Ochrona danych osobowych w Internecie rzeczy w prawie UE

Fragment

Rozdział I. Zachowania użytkowników nowych technologii w odniesieniu do ochrony ich danych osobowych

§ 1. Uwagi ogólne

Problematyka ochrony danych osobowych jest wszechobecna w branży usług cyfrowych i handlu elektronicznego, o czym przekonał się chyba każdy użytkownik nowych technologii. Odzwierciedleniem związanych z nią kontrowersji jest fakt, że w ostatnich latach dyskusja dotycząca ochrony prywatności i danych osobowych w sieci wykroczyła poza ramy debaty akademickiej i stała się przedmiotem codziennych rozważań w niemal wszystkich mediach masowych (telewizja, radio, prasa), na portalach społecznościowych, a także w codziennych rozmowach, żartach i memach internetowych[1]. Dotyczy jej również szereg filmów i seriali, zarówno dokumentalnych (np. „Social Dilemma" z 2020 r. czy rok starszy „The Great Hack"), jak i fabularnych (np. „Black Mirror", „Snowden", „Citizenfour").

Po wejściu w życie RODO prawdopodobnie każdy aktywny użytkownik nowych technologii otrzymał niezliczoną liczbę polityk prywatności, klauzul informacyjnych lub innych podobnych dokumentów dotyczących zasad przetwarzania jego danych osobowych. Dokumenty takie pojawiały się w bardzo zróżnicowanym kontekście, najczęściej w związku z określoną aktywnością użytkownika (np. uruchomienie nowego urządzenia, aktywacja dodatkowych funkcji), ale wiadomości takie były również wysyłane przez usługodawców, z których usług dany użytkownik korzystał już od dłuższego czasu. Niejednokrotnie usługodawcy wymagają w takim przypadku od użytkownika podjęcia określonych decyzji (wyrażenie zgody na przetwarzanie danych osobowych, przekazanie swoich danych kontaktowych, założenie profilu użytkow-

[1] O znaczeniu memów internetowych we współczesnym społeczeństwie zob. m.in. *M. Juza*, Memy internetowe, s. 49–60.

nika itd.), które mają istotny wpływ na jego prywatność. Dzięki rozwojowi Internetu rzeczy skutki podejmowanych decyzji coraz rzadziej ograniczają się do aktywności użytkownika w sieci (przeglądanie stron internetowych, korzystanie z poczty elektronicznej), a coraz częściej dotyczą tej aktywności również w realnym świecie (lokalizacja, aktywność fizyczna, interakcje społeczne). Zbieranie danych przybiera bowiem w Internecie rzeczy bardzo zróżnicowane formy i może odbywać się nawet wówczas, gdy dana osoba fizyczna nie jest – lub nie jest świadoma, że jest – połączona z Internetem (np. przy użyciu sieci czujników w galerii handlowej albo urządzeń przenośnych przesyłających usługodawcy zebrane informacje po przywróceniu łączności).

Liczba decyzji wymaganych od użytkownika, a także realna trudność związana z nimi (np. zrozumienie konsekwencji wynikających z poszczególnych wyborów), sposób prezentacji możliwych opcji (np. wybór pomiędzy koniecznością personalizacji ustawień a wyborem ustawień rekomendowanych) oraz zróżnicowane sposoby zbierania danych osobowych w trakcie korzystania z usług i urządzeń wykorzystujących technologie Internetu rzeczy stanowią duże wyzwanie dla każdego użytkownika. Naturalnie nasuwa się zatem wątpliwość, czy taki system ochrony prywatności rzeczywiście umożliwia użytkownikowi podejmowanie decyzji, które w pełni oddają jego preferencje w zakresie ochrony danych osobowych i prywatności.

§ 2. Zagrożenia prawa do ochrony danych osobowych w Internecie rzeczy

Jednym z najpoważniejszych wyzwań związanych z ochroną prywatności użytkownika Internetu rzeczy jest praktyczna trudność w sprawowaniu kontroli nad swoimi danymi. Powstaje zatem ryzyko wykorzystania tych danych osobowych bez pełnej wiedzy lub wbrew woli tego użytkownika. Reforma przepisów o ochronie danych osobowych, której koronnym rezultatem było przyjęcie ogólnego rozporządzenia o ochronie danych z 2016 r. (RODO), w praktyce jako jeden z głównych celów przyjęła zagwarantowanie wyższej kontroli nad swoimi danymi. Takie podejście w istocie wyraża dążenie prawodawcy do oparcia przepisów o ochronie danych osobowych na koncepcji autonomii informacyjnej. Zakłada ona, że osoba fizyczna powinna mieć zagwarantowaną możliwość decydowania, komu i jakie informacje o samej sobie przekazuje (koncepcja ta zostanie szerzej omówiona w dalszej części pracy).

Choć system ochrony danych osobowych w bardzo wyraźny sposób podkreśla uprawnienia decyzyjne i kontrolne osoby fizycznej, w piśmiennictwie wielokrotnie akcentowano, że nowe technologie (w tym Internet rzeczy) znacznie utrudniają korzystanie z tych uprawnień przez użytkownika.

