Pojęcia kluczowe: *inwigilacja, kapitalizm, ochrona konsumentów, ochrona danych osobowych, regulacje amerykańskie, bezpieczeństwo obrotu danymi*

Artykuły

Tomasz A. Zienowicz

SURVEILLANCE CAPITALISM – ROZWAŻANIA PRAWNOTEORETYCZNE

Artykuł obejmuje problematykę związana z obrotem danymi osobowymi, ich ochroną, zabezpieczeniem przed niepożądanym przejęciem oraz wskazuje na rozwiązania amerykańskie w zakresie praw i obowiązków uczestników rynku danych osobowych.

I

Kapitalizm inwigilacji (*surveillance capitalism*) to pojęcie opisane przez Shoshanę Zuboff[1]. Generalnie jest to model biznesowy, którego rozwój i przewagi konkurencyjne oparte są na zbieraniu, katalogowaniu i przetwarzaniu danych osobniczych. Zważywszy na treści zawarte w rozporządzeniu Parlamentu Europejskiego i Rady 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych

[1] S. Zuboff, *The Age of surveillance capitalism – The Fight for a human future at the new frontier of power*, Profile Books Ltd. 2018. Autorka porusza problematykę największego, jej zdaniem, zwrotu w erze kapitalizmu, nazywając opisywaną sytuację mianem kolonizacji, która dotyczy i dotyka przede wszystkim konsumentów, ich zachowań oraz kwestii kierowania i wpływania na ich wolę. Książka ta nie jest antytechnologiczna, nie opowiada się za zaprzestaniem badań i prowadzenia działań nad rozwojem sztucznej inteligencji, wskazuje kwestie nieuregulowania tego typu rozwiązań biznesowych zasadzających się w głównej mierze na handlu danymi osobowymi. Autorka toczy rozważania na tematy związane z niedaleką przyszłością, w której nastąpi gwałtowny rozwój obrotu danymi i metadanymi dotyczącymi zachowań ludzkich, proponując w tym względzie publiczną debatę. Jej obszerna analiza pokazuje bezprecedensowe wyzwania dla ludzkiej autonomii, społecznej solidarności i demokracji w zakresie zmagania się z tego rodzaju kapitalizmem.

 DOI: 10.54383/0031-0344.2023.1-2.2

w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[2] oraz dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW[3] i ustawie z 10.05.2018 r. o ochronie danych osobowych[4] jest to pojęcie daleko szersze niż ujawniona w przedmiotowych aktach prawnych problematyka, dotyczy bowiem ono praktycznie każdego zakresu przejawu ludzkiego działania (bez ograniczenia np. do konsumentów), takiego jak zbieranie i przetwarzanie danych m.in. dotyczących lokalizacji, emocji, wypowiedzi, pragnień, operacji finansowych, stanu zdrowia, pasji, nawyków *etc*. Wprowadzenie takiego modelu inwigilacji rodzi ogromne zagrożenia zwłaszcza wobec braku zasadniczych regulacji prawnych w przedmiotowym zakresie na płaszczyźnie prawa międzynarodowego publicznego, prywatnego i europejskiego. Pionierem w rozważaniach i wdrożeniach takiego typu postępowania w zakresie szeroko pojętych danych osobowych są Stany Zjednoczone Ameryki. Na tym rynku gwałtownie zmieniające się środowisko ekonomiczne i przedmiot obrotu w dziedzinie informatyki i teleinformatyki napędzany bardzo dużą konkurencją niewątpliwie wyprzedzają reakcję prawodawczą w omawianym zakresie. Algorytmizowanie online wszelkich przejawów ludzkiego działania bez jakichkolwiek regulacji prawnych w przedmiotowym zakresie daje pole do nadużyć, a nawet możliwość wpływania na działanie ludzkie w już uregulowanych prawnie sferach życia. Odrębną problematyką wyłaniającą się z tego zjawiska jest obrót danymi i metadanymi dotyczącymi działań ludzkich na potrzeby handlu, usług, ale także wojska, obronności, wywiadu oraz wszelkich działań podejmowanych nielegalnie nakierowanych na realizację celów niedostępnych w ramach działań konwencjonalnych oraz legalnych.

Pamiętać przy tym wypada, że metadane i dane osobowe można skomercjalizować i mogą one być przedmiotem obrotu w wielu systemach prawnych, w szczególności chodzi tu o rozwiązania i rynki amerykańskie. Głównym impulsem dla obecnej sytuacji rynkowej są zachowania zachodzące w Google Ad-

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), http://data.europa.eu/eli/reg/2016/679/oj.

[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, http://data.europa.eu/eli/dir/2016/680/oj.

