Przemysław Pałka*

Ciało obce: zasady RODO a gospodarka rynkowa[1]

Spis treści

I. Wprowadzenie
II. Logika RODO
1. Zasady ograniczenia celu i czasu przetwarzania oraz minimalizacja danych
2. Zgodność z prawem, rzetelność i warunki legalizujące przetwarzanie
3. Przejrzystość względem osoby udostępniającej swoje dane
4. RODO a cele przetwarzania w sektorze prywatnym
III. Logika rynku
1. Co nie jest zakazane, jest dozwolone
2. Konkurencja doskonała i pełnia informacji o preferencjach
IV. Możliwe ścieżki reformy
1. Efekty zewnętrzne przetwarzania danych osobowych
2. Ustawowa regulacja konkretnych celów przetwarzania
V. Konkluzje

Streszczenie

Artykuł analizuje relacje pomiędzy logiką RODO a logiką rynkową w kontekście tzw. kapitalizmu inwigilacji. Wbrew powszechnie przyjmowanej opinii szkody związane z komercyjnym nadzorem (manipulacja, dyskryminacja, negatywne skutki dla zdrowia psychicznego) często nie wynikają z niewystarczającej egzekucji RODO, a z faktu, że rozporządzenie to nie wypowiada się na temat legalności konkretnych celów przetwarzania danych. W realiach rynkowych, przy braku regulacji, to administratorzy *de facto* decydują o tym, jakie dane wykorzystane mogą być w jakim celu. By wyjść z tego impasu, artykuł proponuje ustawowe uregulowanie dopuszczalności niektórych konkretnych celów przetwarzania danych.

Słowa kluczowe: prawo ochrony danych osobowych; prawo konsumenckie; rynek.

JEL: K24

* Doktor, LL.M., adiunkt na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego, ul. Bracka 12, 31-005 Kraków. ORCID https://orcid.org/0000-0002-6879-1596.

[1] Badania naukowe prowadzące do osiągnięcia tych wyników zostały sfinansowane ze środków Norweskiego Mechanizmu Finansowego na lata 2014–2021, z grantu pt. Prywatne Prawo Danych: Pojęcia, Praktyki, Zasady i Polityczność, Nr 2020/37/K/HS5/02769.

I. Wprowadzenie

Wśród europejskich prawników zajmujących się ochronną danych osobowych panuje przekonanie, że podstawowy problem z RODO[2] to niedostateczna egzekucja przepisów.

W dniach 16–17 czerwca 2022 roku, w Brukseli, odbyła się konferencja pt. „The future of data protection: effective enforcement in the digital world", zwołana przez Europejskiego Inspektora Ochrony Danych, Wojciecha Wiewiórowskiego[3]. Było to wydarzenie polityczne dużej wagi, na którym spotkały się najważniejsze osoby decydujące o kształcie prawa ochrony danych w UE. Wśród ponad stu prelegentów znaleźli się kluczowi politycy (w tym dwie wiceprzewodniczące Komisji Europejskiej, Margrethe Vestager i Věra Jourová), szefowie organów nadzorczych (m.in. Marie-Laure Denis, szefowa francuskiego CNIL, Ulrich Kelber, niemiecki federalny inspektor ochrony danych), prominentni aktywiści (m.in. Max Schrems z NOYB Ursula Pachl z BEUC), przedstawiciele sektora prywatnego (m.in. Julie Brill z Microsoftu, Jane Horvath z Apple'a, William Malcolm z Google'a) i akademicy (m.in. Orla Lynskey z LSE, Paul De Hert z VUB, Michael Veale z UCL).

Motywacją stojącą za tym wydarzeniem było powszechne rozczarowanie znikomym wpływem, jaki RODO miało i ma na cyfrowy kształt gospodarki i społeczeństwa. Po czterech latach stosowania tego prawa mieszkańcy Unii Europejskiej wciąż żyją w „kapitalizmie inwigilacji" (Zuboff, 2019), gdzie ich dane są powszechnie zbierane, analizowane i wykorzystywane do profilowania i wywierania wpływu na ich poglądy i zachowania (Cohen, 2019; Trzaskowski, 2022). Według raportu przygotowanego przez fundację Irish Council for Civil Liberties w maju 2022 r., dane o zachowaniu przeciętnego Europejczyka były zbierane i wysyłane do reklamodawców średnio 376 razy dziennie (ICCL, 2022), podczas gdy w USA – gdzie nie ma federalnych regulacji na temat ochrony danych w sektorze prywatnym (Solove i Schwartz, 2018) – odbywało się to 747 razy dziennie.

Uczestnicy konferencji byli zgodni, że źródłem jest niewystarczająca egzekucja przepisów RODO, szczególnie w sprawach transgranicznych. Według prelegentów RODO to materialne prawo, którego faktyczna blokada stosowania wynika ze zbytniego obciążenia części organów nadzorczych (przede wszystkim irlandzkiego) i nieadekwatnych przepisów dotyczących procedur, niepozwalających przekuć litery w praktykę (Gentile i Lynskey, 2022). W konsekwencji prawodawca unijny musi się skupić na reformie przepisów dotyczących stosowania RODO. Jak konkretnie wyglądać miałaby taka reforma? Tego właśnie dotyczył spór pomiędzy uczestnikami konferencji. Jedni optowali za centralizacją stosowania RODO w sprawach transgranicznych, trochę na kształt prawa antymonopolowego w UE; inni – za przeznaczeniem znacznych środków finansowych na udrożnienie obecnego systemu. Pytanie o usprawnienie egzekucji RODO jest istotne i będzie prawdopodobnie towarzyszyć naukowcom przez najbliższych kilka lat. Nie jest to jednak pytanie, na którym skupia się niniejszy tekst.