L. Moerel i *C. Prins* zauważają, że całe środowisko wokół człowieka generuje znaczne ilości informacji, a ich przetwarzanie odbywa się automatycznie i w czasie rzeczywistym. Dzięki temu decyzje mogą być podejmowane w zasadzie niezwłocznie po zebraniu danych, pozwalając na optymalizację procesów, które od przetwarzania danych są uzależnione[2], ale dysponowanie znacznie dokładniejszymi informacjami o użytkownikach może jednocześnie m.in. otwierać drogę do „ukrytego" wpływania na zachowania konsumentów (np. poprzez wykorzystanie podatności użytkownika na określoną formę marketingu), dyskryminacji cenowej czy wręcz blokowania dostępności produktu lub usługi dla pewnej kategorii osób[3]. Podobne obawy wyrażają również inni autorzy. *M.-H. Maras* zauważa, że „urządzenia w Internecie rzeczy tworzą środowisko, w którym informacje o każdej osobie mogą być przechowywane, analizowane, monitorowane, udostępniane i dzielone z innymi urządzeniami w ramach sieci, a potencjalnie także z innymi użytkownikami", a w efekcie pozwala to na ustalenie bardzo szczegółowych informacji z życia prywatnego użytkowników[4]. Z kolei *R.H. Weber* podkreśla, że znakowanie urządzeń i innych przedmiotów, niezbędne do funkcjonowania technologii Internetu rzeczy, może prowadzić do pozostawiania przez te osoby śladów, a to z kolei może ułatwiać śledzenie tych osób, nawet bez ich wiedzy[5]. *M.-H. Maras* dostrzega natomiast zagrożenie w ograniczonych możliwościach kontroli użytkowników nad swoimi danymi, zwłaszcza jeżeli zostaną one wykorzystane bez wiedzy lub wbrew woli osoby, której dane dotyczą[6].

W piśmiennictwie polskim *W. Wiewiórowski* podkreśla wiele zagrożeń dla prywatności, takich jak m.in. zdalne gromadzenie danych ujawniających wzorce zachowań użytkowników, wykorzystanie danych w innych celach niż te, do których je zebrano, utrata kontroli nad swoimi danymi, profilowanie użytkowników na podstawie pozornie anonimowych danych, a także liczne trudności w procesie wyrażenia zgody (m.in. w zakresie identyfikacji,

[2] *L. Moerel*, *C. Prins*, Privacy for the Homo Digitalis, s. 13–15, 21–22.
[3] *Ibidem*, s. 24–25.
[4] *M.-H. Maras*, Internet of Things, s. 102, tł. własne.
[5] *R.H. Weber*, Internet of Things – New security, s. 24.
[6] *M.-H. Maras*, Internet of Things, s. 103.

komu w ogóle zgoda jest udzielana)[7]. *M. Sakowska-Baryła*, analizując zjawisko tzw. *smart cities*, zauważa, że klasyczne instytucje nie są już wystarczające dla rozwoju technologii i dla nasycenia tkanki miejskiej „inteligentną infrastrukturą", zwłaszcza gdy przetwarzanie danych dokonuje się bez świadomego udziału osoby, której te dane dotyczą (co może grozić m.in. automatycznym podejmowaniem decyzji dotyczących danej osoby, bez jej udziału)[8]. Z kolei *M. Czerniawski* wskazuje na dalsze zagrożenia związane z rozwojem omawianych technologii, takie jak m.in. obawy o wykorzystanie technologii RFID do indywidualizacji cen w zależności od historii zakupów danego użytkownika[9].

Kontrola nad swoimi danymi w przestrzeni nasyconej technologiami Internetu rzeczy staje się zatem coraz trudniejsza, a często wręcz niemożliwa, gdy jednocześnie informacje o danej osobie są zbierane przez kilka, a czasem kilkadziesiąt urządzeń, które udostępniają te informacje całej grupie podmiotów świadczących jednocześnie usługi na rzecz danego użytkownika, a każdy z nich stosuje odmienne, złożone polityki prywatności. Tym bardziej, że przeprowadzone w ramach Global Privacy Enforcement Network (GPEN)[10] badanie Privacy Sweep 2016 obejmujące ponad 300 urządzeń korzystających z technologii Internetu rzeczy wykazało, że statystycznie 6 na 10 urządzeń nie spełnia wymogów stawianych przez przepisy o ochronie danych osobowych: w 59% przypadków firmy nie wykonują należycie obowiązków informacyjnych, a w 72% nie wyjaśniają, w jaki sposób można usunąć dane osobowe z urządzenia[11].

Warto również dodać, że drugą kategorię spośród najczęściej wymienianych wyzwań dla ochrony danych osobowych w warunkach Internetu rzeczy – choć w mniejszym stopniu jest to wyzwanie dla nauk prawnych, a w znacznie większym dla nauk technicznych – stanowią wyzwania związane z bezpieczeństwem danych. Warto w tym miejscu wskazać, że *J. Ziegeldorf*, *O. Morchon*

---

[7] *W. Wiewiórowski*, Ochrona danych osobowych, s. 9–10.

[8] *M. Sakowska-Baryła*, Prywatność w inteligentnym mieście, s. 134–136, 143.

[9] *M. Czerniawski*, Prawne aspekty, s. 114.

[10] Global Privacy Enforcement Network to międzynarodowa inicjatywa służąca współpracy organów ochrony prywatności, podjęta jako odpowiedź na jedną z rekomendacji OECD, szerzej: https://www.privacyenforcement.net (dostęp: 17.11.2021 r.).