[4] Ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

words, gdzie jak się obserwuje, odbywa się największy obrót zarówno w zakresie wolumenu, jak i wysokości transakcji na polu obrotu danymi osobowymi[5]. Gromadzenie danych może oczywiście przyczynić się do tworzenia inteligentnych miast (ruch uliczny, obsługa administracyjna *etc.*), optymalizacji handlu (aplikacje internetowe) oraz może być przydatne w tzw. samoczynnej (osobniczej) optymalizacji, czy też w ogóle do budowy szeroko pojętej sztucznej inteligencji, jednak bez regulacji na poziomie państwowym, jeśli spojrzeć z amerykańskiej perspektywy prawnej, może dojść do użycia tych zbiorów przeciw osobom, których owe dane dotyczą[6]. Zysk, jaki generowany jest z obrotu metadanymi i danymi osobniczymi, uruchomił w Stanach Zjednoczonych działalność lobbingową na rzecz zwiększenia autonomii tego rynku oraz możliwości prawnego usankcjonowania pozyskania i przetwarzania danych na praktycznie wszelkie sposoby mogące przynieść profit z tego typu działalności[7].

Analizując przedmiotowe zjawisko w zakresie ogólnoświatowym, wskazać jednak należy w kontekście przyszłych regulacji międzynarodowych, że nie tylko państwa uważane powszechnie za demokratyczne są na tyle uprzemysłowione technologicznie, że mogą zmagać się z przedmiotową problematyką. Także i inne kraje podejmują działania w zakresie gromadzenia i przetwarzania danych w przedmiotowym zakresie. Liderem są tu Chiny[8]. Chińska Republika Ludowa uruchomiła w dobie walki z pandemią narodową aplikację *close contact detector*, która pozwala dokonać weryfikacji osób zakażonych[9]. Tak zwany detek-

[5] S. Zuboff, *The Age...*

[6] *Quantifiel Self* dotyczyło we wczesnej fazie rozwoju badań typu EKG, EEG, EVG, GSR, oddechu i innych czynności ciała, które można było monitorować. Następnym etapem stało się analizowanie gromadzonych danych dotyczących praktycznie całej parametryki zachowania ludzkiego organizmu oraz możliwość analizy, przetwarzania i obrotu tymi danymi, co doprowadziło do tzw. samopoznania poprzez liczby. Obecnie przodują w tym zakresie serwisy obsługujące monitorowanie np. snu, ruchu, takie jak Fitbit lub Apple Watch, a w połączeniu ze zwiększoną dostępnością Internetu rzeczy w opiece zdrowotnej i sprzęcie do ćwiczeń sprawiło to, że samopoznanie stało się powszechne. Innymi terminami przyjętymi dla problematyki określającej wykorzystanie danych w celu poprawy codziennego funkcjonowania stały się autoanaliza, hakowanie ciała, samoocena, samokontrola, nadzór (rejestracja aktywności osobistej) i informatyka osobista, por. K. Kevin, *The inevitable: understanding the 12 technological forces that will shape our future*, Penguin 2017, s. 247; W.H. James *You, By the Numbers*, „Harvard Business Review" 2012; W. Stephen, *The Personal Analytics of My Life*, stephenwolfram.com. Stephen Wolfram, 2012.

[7] S. Zuboff, *The Age...*

[8] Zob. https://www.bbc.com/news/technology-51439401.

[9] 中國 電子 科技 集團公司, China Electronics Technology Group Corporation założona w 2002 r. jest chińskim przedsiębiorstwem państwowym. Jego działalność obejmuje tworzenie sprzętu komunikacyjnego, komputerowego, sprzętu elektronicznego, rozwój oprogramowania, usługi badawcze, inwestycje i zarządzanie aktywami do zastosowań cywilnych i wojskowych. W marcu 2016 r. rząd zlecił firmie opracowanie oprogramowania do identyfikacji potencjalnych terrorystów; wykorzystanie danych na temat pracy, hobby, nawyków konsumpcyjnych i innych zachowań. W czerwcu 2017 r. CETC z powodzeniem uruchomił największy na świecie rój dronów ze stałopłatami. Drony w roju były komercyjnym modelem ze stałym skrzydłem wyprodukowanym przez Skywalker Technology, firmę z siedzibą w Wuhan. W grudniu 2017 r. CETC zabiegał

tor bliskiego kontaktu informuje użytkowników, czy znajdowali się w pobliżu osoby, u której potwierdzono obecność wirusa lub podejrzewano, że jest jego nosicielem. Aplikacja działa w ten sposób, że użytkownicy skanują kod *Quick Response* (QR) na swoich smartfonach za pomocą aplikacji, takich jak usługa płatności Alipay lub platforma społecznościowa WeChat, i uzyskują informację o osobach zakażonych znajdujących się w ich pobliżu. Aplikacja jest powiązana z numerem telefonu, użytkownicy podają swoje imiona i nazwiska oraz numery identyfikacyjne (ID)[10].

