personal și a listelor de destinatari de e-mailuri

Se recomandă ca, ori de câte ori este posibil, atunci când datele sunt transferate dintr-o locație în alta, acestea să fie pseudonimizate sau criptate pentru a fi protejate împotriva scurgerilor.

Furnizarea de date cu caracter personal în lista de corespondență

Utilizați câmpul BCC (ascuns în mesaj). Câmpul BCC vă permite să trimiteți mesaje în așa fel încât destinatarii să nu-și vadă reciproc adresele. Această opțiune poate fi găsită în fiecare program de poștă electronică.

Transmiterea de date cu caracter personal în fișiere trimise prin e-mail

În documentele trimise prin e-mail pot fi ascunse multe date personale sau alte informații protejate din punct de vedere legal, astfel încât acestea trebuie să fie securizate suplimentar. Metodele de criptare a fișierelor pot varia în funcție de formatul în care acestea sunt stocate. Cu toate acestea, toate au în comun un principiu de bază: transmiterea parolei de acces la documentul criptat printr-un alt mijloc de comunicare decât e-mailul.

Pentru a cripta în mod corespunzător un fișier, programele cel mai frecvent selectate sunt **WinRAR** și **7-zip**. Cu fiecare dintre acestea, după selectarea opțiunii „add to archive" (adăugați la arhivă), se deschide o fereastră care permite, printre altele, să setați o parolă de acces la document.

Faceți în mod regulat copii de siguranță ale datelor și stocați-le pe unități externe

În cazul în care hardware-ul dvs. este infectat cu un virus sau al producerii altor evenimente care pot duce la ștergerea datelor din computer fără a putea fi recuperate, cea mai bună soluție este să faceți periodic **copii de rezervă .**

Copiile de siguranță, cunoscute și sub numele de backup-uri, sunt copii ale informațiilor care sunt stocate în alt loc decât originalul. Primul pas ar trebui să fie acela de a decide dacă doriți să faceți o copie de rezervă pentru:

1. anumite date, care sunt importante dintr-un anumit motiv,
2. întregul sistem de operare.

Majoritatea instrumentelor de backup sunt configurate în mod implicit pentru primul scop și vor copia datele în funcție de documentele pe care le utilizați cel mai des. Dacă nu sunteți sigur ce fișiere să copiați, este recomandat să le arhivați pe toate.

Cât de des să facem copii de rezervă?

Răspunsul depinde de preferințele individuale și de frecvența schimbărilor. Unii oameni o fac din oră în oră, alții o dată pe zi, iar alții o dată pe săptămână. Cu toate acestea, este recomandat să faceți zilnic copii de rezervă ale documentelor.

Cum îmi fac copii de rezervă ale documentelor?

În funcție de sistemul de operare al computerului dumneavoastră, există programe recomandate care vă vor permite să stabiliți perioada de timp la care se face automat o copie de rezervă. Printre acestea se numără Microsoft Windows Backup and Restore sau Time Machine de la Apple. Aceste programe funcționează atât atunci când dispozitivul este utilizat, cât și atunci când acesta este inactiv.

Date pe suporturi externe sau date în cloud?

De preferință, ambele. Suportul de stocare extern poate fi, printre altele, un stick de memorie, un hard disc extern portabil sau alte dispozitive la care vă puteți conecta prin wi-fi. Avantajul utilizării acestora este cu siguranță faptul că pe ele pot fi stocate seturi mari de date într-o perioadă destul de scurtă de timp. Din păcate, fiind vorba de o metodă fizică de backup, aceasta poate suferi aceleași defecțiuni sau deteriorări ca și un computer. O copie de rezervă pe un suport extern poate fi furată, pierdută, inundată, supraîncălzită și așa mai departe. În plus, dacă dispozitivul de pe care provin datele a fost infectat anterior cu programe malware, există, din păcate, riscul ca suportul și, prin urmare, copia de rezervă în sine, să fie, de asemenea, infectate.

Pe de altă parte, backup-ul în cloud presupune plasarea de copii ale documentelor sau ale altor fișiere pe internet. Mai exact, este vorba de colecții de servere și centre de date dispersate la nivel global, unde sunt stocate datele. Acest lucru se întâmplă în mod automat, de obicei prin intermediul unui instrument implicit de pe o platformă de procesare a textelor (de exemplu, Google Docs), care creează o copie de rezervă la fiecare perioadă de timp stabilită sau după fiecare modificare a unui fișier. Un avantaj cert al stocării copiilor de fișiere în cloud este permanența acestora și posibilitatea de a accesa copia de rezervă de pe orice alt dispozitiv (cu condiția, bineînțeles, să aveți o parolă pentru contul în cadrul căruia există cloud-ul). Cu toate acestea, nu este în totalitate lipsit de dezavantaje – dacă doriți să faceți rapid o copie de rezervă a unei cantități mari de date, soluția poate fi mult mai lentă decât o copie de rezervă fizică pe o unitate externă. De asemenea, este posibil să nu mai aveți spațiu în cloud pentru a stoca date noi și să trebuiască să ștergeți unele dintre ele sau să cumpărați resurse suplimentare de la furnizorul de cloud.

Acces securizat la computer, telefon și chiar la întâlnirile online

La fel cum criptarea datelor în sine este necesară pentru a asigura securitatea datelor cu caracter personal, este extrem de important ca și echipamentele pe care le folosim să fie securizate corespunzător. Utilizarea parolelor sau a altor tipuri de criptare garantează că numai persoanele autorizate au acces la anumite resurse.

Există mai multe metode de securizare a echipamentelor:

- **O parolă puternică, adică:**
  - **lungă –** care conține cel puțin opt caractere (cu cât este mai lungă, cu atât mai bine),
  - **complexă –** conține cel puțin un caracter din fiecare categorie: litere majuscule, litere mici, caractere speciale (de exemplu !, ?), numere,
  - **dificil de ghicit –** dacă doriți să alegeți o frază, un citat sau o zicală, asigurați-vă că nu are legătură directă cu dumneavoastră, cu munca dumneavoastră sau cu mediul în care lucrați; cu toate acestea, dacă știți că nu vă veți aminti parola fără asocieri ușoare – înlocuiți cuvintele cu simboluri sau numere adecvate de la tastatură, de exemplu „Ana are mere” **poate fi** scris ca „4N@ar€mer€”,
  - **să fie diferită de parola anterioară pentru dispozitivul în cauză –** dacă schimbați parola pentru un cont existent, aceasta nu trebuie să fie aceeași cu cea anterioară; de asemenea, nu trebuie să modificați parola doar puțin, adăugând, de exemplu, o cifră la sfârșit sau la început.

Recomandare: utilizați un instrument de gestionare a parolelor pentru a stoca parole criptate online – acesta vă va permite să creați parole complexe care conțin litere mari și mici, numere, diverse caractere speciale etc. Acest lucru va crea un șir de caractere fără sens care va fi dificil de spart.