Tezą niniejszego artykułu jest założenie, że RODO, materialnie, nie jest dobrym instrumentem do ukrócenia najbardziej szkodliwych praktyk przedsiębiorców, takich jak Meta i Alphabet, których model biznesowy oparty jest na zbieraniu i monetyzacji danych osobowych. Problem nie leży w tym, że spółki te nie przestrzegają przepisów RODO (a więc należy usprawnić egzekucję, by zmusić je do zastosowania się litery prawa). Przeciwnie, praktyki Google i Facebooka są, poza

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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) (Dz. Urz. UE 2016 L 119/1); dalej: ROOD lub rozporządzenie.

[3] Wszystkie sesje dostępne są online pod adresem: https://www.edpsconference2022.eu/en.

marginalnymi przypadkami, zgodne z europejskim prawem ochrony danych. Wbrew powszechnie panującemu przekonaniu RODO nie jest dobrym prawem, jeśli założymy, że jego celem jest likwidacja wszystkich negatywnych efektów istnienia „kapitalizmu inwigilacji" i związanych z nim negatywnych skutków zewnętrznych dla jednostek, takich jak manipulacja (Mik, 2016; Susser i in., 2019), dyskryminacja (Ali i in., 2019; Xenidis, 2020) czy negatywny wpływ na zdrowie psychiczne (Bhargava i Velasquez, 2021; Zakon, 2020). Wynika to z dwóch powodów.

Po pierwsze, choć RODO wprowadza szereg zasad i reguł ograniczających wykorzystanie danych w różnych celach, nie wypowiada się wprost na temat dopuszczalności konkretnych, poszczególnych celów przetwarzania. Owszem, wprowadza cały szereg wymogów, które należy spełnić przy precyzowaniu celu (oraz wyklucza możliwość realizowania celów niezgodnych z prawem lub wprost godzących w prawa innych osób), ale nie odpowiada na takie pytania jak: czy wolno przetwarzać dane osobowe w celu personalizowania reklam albo w celu uczynienia usług bardziej „angażującymi" (Zakon, 2020). W gospodarce kapitalistycznej, przy braku regulacji konkretnych celów, decyzje dotyczące legalności wykorzystania danych podejmuje rynek – formalnie konsument, w praktyce przedsiębiorca (który sam dokonuje oceny ryzyka). Oczywiście musi się to odbywać z poszanowaniem przepisów RODO (niektóre cele, wprost godzące w prawa osób, których dane dotyczą, będą niedopuszczalne), prawa powszechnie obowiązującego i praw innych osób. Jednakże, w ramach tak zakreślonych, to mechanizm rynkowy odpowie na pytanie, jakie cele przetwarzania są akceptowalne. Po drugie, ogólna logika RODO – zakładająca minimalizację danych – stoi w sprzeczności z logiką rynkową – dążącą do pełni informacji. Wobec braku regulacji i wolności gospodarczej administratorzy tak formułować będą swoje regulaminy i polityki prywatności, tak przeprowadzać procesy analizy ryzyka przetwarzania, by RODO nie tylko nie przeszkodziło im w dążeniu do założonych celów, ale wręcz takie działania legalizowało.

Sposobem na wybrnięcie z tego impasu nie jest usprawnienie egzekucji RODO, lecz materialne uregulowanie przez ustawodawcę konkretnych celów przetwarzania. By to wykazać, artykuł został podzielony na trzy części. W pierwszej – analizie poddano logikę RODO, w tym konkretne przepisy i pojęcia, w celu przedstawienia co mogą one osiągnąć, a czego nie. W drugiej części autor przybliża logikę gospodarki rynkowej, wskazując na rolę jaką w „kapitalizmie inwigilacji" odgrywa swoboda gospodarcza, połączona z indywidualistyczną logiką RODO, dążącą jednak do sprzecznych niż rynek celów. W trzeciej – przedstawiony jest argument za precyzyjną regulacją poszczególnych celów przetwarzania danych.

II. Logika RODO

Choć RODO jest aktem pozornie skomplikowanym, jego centralna logika – przejęta niemal bez zmian z dyrektywy 95/46[4] opartej na Konwencji 108 Rady Europy z 1981 roku, wprowadzającej w życie zalecenia amerykańskiego raportu z 1973 r. (Pałka, 2020) – jest dość prosta. Zanim przyjrzymy jej się bliżej, trzy paragrafy poświęćmy celom i podstawowym pojęciom rozporządzenia oraz zakresowi jego zastosowania.

[4] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE 2016 L 281).

Prawodawca unijny wskazał dwa cele rozporządzenia: (1) ochronę podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych[5] oraz (2) przeciwdziałanie ograniczeniom lub zakazom dotyczącym swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych[6]. Choć w pracach doktrynalnych (Fajgielski, 2018, s. 82; Hijmans, 2020, s. 53) wskazuje się prymat pierwszego z tych celów nad drugim, autorzy badający RODO od strony krytycznej wykazują, że realny kształt przepisów rozporządzenia niejednokrotnie prowadzić może do rezultatów uprzywilejowujących swobodę gospodarczą nad ochroną osób fizycznych (Andrew i Baker, 2021; Padden i Öjehag-Pettersson, 2021; Waldman, 2020).

