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

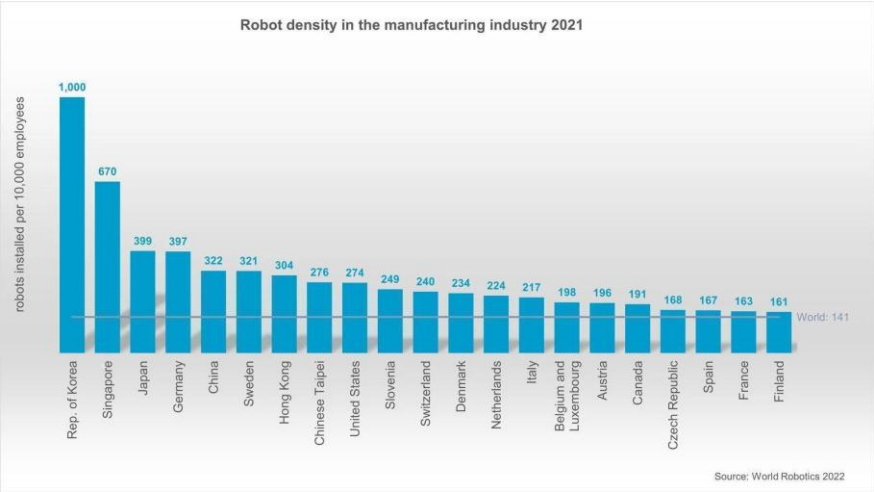
problemów. W zależności od sektora i etapu produkcji, automatyzacja może być wprowadzana jednak w różnym stopniu. Poza poziomem zaangażowania w zadania, roboty można podzielić na wykonujące głównie pracę intelektualną (np. wszelkie narzędzia AI), jak i te odciążające człowieka w powtarzalnych czynnościach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

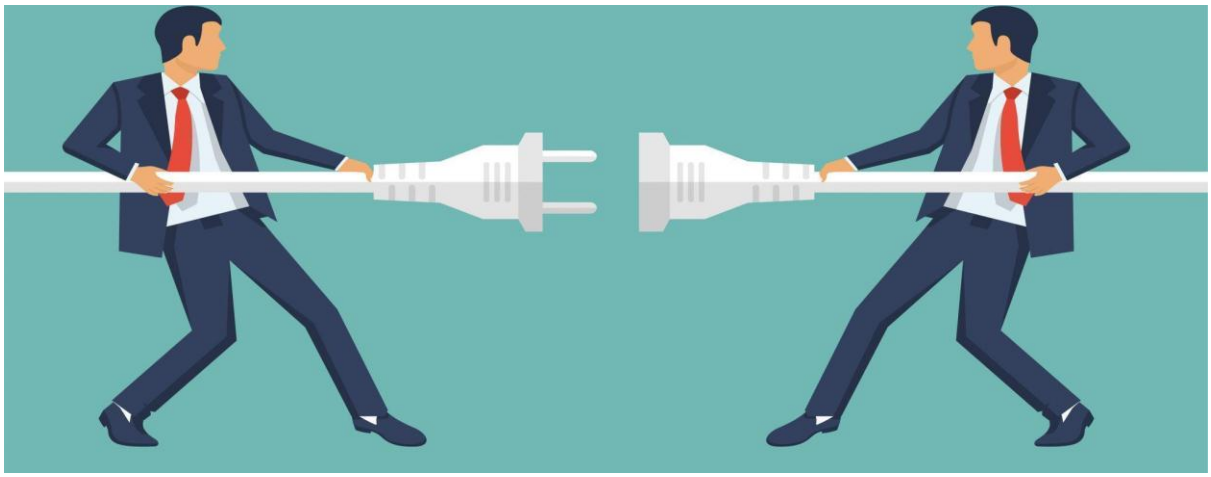
2. Wpływ cyfryzacji na życie prywatne pracowników

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.