[11] An Coimisinéir Cosanta Sonraí, Findings of International Privacy Sweep 2016 published, https://www.dataprotection.ie/docs/23–9-2016-International-Privacy-Sweep-2016/i/1597.htm, (dostęp: 16.12.2018 r.); wersja archiwalna strony: https://web.archive.org/web/20180722112345/https://www.dataprotection.ie/docs/23–9-2016-International-Privacy-Sweep-2016/i/1597.htm); Privacy: "Internet delle cose", utenti poco tutelati. Risultati dell'analisi internazionale per il "Privacy Sweep 2016", https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5443681 (dostęp: 17.11.2021 r.).

i *K. Wehrle* wymieniają i szczegółowo omawiają dość szeroką listę zagrożeń dla ochrony danych i prywatności użytkownika, m.in. identyfikację użytkownika w oparciu o unikatowe identyfikatory, możliwość przypadkowego ujawnienia informacji dotyczących życia prywatnego danej osoby przy okazji interakcji z urządzeniem lub innym użytkownikiem (autorzy posługują się określeniem *privacy-violating interaction and presentation*) czy tzw. „atak wynalazczy" (*inventory attack*), tj. nieupoważnione gromadzenie danych przez twórcę urządzenia[12]. Mimo że zagrożenia te mają często genezę w technicznej warstwie funkcjonowania usługi lub produktu, niektóre (np. wspomniane interakcje skutkujące ujawnieniem zbyt wielu danych innej osobie) mogą również wynikać z czynników związanych ze sprawowaniem kontroli nad swoimi danymi, np. niewłaściwych ustawień urządzenia lub niezrozumienia zasad przetwarzania danych przez usługodawcę.

Mimo że poleganie na mechanizmach kontroli indywidualnej przetwarzania danych (w szczególności na rozbudowanych obowiązkach informacyjnych administratora danych oraz uprawnieniach osoby, której dane dotyczą) stanowi jedną z podstaw unijnego systemu ochrony danych osobowych, podejście takie budzi wątpliwości. Dla jego skuteczności niezbędne byłoby, aby użytkownicy nowych technologii rzeczywiście korzystali z otrzymywanych informacji, tj. zapoznawali się z nimi oraz podejmowali działania w celu sprawowania kontroli nad swoimi danymi osobowymi. Tymczasem dotychczas prowadzone badania, z których część zostanie przytoczona poniżej, dają podstawy do wyciągnięcia odmiennego wniosku. Wynika z nich, że osoby zapoznające się z politykami prywatności i klauzulami informacyjnymi oraz świadomie korzystające ze swoich praw w zakresie ochrony danych osobowych stanowią mniejszość wśród użytkowników Internetu.

Choć nadal dominujące wydaje się przekonanie o konieczności wzmocnienia instrumentów kontroli indywidualnej, w piśmiennictwie coraz częściej można spotkać się z kwestionowaniem np. rozbudowywania dokumentacji usługi (umów, regulaminów, polityk prywatności, pouczeń czy innych klauzul informacyjnych) i konieczności pobierania szeregu zróżnicowanych oświadczeń. Duży zakres udzielanych informacji nie zawsze jest dla użytkownika Internetu korzystny. Biorąc pod uwagę, że jednostka z reguły nie dysponuje nieograniczoną zdolnością przyswajania otrzymywanych informacji oraz ma ograniczone możliwości poznawcze, podejście takie może prowadzić do zja-

[12] *J.H. Ziegeldorf, O.G. Morchon, K. Wehrle*, Privacy in the Internet, s. 2733–2738.

wiska przeciążenia informacyjnego, a to utrudnia jej skuteczną realizację swoich praw.

Kwestionowanie skuteczności klasycznych instrumentów ochrony danych osobowych można dostrzec zarówno w piśmiennictwie europejskim, jak i w literaturze amerykańskiej, gdzie podnoszone są bardzo zbliżone zastrzeżenia do amerykańskiego modelu ochrony prywatności konsumenta w Internecie w oparciu o konstrukcję *notice and consent*. W szczególności podkreśla się ryzyko przeciążenia użytkownika informacjami oraz braku praktycznej możliwości podejmowania przez niego swobodnej decyzji w każdym przypadku, gdy jest to wymagane przepisami prawa.

Wątpliwości te pozostają szczególnie zasadne w odniesieniu do Internetu rzeczy – zjawisko powszechnego przetwarzania (*ubiquitous computing*) wiąże się bowiem ze zbieraniem danych osobowych w zasadzie w każdej chwili funkcjonowania jednostki poprzez stałe śledzenie jej aktywności. W takich okolicznościach zrozumienie wszystkich „cykli życia" oraz zasad wykorzystania danych osobowych może być skomplikowane i może wymagać od użytkownika znacznego nakładu czasu oraz wysiłku, nawet jeżeli zostanie mu zapewniony łatwy dostęp do tych informacji.