RODO reguluje „przetwarzanie" „danych osobowych" w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych[7]. Oba pojęcia rozumiane są szeroko. „Dane osobowe" definiowane są jako „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej"[8], a szerokie pojmowanie „możliwości bycia zidentyfikowanym" doprowadziło pewnych komentatorów do wniosku, że niemalże wszystkie informacje, jeśli tylko dotyczą osób fizycznych, dają się zakwalifikować jako dane osobowe na potrzeby rozporządzenia (Purtova, 2018). „Przetwarzanie", z kolei, „oznacza operację lub zestaw operacji wykonywanych na danych osobowych (…), taką jak zbieranie (…), wykorzystywanie, (…) udostępnianie (…) lub niszczenie"[9]. RODO stosuje się do działań podmiotów prywatnych (graczy rynkowych i trzeciego sektora) i organów publicznych[10], i w każdej sytuacji nakłada takie same obowiązki na administratorów danych, tj. podmioty, które decydują o sposobach i celach przetwarzania[11], oraz przyznaje takie same prawa osobom, których dane dotyczą[12].

Innymi słowy, jeśli jakikolwiek podmiot (lokalna pizzeria, Facebook, szkoła podstawowa, Minister Środowiska itd.) wykonuje jakiekolwiek operacje w sposób całkowicie lub częściowo zautomatyzowany (zbiera, analizuje, dzieli się, usuwa itp.) na danych stanowiących informacje dotyczące osoby fizycznej dającej się zidentyfikować (a w przypadku danych osobowych stanowiących część zbioru danych również gdy przetwarza je w sposób niezautomatyzowany) RODO ma zastosowanie i każdą z tych sytuacji reguluje, opierając się na tym samym schemacie. Dotyczy to tak małych przedsiębiorstw z państw członkowskich UE, uniwersytetów, jak i wielkich międzynarodowych korporacji, nawet z siedzibą poza UE, jeśli tylko te ostatnie oferują mieszkańcom Unii towary i usługi lub monitorują ich zachowanie[13]. Nie ma znaczenia sektor, rozmiar administratora czy rodzaj operacji; każde przetwarzanie danych osobowych – na potrzeby ogólnej logiki rozporządzenia – traktowane jest jednakowo. Jaka jest to logika?

5 Artykuł 1 ust. 2 RODO.
6 Artykuł 1 ust. 3 RODO.
7 Artykuł 2 ust. 1 RODO.
8 Artykuł 4 pkt 1 RODO.
9 Artykuł 4 pkt 2 RODO.
10 Artykuł 4 pkt 7 RODO.
11 Ibidem.
12 Artykuł 4 pkt 1 RODO; art. 12–22 RODO.
13 Artykuł 3 ust. 2 RODO.

Przede wszystkim, każde przetwarzanie musi być zgodne z ogólnymi zasadami rozporządzenia[14] oraz z obowiązkami wynikającymi z uszczegółowiających je konkretnych przepisów. Najważniejsze zasady, z punktu widzenia niniejszego artykułu, to:

1) ograniczenie celu przetwarzania[15],
2) minimalizacja danych[16],
3) ograniczenie przechowywania[17],
4) legalność i rzetelność[18],
5) transparentność[19].

Pierwsze trzy zostaną omówione w następnym punkcie, a kolejne dwie w dwóch kolejnych punktach.

1. Zasady ograniczenia celu i czasu przetwarzania oraz minimalizacja danych

W myśl zasady ograniczenia celu, dane osobowe muszą być „zbierane w konkretnych, wyraźnych i prawnie uzasadnionych [*legitimate* – przyp. aut.] celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami”[20]. Oznacza to, że za każdym razem, kiedy jakiś podmiot zbiera dane (Allegro prosi o adres do dostawy, uczelnia rozsyła ankietę, Facebook pobiera dane o lokalizacji użytkowników itd.) musi on w sposób konkretny określić w jakim celu to robi. Jeśli uniwersytet zbiera adresy mailowe przy rejestracji na konferencję w celu rozesłania programu i linków do logowania, nie powinien ich wykorzystywać do rekrutacji na studia lub badania. Jeśli portal społecznościowy zbiera dane konieczne do wykonania usługi, np. przechowywania zdjęć czy innych treści generowanych przez konsumentów i wyświetlania tych treści innym użytkownikom, nie powinien posługiwać się tymi samymi informacjami do personalizowania reklam. Oczywiście cel można zakreślić szerzej, natomiast musi być on konkretny i sprecyzowany *ex ante.* Jak wskazuje Katarzyna Witkowska-Nowakowska (2018, s. 31) „związanie celem przetwarzania wyłącza możliwość gromadzenia danych na zapas, na poczet przyszłych, nieokreślonych i niesprecyzowanych celów”.

Druga zasada, minimalizacji danych, wymaga by dane były „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane”[21]. Przykładowo, jeśli uniwersytet rejestruje uczestników na seminarium online, może zebrać imię, nazwisko, afiliację czy adres email, ale nie powinien zbierać informacji o wzroście czy miejscu zamieszkania; te drugie nie są niezbędne do rejestracji. Podobnie, jeśli podmiot prywatny świadczy usługę online, poprzez stronę lub aplikację, może zebrać dane o systemie operacyjnym i przeglądarce użytkownika, jeśli jest to konieczne ze względów technicznych, ale nie może zebrać informacji o historii przeglądania innych stron czy o innych aplikacjach, które użytkownik serwisu ma zainstalowane w telefonie. W polskiej doktrynie toczy się spór, czy zasada minimalizacji pozwala „przetwarzać tylko takie dane osobowe, bez których nie da się osiągnąć zamierzonego celu przetwarzania” (Litwiński i in., 2018, s. 263), czy też dopuszczalnym jest przetwarzanie danych, które być może

[14] Artykuł 5 RODO.
[15] Artykuł 5 ust. 1 lit. b) RODO.
[16] Artykuł 5 ust. 1 lit. c) RODO.
[17] Artykuł 5 ust. 1 lit. e) RODO.
[18] Artykuł 5 ust. 1 lit. a) RODO.
[19] Artykuł 5 ust. 1 lit. a) RODO.
[20] Artykuł 5 ust. 1 lit. b) RODO.
[21] Artykuł 5 ust. 1 lit. c) RODO.

nie są bezwzględnie niezbędne do osiągnięcia celu, ale „w istotny sposób mogą pomóc osiągnąć cel przetwarzania" (Fajgielski, 2018, s. 149).

