




**Barbara Surdykowska**

Instytut Spraw Publicznych

 <https://orcid.org/0000-0003-4569-1274>

## O lęku przed nadciągającym chipowaniem pracowników – uwagi na tle powstającego ustawodawstwa w USA

**On the anxiety concerning of imminent prospect  
of the microchipping of employees**

**Remarks in the context of the emerging legislation in the USA**

Summary

Barbara Surdykowska draws attention to legislation, specifically in the US, which prohibits (or emphasizes the importance of the employee's consent to) subcutaneous microchipping in the context of work relations. In Surdykowska's opinion, issue of the use of microchips in the labor context and the potential decisions of the legislator may serve as a litmus test of reactions to the expected technological transformation. The simultaneous and progressive use of subcutaneous microchips is at this point a very early phase of the phenomenon of the cyborgization of the employee's body.

**Keywords:** microchips, work, technological development

Przedmiotem tego tekstu jest zagadnienie używania w kontekście pracy wszczepianych pod skórę mikrochipów z technologią RFID<sup>1</sup>. Jest to ułamek szerszej problematyki cyborgizacji ciała człowieka w sferze pracy<sup>2</sup>. Kwestia ta wydaje się interesująca nie ze względu na skalę zjawiska (szacuje się, że nie więcej niż 20 tys. ludzi na świecie używa

---

<sup>1</sup> D. Rodriguez: *Chipping in at Work: Privacy Concerns Related to the Use of Body Microchip ("RFID") Implants in the Employer-Employee Context*. "Iowa Law Review" 2019, Vol. 104, Issue 3, s. 1581–1611.

<sup>2</sup> S. Adamczyk, B. Surdykowska: *Cyborgizacja człowieka pracy. Czy godność pracy ludzkiej przetrwa? W stulecie urodzin Stanisława Lema*. „Praca i Zabezpieczenie Społeczne” 2021, nr 12, s. 3–11.

podskórnych mikrochipów RFID), ale z uwagi na fakt, że jak w soczewce skupiają się tu racjonalne i – w mojej ocenie – także kompletnie nieracjonalne lęki związane z wykorzystaniem technologii. Oczywiście dla wszystkich obecnych rozważań, w których dotykamy kwestii prywatności, kwestii nadzoru czy wolności w zakresie naszego ciała, kluczowym punktem odniesienia jest pandemia COVID-19 i jej konsekwencje. Chodzi o konsekwencje łączące się z pytaniami, jakie wywołała co do możliwości kontroli przez pracodawcę stanu zdrowia pracownika (np. pomiar temperatury ciała czy kontrola objawów wskazujących na zarażenie), ograniczania dostępu do określonych przestrzeni wspólnych, usług lub możliwości pracy (paszporty covidowe), czy też oczekiwania poddania się określonej procedurze medycznej (obowiązkowe szczepienia jako warunek dopuszczenia do określonej aktywności czy pracy). Związek pomiędzy pytaniami, jakie wywołała i wywołuje pandemia COVID-19, a kwestią mikrochipów jest z łatwością dostrzegalny<sup>3</sup>.

Oczywiście, pytania, które powstały w obszarze prawa do prywatności, przetwarzania danych czy nadzoru w konsekwencji pandemii COVID-19, nie będą w tym tekście wyczerpująco poruszone (prawdopodobnie będą one główną pożywką dla prowadzonych rozważań na kilka następnych lat), ale są one niezbędnym tłem dla spojrzenia na problem potencjalnego oczekiwania ze strony pracodawców na poddanie się określonej procedurze mikrochipowania podskórnego przez pracowników.

Dnia 1 sierpnia 2017 r. niewielka firma technologiczna Three Square Market z River Falls ze stanu Wisconsin zorganizowała przyjęcie dla swoich 80 pracowników. Nie byłoby w tej informacji niczego szczególnego, gdyby nie fakt, że poza standardowymi rozrywkami podczas imprezy pracownikom zaoferowano (oczywiście nie na zasadzie zaskoczenia) możliwość umieszczenia w ich dłoniach mikrochipów, wielkości ziarenka ryżu, za pomocą których mogą otwierać drzwi, logować się do systemów komputerowych czy nabywać przekąski i napoje w automacie. Były to pasywne chipy (o rodzajach mikrochipów dalej), czyli innymi słowy, urządzenia wykorzystujące technologię, którą powszechnie stosujemy od połowy XX w. i którą każdy z nas obserwuje, używając jakiegokolwiek karty kredytowej czy bankomatowej. Pięćdzie-

---

<sup>3</sup> J.S. Gonzalez: *Stop Before It Starts: Regulating Employee Microchipping in the Covid-19 Era*. "Mississippi Law Journal" 2020, Vol. 90, Issue 1, s. 1–34.

sięciu pracowników zdecydowało się na umieszczenie pod skórą chipa. Mimo że zakres ułatwień dla pracownika czy pracodawcy był *de facto* taki sam jak w przypadku umieszczenia mikrochipa na smyczy, którą pracownik nosi na szyi (poza faktem, że wszczepionego mikrochipa nie da się zgubić), zdarzenie wywołało niebywałe zainteresowanie w mediach<sup>4</sup>. Wydaje się, że ekscytacja w dużej mierze wynikała z tego, że do przekroczenia symbolicznej bariery skóry człowieka doszło w kontekście pracy. Innymi słowy – połała się symboliczna krew.