Do zbierania danych osobowych z wykorzystaniem technologii Internetu rzeczy dochodzi bowiem nie tylko podczas świadomego korzystania z komputera (który przed powstaniem Internetu rzeczy był właściwie jedynym, a na pewno głównym kanałem dostępu użytkowników do Internetu), ale w praktyce nieprzerwanie w trakcie codziennej aktywności użytkownika, a często także w nocy (np. coraz popularniejsze opaski monitorujące sen). Dane osobowe coraz rzadziej są przy tym zbierane przez jedno urządzenie (komputer), a coraz częściej jest ich kilka lub kilkanaście (urządzenia przenośne, urządzenia typu *wearable*, sprzęty gospodarstwa domowego, środki komunikacji, nowoczesne instrumenty płatnicze itp.). Doszło wręcz do doktrynalnego wydzielenia kategorii danych osobowych „obserwowanych", czyli danych, które są zbierane przez administratora bezpośrednio z aktywności użytkownika lub sposobu wykonywania umowy – często bez aktywnej świadomości, że osoba fizyczna pozostaje „pod obserwacją" [13].

Wiele urządzeń zbiera dane osobowe w celu korzystania z większej liczby usług. Szczególne znaczenie mają wielofunkcyjne urządzenia przenośne takie jak smartfony, opaski sportowe czy zegarki, które pozwalają gromadzić szcze-

[13] Grupa Robocza Art. 29, Guidelines on the right to data portability (WP 242 rev. 01), 16/EN, 2017, s. 10.

gółowe dane osobowe dla kilku, a nawet kilkudziesięciu wydawców aplikacji jednocześnie, z których każdy przetwarza je w inny sposób, w innych celach oraz w innym zakresie. Dla pełnego obrazu sytuacji należy podkreślić również coraz większe poleganie przez użytkowników na tych urządzeniach w życiu codziennym, czego najbardziej charakterystycznym przykładem może być ikoniczny w kulturze popularnej obraz samochodu zatopionego w jeziorze przez kierowcę bezrefleksyjnie opierającego się na instrukcjach udzielanych przez usługi nawigacji samochodowej.

W zagranicznym piśmiennictwie często przywoływane jest zjawisko określane jako „paradoks prywatności" (*privacy paradox*), które najkrócej można opisać jako zjawisko polegające na tym, że obawy związane z prywatnością pozostają bez związku z zachowaniem jednostki[14]. Innymi słowy, możliwa do zaobserwowania jest rozbieżność pomiędzy deklarowanym a rzeczywistym zachowaniem konkretnej osoby, polegająca na tym, że deklaruje ona znaczne zainteresowanie kwestiami związanymi z ochroną jej prywatności (*privacy concern*), ale w praktyce nie wpływa to na podejmowanie określonych kroków (np. na niższą skłonność do podawania swoich danych osobowych w Internecie czy stosowanie technologii służących ochronie prywatności).

D. Solove zauważa, że możliwość skutecznego korzystania z przyznanych jednostce uprawnień w zakresie zarządzania swoją prywatnością w Internecie jest ograniczona, a przyczyn takiego stanu jest przynajmniej kilka. Wśród największych przeszkód dla skuteczności podejścia opartego na autonomii jednostki wymienia on następujące czynniki:

1) użytkownik Internetu zwykle nie czyta polityk prywatności;
2) jeżeli użytkownik Internetu czyta polityki prywatności, często ich nie rozumie;
3) jeżeli nawet użytkownik Internetu przeczyta i zrozumie politykę prywatności, często nie otrzymuje wystarczających informacji do podjęcia świadomej decyzji w zakresie ochrony swojej prywatności (*informed choice*);
4) nawet jeżeli spełnione są wszystkie powyższe warunki (tj. użytkownik Internetu przeczyta i zrozumie politykę prywatności oraz otrzyma wystarczające informacje), jego wybór może zostać wypaczony przez szereg czynników na etapie procesu decyzyjnego[15].

---

[14] Taką definicję proponują *T. Dienlin* oraz *S. Trepte*, przy czym warto podkreślić, że autorzy jednocześnie polemizują z „paradoksalnym" charakterem zjawiska; szerzej: *T. Dienlin*, *S. Trepte*, Is the privacy paradox, s. 294–295. Zob. też *S. Barth*, *M.D.T. de Jong*, The privacy paradox, s. 1039 i przytoczona tam literatura.

[15] *D. Solove*, Privacy Self-Management, s. 1888–1893.

Problemy związane z ograniczonymi zdolnościami poznawczymi podkreśla także *R. Calo*, zauważając zróżnicowanie umiejętności przyswojenia otrzymywanych informacji wśród populacji. Wskazuje on jednak również, że niezależnie od tego zróżnicowania istnieją problemy wspólne dla wszystkich jednostek, m.in. brak nieograniczonej zdolności do skupienia uwagi. W przypadku, w którym dojdzie do „przeciążenia" danej osoby informacjami (*information overload*), naturalną reakcją jest zapoznanie się z nimi w sposób pobieżny lub wybiórczy[16].

Z kolei *H. Nissenbaum* zauważa, że ochrona prywatności na zasadzie *notice and consent* jest zbliżona do paradygmatu konkurencyjnego, wolnego rynku, w którym transakcje pomiędzy uczestnikami rynku (a w tym wypadku decyzje odnośnie przekazania lub nieprzekazywania swoich danych) są dokonywane po cenach ukształtowanych przez mechanizmy rynkowe – jeżeli zawodzą mechanizmy w zakresie przejrzystości i informacji, działania podejmowane przez poszczególnych uczestników często są wypaczone[17].