Ograniczenie przechowywania, czyli trzecia zasada, nakazuje by dane osobowe były przechowywane „przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane"[22]. Na przykład, jeśli uniwersytet zbiera dane, by zarejestrować uczestników na seminarium online, gdy to seminarium już się odbędzie może przechowywać je przez jakiś czas (np. by wystawić certyfikaty uczestnictwa czy rozesłać wiadomość z podziękowaniami), ale później musi je usunąć. Podobnie, jeśli przedsiębiorca zbiera informacje w celu jednorazowej dostawy i produkt już dostarczy, nie powinien dłużej tych danych przechowywać. Jednakże, jak wskazuje Andrzej Krasuski (2018, s. 196), „przetwarzanie danych osobowych może następować tak długo, jak długo administrator danych może realizować cel przetwarzania danych osobowych".

Wszystkie trzy zasady pozornie ograniczają zdolność przedsiębiorstw do wykorzystywania i monetyzowania danych osobowych. Skoro wolno im zebrać nie więcej danych niż jest to konieczne do realizacji konkretnego celu, nie mogą ich przechowywać dłużej niż jest to konieczne do osiągnięcia celu i nie wolno im wykorzystywać ich w sposób sprzeczny z tym celem, to na poziomie gospodarki i społeczeństwa powinno być zbieranych mniej danych i powinny być one wykorzystywane w bardziej ograniczonym zakresie, niż gdyby tych zasad nie było.

Należy jednak zwrócić uwagę, że RODO nie wypowiada się na temat dopuszczalności konkretnych, poszczególnych celów przetwarzania. Owszem, wprowadza zasadę legalności i rzetelności[23], zgodnie z którą przetwarzanie musi być zgodne z prawem i nie może naruszać podstawowych praw osób, których dane dotyczą. Niemniej, przedsiębiorca, który chce zebrać oraz wykorzystać dane w jakimś celu, np. do personalizowania wyświetlanych treści czy reklam lub do zwiększenia „zaangażowania" użytkowników swojej usługi, co do zasady może to zrobić. Musi jedynie wystarczająco jasno sprecyzować ten cel (oraz zapewnić, że przetwarzanie nie jest niezgodne z prawem), zebrać nie więcej danych niż to konieczne i nie przechowywać ich dłużej niż to konieczne do realizacji tego celu. Jednakże, jeśli celem przedsiębiorcy jest oferowanie usługi mediów społecznościowych, której elementem jest jak najlepsze dopasowywanie treści do zainteresowań użytkownika, przez czas nieokreślony[24], może argumentować, że wolno mu przetwarzać znaczącą ilość danych przez długi czas i na wiele sposobów.

Nie regulując konkretnych, poszczególnych celów przetwarzania, RODO wprowadza jednak wymóg, by przetwarzanie odbywało się „zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą"[25]. Z tego zdania wyprowadzić można trzy kolejne elementy logiki RODO.

2. Zgodność z prawem, rzetelność i warunki legalizujące przetwarzanie

Każde przetwarzanie musi być zatem zgodne z prawem – tekst angielski posługuje się tu sformułowaniem *lawfully* – co realnie przekłada się na trzy odrębne obowiązki. Pierwsze dwa są strukturalnie dość proste. Z jednej strony, administratorom nie wolno przetwarzać danych w celach niezgodnych z prawem powszechnie obowiązującym. Takie ujęcie przepisu sprawia,

[22] Artykuł 5 ust. 1 lit. e) RODO.

[23] Zasady te zostały omówione w następnym punkcie.

[24] Tak, na przykład, charakter swojej usługi opisuje Meta: https://www.facebook.com/terms.php.

[25] Artykuł 5 ust. 1 lit. a) RODO.

że administrator, który łamie prawo, naraża się nie tylko na sankcje wynikające ze złamanych przepisów, lecz także na karę przewidzianą przez RODO. Przykładowo przedsiębiorca, który wykorzystuje dane by rozsyłać do konsumentów informacje handlowe wprowadzające w błąd[26], nie tylko musi liczyć się z sankcjami wynikającymi z prawa konsumenckiego (Howells i in., 2016), lecz także narusza RODO (Hacker, 2021).

Z drugiej strony, każde przetwarzanie musi być zalegalizowane poprzez spełnienie co najmniej jednego z warunków wyliczonych w art. 6 ust. 1 RODO (wcześniej, na kanwie dyrektywy 95/46, mowa była o obecności przynajmniej jednej przesłanki legalizującej). Z punktu widzenia niniejszego artykułu, istotne są trzy:

1) świadoma zgoda[27];
2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy[28];
3) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora[29].

Jeśli więc Meta świadczy usługę dostępu do portalu Facebook, różne kategorie danych w różnych celach przetwarzać będzie na podstawie różnych przesłanek. Przykładowo dane, takie jak imię i nazwisko (konieczne do założenia konta), adres email (konieczny do logowania), dane o używanej przeglądarce czy systemie operacyjnym (konieczne z technicznego punktu widzenia do poprawnego funkcjonowania usługi) itd., będzie przetwarzać w tych konkretnych celach na podstawie „niezbędności do wykonania umowy". Nie jest więc do takiego przetwarzania potrzebna zgoda osoby, której dane dotyczą (Fajgielski, 2018, s. 160).