Osoby, które dotychczas poddały się mikrochipowaniu, zrobiły to najczęściej ze względów medycznych albo dla zabawy. Najlicniejszą grupą osób, która używa mikrochipów w jednym określonym celu, są mieszkańcy Sztokholmu (około 6 tys. osób), którzy na chipie umieszczonym pod skórą kodują bilety w komunikacji publicznej. Jedynym (znanym mi) liczniejszym przypadkiem mikrochipowania podskórnego w związku z pracą była sytuacja w Meksyku, gdzie procedurze tej poddano grupę prokuratorów (około 160 osób), w tym prokuratora generalnego, a mikrochipy miały służyć ułatwieniu ustanowienia ograniczeń w dostępie do tajnych dokumentów (umożliwiły otworenie określonych pomieszczeń, szaf itp.). Prawdopodobnie miały być także pewnym zabezpieczeniem na wypadek porwania (dokładnie na tej samej zasadzie, jak chipowanie bagażu ułatwia jego znalezienie na lotnisku). Piszę: „prawdopodobnie”, ponieważ nie ma jednoznacznej informacji, czy były to chipy pasywne, czy aktywne<sup>5</sup>.

Podobne przykłady jak w odniesieniu do firmy Three Square Market dotyczą takich spółek, jak NewFusion (Belgia) czy Epicenter (Szwecja)<sup>6</sup>.

---

<sup>4</sup> Zainteresowanie w mediach było ogromne, podaję więc tylko kilka przykładów: T. Gillies: *Why Most of Three Square Market's Employees Jumped at Chance to Wear a Microchip*. 13.08.2017. <https://www.cnn.com/2017/08/11/three-square-market-ceo-explains-its-employee-microchip-implant.html> [dostęp: 09.03.2023]; *Wisconsin Company Three Square Market to Microchip Employees*. 24.07.2017. <https://www.bbc.com/news/world-us-canada-40710051> [dostęp: 09.03.2023]; *The Microchip – One Year Later, Where are They?* 26.07.2018. <https://www.prnewswire.com/news-releases/the-microchip---one-year-later-where-are-they-300687606.html> [dostęp: 09.03.2023].

<sup>5</sup> W. Weissert: *Microchips Implanted in Mexican Officials*. 15.07.2004. <https://www.nbcnews.com/id/wbna5439055> [dostęp: 09.02.2023].

<sup>6</sup> B. Williams: *Belgian Company Offers to Make its Employees Cyborgs with Microchip Implants*. 7.02.2017. <https://mashable.com/article/belgian-company-microchips-employees> [dostęp: 09.02.2023]; J. Brooks: *A Swedish Start-Up Has Started Implementing Microchips Into its Employees*. 03.04.2017. <https://www.cnn.com/2017/04/03/start-up-epicenter-implants-employees-with-microchips.html> [dostęp: 09.02.2023].

Jak już wskazałam, na całym świecie mamy prawdopodobnie około 20 tys. zachipowanych ludzi, jednakże nie znamy żadnego przykładu, w którym pracodawca oczekiwałby od pracowników poddania się tej procedurze w jakiegokolwiek jurysdykcji. Równocześnie rozrasta się ustawodawstwo stanowe w USA zabraniające mikrochipowania pracowników lub wymagające zgody pracownika na tę procedurę. W kilku stanach zakazano mikrochipowania bez zgody – są to m.in.: Kalifornia, Maryland, Dakota Północna, Oklahoma i Wisconsin. W dużej liczbie stanów odniesiono się w ich ustawodawstwie wprost do mikrochipowania w kontekście pracy (przykładowo: Arkansas, Indiana<sup>7</sup>, Missouri, Montana, Nevada, Iowa<sup>8</sup>). Czy ta legislacyjna reakcja nie jest nieco przedwczesna?

## 1. Technologia RFID i jej historia oraz sposoby wykorzystania

Technologia RFID (z którą każdy z nas styka się codziennie, używając kart kredytowych, wchodząc do sklepu, gdzie towary są zabezpieczone przed kradzieżą, i w setkach innych zwykłych sytuacji, np. kiedy oznaczamy swojego czworonoga) jest podstawą działania mikrochipa i jak w przypadku większości technologii jej historia łączy się z działaniami wojennymi. W czasie II wojny światowej, gdy technologia radarów wojskowych była już rozwinięta, pojawił się problem z odróżnianiem na radarze samolotów „swoich” od samolotów wroga. Niemieckie lotnictwo rozwiązało tę kwestię, polecając pilotom samolotów wykonywanie przez maszyny uformowane w określonym szyku konkretnych figur, co było sygnałem rozpoznawczym. Alianci na szczęście dla dalszego rozwoju technologii podeszli do sprawy bardziej przełomowo, wprowadzając i testując radarowe znakowanie samolotów (tzw. technologię IFF – Identification Friend or Foe, zresztą po różnych udoskonaleniach stosowaną do dziś w lotnictwie i wojskowym, i cywilnym). I to właśnie technologia IFF była protoplastą RFID<sup>9</sup>.

---

<sup>7</sup> R. Maurer: *Another State Bans Employers Microchipping Workers*. 27.04.2021. <https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/indiana-bans-employers-from-requiring-microchips-workers.aspx> [dostęp: 09.02.2023].