Również *B. Koops*, oceniając europejskie prawo ochrony danych, wskazuje, że koncepcja autonomii informacyjnej jest w praktyce niemożliwa do wyegzekwowania. Z jednej strony przypomina on, że z uwagi na swoją wygodę i ograniczoną zdolność do podejmowania racjonalnych decyzji jednostki nie poświęcają czasu na zapoznawanie się z wszystkimi informacjami od usługodawców. Z drugiej – zwraca uwagę, że użytkownicy często nie wiedzą, w jaki sposób mogą egzekwować swoje prawa i w praktyce tylko osoby wykazujące ponadprzeciętną wiedzę będą potrafiły skutecznie korzystać z instrumentów prawnych przysługujących im na podstawie przepisów o ochronie danych osobowych[18].

E. Carolan podkreśla, że wyrażenie przez osobę fizyczną zgody na przetwarzanie jej danych osobowych nie powinno być traktowane jako w pełni świadome wyrażenie jej poglądów, ponieważ w dużej mierze ulega ona uprzedzeniom, heurystykom czy innym czynnikom wpływającym na jej bardziej lub mniej świadomie podjętą decyzję. Zwraca ona uwagę na bardzo zaawansowany rozwój technik, które mają zwiększyć skłonność użytkowników do wyrażenia zgody, m.in. poprzez odpowiednie konstruowanie stron internetowych czy właściwy dobór barw sprzyjających podniesieniu zaufania. W efekcie autorka

16 *R. Calo*, Against Notice, s. 1052 i n.
17 *H. Nissenbaum*, A Contextual Approach, s. 34.
18 *B.-J. Koops*, The Trouble, s. 251–253.

dochodzi do wniosku, że „każda reguła prawna, która traktuje zgodę jako wytwór racjonalnego procesu myślowego, jest potencjalnie dyskusyjna”[19].

Tego typu techniki szturchnięć (*nudge techniques*), czyli zachowań, które pod pozorem swobodnej decyzji użytkownika kierunkują jego wybór, są zresztą przedmiotem szerszej analizy w wytycznych brytyjskiego ICO. Z dokumentu wynika, że takie praktyki mogą wpływać na zachęcanie użytkowników, a zwłaszcza dzieci, do przekazywania swoich danych w szerszym zakresie, niż byliby skłonni tego dokonać w „normalnych” (tj. niezniekształconych) warunkach. W wytycznych zauważony zostaje jednak również potencjał umożliwiający wykorzystywanie tych samych technik w celu ukierunkowania wyborów podejmowanych przez użytkowników w przeciwnym kierunku, sprzyjając ochronie danych osobowych[20].

W świetle powyższych komentarzy w piśmiennictwie można powziąć wątpliwość, na ile instrumenty ochrony prywatności użytkownika w Internecie, oparte na zasadzie autonomii informacyjnej, której założeniem jest podjęcie świadomej i dobrowolnej decyzji, mogą mieć zastosowanie do szybko rozwijających się technologii, w szczególności technologii Internetu rzeczy. Przytoczone powyżej wątpliwości wskazują, że stałe rozbudowywanie obowiązków informacyjnych nie zawsze ułatwia podjęcie takiej swobodnej decyzji, ale wręcz może utrudniać korzystanie z prawa do informacji poprzez przeciążenie informacyjne osoby, której dane dotyczą. Nadmierny zakres udzielanych informacji sprawia, że znacznie trudniejsze jest wyselekcjonowanie tych elementów, które są w danych okolicznościach kluczowe do podjęcia określonej decyzji.

Zwłaszcza w piśmiennictwie amerykańskim na poparcie ewentualnych uwag krytycznych często przywoływane są konkretne badania empiryczne z zakresu nauk społecznych. Podejście takie jest zasadne – prawo do ochrony danych osobowych ma bowiem wyraźnie zdefiniowaną funkcję społeczną, polegającą na zapewnieniu osobie fizycznej realnej ochrony w związku z przetwarzaniem jej danych osobowych. Przy kształtowaniu i ocenie regulacji dotyczących ochrony danych osobowych kluczowa powinna być zatem analiza empirycznych skutków przyjmowanych regulacji, a nie wyłącznie ich zgodność z konstrukcjami teoretycznymi i dogmatycznymi, wykształconymi w li-

[19] Dosłownie: „any legal rule that treats consent as the product of a rational thought process is potentially open to question”, zob. *E. Carolan*, The continuing problems, s. 472–473.

[20] ICO, Age appropriate design: a code of practice for online services, 2020, https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2–1.pdf, s. 72–76.

teraturze prawniczej. W tym celu należy odnieść się do konkretnych wyników badań, zwłaszcza jeżeli mogą one podważyć skuteczność dotychczasowych instrumentów prawnych w tak istotnej dziedzinie jak ochrona praw podstawowych jednostki.