Wskazać jednak wypada, że wbrew twierdzeniom podmiotów niepowiązanych z rządem Chińskiej Republiki Ludowej aplikacja może stygmatyzować osoby zakażone, narażać je na rozmaite niebezpieczeństwa, co może doprowadzić do odwrotnego od zamierzonego skutku, jaki ma nieść za sobą uruchomienie aplikacji w wydaniu chińskim. Wskazuje się, że pandemia jest tylko przyczynkiem do zacieśnienia kontroli społecznej na terenie ChRL. Aplikacja bowiem nie tylko informuje o kontakcie z osobami zakażonymi lub podejrzanymi o zakażenie, ale także daje możliwość sprawdzenia trzech wybranych osób w tym zakresie, co zdaniem analityków przekracza potrzeby walki z pandemią. Podnosi się także brak definicji ostrej co do pojęcia bliskiego kontaktu oraz niemożliwość weryfikacji, czy autorzy programu na bieżąco nie manipulują przesłankami w tym zakresie. Aplikacja także nie przewiduje analizy testowanych, u których następuje wynik fałszywie ujemny lub fałszywie dodatni, co stanowi lukę, która może w zasadzie

o kontrakty rządowe na wdrażanie systemów rozpoznawania twarzy w prefekturze Hotan. W sierpniu 2020 r. Biuro Przemysłu i Bezpieczeństwa umieściło cztery spółki zależne CETC na liście podmiotów odpowiedzialnych za pracę nad zmilitaryzowaniem sztucznych wysp na Morzu Południowochińskim.

[10] Według państwowej agencji informacyjnej Xinhua aplikacja została opracowana wspólnie przez departamenty rządowe i China Electronics Technology Group Corporation i jest zasilana danymi pochodzącymi od Ministerstw Zdrowia i Transportu. Według strony rządowej w Chinach i całej Azji gromadzenie i przetwarzanie danych nie jest postrzegane jako coś, co powinno podlegać szczególnemu nadzorowi w zakresie wykorzystywania. Z punktu widzenia władz Państwa Środka jest to przydatna usługa będąca narzędziem służącym tylko dobrym celom. Chiński rząd definiuje przy tym tzw. bliski kontakt jako zbliżanie się, bez skutecznej ochrony, do potwierdzonych zakażonych i podejrzewanych o zakażenie lub gdy osoba była chora bezobjawowo. „Bliski kontakt" obejmuje kontakt osób ściśle ze sobą współpracujących, chodzących do tej samej klasy szkolnej lub zamieszkujących razem. Pojęcie to obejmuje także personel medyczny bez względu na narażanie się na kontakt oraz inne osoby, które miały bliski kontakt z pacjentami i ich opiekunami. Następną grupą są pasażerowie i załoga samolotów, pociągów i innych środków transportu z osobą zarażoną. Pojęcie bliskiego kontaktu doprecyzowane jest w ten sposób, że ów kontakt postrzega się wśród pasażerów linii lotniczych znajdujących się w trzech rzędach od osoby zakażonej, a wśród personelu pokładowego wszyscy są postrzegani jako pozostający w bliskim kontakcie. W przypadku pociągów klimatyzowanych wszyscy pasażerowie i członkowie załogi tego samego wagonu uważani są za pozostających w bliskim kontakcie w sytuacji wykrycia osoby zarażonej, http://www.xinhuanet.com/english/2020-02/10/c_138770415.htm (dostęp: 13.01.2023 r.). Powszechnie jednak wiadomo, że chiński rząd wprowadził skrajnie wysoki poziom nadzoru nad obywatelami, w tym nadzoru technologicznego, https://www.bbc.com/news/technology-51439401 (dostęp: 11.02.2020 r.).

czynić ów system bezużytecznym[11]. Przestrzega się także przed wystąpieniem społecznego piętna wśród społeczności chińskiej w stosunku do osób zakażonych. Wprawdzie każdy wirus czy generalnie zachorowanie, o którym społeczeństwo może lub powinno się dowiedzieć, może rodzić takie piętno, ale w zakresie koronawirusa występuje większe ryzyko utrwalenia tego stanu rzeczy. Wskazuje się, że aplikacja sprowokuje zachowania prowadzące do unikania znajomych czy też lokalnej społeczności w celu uniknięcia napiętnowania spowodowanego wykryciem koronawirusa[12]. Należy bowiem pamiętać, że wraz z rozpoczęciem pandemii władze Wuhan nakazały przekazywać informacje o obywatelach z tego miasta do administracji innych miast. Normą jest w Państwie Środka publiczne piętnowanie wykroczeń, urządzanie lokalnych zebrań ludowych w celu pokazania sprawców i ich ukarania czy też wskazania, że takie zachowania są niepożądane społecznie. Ta pragmatyka działania przenosi się niejako dzięki aplikacji do sieci, a tu mogą być one przedmiotem obrotu jako zagregowane dane[13]. Wskazana aplikacja może także zawierać funkcje umożliwiające śledzenie poszczególnych podmiotów w zakresie innych aktywności związanych z czynnościami życia codziennego. Podmioty tworzące tę aplikację ściśle współpracują z wojskiem i rządem na różnych polach, więc w kraju pozbawionym demokratycznych procedur kontrolnych nie ma żadnej gwarancji, że przedmiotowa aplikacja nie jest po prostu narzędziem do inwigilacji obywateli. Podobne działania podejmuje także Google, tworząc np. Google Flu Trends – program do wykrywania grypy, która na dzień dzisiejszy daje 50% prawdopodobieństwa wykrycia jej na danym terenie albo w danej populacji[14]. Nie ma obecnie żadnej kontroli nad tworzeniem map nadzoru nad rozprzestrzenianiem się zjawisk obserwowanych w przedmiotowym zakresie[15]. Innymi podmiotami angażującymi się w sferę *surveillance capitalism* są Alexa i ntechlab – spółki zajmujące się tzw. *Augmenting Intelligence*[16]. Rozwiązania tych podmiotów opierają się na rozpoznawalności twarzy. Oprogramowanie softwarowe jest najczęściej dodatkiem do kamer przemysłowych i ma zastosowanie głównie w handlu detalicznym. Podmioty te gromadzą dane biometryczne, co pozwala w milisekundach rozpoznać podmiot znajdujący się w ich bazie[17]. Spółki te obecnie nie przetwarzają danych klientów ani nie używają pełnej gamy zastosowań swoich produktów, jednak nie ma w tej chwili żadnych