Zgoda jest jednym z możliwych warunków legalizujących, odgrywającym w praktyce rolę przy przetwarzaniu, które nie jest konieczne dla wykonania umowy, ale na którym zależeć może administratorowi lub osobie udostępniającej swoje dane. Na przykład, jeśli kupując coś na Allegro, konsument podaje swoje dane adresowe do dostawy, operator usługi nie potrzebuje jego lub jej zgody, by te dane w tym celu przetwarzać. Jednakże, jeśli chciałby owemu konsumentowi przysyłać informacje handlowe, np. wiadomości email, informujące o promocjach, zawierające kupony i zniżki itd., musi poprosić o zgodę, tak by dopuszczalnym było wykorzystanie tych samych danych w innym celu, na podstawie innego warunku. RODO stawia dość wysokie wymagania względem formy zgody – musi ona być świadoma, nie może być częścią regulaminu itd.[30] (Breen i in., 2020).

Budzącym najwięcej kontrowersji warunkiem legalizującym jest „uzasadniony cel administratora" (Kamara i De Hert, 2018). Będzie on miał zastosowanie, gdy przetwarzanie nie jest co prawda konieczne do wykonania umowy i osoba, której dane dotyczą, nie wyraziła na to wyraźnej zgody, ale administrator uważa, że jego uzasadniony interes jest tu wystarczający (Fajgielski, 2018, s. 173–175). Przykłady takich interesów, które mogą (acz nie muszą) stanowić przesłankę legalizującą, na podstawie dyrektywy 95/45, grupa robocza ds. ochrony osób fizycznych w zakresie

[26] Ustawa z 23.08.2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (Dz.U. 2007 Nr 171 poz. 1206), art. 4.

[27] Artykuł 6 ust. 1 lit. a) RODO, art. 7 RODO.

[28] Artykuł 6 ust. 1 lit. b) RODO.

[29] Artykuł 6 ust. 1 lit. f) RODO.

[30] Artykuł 7 RODO.

przetwarzania danych osobowych (poprzednik Europejskiej Rady Ochrony Danych Osobowych) wskazała m.in.: konwencjonalny marketing bezpośredni, dochodzenie swoich praw (np. dochodzenie wierzytelności od użytkownika), przetwarzanie dla celów zachowania bezpieczeństwa sieci itd.[31]. Podobne stanowisko prezentuje Paweł Fajgielski (2018, s. 175) pisząc, że w poprzednim stanie prawnym ustawodawca jasno wskazał na dopuszczalność uznawania za uzasadniony cel administratora „marketing bezpośredni własnych produktów i usług administratora oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej. Wydaje się, że wskazane (…) przypadki mogą być nadal uznawane za prawnie uzasadniony cel interes na gruncie komentowanego przepisu".

Co istotne, te same dane mogą być przetwarzane w różnych celach na podstawie różnych warunków z art. 6. Jednakże, by przetwarzanie było zgodne z prawem, musi wystąpić jeden z tych warunków. „Zgoda" jest warunkiem najpewniejszym od strony dowodowej, ale nie zawsze jest konieczna. Dodatkowo pamiętać należy, że zgodność każdego przetwarzania z zasadami wymienionymi w art. 5 oraz spełnienie co najmniej jednego z warunków wymienionych w art. 6, to dwa odrębne obowiązki nałożone na administratora.

Trzeci z obowiązków wynikających z zasady legalności i rzetelności jest strukturalnie bardziej złożony. Można bronić poglądu, zgodnie z którym art. 5 ust. 1 lit. a) RODO, interpretowany funkcjonalnie w świetle celu rozporządzenia, jakim jest ochrona podstawowych praw i wolności osób fizycznych[32], nakłada na administratorów danych obowiązek nie tylko przestrzegania reguł obowiązującego prawa przy precyzowania *celów* przetwarzania, lecz także rozważenia wpływu jaki konkretny cel i sposób przetwarzania miałby na prawa podstawowe osób, których dane dotyczą.

Jeśli chodzi o sposób przetwarzania, wymóg ten jest bezsporny. Artykuł 24 RODO wymaga, by „Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża[ł] odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać"[33]. Dalej, w artykule 25, RODO wprowadza wymóg, by: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu *sposobów* przetwarzania, jak i w czasie samego przetwarzania – wdraża[ł] odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą"[34].

Powyższe podejście, w żargonie branżowym nazywane *data protection by design* oraz *by default* (Tamò-Larrieux, 2018), wynika z faktu, że przetwarzania danych często odbywa się

[31] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, s. 25. Pozyskano z: https://www.dataprotection.ro/servlet/ViewDocument?id=1086.

[32] Artykuł art. 1 ust. 2 RODO.

[33] Artykuł 24 ust. 1 RODO.

[34] Artykuł 21 ust. 1 RODO.

w skomplikowanych systemach informatycznych oraz strukturach organizacyjnych, mających wiele potencjalnie słabych punktów. Przykładowo, choć prawne stwierdzenie, że administratorem danych osobowych studentów jest uniwersytet mogłoby wskazywać na dość prostą relację dwóch osób (fizycznej i prawnej), w rzeczywistości do danych dostęp mieć będzie bardzo dużo pracowników owego uniwersytetu (pracownicy dziekanatu, pionów centralnych, wykładowcy itd.) przetwarzających je na szeregu różnych urządzeń. Administrator musi więc zapewnić, że od stron zarówno technicznej (używany sprzęt i oprogramowanie), jak i organizacyjnej (szkolenia, obowiązki regulaminowe) ryzyko naruszenia RODO jest minimalizowane.