NU UITAȚI!

- nu folosiți o parolă care este și un nume sau care este similară cu un nume de utilizator, numele companiei etc..,
- nu utilizați o secvență de litere sau de numere de la tastatură sau din alfabet,
- nu folosiți mai mult de două litere sau numere care se repetă (de exemplu, abba),
- nu folosiți datele personale ale nimănui pentru a crea o parolă,
- nu folosiți versiuni ortografice inversate ale cuvintelor (de exemplu, ionel1 ca 1lenoi),

- nu vă introduceți parola în prezența altor persoane,
- nu vă notați parola pe hârtie – dacă trebuie să o scrieți, utilizați un instrument de gestionare a parolelor pe un stick USB și să purtați-l cu dumneavoastră,
- nu utilizați aceeași parolă pentru toate dispozitivele sau site-urile,
- nu vă conectați la un dispozitiv care nu este al dumneavoastră,
- nu vă trimiteți parola într-un e-mail,
- nu partajați parolele online – dacă trebuie să comunicați informațiile de conectare unui coleg, sunați-l pentru a-i comunica detaliile, în loc să-i trimiteți parola. prin e-mail, SMS sau alt tip de mesagerie,
- dacă computerul/site-ul dvs. a fost spart, schimbați-vă imediat parola.

Anti-ghid – o listă cu cele mai puțin sigure parole de acces [9] :

1. password
2. 123456
3. 123456789
4. guest
5. qwerty
6. 12345678
7. 111111
8. 12345
9. col123456
10. 123123
11. 1234567
12. 1234
13. 1234567890

[9] Potrivit unui studiu realizat de NordPass, Top 200 most common passwords, https://nordpass.com/most-common-passwords-list/.

14. 000000
15. 555555
16. 666666
17. 123321
18. 654321
19. 7777777
20. 123

Autentificare multi-factor

Autentificarea multi-factor (MFA sau 2FA) este o metodă de securitate care necesită utilizarea a cel puțin două componente independente pentru a autentifica o acțiune (de exemplu, introducerea parolei unui cont și apoi introducerea unui cod SMS). Această metodă previne majoritatea atacurilor bazate pe credențiale de identitate.

Multe aplicații sau platforme oferă deja posibilitatea de a activa acest tip de securitate (de exemplu, Apple ID, Microsoft, Google, Twitter sau Facebook). Cea de-a doua componentă de autentificare poate fi un cod SMS, un cod unic de la o aplicație (Google Authenticator sau Microsoft Authenticator) sau un cod permanent propus de furnizorul instrumentului în cauză și ales de utilizator.

Cheie U2F

Potrivit experților în securitate cibernetică, cheia U2F este singura metodă de autentificare în doi pași care protejează 100% împotriva atacurilor de *phishing* (dar nu și împotriva altor atacuri, cum ar fi cele *malware*). Asta pentru că, dacă o persoană aflată în posesia unei chei U2F este

păcălită de infractorii cibernetici și introduce un nume de utilizator și o parolă pe un site web fals, atacatorul nu va reuși să preia detaliile contului utilizatorului.

Acest lucru se datorează unui *secure element* (un așa-numit calculator mic) încorporat în cheia U2F. Acesta funcționează în așa fel încât, atunci când cheia este introdusă într-un port USB (sau când este apropiată de un cititor pe un smartphone), cheia pornește și poate efectua operațiuni criptografice pe sistemul său intern și nu pe dispozitivul utilizatorului.

În plus, este o idee bună să obțineți două chei – deși aceeași cheie poate fi conectată la diferite servicii, merită să aveți una de rezervă. Odată achiziționată, cheia trebuie configurată. Multe servicii oferă opțiunea de a adăuga o cheie ca formă de autentificare pe mai multe niveluri. Diferite rețele sociale, Amazon, GitHub sau conturi de e-mail recomandă, de asemenea, această soluție. Dacă decideți să folosiți cheia U2F, celelalte metode de autentificare pe două niveluri trebuie eliminate.

Securizarea întâlnirilor online

Nu numai hardware-ul trebuie să fie securizat, ci și întâlnirile în rețea și videoconferințele. Lucrul de la distanță înseamnă deseori să te bazezi pe un software de videoconferință, care, la rândul său, creează potențiale riscuri de securitate pentru dispozitiv. În urma unei serii de atacuri asupra platformei Zoom, care au implicat persoane neinvitate care au intrat în sistemul de videoconferință pentru a intimida sau hărțui participanții (*zoom bombing)*, compania a fost nevoită să remedieze deficiențele de securitate. În ciuda numelui său, *zoom bombing* poate apărea și pe alte platforme. Acest tip de atac poate duce la scurgerea de informații confidențiale despre companie, clienți, alți angajați sau despre utilizatorul însuși.

Ca răspuns la „bombardarea" de la Zoom, FBI a publicat recomandări pentru a-i ajuta pe utilizatori să se protejeze atunci când folosesc programe de videoconferință:

1. Verificați dacă întâlnirea este privată, solicitând o parolă pentru a participa la întâlnire sau controlând accesul invitaților din sala de așteptare.
2. Luați în considerare cerințele de securitate atunci când selectați furnizorii. Criptarea *end-to-end* (care ascunde mesajul la expeditor și îl decriptează doar la destinatar) asigură confidențialitatea și securitatea – deci verificați dacă softul de videoconferință pe care îl utilizați dispune de această funcție.
3. Asigurați-vă că softul dvs. este actualizat prin instalarea celor mai recente ameliorări și actualizări.

Cea mai sigură platformă pentru videoconferințe este în prezent Microsoft Teams. Integrarea perfectă a tuturor aplicațiilor Office permite, de asemenea, setări de securitate suplimentare,

astfel încât toți membrii organizației pot lucra împreună, rămânând în siguranță chiar și în biroul de acasă.

Instalați și mențineți la zi softul antivirus și de protecție împotriva programelor malware.

Actualizarea sistemelor, aplicațiilor și browser-elor este adesea neglijată și amânată pentru mai târziu. De fapt, dacă o faceți la momentul potrivit, puteți preveni o mare parte din atacuri. Așadar, asigurați-vă că folosiți un software antivirus modern și actualizat. Actualizările conțin modificări importante care îmbunătățesc performanța și securitatea dispozitivelor. În prezent, sunt lansate actualizări chiar și lunar, dar merită să activați modul de backup zilnic. Acest lucru sporește semnificativ securitatea, deoarece dezvoltatorii pot remedia rapid orice vulnerabilități de securitate care sunt identificate, protejând și mai mult dispozitivele de malware.

Un pas simplu de făcut este, de asemenea, să vă asigurați că este instalat și utilizat un soft de protecție împotriva programelor *malware*, în plus față de softul antivirus standard. Acest instrument poate nu numai să ofere protecție împotriva atacurilor, ci și să alerteze utilizatorul atunci când se încearcă un atac.