<sup>8</sup> <https://eu.desmoinesregister.com/story/news/politics/2020/02/05/iowa-bill-would-prevent-requiring-microchip-implants/4669429002/> [dostęp: 09.02.2023]; <https://legiscan.com/IA/text/HF259/id/2262989> [dostęp: 09.02.2023].

<sup>9</sup> Czyli RFID to technologia, która wykorzystuje fale radiowe do przesyłania danych oraz zasilania elektronicznego układu (etykieta RFID) stanowiącego etykietę obiektu przez czynniki, w celu identyfikacji obiektu. Technika umożliwia odczyt, a czasami także

Pierwszym komercyjnym zastosowaniem technologii RFID już w latach 50. XX w. było oznakowanie droższych produktów w sklepach jako ochrona przed złodziejami. W kolejnych dekadach zaczęto używać tej technologii do znakowania bydła w stadach, oznaczania pojazdów i pobierania różnorodnych opłat. Dynamiczny rozwój komercyjnych zastosowań miał miejsce w latach 90. ubiegłego wieku – był to pobór różnego rodzaju opłat za parkowanie, używanie dróg *etc.* W miarę upływu czasu i rozwoju technologii zmniejszano również wielkość mikrochipów, które teraz w większości są tak małe, że *de facto* niezauważalne dla ludzkiego oka.

Oczywiście były też próby kompleksowego użycia technologii RFID, które ostatecznie zrealizowano tylko częściowo. Przykładowo, w 2003 r. Walmart ogłosił, że będzie oczekiwał od swoich wszystkich dostawców oznaczania mikrochipem każdego towaru dostarczonego do magazynów, aby raz na zawsze rozwiązać wszelkie problemy z ustalaniem stanów magazynów. Ostatecznie wycofano się z tego projektu i równoległe korzystano z technologii RFID oraz kodów kreskowych do oznaczania towarów<sup>10</sup>. W 2016 r. natomiast Macy's przeszedł na wyłączne stosowanie technologii RFID do oznaczania towarów i zarządzania magazynami<sup>11</sup>.

Naturalnie wykorzystanie technologii wywoływało i wywołuje określone kontrowersje, przede wszystkim w zakresie ochrony prawa do prywatności<sup>12</sup>. Druga grupa obaw dotyczy tego, czy istnieje niebezpieczeństwo kradzieży informacji z chipa lub ich zhakowania<sup>13</sup>.

---

zapis układu RFID. W zależności od konstrukcji pozwala na odczyt etykiet z odległości do kilkudziesięciu centymetrów lub kilku metrów od anteny czytnika. System odczytu umożliwia identyfikację wielu etykiet znajdujących się jednocześnie w polu odczytu.

<sup>10</sup> P. Rosenblum: *How Walmart Could Solve Its Problem and Improve Earnings*. 22.05.2014. <https://www.forbes.com/sites/paularosenblum/2014/05/22/walmart-could-solve-its-inventory-problem-and-improve-earnings/> [dostęp: 09.02.2023].

<sup>11</sup> B. Thau: *Is the 'RFID Retail Revolution' Finally Here? A Macy's Case Study*. 15.05.2017. <https://www.forbes.com/sites/barbarathau/2017/05/15/is-the-rfid-retail-revolution-finally-here-a-macys-case-study/?sh=722ce7ac3294> [dostęp: 09.02.2023].

<sup>12</sup> C. Mutigwe, F. Aghdasi: *Research Trends in RFID Technology*. "Interim: Interdisciplinary Journal" 2007, Vol. 6, Issue 1, s. 68–82. <https://www.semanticscholar.org/paper/Research-trends-in-RFID-technology-Mutigwe-Aghdasi/4b7450d3083b5fbb3f2a5192e701b8fb81c59562> [dostęp: 09.02.2023].

<sup>13</sup> Sh. Firfiray: *Microchips Implants are Threatening Workers' Rights*. 22.11.2018. <https://theconversation.com/microchip-implants-are-threatening-workers-rights-107221> [dostęp: 09.02.2023].

Mikrochip wykorzystujący technologię RFID może być pasywny (nadaje się tylko do odczytu, zazwyczaj nie posiada własnego źródła zasilania – występuje np. w karcie kredytowej, która do odczytu potrzebuje energii z czytnika) albo aktywny (zdolny do bycia odczytanym i do kodowania, np. może służyć do wysyłania w czasie rzeczywistym informacji o położeniu obiektu; taki mikrochip musi mieć własne źródło zasilania).

Przykładowo, The American Civil Liberties Union (ACLU) protestowało, gdy jedno z przedszkoli w stanie Kalifornia oznaczało aktywnymi mikrochipami koszulki noszone przez przedszkolaki, aby można było je „namierzyć” (w sensie: znaleźć i zidentyfikować w razie np. zagubienia). Oczywiście powodowało to także, iż można było zlokalizować (w sensie: wysledzić) dziecko ubrane w dany strój. Wydaje mi się, że zarzuty wobec stosowania takiego rozwiązania szły w dwóch wzajemnie wykluczających się kierunkach: z jednej strony wskazywano, że narusza to prywatność dzieci (czyli że mikrochipy są skuteczne), a z drugiej – że aktywny mikrochip wykorzystujący RFID można stosunkowo łatwo podrobić, co może ułatwić porwanie dziecka (ktoś fałszuje mikrochip i za jego pomocą ukrywa porwanie dziecka – co pokazywałoby, że mikrochipy są nieskuteczne). W każdym razie sprawa była szeroko dyskutowana w mediach<sup>14</sup>.