§ 3. Niechęć do zapoznawania się z zasadami ochrony danych osobowych usługodawców zawartymi w politykach prywatności

Dotychczasowe analizy wskazują, że użytkownicy Internetu niechętnie zapoznają się z przekazywanymi im informacjami dotyczącymi zasad przetwarzania ich danych osobowych. Co więcej, odsetek osób rzeczywiście zapoznających się z tymi informacjami jest z reguły niższy niż odsetek osób deklarujących czytanie polityk prywatności i klauzul informacyjnych. Badania przeprowadzone w 2001 r. przez *G. Milne'a* i *M. Culnan* wykazały, że już nawet na płaszczyźnie deklaracji składanych przez osoby uczestniczące w badaniu odsetek osób zapoznających się z informacjami dotyczącymi ochrony danych osobowych jest niewielki. Tylko 4,5% badanych zawsze czyta klauzule dotyczące prywatności (*privacy notices*), 14,1% deklaruje częste zapoznawanie się z nimi, a 31,8% czyta je wyłącznie czasami. Jednocześnie 33,3% przyznaje, że klauzule te czyta rzadko[21].

Badania te były przeprowadzone dwie dekady temu, zatem wydawałoby się, że sytuacja mogła od tego czasu ulec zmianie (np. wraz z upowszechnianiem się świadomości dotyczącej ochrony prywatności w sieci). Tymczasem nowsze badania nie potwierdzają takich przypuszczeń. Eurobarometer z 2015 r. wykazał, że tylko 18% badanych czyta polityki prywatności w całości, a 31% nie czyta ich w ogóle[22]. Wyniki te są zatem zbliżone do tych, które otrzymano w badaniach *G. Milne'a* i *M. Culnan*. Spośród osób uczestniczących w badaniu Eurobarometer ponad 2/3 (67%) twierdzi, że nie czyta polityk prywatności, ponieważ są zbyt długie, 36% uważa je za zbyt skomplikowane i trudne do

[21] *G.R. Milne*, *M.J. Culnan*, Strategies for reducing, s. 21–22.

[22] Eurobarometer, Special Eurobarometer 431: Data protection. Report, Wave EB83.1 – TNS opinion & social, 2015, https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=49628, s. 86.

zrozumienia, a 15% sądzi, że nie będą one przestrzegane. Jednocześnie 14% badanych uważa, że prawo będzie ich chronić tak czy inaczej[23].

W przeciwieństwie do wyników otrzymanych przez *G. Milne'a* i *M. Culnan* oraz sondaży w ramach Eurobarometer, które opierały się na odpowiedziach użytkowników na zadane im pytania, jedna z grup amerykańskich badaczy zestawiła deklarowane odpowiedzi z realnym zachowaniem danej osoby. Analiza otrzymanych odpowiedzi wykazała, że 23,7% osób deklarowała zamiar zapoznania się z polityką prywatności, odwiedzając daną stronę internetową pierwszy raz, przy czym 7,5% spośród osób badanych twierdziła, że zapoznaje się z polityką prywatności nawet wówczas, gdy strona nie wymaga podawania swoich danych, a aż 43% – przed dokonaniem zakupów w sklepie internetowym. Jednocześnie 19,4% badanych twierdziła, że treść polityk prywatności często (*frequently*) wywiera wpływ na ich zachowanie[24]. Następnie deklarowane odpowiedzi zestawiono z rzeczywistym zachowaniem tych osób w zainscenizowanym scenariuszu dokonywania zakupów internetowych – stronę z polityką prywatności odwiedziło jedynie 25,9% badanych, co jest wprawdzie wynikiem zbliżonym do deklaracji w zakresie stron internetowych odwiedzanych pierwszy raz przez użytkowników, ale jednocześnie odsetek ten jest znacznie niższy od rezultatu otrzymanego w badaniach opartych o deklarowane odpowiedzi osób ankietowanych w odniesieniu do scenariusza sklepu internetowego. Jednocześnie sami autorzy podkreślają, że wynik ten otrzymany został w warunkach eksperymentu i jest prawdopodobnie wyższy niż rzeczywisty odsetek tych osób w warunkach poza badaniem – osoby uczestniczące zdawały sobie bowiem sprawę, że pozostają pod obserwacją[25].

Wniosek taki wyraźnie potwierdzają inne publikacje naukowe. Badania prowadzone na osobach nieświadomych tego, że są obserwowane, wskazują, że odsetek osób zapoznających się z politykami prywatności jest znacząco niższy. Nieco zaskakujące wyniki w tym zakresie ujawnił eksperyment, podczas którego stworzono stronę internetową służącą do aplikowania o ubezpieczenie komunikacyjne. Celem eksperymentu było zbadanie wpływu treści polityki prywatności na decyzje podejmowane przez konsumentów. W ramach badania posłużono się dwiema wersjami polityki prywatności, przy czym jedna zakładała restrykcyjne zasady ochrony danych, a druga – liberalne. Stronę internetową odwiedziło 2313 osób. Spośród nich 269 złożyło wniosek i podało

[23] *Ibidem*, s. 87.
[24] *C. Jensen*, *C. Potts*, *Ch. Jensen*, Privacy Practices, s. 211.
[25] *Ibidem*, s. 215.

swoje dane osobowe, ale tylko 7 osób kliknęło hiperłącze prowadzące do polityki prywatności (przy czym nie wiadomo, ile z tych osób faktycznie zapoznało się z zamieszczonymi w niej informacjami). Eksperyment porównano ze statystykami sklepu internetowego, który w okresie sześciu miesięcy odwiedziło 178 207 osób – tylko 173 z nich kliknęło hiperłącze do polityki prywatności, znajdujące się w stopce strony internetowej. W praktyce oznacza to, że tylko 0,3% (dla przypadku nr 1) i 0,1% (dla przypadku nr 2) użytkowników strony internetowej zamierzało zapoznać się z jej polityką prywatności[26].