Evitați să vă conectați dispozitivele la rețele publice

Utilizarea unei rețele publice, adică a unei rețele la care se poate conecta oricine, prin simplul fapt că este complet deschisă, poate fi un canal pentru numeroase atacuri și implică riscul de scurgere de date. Dacă trebuie să lucrați într-un spațiu public, asigurați-vă că vă conectați doar la rețele de încredere și întotdeauna cu ajutorul unui VPN sau al unei conexiuni de pe telefon (prin intermediul unui așa-numit hotspot).

Deci, ce este un VPN?

Acestea sunt rețele private virtuale care oferă conexiuni directe și sigure la rețeaua de calculatoare a unei organizații. Acestea pot fi esențiale atunci când se accesează fișiere, se lucrează
cu informații confidențiale sau pentru a utiliza anumite site-uri web.

VPN-ul criptează conexiunile utilizatorilor la serverele sale, permițând accesul sigur și securizat la rețeaua organizației. Un tunel VPN corporativ criptat va contribui, de asemenea, la asigurarea securității datelor pe măsură ce sunt transmise. De asemenea, va împiedica atacatorii care
nu au un VPN corporativ, să aibă acces la servere.

Securitatea VPN poate fi îmbunătățită prin utilizarea unei metode de autentificare solide. Multe VPN-uri utilizează un nume de utilizator și o parolă, dar vă puteți gândi și la modernizare și utilizarea cardurilor inteligente (*smart cards*) pentru a proteja procesul de logare a utilizatorilor și pentru a controla mai bine accesul la cont.

Desigur, nu contează cât de puternic este VPN-ul. Dacă parola este spartă, hackerii vor putea intra cu ușurință în el. Prin urmare, ar trebui să fie actualizată în mod regulat. Este o idee bună să limitați utilizarea unui VPN doar la situațiile în care este necesar. În cazul în care dispozitivele profesionale pentru uz personal sunt utilizate seara sau în weekend (dacă acest lucru este în conformitate cu politica companiei), cel mai bine este să dezactivați VPN-ul.

Ce altceva pe lângă VPN?

O altă opțiune este utilizarea unei rețele 5G. Aceasta oferă o conectivitate mai bună și promite o securitate mai mare decât utilizarea conexiunilor wi-fi sau chiar a conexiunilor VPN. Latența mai puțin frecventă anunțată pentru 5G ar putea face din aceasta o alternativă viabilă la wi-fi. Tehnologia dispune de criptare încorporată prin intermediul unor instrumente care împiedică urmărirea sau *spoofing-ul*.

Atunci când lucrați de acasă, este esențial să vă securizați și routerul de acasă. Acesta ar trebui să fie actualizat și securizat cu o parolă lungă și unică – diferită de parola automată cu care este echipat fiecare router. Pentru a face acest lucru, puteți merge la pagina de setări a routerului, tastând fraza corespunzătoare în browser și să schimbați parola acolo. Pe aceeași pagină, de obicei, puteți schimba și SSID-ul, adică numele rețelei wireless, pentru a îngreuna identificarea și accesul terților la rețeaua wi-fi de acasă. Nu folosiți numele dumneavoastră, adresa de domiciliu sau orice altceva care ar putea fi folosit pentru identificare.

De asemenea, trebuie să vă asigurați că este activată criptarea rețelei, ceea ce poate fi făcut de obicei în setările de securitate de pe pagina de configurare a rețelei fără fir. Există mai multe metode de securitate din care puteți alege, cum ar fi WEP, WPA și WPA2. Cea mai puternică dintre acestea este WPA2, care necesită un echipament de după 2006.

3. Impactul digitalizării asupra pieței muncii

3.1 Tratament discriminatoriu în procesele de recrutare

În lumea dinaintea progresului tehnologic, toate deciziile referitoare la angajarea și evaluarea unui angajat erau luate de oameni. Aceste decizii țineau cont, de obicei, de contextul local, de considerente etice, de aspecte juridice în ceea ce privește transparența procesului și legitimitatea alegerilor conducerii. Astăzi, însă, multe companii folosesc sisteme IT care oferă o mai mare eficiență și reduc analiza plictisitoare a documentelor în căutarea unor informații specifice.

Aceste sisteme, cunoscute sub numele de ADS (sisteme algoritmice de decizie, eng. *algorithmic decision systems), se* bazează pe analiza unor cantități mari de date care sunt procesate pentru a produce rezultate, care constituie apoi baza pentru luarea deciziilor. Intervenția umană în acest proces este de obicei neglijabilă și, în unele cazuri, poate fi complet eliminată. Cu toate acestea, impactul unei anumite decizii asupra unei anumite persoane poate fi de mare importanță, deoarece îi va modela situația de viață.

Prin urmare, dependența totală de ADS în procesul decizional ridică o serie de probleme de ordin etic, politic sau juridic. Din cauza riscului ca sistemele algoritmice să transmită prejudecățile creatorilor lor, încrederea nelimitată în tehnologie este controversată în special în domenii precum ocuparea forței de muncă sau accesul la servicii private și publice (de exemplu, asistența medicală, sistemele de evaluare a bonității în cazul creditelor).

3.1.1. Ce poate face o persoană afectată de discriminarea algoritmică

Se presupune că în procesul de recrutare ar trebui să se aplice dispozițiile privind egalitatea de tratament la angajare (în Polonia, această chestiune este reglementată de articolul 18 [3a] și următoarele din Codul muncii) și interzicerea discriminării (articolul 11 [3] din Codul muncii). Aceasta înseamnă că orice discriminare la angajare (în special pe motive de sex, vârstă, dizabilitate, rasă, religie, naționalitate, convingeri politice, apartenență sindicală, origine etnică, religie, orientare sexuală) este inacceptabilă.

Cu toate acestea, există cazuri de comportament discriminatoriu în procesul de recrutare. Printre acestea se numără preferința acordată candidaților de sex masculin, refuzul de a angaja femei tinere căsătorite sau femei cu copii sau includerea unor clauze discriminatorii împotriva străinilor. Criteriile de excludere pot fi cu atât mai răspândite cu cât o companie utilizează mai mult recrutarea electronică bazată pe sisteme automatizate de luare a deciziilor. În acest caz, nu numai că poate exista o discriminare neintenționată a candidaților prin intermediul unei

inteligențe artificiale părtinitoare, dar conducerea unei companii poate introduce în mod deliberat în sistem criterii descalificatoare.

În cazul unei discriminări în procesul de recrutare, manifestată prin conținutul de excludere al unui anunț sau prin întrebări indiscrete privind viața privată și de familie, persoana afectată poate solicita în instanță protecția intereselor sale. Obligația de a proba în astfel de proceduri revine angajatorului, iar potențialul candidat trebuie doar să arate că existența unei discriminări este probabilă (articolul 18 [3b] din Codul muncii). În cazul în care instanța confirmă încălcarea, angajatorul va fi obligat să plătească persoanei discriminate o compensație în valoare nu mai mică decât salariul minim.