Wobec omawianej technologii stawiane są następujące zarzuty: po pierwsze, mikrochipy mogą być umieszczane na przedmiotach bez wiedzy/świadomości/zgody ich użytkowników/właścicieli; po drugie, globalne, masowe znakowanie przedmiotów spowoduje stworzenie globalnego rejestru posiadaczy wszystkiego; po trzecie, umieszczanie mikrochipów wiąże się z możliwością pozyskiwania olbrzymiej liczby danych (nawet jeżeli będą to mikrochipy pasywne i pozbawione własnego źródła zasilania, to dane będą powstawały w sytuacjach, gdy przedmioty znajdują się w zakresie oddziaływania czytnika). Wszystkie te kwestie potraktowane łącznie stanowią fundamentalne zagrożenie dla prawa do prywatności.

---

<sup>14</sup> <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/rfid-chips> [dostęp: 09.02.2023].



## 2. RFID w związku z pracą

Najczęściej chipy zamontowane w różnego rodzaju przywieszkach/ smyczkach/bransoletach służą do tak prozaicznych kwestii, jak otwieranie bramek, drzwi, logowanie się do różnorodnych systemów.

Jeżeli chipy są aktywne i mają swoje zasilanie, rodzi się wręcz niekończące się spektrum zastosowań. Są to chipy umieszczane zazwyczaj w bransoletce (tak, aby reakcja chipa mogła być „powiązana” z dłonią pracownika). Przykładowo, UPS, stosując setki chipów, ma dostęp do informacji o technice jazdy zatrudnianych kurierów, np. o tym, czy zapinają pasy i ile czasu im to zabiera, czy o ich technikach parkowania *etc.* Firma w pierwszej dekadzie XXI w. wskazywała, że implementacja tego systemu pozwoliła jej zmniejszyć flotę samochodów o 10% oraz znacząco zmniejszyć zużycie paliwa<sup>15</sup>. Z kolei Amazon wprowadza bransolety, które wibrują, gdy pracownik magazynu kieruje rękę w stronę niewłaściwej półki, i w ten sposób w czasie rzeczywistym poprawiane/usprawniane są jego ruchy<sup>16</sup>.

## 3. Ocena w kontekście Proactionary Principle

Oczywiście w artykule opublikowanym w czasopiśmie, którego przedmiot stanowi prawo pracy i zabezpieczenie społeczne, najbardziej naturalne jest odnoszenie danego zjawiska do zagrożeń czy korzyści dla pracowników i pracodawców. Warto jednak spojrzeć na zachodzący proces – wykorzystanie technologii RFID i potencjalne wykorzystanie tej technologii (piszę „potencjalne”, ponieważ jak już wskazałam, skala takich przypadków na świecie jest jeszcze mocno ograniczona) – z punktu widzenia rozwoju technologii jako takiej. Wydaje się, że jest to tym ważniejsze, że coraz częściej (w każdym razie w mojej ocenie) w obszarze regulacji pracy będziemy mieli do czynienia z dylematami, które będą mniej czy bardziej bezpośrednim odzwierciedleniem wyraźnego postępu technologicznego. Na takie spojrzenie zwraca się

---

<sup>15</sup> E. Kaplan: *The Spy who Fired Me. The Human Costs of Workplace Monitoring*. March 2015. <https://harpers.org/archive/2015/03/the-spy-who-fired-me/> [dostęp: 09.02.2023].

<sup>16</sup> *Amazon Patents Wristband that Tracks Warehouse Workers' Movements*. 01.02.2018. <https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking> [dostęp: 09.02.2023].

uwagę w literaturze<sup>17</sup>. Przykładowo, można odwołać się do tzw. zasady proaktywnej (Proactionary Principle), sformułowanej przez filozofa i futurystę Maxa More'a<sup>18</sup>. Zasada ta ma ułatwić dokonanie oglądu, kiedy i w jakim zakresie jakaś technologia czy procedura powinna ulegać ograniczeniu. Max More wskazuje, że wolność ludzi w zakresie innowacji technologicznych jest bardzo cenna. Wiąże się z tym kilka imperatywów przy proponowaniu środków ograniczających, mianowicie należy:

- oceniać ryzyko i możliwości zgodnie z dostępną nauką, a nie z powszechną percepcją;
- uwzględniać zarówno koszty samych ograniczeń, jak i koszty utraconych możliwości;
- faworyzować środki, które są proporcjonalne do prawdopodobieństwa i wielkości skutków oraz które mają wysoką wartość oczekiwaną;
- chronić wolność ludzi do eksperymentowania, innowacji i postępu<sup>19</sup>.

Szczegółowe rozpisanie zasady proaktywnej wygląda następująco:  
„1. Wolność ludzi w kwestii wprowadzania innowacji technologicznych jest cenna dla ludzkości. Dlatego ciężar dowodu spoczywa na tych, którzy proponują środki ograniczające. Wszystkie proponowane środki powinny być dokładnie przeanalizowane.

2. Oceniamy ryzyko zgodnie z dostępną nauką, a nie powszechną percepcją, i pozwólmy na powszechne uprzedzenia w rozumowaniu.

3. Dajmy pierwszeństwo łagodzeniu znanych i udowodnionych zagrożeń dla zdrowia ludzkiego i jakości środowiska naturalnego przed działaniem przeciwko hipotetycznym zagrożeniom.