[11] M. Schoch-Spana, https://www.technologyreview.com/2020/02/13/844805/coronavirus-china-app-close-contact-surveillance-covid-19-technology/ (dostęp: 13.01.2023 r.).

[12] C. Lynteris, https://www.technologyreview.com/2020/02/13/844805/coronavirus-china-app-close-contact-surveillance-covid-19-technology/ (dostęp: 13.01.2023 r.).

[13] C. Lynteris, https://www.technologyreview.com/2020/02/13/844805/coronavirus-china-app-close-contact-surveillance-covid-19-technology/ (dostęp: 13.01.2023 r.).

[14] D. Stellmach,[https://www.technologyreview.com/2020/02/13/844805/coronavirus-china-app-close-contact-surveillance-covid-19-technology/ (dostęp: 13.01.2023 r.).

[15] Zob. https://www.technologyreview.com/2020/02/13/844805/coronavirus-china-app-close-contact-surveillance-covid-19-technology/ (dostęp: 13.01.2023 r.).

[16] Zob. www.ntechlab.com (dostęp: 20.02.2020 r.), www.alexa.com (dostęp: 13.01.2023 r.).

[17] www.ntechlab.com (dostęp: 20.02.2020 r.), www.alexa.com (dostęp: 13.01.2023 r.).

podstaw prawnych na terenie Stanów Zjednoczonych na poziomie federalnym, aby takie usługi legalnie dostarczać wraz z przetwarzaniem i sprzedażą danych w tym zakresie.

II

Jedną z pierwszych materialnoprawnych reakcji na zmieniającą się rzeczywistość była nowelizacja kodeksu cywilnego stanu Kalifornia. Począwszy od 23.09.2018 r. nastąpiła szeroka nowelizacja art. 1798 kodeksu cywilnego Kalifornii, obejmująca zmiany dotyczące problematyki danych osobowych[18] konsumentów i grup konsumentów[19] w zakresie ich zbierania (gromadzenia)[20], przetwarzania[21] i obrotu nimi[22]. Nowelizacja uregulowana pod nazwą California Consumer Privacy Act of 2018 wprowadza szereg regulacji nieznanych dotychczas ustawodawstwu amerykańskiemu. Od 1.01.2020 r. ustawa przyznaje konsumentowi w odniesieniu do jego danych osobowych obligatoryjny obowiązek

[18] W zakres tego pojęcia, w myśl art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act), wchodzi pojęcie informacji biometrycznych, które w rozumieniu ustawy oznaczają fizjologiczne, biologiczne lub behawioralne cechy danej osoby, w tym kwas dezoksyrybonukleinowy (DNA) danej osoby, które można wykorzystać pojedynczo lub w połączeniu ze sobą lub z innymi danymi identyfikującymi w celu ustalenia indywidualnej tożsamości. Informacje biometryczne obejmują między innymi zdjęcia tęczówki, siatkówki, odcisków palców, twarzy, dłoni, wzorów żył i nagrania głosu, na podstawie których można wyodrębnić szablon identyfikacyjny lub odcisk głosu, oraz wzorce lub rytmy naciśnięć klawiszy, wzorce chodu lub rytm snu, a także dane dotyczące snu, zdrowia lub ćwiczeń, które zawierają informacje identyfikujące.

[19] Zgodnie z art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act) informacje o konsumentach oznaczają informacje odnoszące się do określonych grup lub kategorii konsumentów, z których usunięto tożsamość indywidualnych konsumentów, które nie są powiązane ani nie można ich w racjonalny sposób połączyć z żadnym konsumentem lub gospodarstwem domowym, w tym za pośrednictwem urządzeń zdalnych. Zagregowane informacje o konsumentach nie odnoszą się do indywidualnych rekordów konsumentów zidentyfikowanych.

[20] Ustawa wskazuje tu na pojęcie zbierania; na płaszczyźnie prawa polskiego występuje raczej pojęcie gromadzenia, i według art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act) pojęcie to oznacza kupowanie, wypożyczanie, gromadzenie, uzyskiwanie, otrzymywanie lub uzyskiwanie dostępu do jakichkolwiek danych osobowych dotyczących konsumenta w jakikolwiek sposób. Obejmuje to czynne lub bierne otrzymywanie informacji od konsumenta lub uzyskiwanie ich poprzez obserwację zachowania konsumenta.

[21] Według art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act) przetwarzanie oznacza dowolną operację lub zestaw operacji wykonywanych na danych osobowych lub na zbiorach danych osobowych, w sposób zautomatyzowany lub nie.