W innym badaniu, prowadzonym na użytkownikach Facebooka, 21% respondentów potwierdziło, że przeczytało politykę prywatności portalu, a 15% – jego regulamin. Jednocześnie aż 61% osób deklarujących znajomość polityki prywatności Facebooka nie wiedziała, że jej postanowienia zastrzegały prawo portalu do udostępnienia danych osobowych użytkowników osobom trzecim[27].

Z kolei inne badanie, prowadzone przez firmę marketingową Amazee Metrics w okresie pierwszych 30 dni stosowania RODO, wykazało, że przeważająca większość – ponad trzy czwarte (76%) spośród obserwowanych 100 000 użytkowników – w ogóle nie zareagowała na komunikat dotyczący używania *cookies* na stronach internetowych. Co dziewiąta osoba (11%) aktywnie zaakceptowała korzystanie z *cookies*, możliwość indywidualnego skonfigurowania ustawień wybrało tylko 0,5% badanych[28].

Obrazowym przykładem tego, że regulaminy i polityki prywatności mają niewielkie znaczenie dla świadomości użytkowników Internetu, jest przypadek jednego z brytyjskich przedsiębiorców. W ramach eksperymentu zdecydował się on zamieścić w regulaminie udostępnianych *hotspotów* (publicznych punktów dostępu do Internetu z wykorzystaniem sieci Wi-Fi) klauzulę, która zobowiązywała użytkowników – wg woli usługodawcy – m.in. do czyszczenia publicznych toalet na festiwalach, przytulania bezdomnych zwierząt i zdrapywania gumy do żucia z ulic, w wymiarze 1000 godzin[29]. Regulamin został za-

[26] *R.A. Malaga*, Do Web Privacy, s. 96–98.

[27] *O. Pitkänen*, *V.K. Tuunainen*, Disclosing Personal Data Socially, s. 18–19.

[28] *R. Mueller*, 76% Ignore Cookie Banners – The User Behavior After 30 Days of GDPR, https://amazeemetrics.com/en/blog/76-ignore-cookie-banners-the-user-behavior-after-30-days-of-gdpr/ (dostęp: 17.11.2021 r.).

[29] Zgodnie z informacją na stronie Purple WiFi Ltd.: „The user may be required, at Purple's discretion, to carry out 1,000 hours of community service. This may include the following: / – Cleansing local parks of animal waste / – Providing hugs to stray cats and dogs / – Manually relieving sewer blockages / – Cleaning portable lavatories at local festivals and events / – Painting snail

akceptowany przez 22 000 osób, przy czym tylko jedna zgłosiła zastrzeżenia do tej klauzuli[30].

Dużym echem odbiła się także zorganizowana przez norweską Forbrukerrådet (Radę Konsumentów) akcja społeczna w formie maratonu czytania regulaminów popularnych aplikacji, z których korzystają konsumenci. Jak wskazali organizatorzy, wybrano 33 aplikacje (średnia liczba aplikacji zainstalowanych przez użytkownika w Norwegii), których regulaminy miały łącznie objętość przekraczającą objętość biblijnego Nowego Testamentu (ok. 250 000 słów), a ich lektura zajęła ponad dobę[31].

W praktyce rezultaty te nie powinny zaskakiwać, biorąc pod uwagę koszt alternatywnego scenariusza, w którym wszyscy użytkownicy zapoznają się z udostępnianymi im politykami prywatności. Przeprowadzone analizy wykazały, że gdyby każdy Amerykanin korzystający z Internetu czytał polityki prywatności w całości, wymagałoby to od niego poświęcenia 201 godzin rocznie, co w efekcie generowałoby koszt ponad 3500 USD *per capita*, a w skali całej amerykańskiej gospodarki czas poświęcony na czytanie polityk skutkowałby stratami rzędu ok. 781 mld USD. Autorki badań podkreślają przy tym, że koszt ten wielokrotnie przekraczałby wartość całego rynku reklamy behawioralnej w Internecie, która w 2007 r. (tj. w roku, w którym badanie zostało przeprowadzone) była wyceniana na ponad 35-krotnie mniej (21 mld USD)[32]. W praktyce zatem próba pełnego wdrożenia modelowych założeń systemu ochrony danych osobowych opartego na autonomii informacyjnej generowałaby koszty, które najprawdopodobniej wielokrotnie przekraczałyby społeczną zdolność do ich absorpcji.

shells to brighten up their existence / – Scraping chewing gum off the streets", *J. Thomas*, 22,000 people willingly agree to community service in return for free WiFi, https://purple.ai/purple-community-service (dostęp: 17.11.2021 r.).

30 *Ibidem*.

31 Forbrukerrådet, 250,000 words of app terms and conditions, https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/.

32 *A.M. McDonald*, *L.F. Cranor*, The Cost of Reading, s. 562–563.

§ 4. Trudności ze zrozumieniem informacji o zasadach ochrony danych osobowych zawartych w politykach prywatności

Badania wskazują również, że nawet użytkownicy, którzy zapoznają się z udzielanymi im informacjami, mogą mieć trudności z uzyskaniem niezbędnych danych z powodu niezrozumienia otrzymywanych polityk i klauzul informacyjnych. Problem ten jest szczególnie istotny, biorąc pod uwagę relatywnie trudny język stosowany w tego rodzaju dokumentach, a także ich objętość i konstrukcję utrudniającą odszukanie konkretnych, interesujących czytelnika informacji.