4. Traktujmy ryzyka technologiczne na tych samych zasadach, co ryzyka naturalne; unikajmy niedoceniań ryzyka naturalnego i prze-

---

<sup>17</sup> J.Z. Wasbin: *Examining the Legality of Employee Microchipping Under the Lens of the Transhumanistic Proactionary Principle*. "Washington University Jurisprudence Review" 2019, Vol. 11, Issue 2, s. 401–425.

<sup>18</sup> M. More: *The Proactionary Principle*. 28.03.2008. <http://strategicphilosophy.blogspot.com/2008/03/proactionary-principle-march-2008.html> [dostęp: 09.02.2023].

<sup>19</sup> Por. tamże: "People's freedom to innovate technologically is highly valuable, even critical, to humanity. This implies several imperatives when restrictive measures are proposed: Assess risks and opportunities according to available science, not popular perception. Account for both the costs of the restrictions themselves, and those of opportunities foregone. Favor measures that are proportionate to the probability and magnitude of impacts, and that have a high expectation value. Protect people's freedom to experiment, innovate, and progress".



ceniania ryzyka związanego z działalnością człowieka. Dokonujemy pełnego uwzględnienia korzyści płynących z postępu technologicznego.

5. Szacujemy konsekwencje wynikające z zaniechania danej technologii oraz uwzględniamy koszty i zagrożenia związane z zastąpieniem jej innymi wiarygodnymi opcjami, szacujemy ze starannym uwzględnieniem skutków o szerokim zasięgu i skutków następczych.

6. Rozważmy środki ograniczające tylko wtedy, gdy potencjalny wpływ danej działalności ma zarówno znaczne prawdopodobieństwo, jak i dotkliwość. W takich przypadkach, jeżeli działanie przynosi również korzyści, należy zdyskontować wpływy zgodnie z możliwością dostosowania się do niekorzystnych skutków. Jeżeli środki mające na celu ograniczenie postępu technologicznego wydają się uzasadnione, należy zapewnić, że zakres tych środków będzie proporcjonalny do zakresu prawdopodobnych skutków.

7. Dokonując wyboru spośród środków mających na celu ograniczenie innowacji technologicznych, uszeregujemy kryteria decyzyjne w następujący sposób: nadajmy pierwszeństwo zagrożeniom dla życia ludzkiego i innych inteligentnych gatunków nad zagrożeniami dla innych gatunków; nadajmy pierwszeństwo zagrożeniom, które nie są śmiertelne dla zdrowia ludzkiego, nad zagrożeniami ograniczonymi do środowiska (w rozsądnych granicach); nadajmy pierwszeństwo zagrożeniom bezpośrednim nad zagrożeniami odległymi; preferujmy środek o największej wartości oczekiwanej, nadajmy pierwszeństwo zagrożeniom bardziej pewnym nad mniej pewnymi oraz nieodwracalnym lub trwałym skutkom nad skutkami przejściowymi<sup>20</sup>.

---

<sup>20</sup> Tamże: "1. People's freedom to innovate technologically is valuable to humanity. The burden of proof therefore belongs to those who propose restrictive measures. All proposed measures should be closely scrutinized.

2. Evaluate risk according to available science, not popular perception, and allow for common reasoning biases.

3. Give precedence to ameliorating known and proven threats to human health and environmental quality over acting against hypothetical risks.

4. Treat technological risks on the same basis as natural risks; avoid underweighting natural risks and overweighting human-technological risks. Fully account for the benefits of technological advances.

5. Estimate the lost opportunities of abandoning a technology, and take into account the costs and risks of substituting other credible options, carefully considering widely distributed effects and follow-on effects.

6. Consider restrictive measures only if the potential impact of an activity has both significant probability and severity. In such cases, if the activity also generates benefits,

Dokonując analizy obecnych potencjalnych korzyści wynikających z mikrochipowania podskórnego, nie można wskazać, aby ta technologia w widoczny sposób poprawiała kondycję człowieka, ale równocześnie nie powinna być ograniczana ze względu na strach, który wywołuje, czy obawy dotyczące jej rezultatów. W ocenie Joshuy Z. Wasbina reakcje ustawodawstw stanowych w USA są uzasadnione w kontekście dominującego w tym państwie zatrudnienia „*employment at will*”, pozwalającego pracodawcy rozwiązać stosunek pracy bez podania przyczyny<sup>21</sup>.

Należy podkreślić, że mikrochipowanie nie musi wiązać się z przetwarzaniem danych osobowych. Jeżeli jest ono stosowane wyłącznie w celu uzyskiwania dostępu do pomieszczeń, wydaje się bezpieczniejsze z punktu widzenia ochrony danych niż technologie bezpieczeństwa stosowane w niektórych miejscach pracy, takie jak skanowanie odcisków palców lub siatkówki oka.

Nie jest tak, że nie mam świadomości zagrożeń, jakie rodzi wykorzystywanie technologii. W większości jurysdykcji na świecie pracodawca ma lub będzie miał (jeżeli zainwestuje w określoną technologię) dostęp do danych pracownika mówiących np. o rytmie jego serca, godzinach snu czy konsumpcji alkoholu poza godzinami pracy. Polecenie noszenia bransoletek, które pozwalają na pozyskiwanie takich danych, nawet jeżeli będzie wymagało zgody pracownika (a często ma ona charakter czysto formalny, co wynika z nierównowagi siły pomiędzy stronami stosunku pracy), będzie prowadziło do sytuacji, gdy na podstawie analizy takich czynników jak wskazane pracodawcy będą podejmowali decyzje o zwolnieniu pracownika, promocji czy zmianie zakresu zadań<sup>22</sup>.