[22] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 (dostęp: 13.01.2023 r.), CHAPTER 735, An act to amend Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.185, 1798.192, 1798.196, and 1798.198 of, and to add Section 1798.199 to, the Civil Code, relating to personal information, and declaring the urgency thereof, to take effect immediately.

stosowania zgody konsumenta na gromadzenie, przetwarzanie i obrót danymi osobowymi, chyba że ustawa wskazuje cele specjalne[23], co do których zgoda nie jest wymagana[24]. Ustawa nakłada na podmioty gospodarcze obowiązek poinformowania klienta będącego konsumentem o tym, że zbiera jego dane osobowe, musi także pouczyć go o prawie żądania usunięcia danych osobowych. Wszystkie te regulacje dotyczą m.in. plików *cookies* oraz wszelkiej aktywności na stronach internetowych i produktach online. Wskazane regulacje nie mają zastosowania, jeżeli prawa lub obowiązki naruszałyby niekomercyjną działalność osób i podmiotów opisanych w określonym przepisie konstytucji Kalifornii odnoszącym się do środków masowego przekazu. Ustawy nie stosuje się do danych osobowych gromadzonych, przetwarzanych, sprzedawanych lub ujawnianych zgodnie z określonym prawem federalnym dotyczącym m.in. banków, domów maklerskich, firm ubezpieczeniowych i agencji informacji kredytowej, a także wyłącza się jej stosowanie zgodnie z ustawą California Financial Infor-

[23] Głównym celem jest cel biznesowy, który według art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act) oznacza wykorzystywanie danych osobowych do celów operacyjnych firmy lub usługodawcy lub do innych celów, pod warunkiem że wykorzystanie danych osobowych jest racjonalnie konieczne i proporcjonalne do osiągnięcia celu operacyjnego, dla którego dane osobowe zostały zebrane lub przetworzone, lub w innym celu operacyjnym zgodnym z kontekstem, w którym zebrano dane osobowe. Cele biznesowe to: audyty związane z bieżącą interakcją z konsumentem i równoległymi transakcjami, w tym między innymi zliczanie wyświetleń reklam użytkownikom, weryfikacja pozycjonowania i jakości wyświetleń reklam oraz audyt zgodności z niniejszą specyfikacją i innymi standardami, wykrywanie incydentów w zakresie bezpieczeństwa, ochrona przed złośliwą, oszukańczą lub nielegalną działalnością oraz ściganie osób odpowiedzialnych za tę działalność, monitorowanie w celu identyfikacji i naprawy błędów, które osłabiają istniejącą funkcjonalność, krótkotrwałe, przejściowe użycie, pod warunkiem że dane osobowe nie są ujawniane innej stronie i nie są wykorzystywane do budowania profilu konsumenta ani w inny sposób zmieniania danych indywidualnego konsumenta poza bieżącą interakcją, w tym między innymi do dostosowywania kontekstowego reklam wyświetlanych w ramach tej samej interakcji, wykonywanie usług w imieniu firmy lub usługodawcy, w tym utrzymywanie lub obsługa rachunków, obsługa klienta, przetwarzanie lub realizacja zamówień i transakcji, weryfikacja informacji o klientach, przetwarzanie płatności, zapewnianie finansowania, świadczenie usług reklamowych lub marketingowych, świadczenie usług analitycznych lub świadczenie podobnych usług w imieniu firmy lub usługodawcy, prowadzenie wewnętrznych badań w zakresie technologii i rozwoju oprogramowania, podejmowanie działań w celu weryfikacji lub utrzymania jakości lub bezpieczeństwa usługi lub urządzenia, które są własnością danego podmiotu, są przez nią produkowane lub kontrolowane, oraz w celu ulepszania usługi lub urządzenia, które są własnością danego podmiotu, są wytwarzane wyprodukowane dla danego podmiotu lub przez niego kontrolowane. Od celów biznesowych należy odróżnić cele komercyjne, którymi są: wspieranie interesów handlowych lub ekonomicznych danej osoby, na przykład nakłanianie innej osoby do kupowania, wynajmowania, dzierżawy, przyłączania się, subskrybowania, dostarczania lub wymiany produktów, towarów, majątku, informacji lub usług, lub umożliwienie lub wykonanie, bezpośrednio lub pośrednio, transakcji handlowej. Termin ten nie obejmuje przemówień, które sądy stanowe lub federalne uznały za przemówienia niekomercyjne, w tym przemówień politycznych i dziennikarskich.

[24] Preambuła do California Consumer Privacy Act of 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 (dostęp: 13.01.2023 r.).