Co jednak w sytuacji, kiedy to nie sposób (np. niewystarczające standardy bezpieczeństwa danych), a sam cel przetwarzania godzi w prawa i wolności osób, które dane udostępniają? W teorii administrator powinien to ustalić przed rozpoczęciem przetwarzania (np. realizując obowiązek oceny skutków przetwarzania na podstawie art. 35 RODO), również w procesie konsultacji z organem nadzorczym[35]. W praktyce można zaś wyobrazić sobie trzy modelowe kategorie takich sytuacji, gdy cel przetwarzania:

(1) godzi w prawa osób chronione w Konstytucji lub w traktatach (np. celem przetwarzania jest dyskryminacja ze względu na orientację seksualną);
(2) godzi w prawa osób chronione przez ustawy lub prawo wtórne UE (np. celem przetwarzania jest nakłonienie konsumentów do zakupu dobra lub usługi za wszelką cenę, potencjalnie poprzez wprowadzenie błąd);
(3) nie godzi wprost w prawa osób, których dane dotyczą (np. personalizacja wyświetlanych treści, rekomendacje treści, wyświetlanie reklam niewprowadzających w błąd), ale efektem owego przetwarzania może być naruszenie praw lub interesów tych osób (np. spędzanie na korzystaniu z usług typu Facebook więcej czasu niż konsumenci by chcieli (Zakon, 2020), „dyskryminujące" efekty personalizacji reklam (Ali i in., 2019)).

Pierwsze dwie kategorie celów są oczywiście niezgodne z RODO i niedopuszczalne. Jednakże w przypadku trzeciej kategorii sytuacja jest bardziej skomplikowana. Po pierwsze, w sytuacjach, w których jakieś działanie nie jest wprost zakazane przez prawo (np. takie konstruowanie usługi, by konsumenci spędzili jak najwięcej czasu na korzystaniu z niej) lub wyświetlanie różnych kategorii reklam osobom o różnych cechach, pytanie o to, czy podstawowe prawa zostają naruszone pozostaje otwarte. W pierwszym przypadku można argumentować, że takie działanie godzi w prawo do ochrony zdrowia psychicznego, ale równie dobrze podnosić, że jest to działanie prokonsumeckie, zwiększające jakość usługi. W drugim przypadku można twierdzić, że takie działanie godzi w prawo osób do bycia wolnym od dyskryminacji, jak również utrzymywać, że skoro nie jest zakazane przez prawo wtórne, zabraniające *de lege lata* dyskryminacji w dostępie do dóbr i usług, a nie w wyświetlanych reklamach (Xenidis, 2020), to jest to działanie w interesie konsumentów, którzy widzą wyłącznie reklamy produktów, którymi są realnie zainteresowani.

Po drugie, należy zwrócić uwagę, że oceny tej dokonuje – co do zasady – administrator danych, który z konieczności kieruje się swoim własnych wachlarzem motywacji (*incentive structure*). Skoro odpowiedź na pytanie jest sporna, a udziela jej podmiot żywotnie zainteresowany takim

[35] Artykuł 36 RODO.

a nie innym rozwiązaniem, możliwym jest, że w taki sposób przeprowadzi ocenę ryzyka i opisze cele, by efektem analizy była konkluzja, że niczyje prawa nie są zagrożone.

Jest to duży mankament tzw. zasady ryzyka, na której oparte jest stosowanie RODO (Dunn i Gregorio, 2022). Należy pamiętać, że „zasada ryzyka" nie jest zasadą o równej wadze normatywnej, jak zasady wymienione w art. 5 RODO (ograniczenia celu, minimalizacji danych itd.), a raczej pewną metafilozofią regulacji, jak w swojej przełomowej pracy w tym temacie określił ją Raphaël Gellert (2020, s. 136–138). W tym ujęciu decyzje o dopuszczalności konkretnych sposobów i celów przetwarzania ustawodawca „deleguje" na administratorów (Sobczyk, 2019). Jak celnie zauważają Andrzej Krasuski i Przemysław Siembida (2022, s. 60), „prawodawca unijny nie zdefiniował pojęcia ryzyka w RODO" i postulują, by jego treść ustalać na podstawie innych przepisów rozporządzenia.

Choć pojęcie ryzyka jest oczywiście bardziej złożone, to, ze względu na zakres problematyki poruszanej w niniejszym artykule, znaczenie mają dwie kategorie ryzyka. Z jednej strony, istnieje ryzyko techniczno-organizacyjne, tj. niebezpieczeństwo, że prawo do ochrony danych osobowych zostanie naruszone poprzez naruszenie RODO wynikające z nieprzestrzegania standardów bezpieczeństwa. W tym wypadku wprowadzona przez RODO zasada ryzyka wydaje się jak najbardziej uzasadniona: to administrator, który najlepiej zna swoje uwarunkowania organizacyjne, dokonuje wyboru środków koniecznych do zapewnienia zgodności przetwarzania z RODO. Ocena taka ma charakter techniczny, faktyczny i ekspercki.

Z drugiej strony, przywoływane wyżej ryzyko naruszenia praw osób poprzez wybór celu przetwarzania (niezabronionego wprost przez prawo) ma zupełnie inny charakter: ocenny i dyskusyjny. Oczywiście, jak już wspomniano, cele lub skutki wprost godzące w prawa wprost wyrażone w prawie stanowionym będą z definicji niedopuszczalne. Jednak nie takie cele i skutki są przedmiotem zainteresowania niniejszego artykułu, w którym pochylono się nad sytuacjami, gdzie cele przetwarzania nie są zabronione przez prawo – np. takie konstruowanie usługi, by skłonić konsumentów do spędzania jak najwięcej czasu na korzystaniu z niej – i gdzie można argumentować zarówno za tym, że takie przetwarzanie godzi w prawa osób udostępniających dane, jak i za tym, że w te prawa nie godzi, a wręcz je realizuje. RODO pozostawia tu dużą swobodę przedsiębiorcom, którzy sami, jako pierwsi, dokonują takiej oceny.