---

discount the impacts according to the feasibility of adapting to the adverse effects. If measures to limit technological advance do appear justified, ensure that the extent of those measures is proportionate to the extent of the probable effects.

7 When choosing among measures to restrict technological innovation, prioritize decision criteria as follows: Give priority to risks to human and other intelligent life over risks to other species; give non-lethal threats to human health priority over threats limited to the environment (within reasonable limits); give priority to immediate threats over distant threats; prefer the measure with the highest expectation value by giving priority to more certain over less certain threats, and to irreversible or persistent impacts over transient impacts”.

<sup>21</sup> J.Z. Wasbin: *Examining the Legality...*

<sup>22</sup> W. Turner: *Chipping Away at Workplace Privacy: The Implementation of RFID Microchips and Erosion of Employee Privacy*. “Washington University Journal of Law & Policy” 2020, Vol. 61, s. 275–297.

Naturalnie w pewnych sytuacjach może się pojawić opór zbiorowy – przykładowo, australijskie związki zawodowe zablokowały regulację, według której kierowca ciężarówki otrzymywałby lekkie uderzenie prądem w sytuacji, gdy urządzenia pokazywałyby, że zamykają mu się oczy. Należy tu uściślić, że takie rozwiązanie zaproponowało australijskie ministerstwo transportu pod wpływem tragicznego wypadku z udziałem ciężarówki, a nie pracodawcy<sup>23</sup>. Inny przykład to wycofanie się „Daily Telegraph” z używania urządzenia OccupEye kontrolującego działania pracowników biurowych<sup>24</sup>.

#### 4. Uwagi końcowe

W tekście pokazano przykłady ustawodawstw stanowych z USA wprost zakazujących (i wprowadzających sankcje) w razie oczekiwania przez pracodawcę, że pracownik podda się procedurze mikrochipowania (także w wypadku chipów pasywnych, których używanie nie różni się zasadniczo od zawieszanej na szyi smyczy czy bransolety, gdzie znajdowałby się chip). Wydaje się, że dość energiczna reakcja amerykańskiego ustawodawstwa wynika z kilku przyczyn.

Po pierwsze, mamy do czynienia z jurysdykcją, w której w zdecydowanej większości stanów istnieje koncepcja „*employment at will*”, pozwalająca pracodawcy w każdej chwili rozwiązać umowę o pracę (tak długo, jak jego działanie nie ma charakteru dyskryminującego ze względu na, przykładowo, rasę albo działalność związkową). Jest jeden wyjątek (Montana), w którym regulacja przypomina konstrukcję powszechnej ochrony przed wypowiedzeniem (konieczność uzasadnienia działania zmierzającego do zakończenia trwania relacji), równocześnie wiele stanów wymaga od pracodawcy działania w dobrej wierze, ale niezależnie od tego niewątpliwie pozycja pracownika wobec pracodawcy jest zdecydowanie słabsza w USA niż w UE<sup>25</sup>. Jest

---

<sup>23</sup> <https://www.news.com.au/technology/innovation/motoring/proposal-to-electrocute-drowsy-truck-drivers-in-wake-of-fatal-crashes-slammed/news-story/d69c25f8fe814993848509b6dad40731> [dostęp: 09.02.2023]; <https://www.dailymail.co.uk/news/article-5279261/Minister-shocks-trucking-industry-electric-jolt-idea.html> [dostęp: 09.02.2023].

<sup>24</sup> <https://www.theguardian.com/media/2016/jan/11/daily-telegraph-to-withdraw-devices-monitoring-time-at-desk-after-criticism> [dostęp: 09.02.2023].

<sup>25</sup> W Montanie zasada zatrudniania „*employment at will*” dotyczy tylko 6-miesięcznego okresu próbnego, następnie, aby rozwiązać umowę, pracodawca musi wskazać

to jedna z przyczyn, dla których legislacja próbuje go ochronić przed niebezpieczeństwem przymusowego mikrochipowania<sup>26</sup>.

Po drugie, w USA nie ma odpowiednika RODO na poziomie federalnym, a co za tym idzie – ochrona (w każdym razie na poziomie federalnym) przed pozyskiwaniem i przetwarzaniem danych osobowych jest zdecydowanie słabsza niż w UE.

Po trzecie, społeczeństwo USA „mentalnie” wyjątkowo ciężko zniosło ograniczenia wolności i swobody oraz zagrożenia związane z ochroną prywatności wynikające z pandemii COVID-19.

Po czwarte, jak pokazują dyskusje i komentarze w procesach legislacyjnych, w niektórych stanach mikrochipy jednoznacznie przypisywane są mrocznym siłom ostatecznym, znakowaniu przez Antychrysta itp. – co z europejskiej perspektywy wydaje się niezbyt poważnym podejściem<sup>27</sup>.

Interesujące będzie dalsze obserwowanie reakcji społecznych i reakcji ustawodawców na potencjalne modyfikacje ciała człowieka w związku z pracą.