mation Privacy Act[25]. Co do zasady danymi osobowymi w rozumieniu ustawy są informacje, które identyfikują, dotyczą, opisują, mogą być bezpośrednio lub pośrednio powiązane z określonym konsumentem lub gospodarstwem domowym. Dane osobowe obejmują między innymi następujące informacje: identyfikatory, takie jak prawdziwe imię i nazwisko, adres pocztowy, niepowtarzalny identyfikator osobisty, identyfikator internetowy, adres protokołu internetowego, adres e-mail, nazwa konta, numer ubezpieczenia społecznego, numer prawa jazdy, numer paszportu lub inne podobne identyfikatory, informacje handlowe, w tym zapisy dotyczące mienia osobistego, produktów lub usług zakupionych, uzyskanych lub rozważanych, lub inne historie aktywności lub tendencje dotyczące zakupów lub konsumpcji, informacje biometryczne, informacje o aktywności w Internecie lub innych sieciach elektronicznych, w tym między innymi historię przeglądania, historię wyszukiwania oraz informacje dotyczące interakcji konsumenta z witryną internetową, aplikacją lub reklamą, dane geolokalizacyjne, informacje dźwiękowe, elektroniczne, wizualne, termiczne, węchowe lub podobne, informacje zawodowe lub związane z zatrudnieniem, informacje edukacyjne, zdefiniowane jako informacje, które nie są publicznie dostępne, dane osobowe, zgodnie z definicją zawartą w ustawie o rodzinnych prawach do edukacji i prywatności (20 U.S.C. sekcja 1232g, 34 C.F.R. część 99), przetworzone dane z wszelkich informacji zidentyfikowanych wyżej w celu stworzenia profilu konsumenta odzwierciedlającego jego preferencje, cechy, trendy psychologiczne, predyspozycje, zachowanie, postawy, inteligencję i zdolności. Dane osobowe nie obejmują publicznie dostępnych informacji[26]. W tym zakresie pojęcie „publicznie dostępne" oznacza informacje,

[25] Preambuła do California Consumer Privacy Act of 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 (dostęp: 13.01.2023 r.). Wyłączenie dotyczy informacji kredytowej oraz danych osobowych, którymi dysponują banki i inne podmioty nadzorowane w zakresie usług bankowych. Regulacje wyłączające stosowanie owych przepisów znajdują się także w prawodawstwie Kalifornii w regulacjach dotyczących opieki zdrowotnej, bezpieczeństwa kierowców oraz danych z badań klinicznych. Ustawa daje prawo wniesienia powództwa o ochronę swoich danych osobowych oraz możliwość nałożenia grzywny na podmioty umyślnie naruszające wprowadzone regulacje.

[26] W myśl art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act) podmiot prowadzący działalność gospodarczą nie dokonuje obrotu danymi osobowymi, gdy: są one opatrzone tylko identyfikatorem probabilistycznym, tj. oznaczeniem identyfikacji konsumenta tylko poprzez prawdopodobny schemat jego działania w oparciu o jakiekolwiek kategorie danych osobowych zawartych w kategoriach wymienionych w definicji danych osobowych lub podobne do nich, pseudonimizacją, czyli są przetwarzane w sposób, który powoduje, że nie można ich już przypisać konkretnemu konsumentowi bez użycia dodatkowych informacji, pod warunkiem że dodatkowe informacje są przechowywane osobno i podlegają środkom technicznym i organizacyjnym zapewniającym, że dane osobowe nie zostaną przypisane zidentyfikowanemu lub możliwemu do zidentyfikowania konsumentowi lub są przeznaczone do prowadzenia badań rozumianych jako naukowe, statystyczne i opierające się m.in. na danych podstawowych lub kwalifikowanych, których przetwarzanie leży w interesie publicznym i są zgodne ze wszystkimi innymi obowiązującymi przepisami oraz są zgodne z zasadami etyki i z poszanowaniem prywatności lub celem badań prowadzonych w interesie

które są zgodnie z prawem udostępniane z rejestrów federalnych, stanowych lub lokalnych władz, jeśli istnieją warunki umożliwiające udostępnienie takich informacji. Pojęcie „publicznie dostępne" nie oznacza w tej sytuacji informacji biometrycznych konsumenta zebranych przez jakikolwiek podmiot bez jego wiedzy. Informacje nie są publicznie dostępne, jeśli dane te są wykorzystywane do celu, który nie jest zgodny z celem, w którym dane są przechowywane i udostępniane w rejestrach rządowych lub w którym są publicznie przechowywane. Pojęcie „publicznie dostępne" nie obejmuje również informacji o konsumentach, które są niezidentyfikowane lub zagregowane[27].

Na zasadach ogólnych znanych z regulacji polskich i europejskich według kalifornijskiej ustawy przedsiębiorstwo, które zbiera dane osobowe konsumenta, ujawnia mu kategorie i określone dane osobowe podlegające zebraniu. Przedsiębiorstwo, które otrzyma od konsumenta żądanie zweryfikowania dostępu do danych osobowych, niezwłocznie podejmie kroki w celu ich ujawnienia i nieodpłatnego dostarczenia konsumentowi[28]. Weryfikacja określana jest tu jako możliwość żądania danych, które zostały przez przedsiębiorstwo; ujawnione, zebrane, sprzedane, ujawnione do sprzedaży (jeśli ta nie została sfinalizowana)[29]. Do obecnie obowiązującego stanu prawnego dodana została instytucja prawa do rezygnacji czy też żądanie rezygnacji, którą dysponuje konsument w kwestiach sprzedaży (zbiorczych)[30] danych osobowych uregulowanych ustawą[31]. Prawo to zasadza się na zakazie wydanym przez konsumenta sprzedaży jego danych osobowych, w których posiadaniu jest dany przedsiębiorca[32]. Przedsiębiorca ma także całkowity zakaz dyskryminacji konsumenta z uwagi na skorzystanie przez niego z prawa do rezygnacji z obrotu jego danymi osobowymi zarówno

publicznym w dziedzinie zdrowia publicznego. Badania mogą polegać na analizie danych osobowych, które mogły zostać zebrane od konsumenta w trakcie interakcji konsumenta z usługą firmy lub jakimkolwiek jej urządzeniem.