Cu toate acestea, în cazul procesului decizional algoritmic, este mult mai dificil să demonstrezi și să pretinzi că ai fost respins nejustificat în procesul de recrutare. Acest lucru este legat de așa-numita problemă a cutiei negre (*black box problem*)*, și* anume lipsa de transparență în funcționarea instrumentelor de inteligență artificială. Acest lucru înseamnă că, adesea, chiar și dezvoltatorii înșiși și, prin urmare, și angajatorii care implementează un instrument de inteligență artificială nu sunt conștienți de funcționarea necorespunzătoare a acestuia. Cu toate acestea, acest lucru nu înseamnă că aceștia sunt scutiți de răspundere în cazul unei încălcări. O persoană care suspectează că a fost respinsă în mod nedrept de un algoritm poate lua măsuri concrete pentru a-și proteja interesele și pentru a schimba decizia luată de sistem.

Articolul 22 din regulamentul GDPR rămâne esențial în această privință. Această dispoziție îl obligă pe operatorul de date să pună în aplicare măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanelor vizate (de date și, prin urmare, și de decizii), precum și mecanisme care să permită unei anumite persoane să conteste o decizie bazată exclusiv pe prelucrarea automată.

Dacă, **în opinia dumneavoastră**, **candidatura dumneavoastră a fost respinsă pe nedrept în cadrul unui proces de recrutare electronică:**

1. Verificați dacă decizia a fost complet automatizată. Pentru a face acest lucru, citiți cu atenție termenii și condițiile de recrutare sau contactați departamentul de resurse umane al companiei și stabiliți modul în care funcționează algoritmul în contextul procesului de aplicare pentru un loc de muncă.
2. Cereți companiei (operatorului de date) să vă ofere posibilitatea de a vă prezenta punctul dumneavoastră de vedere și de a explica de ce credeți că respingerea a fost nedreaptă.
3. Solicitați companiei o explicație privind decizia și cereți ca aplicația dumneavoastră să fie analizată din nou, dar de data aceasta de către un om. Operatorul trebuie să răspundă, la o astfel de cerere, cât mai curând posibil (în termen de maximum o lună). În termen de o

lună, operatorul trebuie, de asemenea, să vă informeze că cererea a fost respinsă și să vă prezinte motivele pentru aceasta.

4. Dacă, totuși, operatorul ignoră cererea sau dacă răspunsul nu este satisfăcător, puteți solicita sprijinul autorităților de protecție a datelor și puteți depune o plângere.
5. În plus, indiferent de procedura în fața autorității de protecție a datelor, aveți dreptul de a vă proteja drepturile în fața unei instanțe civile. Dacă considerați că prelucrarea datelor dvs. încalcă legea, puteți da în judecată operatorul de date sau persoana împuternicită de operator. În instanță, puteți solicita despăgubiri pentru încălcarea legislației privind protecția datelor, precum și să ridicați probleme de discriminare care au cauzat daune materiale sau nepatrimoniale.

3.1.2. Reglementările UE privind AI și procesul de recrutare

După cum s-a menționat deja, în proiectul de regulament privind inteligența artificială (AI Act), aspectele legate de ocuparea forței de muncă și de gestionarea resurselor umane au fost puse pe lista sistemelor cu risc ridicat. Aceasta înseamnă că instrumentele folosite, să spunem, pentru evaluarea automată a unui candidat pentru un post vor trebui să parcurgă o cale specială pentru a fi autorizate.

Multe obligații vor reveni furnizorilor de sisteme AI, care vor fi supuși unor cerințe stricte în ceea ce privește proiectarea, testarea, auditarea și certificarea sistemelor de inteligență artificială. În plus, cei care utilizează sistemele AI propuse de furnizori (de exemplu, firmele) vor fi obligați să le utilizeze în conformitate cu legea și cu instrucțiunile de utilizare și să asigure caracterul adecvat al datelor introduse în sisteme, monitorizarea acestora și păstrarea jurnalelor de evenimente în caz de incidente.

Se așteaptă ca noile norme să ofere garanții suplimentare împotriva deciziilor discriminatorii care nu au un factor uman. În același timp, AI Act nu acordă puteri suplimentare chiar entităților afectate de astfel de decizii. Cu toate acestea, cadrul european va fi completat de planificata *Directivă privind răspunderea pentru IA* (*AI Liability Directive*, AILD), care va introduce, pentru prima dată, dispoziții privind daunele cauzate de sistemele de inteligență artificială. Scopul acesteia este de a stabili o protecție mai largă pentru cei prejudiciați de inteligența artificială aplicată și de a le facilita obținerea de despăgubiri. Astfel, reglementările propuse reprezintă un pas înainte în asigurarea unui acces efectiv la căi de atac și în cazurile de discriminare în utilizarea sistemelor de angajare. Acest lucru se datorează faptului că acestea presupun că angajatorul este cel care nu și-a îndeplinit obligația de diligență necesară prin utilizarea unui sistem de angajare care discriminează anumite categorii de persoane.

Lucrul, atât la proiectul de regulament privind inteligența artificială (AI Act) cât și la iirectivei privind răspunderea pentru IA, se află deja într-un stadiu avansat. Cu toate acestea, conform formulării actuale a noilor reglementări, dispozițiile acestora nu se vor aplica în toate statele membre ale UE decât după doi ani de la adoptarea lor.

3.2 Munca în viitor

3.2.1. Ocupații care dispar, competențele viitorului și responsabilitatea angajatorului de a adapta competențele lucrătorilor la automatizare

Până la 40% dintre respondenții unui studiu recent realizat de Centre for Economic Policy Research (CEPR) spun că există o probabilitate mai mare de 50% să fie înlocuiți de o mașină, un robot sau un algoritm în următorul deceniu. Temerile legate de șomajul tehnologic nu sunt complet nefondate. Potrivit raportului *„Future Jobs”*, se înregistrează o creștere semnificativă a ponderii noilor tehnologii în sarcinile îndeplinite. În 2018, în medie, 71% din timpul de lucru a fost reprezentat de activități umane și 29% de cele efectuate de mașini. Se preconizează că aceste proporții se vor schimba semnificativ până în 2025. Oamenii vor fi responsabili pentru aproximativ 48% dintre activități, în timp ce restul de 52% dintre sarcini vor fi complet automatizate.

În ceea ce privește impactul automatizării, se poate presupune că vor fi afectați în cea mai mare măsură cei care fac muncă manuală, care poate fi ușor de înlocuit de roboți (adică pe baza unor
secvențe previzibile). Cu toate acestea, digitalizarea ar putea afecta și unii specialiști. Potrivit raportului *„Future of Jobs”,* printre profesiile redundante, precum cea de mecanic, magazioner sau manager de producție, vom găsi și analiștii financiari sau funcționarii. Cu toate acestea, experții de la McKinsey Global Institute temperează aceste temeri – întrucât se estimează că, la nivel global, doar 5% dintre profesii vor fi eliminate complet.