Patrząc z perspektywy UE, zainteresowanie „legislacyjne” tematem jest dość umiarkowane. Można wskazać na ekspertyzę zamówioną przez Parlament Europejski w 2018 r.<sup>28</sup>. W opracowaniu wskazuje się, że postanowienia RODO (a mówiąc bardziej konkretnie, punkty 32, 33, 50 Preambuły do Rozporządzenia oraz art. 4, 7, 9, 11, 13 (3), a także 49)

---

powód. Wiele stanów wprowadziło *de facto* ograniczenie zasady „*employment at will*” poprzez wymóg działania pracodawcy w dobrej wierze (*covenant of good faith*). Na przykład, rozwiązanie stosunku pracy pracownika tuż przed tym, jak miał on otrzymać dużą prowizję, może być interpretowane jako działanie w złej wierze. Podobnie pracodawca nie może podawać nieprawdziwych powodów wypowiedzenia pracownikowi umowy o pracę. Działanie w dobrej wierze może zostać naruszone również w przypadku, gdy pracownik został zwolniony po długim czasie, gdy otrzymywał pozytywne oceny pracy i był przekonany, że jego miejsce pracy jest stabilne – aby udowodnić, że zwolnienie nie zostało dokonane w złej wierze, pracodawca może być zmuszony do wykazania „słusznej przyczyny”.

<sup>26</sup> S. Simpson: *Comment: Microchipping Employees and Privacy Implications – Does My Boss Know Where I am Right Now?* “Marquette Benefits and Social Welfare Law Review” 2019, Vol. 20, Issue 2, s. 279–298.

<sup>27</sup> D. Tencer: *Virginia Delegates Pass Bill Banning Chip Implants as ‘Mark of the Beast’*. 10.02.2010. <https://www.rawstory.com/2010/02/virginia-passes-law-banning-chip-implants-mark-beast/> [dostęp: 09.02.2023].

<sup>28</sup> R. Graveling, T. Winski, K. Dixon: *The Use of Chips Implants for Workers*. European Parliament, 2018. <https://op.europa.eu/pl/publication-detail/-/publication/34cb538d-58b7-11e8-ab41-01aa75ed71a1/language-en> [dostęp: 09.02.2023].

stanowią adekwatne zabezpieczenie interesów pracownika. Podobnie jako wystarczającą podstawę ochrony autorzy podają art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności oraz powstałe na jego bazie orzecznictwo, które szeroko definiuje pojęcie „życie prywatne” (takie jak przykładowo Niemietz v. Niemcy albo Bărbulescu v. Rumunia). W konkluzji autorzy sygnalizują, że należy obserwować zjawisko, ale nie podejmować działań przygotowujących do szczególnej legislacji. Postulują za to badania o charakterze medycznym, mające na celu ocenę długookresowych skutków używania podskórnych mikrochipów.

Z polskiej perspektywy według mnie obecnie ważniejsze niż proponowanie działań legislacyjnych dotyczących mikrochipów wydają się postulaty ujednoczenia standardu ochrony prawa do prywatności w miejscu pracy w sposób niezależny od podstawy zatrudnienia. Jak wskazuje Jakub Kowal, przyjęte przez polskiego ustawodawcę rozwiązanie (na podstawie upoważnienia w art. 88 RODO) w istotny sposób różnicują zakres ochrony osób zatrudnionych na podstawie stosunku pracy oraz na podstawie umów cywilnoprawnych. Przykładowo, do tych drugich nie mają zastosowania zasady dotyczące użycia monitoringu. Tylko w odniesieniu do pracowników w rozumieniu art. 2 k.p. mamy do czynienia z zamkniętym katalogiem danych osobowych, jakie przetwarza pracodawca na etapie ubiegania się o zatrudnienie oraz po zatrudnieniu, z zastosowaniem dodatkowych wymogów w zakresie zgody na przetwarzanie danych należących do szczególnych kategorii. Należy podzielić konstatację autora, że dysproporcji tych nie można uzasadnić prawną specyfiką stosunku pracy<sup>29</sup>.

Oczywiście ta mikroopowiastka o mikrochipach podskórnych może rodzić bardziej zasadnicze (w każdym razie w mojej ocenie) pytania – przede wszystkim o rolę i naturę *big data*. Jeżeli uznamy, że w kontekście zmiany klimatycznej i konieczności wdrażania określonych polityk klimatycznych do ich realizacji potrzebujemy określonych zasobów *big data* – np. w celu uzyskania wiedzy na temat przemieszczania się ludzi, aby tworzyć bardziej wydajne, ekologiczne, a co za tym idzie: generujące mniejszy ślad węglowy systemy transportowe – to rodzi się

---

<sup>29</sup> J. Kowal: *Wybrane aspekty ochrony prywatności osób zatrudnionych a forma zatrudnienia – uwagi na tle polskich regulacji*. „Praca i Zabezpieczenie Społeczne” 2021, nr 4, s. 36–43.

pytanie: w jaki sposób przy naszym obecnym podejściu do ochrony prywatności dane te mają być pozyskiwane? Pozostaje jeszcze kwestia ich anonimizacji, ale to już jest krok drugi, gdyż najpierw musimy zaakceptować myśl o potrzebie ułatwień dla pozyskiwania danych<sup>30</sup>. Podobnie, w mojej ocenie, rodzi się kolejne pytanie: czy jeżeli uznamy, że niezbędne jest (np. ze względu na zachodzącą zmianę demograficzną i kurczenie się zasobów naturalnych) zwiększenie efektywności pracy pracowników, to czy w takim razie nie musimy zmienić naszego spojrzenia na zasysanie danych dotyczących sposobu wykonywania przez nich pracy? Naturalnie takie spojrzenie na tę kwestię wymagałoby przyjęcia, że nie mamy obecnie do czynienia ze „standardową” sytuacją, ale taką, w której ze względu na zagrożenia związane z koniecznością ograniczenia emisji dwutlenku węgla, zmianę demograficzną czy inny czynnik musimy fundamentalnie przemodelować stosunek do pozyskiwania danych<sup>31</sup>.