Szereg problemów związanych z przejrzystością i zakresem zastosowania polityk prywatności nakreślił zespół badaczy z Queen Mary University of London, który przeprowadził analizę regulaminów i polityk prywatności najpopularniejszych dostawców usług internetowych. Wskazali oni m.in. że dokumenty te często są dostępne wyłącznie w języku angielskim, nie precyzują, czy mają zastosowanie w państwie, w którym z usługi korzysta dany użytkownik, a czasami są nawet trudne do odnalezienia na stronie internetowej usługodawcy[33]. Problemy sprawia również ustalenie, który spośród dokumentów ma zastosowanie do konkretnej usługi lub jej wariantu, a zmiany informacji zawartych w ich treści są wprowadzane relatywnie często i w sposób niezbyt przejrzysty dla użytkowników[34].

Zrozumienie języka stosowanego w dokumentach informacyjnych również często sprawia problemy użytkownikom. Jeden z projektów badawczych, którego celem była ocena polityk stosowanych przez strony internetowe adresowane do pacjentów ze stwierdzoną przewlekłą chorobą nerek, wykazał, że polityki prywatności są często redagowane w sposób trudny do zrozumienia, zwłaszcza dla dzieci i młodzieży. Zgodnie z przeprowadzonymi przez autorów obliczeniami, przeciętna wartość wskaźnika mglistości tekstu Gunninga (*Gunning Fog Index*) wymagała 15 lat edukacji w celu zrozumienia jej treści. Zgodnie z amerykańskim systemem edukacji oznacza to zrozumiałość tekstu dla studenta pierwszego roku college'u. Podobne wnioski dało badanie innym tego typu narzędziem, wskaźnikiem Flescha, które również wykazało, że analizowane teksty wymagają, przynajmniej częściowo, poziomu edukacji akade-

[33] *D. Kamarinou*, *C. Millard*, *W.K. Hon*, Cloud privacy, Part I, s. 84.
[34] *D. Kamarinou*, *C. Millard*, *W.K. Hon*, Cloud privacy, Part II, s. 184.

mickiej[35]. Nieco inne, starsze badania polityk prywatności na stronach internetowych poświęconych tematyce zdrowia wykazały, że do zrozumienia przekazywanych informacji niezbędne były nawet dwa lata edukacji akademickiej, pomijając zresztą fakt, że 30% (24 z 80) badanych stron internetowych w ogóle nie posiadało polityki prywatności[36].

Z kolei badania prowadzone na próbce statystycznej studentów i absolwentów California State University, Long Beach, wykazały, że nawet jeśli informacje są przekazywane językiem o trudności zbliżonej do poziomu edukacji uczestników, zrozumienie polityki prywatności jest często niskie. Autorzy oceniają, że przyczyny takiego stanu rzeczy należy upatrywać w sposobie sformułowania polityk prywatności, które często posługiwały się niezbyt precyzyjnymi wyrażeniami oraz wieloma stwierdzeniami warunkowymi[37].

Ważnych wniosków dostarczają w tej kwestii także analizy przeprowadzone przez *I. Pollach*, która oceniała 50 polityk prywatności przedsiębiorstw prowadzących działalność w różnych obszarach życia gospodarczego. Wykazała ona, podobnie jak poprzednie przytoczone badania, że język polityk prywatności nie jest w pełni precyzyjny, zwracając jednocześnie uwagę, że zjawisko niejasności językowych dotyczyło zwłaszcza informowania o praktykach, które pozostają wątpliwe z punktu widzenia zasad ochrony prywatności i danych osobowych użytkowników (m.in. poprzez umniejszanie ich częstotliwości albo pomijanie bezpośrednich odniesień do usługodawcy we fragmentach odnoszących się do nieetycznych zachowań). Autorka podkreśla, że na podstawie badań nie można przesądzić, czy taki stan rzeczy wynika z niskich umiejętności osoby sporządzającej dokument czy z zamierzonej praktyki usługodawcy, w jej ocenie jednak sposób sporządzenia polityk prywatności wskazuje, że służą one raczej ochronie przed ewentualnym sporem, niż mają związek z przywiązaniem do dobrych praktyk w zakresie zarządzania danymi[38]. Co ciekawe, również w analizowanych powyżej publikacjach wskazuje się, że polityki prywatności często służą zapewnieniu zgodności (*compliance*), a ich objętość

[35] *L. Costello Kaitlin*, Information quality, s. 4.

[36] *M.A. Graber*, *D.M. D'Alessandro*, *J. Johnson-West*, Reading level, s. 642–645.

[37] *K.-P.L. Vu*, *V. Chambers*, *F.P. Garcia*, *B. Creekmur*, *J. Sulaitis*, *D. Nelson*, *R. Pierce*, *R.W. Proctor*, How Users Read, s. 810–811.

[38] Dosłownie: „The findings noted here suggest that online privacy policies have been drafted with the threat of privacy litigations in mind rather than commitment to fair data handling practices", zob. *I. Pollach*, What's Wrong, s. 107.