Ceea ce se va schimba, fără îndoială, este modul de îndeplinire a sarcinilor de serviciu (o pondere mai mare a sistemelor și echipamentelor IT în sarcinile îndeplinite) și competențele dorite de angajați. Având în vedere că multe sarcini vor fi îndeplinite de mașini, va exista o cerere sporită de competențe pe care computerele nu le pot reproduce cu exactitate. Este vorba despre competențe soft, adică cele care necesită creativitate, inteligență emoțională, gândire critică. Digitalizarea va crește, de asemenea, cererea de competențe tehnice și va crea locuri de muncă pentru lucrători intelectuali bine calificați, capabili să opereze noile sisteme. Pe de altă parte, acest lucru ar putea genera preocupări legate de o polarizare tot mai mare a pieței (inferioritatea lucrătorilor fizici, cu o importanță tot mai mare acordată celor cu studii superioare). Aceste preocupări par să fie confirmate de rezultatele unui studiu realizat de Centrul European pentru Dezvoltarea Formării Profesionale (Cedefop), care a constatat că peste 70% dintre persoanele angajate au nevoie cel puțin de competențe informatice de bază pentru a

se descurca pe piața actuală a muncii, dar nu mai puțin de 30% dintre acestea prezintă risc permanent de a nu putea dobândi competențele dorite (și, prin urmare, să își piardă locul de muncă).

3.2.2. Competențele viitorului și profesiile redundante în era digitalizării

Datorită utilizării tot mai frecvente a tehnologiei, competențele dorite pe piața forței de muncă se vor schimba semnificativ în următorii ani. Se preconizează că, odată cu automatizarea și algoritmizarea, cererea de competențe care sunt ușor de înlocuit de mașini va scădea. Vorbim aici atât de competențele manuale (în cazul lucrătorilor manuali, din producție), cât și de cele legate de munca intelectuală (de exemplu, abilitățile de calcul sau de scriere creativă). Pe de altă parte, va exista o cerere crescută de **competențe ale viitorului,** așa cum sunt definite în raportul DELab (*Competențele viitorului. Cum să le modelăm într-un ecosistem educațional flexibil*?) ca fiind: *abilități specifice pentru a întreprinde și a îndeplini sarcini într-un mediu de lucru care este în mod fundamental flexibil, dispersat geografic, predispus la schimbări frecvente și rapide, care implică necesitatea de a utiliza tehnologii digitale și de a coopera cu sisteme automate și mașini care utilizează inteligența artificială*.

McKinsey a împărțit aceste competențe în trei grupe: tehnice și digitale, sociale și cognitive.

Competențele viitorului	
Tehnice și digitale	• Există indicii că cererea de competențe digitale **de bază** va crește cu 65%. Este vorba despre capacitatea de a utiliza tehnologia în activitatea de zi cu zi, în special în domeniul rezolvării problemelor și al căutării de informații. • Până în 2030, lucrătorii din Europa vor petrece cu peste 40% mai mult timp în activități care utilizează competențe digitale avansate. Mai mult, cererea de competențe de programare și IT va crește cu 90%.
Sociale	• Până în 2030, cererea de competențe sociale pe piața europeană a muncii, în special de spirit antreprenorial și de capacitate de a lua inițiative, va crește cu 22%.
Cognitive (superioare): gândire critică, creativitate, capacitatea de a gestiona oameni	• Cererea de competențe cognitive superioare va crește cu 14% până în 2030. În același timp, importanța competențelor cognitive de bază, cum ar fi cititul, scrisul și prelucrarea de bază, va scădea cu 23%.

Kompetencje przyszłości w podziale na trzy grupy umiejętności: poznawcze, społeczne i techniczne

Forumul Economic Mondial (WEF) arată că, în următorii ani, cele mai importante vor fi competențe precum:

- **gestionarea personalului (resurse umane) –** constituirea colectivului prin găsirea celor mai bune persoane pentru sarcini specifice; motivarea și gestionarea oamenilor în timpul activității lor,
- **abilități de negociere –** capacitatea de a rezolva conflicte și de a depăși diferențele de opinie; demonstrarea puterii de convingere,
- **inteligența emoțională –** capacitatea de a identifica și de a denumi emoțiile proprii și ale altora; capacitatea de a gestiona și de a utiliza emoțiile în emiterea de evaluări li luarea de decizii; înțelegerea nevoilor celorlalți (angajați și clienți),
- **colaborarea cu ceilalți –** capacitatea de a lucra în grup,
- **flexibilitate cognitivă –** capacitatea de a „comuta" între sarcini,
- **rezolvarea de probleme complexe –** capacitatea de a găsi soluții care nu sunt evidente în diferite contexte,
- **gândire critică –** utilizarea logicii și a raționamentului pentru a identifica punctele forte și punctele slabe ale unor soluții, concluzii sau abordări alternative ale problemelor,
- **creativitate –** capacitatea de a gândi „în afara cutiei", de a veni cu idei inovatoare, de a rezolva probleme în moduri neevidente.

În plus, în raportul său, WEF enumeră și **profesiile care își vor pierde din importanță în era digitalizării**. Printre acestea se numără profesii precum: operator introducere date, lucrător contabil și salarizare, secretar administrativ și executiv, lucrător asamblare și producție, lucrător departament informare și servicii clienți, manager administrativ și comercial, contabil și expert contabil, magazioner, manager principal și manager de operațiuni, funcționar poștal, analist financiar, casier și controlor de bilete, mecanic, telemarketer, instalator de echipamente electronice și de telecomunicații, bancher, șofer, broker și agent de vânzări, vânzător și agent de vânzări din ușă în ușă, agent de asigurări, lucrător departament statistică și financiar, jurist.

Źródło: World Economic Forum (2018) The Future of Jobs Report 2018, s. 9. Zawody oznaczone * występują w więcej niż jednej kolumnie tabeli, co spowodowane jest różnicami między poszczególnymi sektorami.

3.2.3. Digitalizarea și tendințele în managementul afacerilor - rolul angajatorilor

Pentru a profita pe deplin de digitalizare și de beneficiile implementării noilor tehnologii, companiile vor trebui să își reorganizeze structurile și să își schimbe abordarea actuală a muncii. Acest lucru va necesita reproiectarea organizării formale a companiei, adăugarea de personal cu noi competențe, recalificarea sau dezvoltarea talentelor existente. Potrivit McKinsey, date fiind

schimbările în ceea ce privește profesiile căutate și a celor mai apreciate competențe, organizațiile vor fi nevoite să **actualizeze cinci domenii-cheie** - mentalitatea, structura organizațională, alocarea muncii, componența colectivului și responsabilitățile conducerii și departamentului HR.