### Bibliografia

- Adamczyk S., Surdykowska B.: *Cyborgizacja człowieka pracy. Czy godność pracy ludzkiej przetrwa? W stulecie urodzin Stanisława Lema. „Praca i Zabezpieczenie Społeczne”* 2021, nr 12, s. 3–11.
- Firfiray Sh.: *Microchips Implants are Threatening Workers’ Rights*. 22.11.2018. <https://theconversation.com/microchip-implants-are-threatening-workers-rights-107221> [dostęp: 09.02.2023].
- Giest S.: *Big Data Analytics for Mitigating Carbon Emissions in Smart Cities: Opportunities and Challenges*. “European Planning Studies” 2017, Vol. 25, Issue 6, s. 941–957.
- Gonzalez J.S.: *Stop Before It Starts: Regulating Employee Microchipping in the Covid-19 Era*. “Mississippi Law Journal” 2020, Vol. 90, Issue 1, s. 1–34.
- Graveling R., Winski T., Dixon K.: *The Use of Chips Implants for Workers*. European Parliament, 2018. <https://op.europa.eu/pl/publication-detail/-/publication-n/34cb538d-58b7-11e8-ab41-01aa75ed71a1/language-en> [dostęp: 09.02.2023].
- Kowal J.: *Wybrane aspekty ochrony prywatności osób zatrudnionych a forma zatrudnienia – uwagi na tle polskich regulacji*. „Praca i Zabezpieczenie Społeczne” 2021, nr 4, s. 36–43.

---

<sup>30</sup> S. Giest: *Big Data Analytics for Mitigating Carbon Emissions in Smart Cities: Opportunities and Challenges*. “European Planning Studies” 2017, Vol. 25, Issue 6, s. 941–957.

<sup>31</sup> V. Vijay, M. Fekete Farkas: *The Era of Big Data and Path towards Sustainability*. June 2018. [https://www.researchgate.net/publication/325996293\\_The\\_Era\\_of\\_Big\\_Data\\_and\\_Path\\_towards\\_Sustainability](https://www.researchgate.net/publication/325996293_The_Era_of_Big_Data_and_Path_towards_Sustainability) [dostęp: 09.02.2023].



- More M.: *The Proactionary Principle*. 28.03.2008. <http://strategicphilosophy.blogspot.com/2008/03/proactionary-principle-march-2008.html> [dostęp: 09.02.2023].
- Mutigwe C., Aghdasi F.: *Research Trends in RFID Technology*. "Interim: Interdisciplinary Journal" 2007, Vol. 6, Issue 1, s. 68–82. <https://www.semanticscholar.org/paper/Research-trends-in-RFID-technology-Mutigwe-Aghdasi/4b7450d3083b5fbb3f2a5192e701b8fb81c59562> [dostęp: 09.02.2023].
- Rodriguez D.: *Chipping in at Work: Privacy Concerns Related to the Use of Body Microchip ("RFID") Implants in the Employer-Employee Context*. "Iowa Law Review" 2019, Vol. 104, Issue 3, s. 1581–1611.
- Simpson S.: *Comment: Microchipping Employees and Privacy Implications – Does My Boss Know Where I am Right Now?* "Marquette Benefits and Social Welfare Law Review" 2019, Vol. 20, Issue 2, s. 279–298.
- Turner W.: *Chipping Away at Workplace Privacy: The Implementation of RFID Microchips and Erosion of Employee Privacy*. "Washington University Journal of Law & Policy" 2020, Vol. 61, s. 275–297.
- Vijay V., Fekete Farkas M.: *The Era of Big Data and Path towards Sustainability*. June 2018. [https://www.researchgate.net/publication/325996293\\_The\\_Era\\_of\\_Big\\_Data\\_and\\_Path\\_towards\\_Sustainability](https://www.researchgate.net/publication/325996293_The_Era_of_Big_Data_and_Path_towards_Sustainability) [dostęp: 09.02.2023].
- Wasbin J.Z.: *Examining the Legality of Employee Microchipping Under the Lens of the Transhumanistic Proactionary Principle*. "Washington University Jurisprudence Review" 2019, Vol. 11, Issue 2, s. 401–425.

## O lęku przed nadciągającym chipowaniem pracowników – uwagi na tle powstającego ustawodawstwa w USA

### Streszczenie

W artykule zwrócono uwagę na ustawodawstwo w poszczególnych stanach USA, w którym zakazuje się (lub podkreśla znaczenie wyrażenia na to zgody) mikrochipowania podskórnego w relacjach pracy. W ocenie autorki problematyka stosowania mikrochipów w kontekście pracy i potencjalne reakcje ustawodawstwa mogą być dobrym papierkiem lakmusowym reakcji na następującą zmianę technologiczną. Równocześnie postępujące wykorzystywanie mikrochipów podskórnych jest bardzo wczesną fazą zjawiska cyborgizacji ciała pracownika.

**Słowa kluczowe:** mikrochipy, praca, rozwój technologii