Można oczywiście twierdzić, że ponieważ ocena ryzyka przez administratora podlega kontroli organów nadzorczych, teza niniejszego tekstu – że to materialne założenia RODO, a nie niewystarczająca egzekucja przepisów są źródłem trwania „kapitalizmu inwigilacji" – jest błędna. Wszak, w hipotetycznym świecie, w którym organy nadzorcze mają nieograniczone zasoby do przeprowadzania kontroli, mogłyby każdorazowo kwestionować ocenę ryzyka dokonaną przez administratora, a szansa naruszeń interesów osób spadłaby niemal do zera. Zarzut ten jest do pewnego stopnia trafny. Można odnieść się do niego na dwa sposoby. Po pierwsze, podnieść należy, że taka pozycja faktyczna organów nadzorczych – związana z wielokrotnym zwiększeniem ich załogi i środków budżetowych – może być w praktyce trudna do osiągnięcia. W świecie, w którym kontrola nie jest pewna, administrator pozostaje *de facto* jedynym podmiotem dokonującym oceny. Po drugie, nawet gdyby było to faktycznie możliwe, pozostaje pytanie o normatywną zasadność takiego rozwiązania. Czy w państwie demokratycznym, w którym wielokrotnie ważyć trzeba interesy i prawa różnych kategorii podmiotów, faktycznie to wyspecjalizowany organ nadzorczy,

ze swej natury niezależny i niekontrolowany politycznie, powinien podejmować te decyzje? Do drugiego pytania odnoszę się punkcie IV.2. niniejszego artykułu.

Podsumowując, według RODO administrator może przetwarzać dane w następujących sytuacjach:

(1) gdy sprecyzował, zgodny z prawem, cel przetwarzania danych (w tym ocenił czy cel przetwarzania nie godzi w prawa osób, których dane dotyczą) oraz
(2) gdy przetwarzanie konkretnych danych jest konieczne do realizacji tego celu, oraz
(3) gdy zabezpieczył dla tego celu jeden z warunków z art. 6.

Administrator musi wykazać spełnienie tych warunków „wewnętrznie", np. w dokumentacji, którą prowadzi dla celów rozliczalności, w analizie ryzyka, i materialnie, tj. faktyczne zaistnienie tych okoliczności jest konieczne, by przetwarzanie było zgodne z RODO. Dodatkowo musi wykazać to „zewnętrznie" osobom, których dane są przetwarzane, zgodnie z zasadą przejrzystości. To ostatni istotny, z uwagi na poruszaną w artykule tematykę, element RODO.

3. Przejrzystość względem osoby udostępniającej swoje dane

Każde przetwarzanie odbywać musi się w sposób przejrzysty. RODO, w art. 12, 13 i 14 (w rozdz. III dotyczącym praw osób udostępniających swoje dane), nakazuje administratorowi „w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem (…) udzielić osobie, której dane dotyczą, wszelkich informacji (…)"[36] o sobie[37], o celach przetwarzania danych osobowych oraz podstawach prawnych przetwarzania[38], okresie przetwarzania[39] i szeregu innych okoliczności[40]. Jest to więc typowy obowiązek informacyjny, znany z innych dziedzin prawa (Namysłowska i Jabłonowska, 2019), spełnienie którego jest konieczne, by przetwarzanie było legalne. W szczegółach na temat tej zasady wypowiedziała się grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, której opinię, na potrzeby stosowania RODO, zmieniła i przyjęła Europejska Rada Ochrony Danych Osobowych[41].

Przepisy te są prawnym powodem istnienia polityk prywatności na stronach internetowych i w aplikacjach dostępnych dla użytkowników na terenie Unii Europejskiej (Contissa i in., 2018; Liepiņa i in., 2019). Błędnie sformułowana polityka stanowić może samoistne naruszenie RODO, można więc wyobrazić sobie sytuację, w której przetwarzanie jest materialnie zgodne z rozporządzeniem, ale naruszony zostaje obowiązek informacyjny, np. gdy administrator ma konkretny cel, zabezpieczył podstawę przetwarzania, ale w sposób niewystarczająco zrozumiały poinformował o tym celu osobę, która swoje dane udostępniła.

Takie sformułowanie przepisów dotyczących przejrzystości, tj. wymóg, by administrator bezpośrednio informował o celach i podstawach przetwarzania osoby, których dane dotyczą, w sposób jasny i zrozumiały, podkreśla indywidualistyczny charakter logiki RODO. W ostatecznym

[36] Artykuł 12 ust. 1 RODO.
[37] Artykuł 13 ust. 1 lit. a) i b) RODO.
[38] Artykuł 13 ust. 1 lit. c) RODO.
[39] Artykuł 13 ust. 2 lit. a) RODO.
[40] Artykuł 13 i art. 14 RODO.
[41] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018, https://ec.europa.eu/newsroom/article29/items/622227.

rozrachunku to podmiot danych ma decydować czy informacje jego lub jej dotyczące mogą być przetwarzane w taki, a nie inny sposób (oczywiście w ramach obowiązującego prawa; w przypadku, w którym cel lub sposób przetwarzania godzi w prawo stanowione, lub prawa osób, których dane dotyczą, zgoda takiego przetwarzania nie może zalegalizować).

4. RODO a cele przetwarzania w sektorze prywatnym

RODO, będące aktem bogatym w treść, zawiera cały szereg innych zasad i reguł. Rozporządzenie wprowadza specjalne zasady dla przetwarzania tzw. szczególnych kategorii danych osobowych[42], nadaje osobom, których dane dotyczą cały szereg praw względem administratora[43], nakłada konkretne obowiązki na administratorów i tzw. podmioty przetwarzające dane[44], wypowiada się na temat roli kodeksów postępowania i certyfikacji[45], reguluje kompetencje organów nadzorczych oraz współpracę pomiędzy organami[46], transfery danych poza teren UE[47] itp. Oprócz rozporządzenia na prawo ochrony danych w UE składają się też orzecznictwo TS, decyzje organów nadzorczych i, jako tzw. *soft law*, opinie Europejskiej Rady Ochrony Danych. Cała ta skomplikowana konstrukcja nie powinna jednak przesłonić w gruncie prostej logiki rozporządzenia.