În ceea ce privește mentalitatea în firmă, cheia succesului viitor al organizației va fi promovarea tendinței așa-numitei învățări pe tot parcursul vieții (*lifelong learning*), adică oferirea angajaților posibilitatea de a dobândi noi competențe și cunoștințe pe tot parcursul carierei lor, nu doar la început. În ceea ce privește structura organizațională, introducerea unor moduri de management mai dinamice și mai inovatoare, precum și o colaborare mai frecventă între echipe și schimbul de cunoștințe și funcții între angajați sunt indicate ca priorități pentru anii următori.

Companiile care implementează automatizarea pe scară largă se așteaptă, de asemenea, să transfere sarcini efectuate în prezent de lucrători cu înaltă calificare către lucrători mai puțin calificați (cu ajutorul mașinilor și al computerelor). În ceea ce privește resursele umane, se anticipează o utilizare sporită a diferitelor tipuri de liber-profesioniști și de lucrători temporari. Acest lucru va rezulta din creșterea așa-numitei economii colaborative/economii la cerere (*sharing economy; on-demand economy*), și anume modele de afaceri bazate pe intermedierea platformelor de colaborare, care creează o piață cu acces liber pentru utilizarea temporară a bunurilor sau serviciilor, adesea furnizate de persoane private.

Păstrarea competitivității companiei, sprijinind în același timp angajații în procesul de digitalizare

În raportul *Beyond Hiring. How companies are re-skilling to address talent shortages (Cum se recalifică companiile pentru a face față deficitului de talente),* McKinsey a prezentat diverse tactici pentru a menține companiile competitive și pentru a reduce decalajul dintre competențele dorite și cele disponibile ale angajaților din sectorul privat. Printre practicile pe care ar trebui să le ia în considerare angajatorii care doresc să își dezvolte afacerile și să își creeze o forță de muncă competentă se numără următoarele:

- **Reconversie profesională –** încurajarea dobândirii de noi competențe și a îmbunătățirii competențelor existente de către angajații existenți, precum și implementarea și educarea noilor angajați în ceea ce privește capacitățile dorite. Un aspect esențial pentru firme va fi decizia privind modul în care se va asigura instruirea: intern (utilizând resursele și programele disponibile) sau extern (în cooperare cu o instituție de învățământ sau un centru de instruire). În ceea ce privește domeniile în care antreprenorii intenționează să investească, acestea se referă cel mai adesea la dezvoltarea unor competențe care sunt strategice pentru compania lor, de exemplu, competențe IT avansate, abilități de scriere creativă, gândire critică, abilități de rezolvare a problemelor.

Pe de altă parte, pentru competențe mai puțin complexe, angajatorii declară posibilitatea de a angaja persoane din afara organizației.

- **Transferuri în interiorul companiei –** mutarea angajaților cu competențe specifice în departamente/echipe în care își pot folosi mai bine abilitățile. Într-un sondaj McKinsey realizat în februarie 2018 în rândul managerilor de companii, 55% dintre respondenți au declarat că ar prefera să mute unii angajați pe posturi diferite sau complet noi, în loc să îi concedieze complet.

- **Angajarea –** găsirea de persoane sau de echipe întregi cu competențele specifice necesare (deși este posibil ca oferta de experți de pe piață să nu fie suficientă pentru ca toate companiile să urmeze această strategie). Pe de o parte, costul angajării poate fi mai mic decât cel al reconversiei profesionale, dar, pe de altă parte, recrutarea de noi membri ai echipei implică un risc legat de modul în care individul va performa. Prin urmare, pentru a atrage cu succes noi talente cheie, companiile ar trebui să inoveze în modul în care recrutează candidații, precum și să ofere o cultură de lucru atractivă și beneficii nesalariale.

- **Crearea de noi forme de colaborare –** companiile pot beneficia de competențele aduse de persoane din afara organizației (liber-profesioniști, experți, agenți temporari de la agențiile de recrutare). Totuși, dezavantajul acestui model este riscul de a transfera secrete comerciale (de exemplu, know-how, lucrări acoperite de drepturi de proprietate intelectuală) către persoane din exterior, precum și dificultatea de a se integra în cultura și modul de lucru al companiei. Din acest motiv, angajatorii declară că ocupă posturi care nu au legătură cu activitățile principale ale întreprinderii sau care necesită calificări scăzute cu contractori independenți.

- **Posibile disponibilizări –** În unele companii ar putea fi necesare disponibilizări, în special în sectoarele care nu se dezvoltă suficient de rapid și în care automatizarea va înlocui în mod semnificativ forța de muncă. O strategie de disponibilizare poate fi pusă în aplicare prin reducerea sau oprirea angajării de noi lucrători, permițând în același timp continuarea procesului normal de pensionare și retragere a celor deja angajați.

Deși sunt posibile disponibilizări din cauza utilizării sporite a mașinilor, este greu de crezut că angajații din toate sectoarele vor trebui să se teamă pentru locurile lor de muncă. Cu toate acestea, vor exista, fără îndoială, noi tehnologii, sisteme și programe care vor necesita dobândirea de competențe IT suplimentare.

Cum își pot sprijini angajatorii angajații în digitalizarea întreprinderii?

În primul rând, ei pot:

- să îi familiarizeze pe angajați cu noile instrumente – să elimine teama și conservatorismul față de noile tehnologii și să arate cum pot fi utilizate instrumentele digitale în activitatea de zi cu zi,
- crește gradul de conștientizare a angajaților – explicând de ce și cum utilizează compania tehnologia; având informații în acest domeniu, angajații vor înțelege mai bine noile instrumente de lucru și vor fi motivați să le folosească,
- să pregătească bine managerii pentru schimbările care urmează – managerii ar trebui să cunoască răspunsurile la întrebările de bază despre noile instrumente de lucru și să le arate celorlalți membri ai echipei cum să utilizeze tehnologiile care sunt implementate,
- să asigure instruire profesională pentru noile sisteme – chiar și angajații care stăpânesc bine tehnologia au nevoie de timp pentru a se familiariza cu noile softuri și instrumente digitale pe care nu le-au mai folosit până acum; compania ar trebui să asigure instruire profesională pentru toți angajații.

3.2.4. Alte entități cu un rol important în digitalizarea muncii și în reconversia profesională a lucrătorilor

Instituțiile de învățământ

Rolul educației în procesul de digitalizare este deja recunoscut de organismele Uniunii Europene. În concluziile Consiliului European au subliniat faptul că accesul la o educație de înaltă calitate susținută de tehnologiile digitale este o condiție prealabilă pentru transformarea sectoarelor individuale și pentru continuarea creșterii economice.