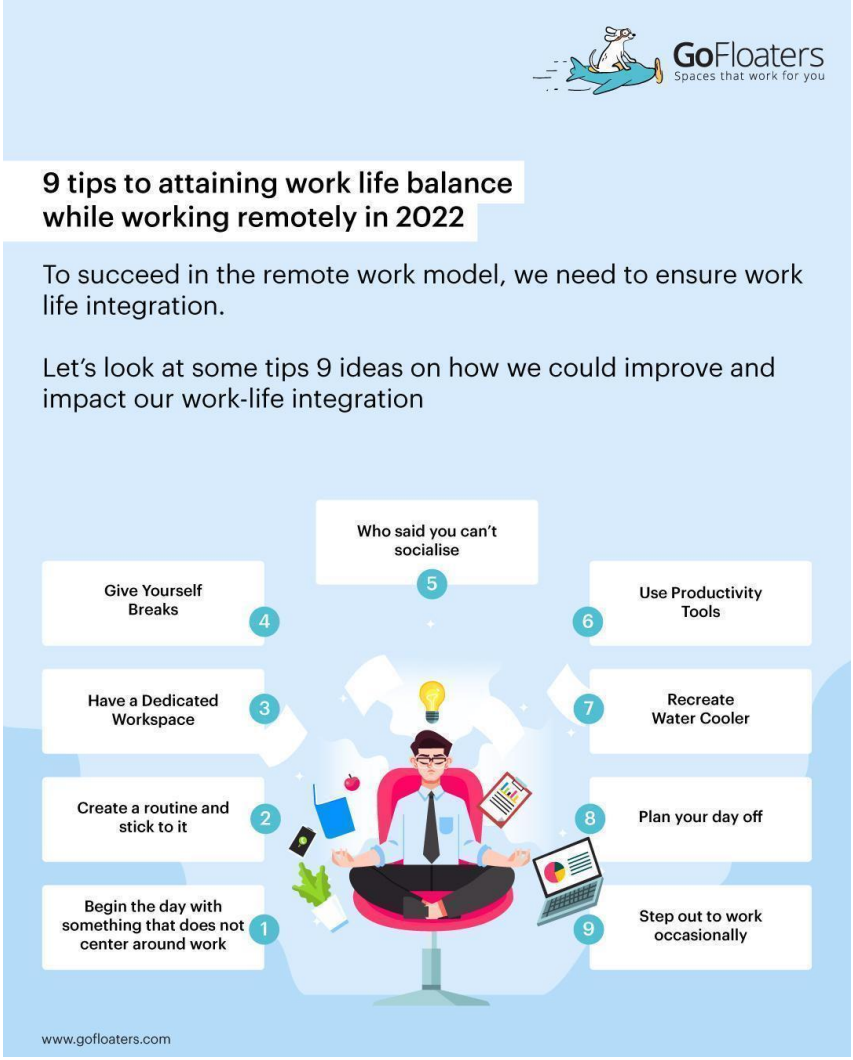
Jak pracodawca może poprawić *work-life balance* swoich pracowników?

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

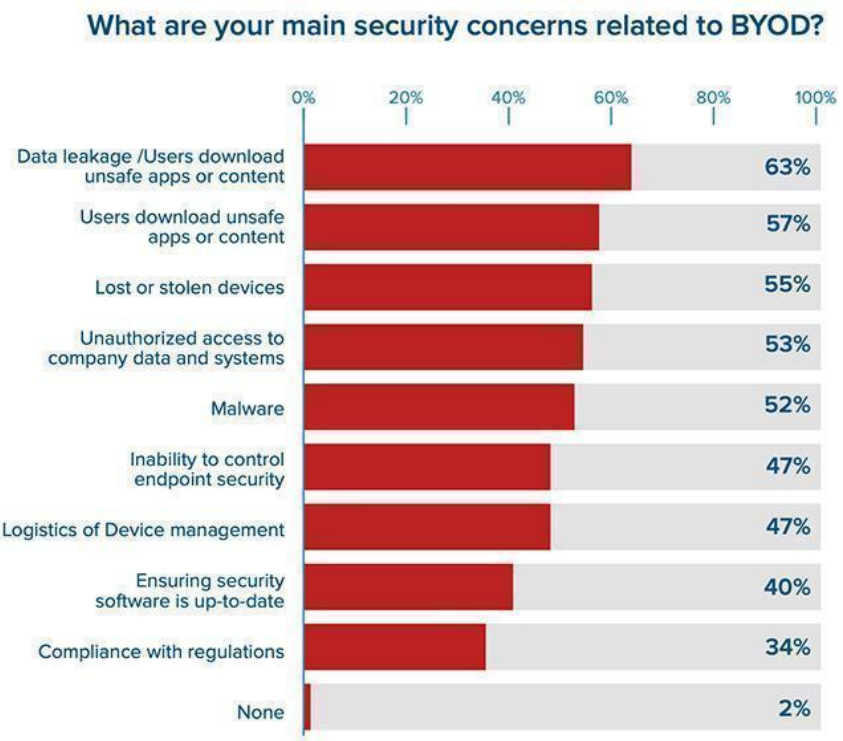
2.2.1. Czym jest polityka BYOD (bring your own device)