27 Art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

28 Art. 1798.100 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

29 Art. 1798.115 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

30 Według art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act) pojęcie „zbiorcze informacje dla konsumentów" oznacza odnoszące się do grupy lub kategorii konsumentów informacje, z których usunięto tożsamość indywidualną, które nie są ze sobą powiązane ani nie można ich w racjonalny sposób połączyć z żadnym konsumentem lub gospodarstwem domowym.

31 Art. 1798.120 Kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

32 Art. 1798.120a kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act). Tu wskazać wypada, że niezależnie od omawianej regulacji przedsiębiorcę obejmuje zakaz sprzedaży danych osobowych konsumentów, co do których ma wiedzę, że konsument nie ukończył 16 lat, chyba że zgodę na te czynności wyraził rodzic lub opiekun takiego podmiotu.

w zakresie oferty, sprzedaży, rabatów, poziomu obsługi i dostawy towarów[33]. Przedsiębiorca prowadzący obrót danymi osobowymi może dokonywać na rzecz konsumentów zachęt stanowiących rekompensatę za czynności podejmowane w zakresie obrotu danymi dotyczące cen, stawek i jakości usług[34]. Zachęty mogą mieć miejsce po uprzednim poinformowaniu konsumenta[35] oraz po wyrażeniu przez niego zgody na tego typu czynności[36]. W zakresie realizacji prawa do rezygnacji przedsiębiorca musi: udostępnić konsumentom dwie lub więcej wyznaczonych metod składania wniosków o udzielenie informacji, w tym co najmniej bezpłatny numer telefonu, oraz umieścić informacje na swojej stronie internetowej[37], nieodpłatnie ujawniać i dostarczać konsumentowi wymagane informacje w ciągu 45 dni. Termin dostarczenia wymaganych informacji może zostać jednorazowo przedłużony o dodatkowe 45 dni, jeżeli jest to uzasadnione, pod warunkiem że konsument zostanie powiadomiony o przedłużeniu tego terminu w ciągu pierwszych 45 dni. Ujawnienie danych obejmuje 12-miesięczny okres poprzedzający wniosek konsumenta. Informacja zawiera zakres podmiotowy, tj. komu owe dane zostały sprzedane, oraz zakres przedmiotowy, czyli co było przedmiotem sprzedaży, oraz okres, tj. datę transakcji[38]. Konsument może zakazać podmiotowi posiadającemu jego dane osobowe ich celowego udostępnienia, przetworzenia na rzecz osoby trzeciej, pod warunkiem że osoba trzecia nie sprzedaje zawodowo danych osobowych. Zakaz ten może mieć miejsce, gdy konsument zamierza wchodzić w interakcję ze stroną trzecią za pośrednictwem jednej lub kilku transakcji. Przedsiębiorca ma obowiązek poinformować podmioty wykorzystujące lub udostępniające dane konsumenta, że konsument zrezygnował ze sprzedaży danych osobowych[39].

Co do wtórnego obrotu danymi osobowymi, należy zauważyć, że przedsiębiorca może przekazać osobie trzeciej dane osobowe konsumenta jako składnik aktywów, które są częścią fuzji, przejęcia, upadłości lub innej transakcji, w której osoba trzecia przejmuje kontrolę nad całością lub częścią przedsiębiorstwa, pod warunkiem że dane te są wykorzystywane lub udostępniane zgodnie z art. 1798.110 CCPA i art. 1798.115 CCPA. Jeżeli osoba trzecia w istotny sposób

[33] Art. 1798.125 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

[34] Art. 1798.125b kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

[35] Art. 1798.125b kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

[36] Art. 1798.125b kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

[37] Według art. 1798.135 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act) przedsiębiorca musi na stronie internetowej umieścić wyraźny, intuicyjny link z hasłem „nie sprzedawaj moich danych".

[38] Art. 1798.130 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

[39] Art. 1798.140 kodeksu cywilnego Kalifornii dodanego przez § 3 CCPA (California Consumer Privacy Act).

zmienia sposób, w jaki wykorzystuje lub udostępnia dane osobowe konsumenta, który jest istotnie niezgodny z wcześniej złożonymi deklaracjami w momencie ich zbierania, uprzedza konsumenta o nowej lub zmienionej praktyce. Powiadomienie powinno być wystarczająco dostateczne, tak by nie było wątpliwości co do skuteczności tego zawiadomienia, aby zapewnić obecnym konsumentom możliwość łatwego dokonywania wyborów zgodnie z art. 1798.120 CCPA. Regulacje nie dają prawa przedsiębiorcom do dokonywania istotnych zmian w polityce prywatności z mocą wsteczną ani do wprowadzania innych zmian w polityce prywatności w sposób, który naruszałby ustawę.