De asemenea, Comisia Europeană a inclus crearea unui plan de acțiune pentru educația digitală pentru 2021-2027, care să stabilească o viziune pentru educația digitală în Europa. Scopul ambelor inițiative a fost acela de a încuraja universitățile, școlile și cadrele didactice să joace un rol mai activ în dezvoltarea competențelor digitale și în satisfacerea nevoilor pieței muncii. Rolul acestor instituții în transformarea digitală pare să fie confirmat și de publicațiile economice, cum ar fi raportul PwC și WEF *„Upskilling for Shared Prosperity”* (2021), care subliniază că instituțiile de

învățământ superior au potențialul de a impulsiona schimbarea – de a ridica nivelul de cunoștințe, abilitățile și competențele generale ale studenților și ale societății.

Autoritățile publice

Rolul statului este de a sprijini atât antreprenorii, cât și angajații în procesul de digitalizare. Prin urmare, este important ca factorii de decizie să pună în aplicare politici care să încurajeze dobândirea de competențe digitale sau reconversia profesională a angajaților (de exemplu, prin programe de subvenționare a formării pentru întreprinderile mici și mijlocii). În plus, este important să se stimuleze piața forței de muncă și să se evite șomajul prin politici active de ocupare a forței de muncă – în loc să pună accentul pe indemnizațiile de șomaj, statul ar trebui să investească în agenții de ocupare a forței de muncă care să devină centre de plasare a forței de muncă și să faciliteze reconversia profesională a șomerilor.

ONG-urile

ONG-urile și grupurile de reflecție (Think Tank) acționează adesea ca incubatoare pentru soluții benefice din punct de vedere social. Acestea tind să aibă mai multă libertate de acțiune decât instituțiile de stat și pot veni cu soluții diferite la probleme. Din acest motiv, unele companii întreprind inițiative filantropice sau cooperează cu fundații în domenii legate de dobândirea de noi competențe de către angajați. Un exemplu este inițiativa Generation, care are ca scop combaterea șomajului prin eliminarea deficitului de competențe în rândul tinerilor, precum și sprijinirea adulților în găsirea unor locuri de muncă potrivite pentru ei prin recrutare, instruire și mentoring.

Sindicatele și organizațiile profesionale

În calitate de parteneri sociali, asociațiile profesionale și sindicatele joacă un rol important în digitalizarea pieței muncii. În Suedia, de exemplu, se înființează consilii de protecție a muncii finanțate de întreprinderi și sindicate. Aceste entități instruiesc persoanele care și-au pierdut locul de muncă, le oferă sprijin financiar temporar și le facilitează procesul de reconversie profesională, astfel încât șomerii să revină mai repede pe piața muncii.

3.3 Noile modele de afaceri și impactul lor asupra pieței muncii

3.3.1. Erodarea puterii de negociere a lucrătorilor – cum noile tehnologii îngreunează sindicalizarea lucrătorilor

Noile tehnologii facilitează comunicarea și conectează utilizatorii între ei, în ciuda distanței care îi separă. În același timp, însă, ele conduc la o mai mare înstrăinare și la o interacțiune umană din ce în ce mai redusă. Acest fenomen nu se aplică doar în sfera vieții private, ci și în cea profesională. Digitalizarea și trecerea la munca în lumea online au făcut ca angajații să stabilească doar sporadic relații durabile și să se întâlnească și să discute mai rar problemele la locul de muncă.

Noile tehnologii favorizează izolarea, și nu numai în cazul muncii la distanță. Instrumentele AI utilizate de întreprinderi pentru a controla angajații și a le măsura productivitatea sunt, de asemenea, adesea folosite pentru a monitoriza și a obstrucționa asocierii lucrătorilor.

Se întâmplă uneori ca modelele de afaceri ale marilor companii să se bazeze pe un control extins al lucrătorilor și pe o creștere constantă a ritmului de lucru. Prin urmare, sindicalizarea lucrătorilor pentru a le reprezenta drepturile și interesele colective și individuale reprezintă un risc real pentru un sistem care este preocupat doar de maximizarea profiturilor patronatului. Din acest motiv, corporațiile iau măsuri pentru a-i împiedica pe lucrători să se sindicalizeze. Această practică s-a intensificat în timpul pandemiei COVID-19, când recomandările privind sănătatea și siguranța introduse în acea perioadă au început să fie folosite pentru a implementa instrumente la locul de muncă pentru a măsura distanța dintre oameni în depozite, interzicându-le în același timp să fie prea aproape unul de celălalt. Companiile au început să achiziționeze programe informatice care au făcut posibilă analiza și vizualizarea datelor privind relațiile din cadrul locurilor de muncă (de exemplu, geoSPatial Operating Console sau SPOC). În plus, departamentele de resurse umane monitorizau listele de corespondență ale angajaților utilizate în scopuri activiste sau grupurile de angajați de pe rețelele de socializare.

În cazul platformei de lucru, impactul noilor tehnologii asupra asocierii lucrătorilor nu este clar pozitiv sau negativ. Aplicațiile utilizate pentru furnizarea de servicii pot facilita mobilizarea curierilor și a șoferilor – camerele de chat interne disponibile pe sistemele lor oferă lucrătorilor prin intermediul platformelor (*gig-workers*) un spațiu pentru a face schimb de informații, iar rețelele de comunicare în masă pot conecta curierii individuali la nivel de oraș, regiune și chiar țară.

În același timp, eficiența sindicatelor lucrătorilor prin intermediul platformelor depinde adesea de sprijinul autorităților publice pentru diverse forme de autoorganizare. În Bologna, de exemplu, a fost creată, în colaborare cu sindicaliștii, o Cartă *a drepturilor fundamentale ale muncii digitale în contextul urban* (în italiană: *Carta dei diritti fondamentali del lavoro digitale nel Contesto Urbano),* care stabilește un cadru de standarde minime pentru salarii, timp de lucru și

protecție prin asigurări pentru lucrătorii prin intermediul platformelor. Semnificativ este faptul că însuși primarul din Bologna și-a manifestat sprijinul pentru această inițiativă și a cerut clienților să boicoteze platformele care nu au semnat carta.

În țările în care statul nu oferă asistență angajaților care lucrează prin intermediul platformelor, nivelul de sindicalizare al acestora este mult mai scăzut, iar puterea lor de negociere este mai redusă. De acest lucru abuzează uneori platformele, care folosesc mecanismele din aplicații pentru a controla mai bine curierii sau șoferii și pentru a zădărnici încercările de a se opune politicilor companiei.

Un exemplu al modului în care giganții economiei colaborative folosesc tehnologia pentru a limita inițiativele lucrătorilor care luptă pentru drepturile lor este greva înăbușită rapid a curierilor polonezi livratori de mâncare, din aprilie 2021. Motivul grevei a fost modul incorect prin care algoritmul distribuia comenzile și remunerațiile, iar metoda de protest a fost faptul că curierii au încetat să mai onoreze comenzile, în ciuda dorinței lor declarate de a lucra în aplicație. Șoferii sperau să pună presiune pe patronat și să-l determine să discute cu reprezentanții lor. Totuși, compania, fără nicio încercare de a comunica cu curierii, prin intermediul aplicației, i-a blocat pe greviști și a transmis comenzile lor unor persoane care erau dispuse să facă munca în ciuda condițiilor incorecte.