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,

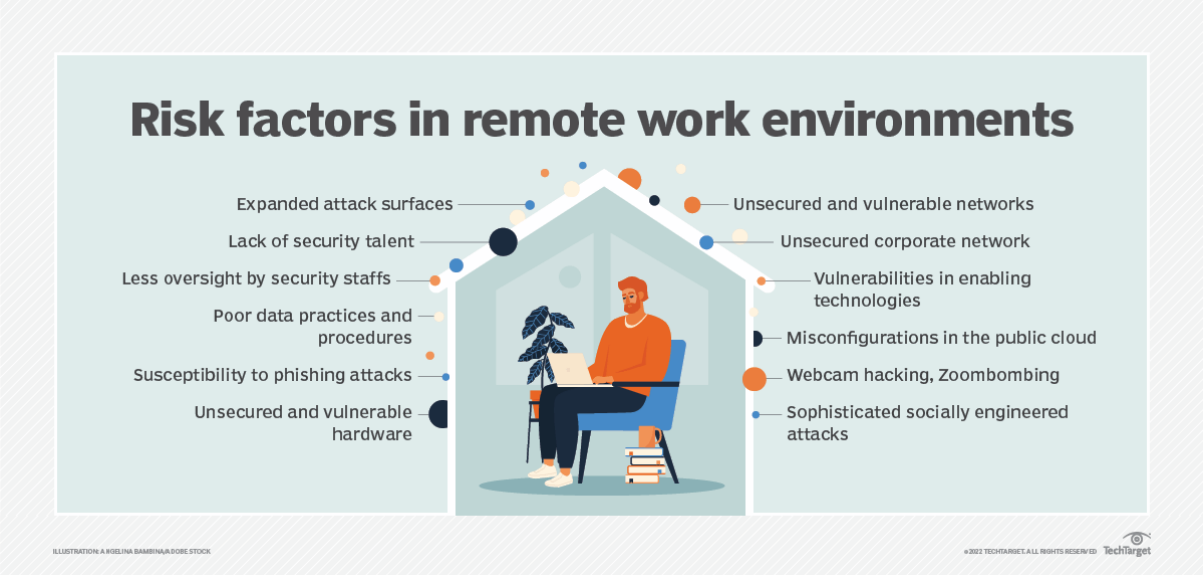
b) zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych,

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.

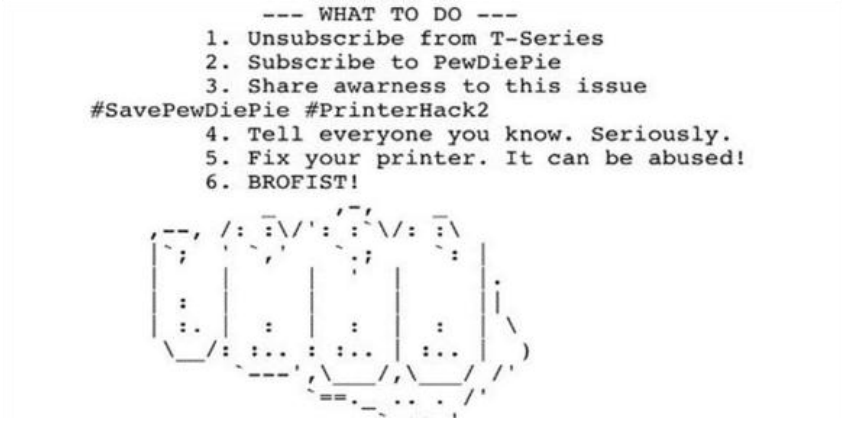
2. **Przechowuj dokumenty w bezpiecznej, zamykanej przestrzeni w miejscu odbywania pracy zdalnej**

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?

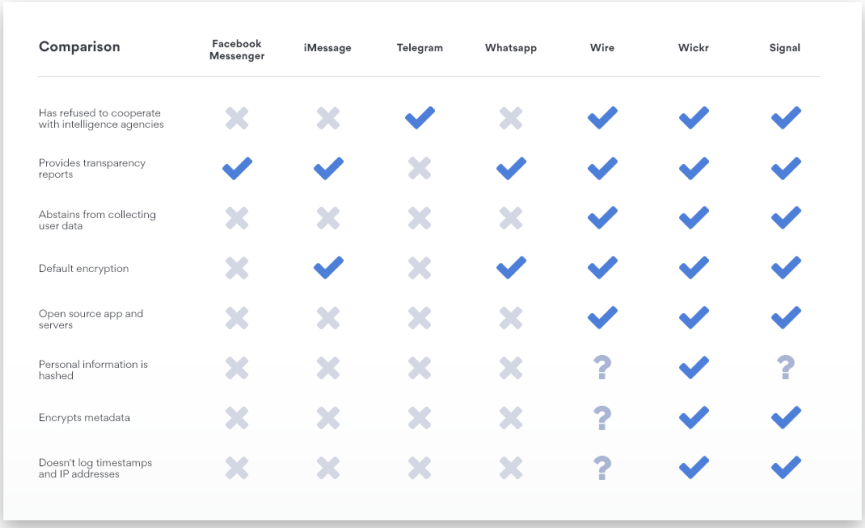
Podobnie jak pseudonimizacja, szyfrowanie ukrywa informacje poprzez zastąpienie identyfikatorów czymś innym. O ile jednak pseudonimizacja umożliwia każdemu, kto ma dostęp do danych, wgląd w część zbioru danych, o tyle szyfrowanie pozwala na dostęp do pełnego zbioru danych tylko zatwierdzonym użytkownikom.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