III

Wskazać jednak wypada, że całokształt regulacji tu opisanych jest w dużej mierze i w dużym uproszczeniu niczym innym jak tylko rozwiązaniem podobnym do np. polskich, a co za tym idzie europejskich regulacji w zakresie ochrony danych osobowych przywołanych na wstępie niniejszego opracowania. Jednak nie to jest przecież przedmiotem pojęcia *surveillance capitalism.* Zasadniczą dyferencjacją pomiędzy omawianym pojęciem tzw. kapitalizmu inwigilacji a regulacjami amerykańskimi jest, co oczywiste, adresat, tj. podmiot dotknięty działaniem obu zjawisk. W pierwszej sferze może to być każdy, w drugiej konsument. Wyjaśnianie, kiedy i kto oraz pod jakimi warunkami staje się konsumentem, przekracza ramy niniejszego opracowania i jest zbędne na tym poziomie przynajmniej na gruncie prawa polskiego, jednak nie sposób zauważyć, że krąg podmiotów mogących być w polu zainteresowania czynności z zakresu kapitalizmu inwigilacji jest daleko szerszy niż tylko zbiór konsumentów.

Zatem zakres ewentualnego oddziaływania zjawiska kapitalizmu inwigilacji nosi znamiona powszechności. Toteż zjawisko to tym bardziej powinno być przedmiotem zainteresowania państwowych regulatorów w państwach demokratycznych stojących m.in. na straży praw człowieka, prawa do prywatności *etc*. Całkowita inwigilacja nakierowana w pierwszej kolejności na rozpoznanie konsumenta, ale w gruncie rzeczy niosąca za sobą wiele ryzyk związanych z prywatnością i bezpieczeństwem, nie może pozostać indyferenta normatywnie. Oczywiście w pierwszej kolejności narzuca się tu pytanie, czy w ogóle można gromadzić, a jeśli tak, to w jakich celach, pod jakimi precyzyjnie określonymi przesłankami, dane dotyczące właściwie każdego przejawu ludzkiej egzystencji. Jeśli odpowiedź ma tu być negatywna, to w zasadzie rolą prawa jest budowa zakazów na tyle szczelnych, tj. takich, które nie mogą być w procesie stosowania prawa przedmiotem np. działań *contra legem*, by działalność taką uniemożliwić. Natomiast jeśli odpowiedź miałaby być pozytywna, to powinna – jak się wydaje – być obwarowana określonymi warunkami nie tylko podmiotowymi i przedmiotowymi, ale przede wszystkim zawierającymi konglomerat przepisów teleologicznych.

Co za tym idzie – w myśl regulacji prawnych już obowiązujących w większości państw i organizmów ponadpaństwowych – powinny powstać instytucje nadzorcze albo też w już istniejących powinna powstawać aparatura służąca wykonaniu tego typu regulacji. Powinna zostać także uregulowana droga sądowej kontroli decyzji zapadłych w toku realizacji praw i obowiązków poszczególnych podmiotów, jak też umożliwiająca realizację praw i obowiązków z zakresu prawa cywilnego mogących wystąpić sporów przy realizacji określonych regulacji wynikających z nowego stanu prawnego porządkującego i regulującego przedmiotowy stan faktyczny. Oczywista jest także konieczność odpowiedzenia na pytanie, czy w ogóle takie regulacje mogłyby mieścić się w polskim, a przede wszystkim europejskim porządku prawnym, z uwzględnieniem ich zhierarchizowanej struktury. Wszystkie te zagadnienia nie mogą być analizowane bez namysłu o charakterze międzynarodowym, tj. bez dokonania analizy regulacji wiodących w zakresie ochrony danych osobowych państw demokratycznych, których dorobek legislacyjny, naukowy i intelektualny świadczy o wysokim pozycjonowaniu owej problematyki w systemach prawa, skoro już dziś wiadomo, że niektóre kraje milcząco lub przez celowe działania dozwalają na tego typu działalność. Analiza porównawcza mogłaby stać się zaczynem do rozwiązań transeuropejskich oraz światowych. Brak bowiem regulacji o charakterze międzynarodowym doprowadzi do swoistego arbitrażu prawnego polegającego na korzystaniu przez zainteresowane podmioty z systemów prawa państw o dogodniejszym niż inne regulacjach prawnych w przedmiotowym zakresie.

ABSTRACT

dr Tomasz A. Zienowicz

The author is a doctor of laws, an advocate (District Bar Association in Gdansk).

Surveillance capitalism – reflections from the perspective of legal theory

The article covers issues related to trade in personal data, data protection or security against undesirable interception and indicates American solutions in the field of rights and duties of participants of the personal data market.

Keywords: *surveillance, capitalism, legal protection of consumers, personal data protection, US law regulations, data trade security*

dr Tomasz A. Zienowicz
ORCID: 0000-0003-1920-9608; e-mail: kancelaria@zienowicz.com

Autor jest doktorem nauk prawnych, adwokatem (Izba Adwokacka w Gdańsku).

BIBLIOGRAFIA ZAŁĄCZNIKOWA

Zuboff Shoshana, *The Age of surveillance capitalism – The Fight for a human future at the new frontier of power*, Profile Books Ltd. 2018