3.3.2. Impactul digitalizării asupra pieței muncii – munca prin intermediul platformelor

Platforma de lucru este o formă de angajare în cadrul căreia angajatul folosește o platformă digitală pentru a avea acces la alte organizații sau persoane, cu scopul de a furniza servicii specifice și în schimbul unei remunerații. Printre sarcinile efectuate contra cost prin intermediul platformelor digitale se numără serviciile de taxi și de curierat, livrările, service-urile de reparații la domiciliu, precum și activități intelectuale precum copywriting sau contabilitatea. Deși aplicații precum Uber și Bolt se dezvoltă în spațiul european abia de un deceniu, lucrătorii care prestează servicii prin intermediul platformelor de acest tip reprezintă în prezent o parte semnificativă a forței de muncă (28,3 milioane de lucrători în 2022 în Uniunea Europeană). Această cifră este comparabilă cu numărul de persoane angajate în sectoarele de producție industrială (29 de milioane de lucrători). În plus, potrivit Comisiei Europene, se așteaptă ca platformele să adauge încă 15 milioane de angajați până în 2025. Printre cele mai populare platforme din UE se numără Uber, Deliveroo, Amazon Mechanical Turk, Fiverr, Upwork, Appjobs, Glovo sau JustEat (cunoscută în Polonia sub numele de Pyszne.pl).

Modelul de afaceri al platformelor de lucru se bazează pe tehnologii care utilizează algoritmi pentru a corela în mod eficient cererea și oferta de lucrători și serviciile pe care aceștia le oferă. În plus, utilizarea unor aplicații concepute în mod corespunzător permite luarea de decizii fără contact, automatizate cât și monitorizarea sarcinilor efectuate. Cu un sistem de management

bazat pe algoritmi, este posibil să se renunțe la personalul de management tradițional. Acest lucru, la rândul său, determină platformele să susțină că acționează mai degrabă ca un simplu intermediar care oferă servicii pentru a pune în legătură persoanele care desfășoară activități independente cu potențiali clienți, decât ca un angajator.

Cine este cel mai probabil să caute un loc de muncă prin intermediul platformelor de lucru?

- tineri,
- bărbați,
- imigranți (în special în ceea ce privește munca fizică),
- persoanele cu studii postliceale, pentru care această muncă reprezintă o sursă suplimentară de venit.

În plus, lucrătorii prin intermediul platformelor pot fi împărțiți în două grupuri extreme pe piața muncii. Primul grup include lucrătorii care fac muncă intelectuală, privilegiați din punct de vedere al competențelor lor, de exemplu programatori care pot influența termenii și condițiile de cooperare cu clienții (freelancing, prestarea de servicii IT). Al doilea grup, pe de altă parte, include persoane cu competențe reduse, ușor de înlocuit, a căror putere de negociere pe piața muncii este redusă (de exemplu, imigranții care prestează servicii de taxi).

Avantajele și dezavantajele muncii prin intermediul platformelor

Avantajele muncii prin intermediul platformelor includ:

- program de lucru flexibil și posibilitatea de a planifica propriul program de lucru,
- contactul direct cu clientul,
- o mai mare independență.

Cu toate acestea, în forma actuală a platformelor digitale, sunt evidente o serie de dezavantaje ale acestui tip de angajare:

- Probleme din sfera protecției muncii:
    - lipsa unor norme de sănătate și siguranță reglementate,
    - riscuri fizice,
    - stresul cauzat de nesiguranța locului de muncă;
- condițiile de angajare:

- 5,5 milioane de persoane care lucrează prin intermediul platformelor de lucru în UE sunt clasificate greșit ca fiind lucrători independenți,
- persoanele clasificate în mod eronat ca lucrători independenți nu beneficiază de aceleași drepturi și beneficii ca și persoanele angajate;

- problemele care decurg din algoritmizarea muncii,
- posibilități limitate de asociere,
- venituri și ore de lucru imprevizibile (potrivit Comisiei Europene, 41% din timpul de lucru al lucrătorilor prin intermediul platformelor constă în sarcini neplătite, cum ar fi verificarea anunțurilor sau așteptarea comenzilor).

Legislația UE și munca prin intermediul platformelor

Unele state membre au introdus deja reglementări pentru munca prin intermediul platformelor
în legislația națională. La nivel comunitar au loc, de asemenea, discuții privind acest tip special de angajare. Conceptul de lucrători prin intermediul platformelor a fost deja introdus în legislația UE, de exemplu prin Directiva privind condițiile de muncă transparente și previzibile în Uniunea Europeană. Cu toate acestea, un progres decisiv în acest sens urmează să fie **Directiva privind îmbunătățirea condițiilor de muncă ale lucrătorilor prin intermediul platformelor**, al cărei proiect a fost prezentat de Comisia Europeană la sfârșitul anului 2021.

Principalele dispoziții incluse în proiectul de directivă privind îmbunătățirea condițiilor de lucru prin intermediul platformelor:

- Persoanele care lucrează prin intermediul platformelor digitale vor obține un statut de angajare care să corespundă condițiilor lor reale de muncă, care va fi verificat prin stabilirea criteriilor necesare pentru a recunoaște platforma ca angajator.
- O platformă va fi considerată angajator dacă îndeplinește cel puțin două dintre următoarele criterii:
  - stabilește nivelul remunerației sau un plafon al acesteia,
  - supraveghează, prin mijloace electronice, executarea muncii,
  - restricționează libertatea de a alege orele de lucru sau perioadele de absență, libertatea de a accepta sau de a refuza sarcini sau libertatea de a recurge la subcontractanți sau înlocuitori,
  - stabilește norme obligatorii specifice privind aspectul și comportamentul față de beneficiarul serviciului sau de clientul care a comandat lucrarea,

    - restricționează capacitatea de a extinde baza de clienți sau de a efectua lucrări pentru terți.

- Lucrătorii prin intermediul platformelor ar trebui să beneficieze de drepturi sociale și de muncă în funcție de statutul lor de angajat:
    - timp de odihnă garantat și concedii plătite,
    - salariu minim,
    - posibilitatea de negociere colectivă,
    - siguranța și protecția sănătății,
    - indemnizații de șomaj și de boală,
    - pensii bazate pe contributivitate.

- Platforma poate contesta clasificarea, dar trebuie să dovedească faptul că nu există o relație de muncă.
- Platformele vor fi obligate să sporească transparența în utilizarea algoritmilor și să asigure monitorizarea condițiilor de muncă de către om.
- Angajații vor avea dreptul de a contesta deciziile automatizate.