Najważniejszą rzeczą dla legalizacji przetwarzania danych jest wskazanie celu. To w oparciu o ten cel analizować można później, czy przestrzegane są zasady ograniczenia celu, minimalizacji danych itd. Dodatkowo cel musi być zalegalizowany, np. poprzez zgodę lub konieczność do wykonania umowy. Cel musi być ponadto zgodny z prawem i nie może naruszać praw osób, których dane dotyczą. Wszystko to musi odbywać się transparentnie.

RODO nie wypowiada się jednak na temat dopuszczalności poszczególnych, konkretnych celów przetwarzania. Z RODO nie wynika odpowiedź na pytanie „czy przedsiębiorca może używać danych osobowych do personalizowania reklam?" ani „czy wolno naukowcowi kolportować newsletter o tym, co robi jego jednostka na uniwersytecie?". RODO mówi jedynie co takiego podmioty muszą zrobić, by przetwarzanie, w wybranym przez nie celu, było legalne. Elementem tych obowiązków jest ocena, czy cel przetwarzania nie narusza praw osób udostępniających swoje dane, ale w sytuacjach ocennych – gdy nie jest wiadomo, czy przetwarzanie narusza owe prawa i gdy cel przetwarzania nie jest wprost zabroniony przez prawo – to administrator danych decydować będzie czy, w jego ocenie, ryzyko jest akceptowalne.

W tym ujęciu zupełnie inaczej wygląda pozycja organów publicznych i podmiotów prywatnych. Te pierwsze, w polskim porządku prawnym (i większości systemów zachodnich) działać mogą wyłącznie na podstawie i w granicach prawa (Niewiadomski, 2010; Waldron, 2021). Nie wybierają zatem celów przetwarzania samodzielnie, a raczej dostrzegają konieczność przetwarzania dla realizacji zadań i kompetencji wynikających z przepisów prawa, ustaw i rozporządzeń, samych podlegających kontroli politycznej i konstytucyjnej (Jabłońska, 2020; Matczak, 2010; Sadurski, 2002). RODO przewiduje dla takich sytuacji osobną przesłankę legalizującą[48]. Tym samym szkoła,

[42] Artykuł 9 RODO.
[43] Artykuł 12–23 RODO.
[44] Artykuł 24–39 RODO.
[45] Artykuł 40–43 RODO.
[46] Artykuł 51–84 RODO.
[47] Artykuł 44–50 RODO.
[48] Artykuł 6 ust. 1 lit. e) RODO.

komisariat policji czy urząd skarbowy zbierają dane w celach wskazanych przez ustawodawcę, w podlegających kontroli przepisach i mają niewielką – jeśli jakąkolwiek – swobodę w wyborze celów. Jeśli organ podatkowy, zebrawszy dane na potrzeby rozliczeń podatkowych, użyje ich by reklamować książkę swego kierownika, przekroczy swoje kompetencje (Matczak, 2010). Naruszy nie tylko RODO, lecz także cały szereg przepisów administracyjnych wskazujących co owemu organowi wolno czynić na podstawie i w granicach prawa. Nie wolno mu tego zrobić, ponieważ wolno mu zrobić tylko to, do czego prawo daje mu kompetencje. Trafnie w swym komentarzu ujął to Paweł Fajgielski (2018, s. 147) pisząc: „W przypadku podmiotów publicznych cele przetwarzania danych powinny być określone w przepisach prawa, co wynika z zasady legalności działań administracji publicznej, natomiast w przypadku podmiotów prywatnych (np. przedsiębiorców), oprócz realizacji celów określonych przepisami, administratorzy mogą sami wyznaczać dodatkowe cele przetwarzania danych (np. cele marketingowe)".

Odwrotnie sytuacja przedstawia się z podmiotami prywatnymi, które w polskim porządku prawnym działają nie na podstawie prawnie wskazanych kompetencji, a na podstawie zasady autonomii woli (Safjan, 2012, s. 329–339). Przedsiębiorca może robić wszystko, czego prawo mu nie zakazuje, tak długo, jak działa w ramach istniejących procedur, przepisów prawa materialnego i z poszanowaniem praw innych osób (Safjan, 2012). W tym ujęciu sam wybiera cele, jakie realizuje oraz sposoby ich osiągnięcia. Jeśli zatem przedsiębiorca chce zebrać i wykorzystać dane osobowe w celu skłonienia użytkowników do spędzania jak najwięcej czasu na mojej platformie, oraz personalizowania reklam, by zwiększyć szansę zakupu, musi:

(1) mieć pewność, że te cele nie są niezgodne z prawem (w tym nie godzą w prawa innych osób);
(2) dobrze opisać te cele i wskazać, dlaczego przetwarzanie konkretnych danych jest konieczne do ich realizacji;
(3) zabezpieczyć przesłanki legalizujące, np. konieczność do realizacji umowy;
(4) poinformować w sposób przejrzysty swoich użytkowników.

Jeśli przedsiębiorca spełni te wymogi, może dane zbierać i wykorzystywać. RODO czyni jego pracę trudniejszą, bardziej kosztowną, ale – co do zasady – nie ogranicza katalogu celów, jakie wolno mu realizować. Owszem, jak wskazano powyżej, przedsiębiorca musi dokonać oceny ryzyka, jakie niesie ze sobą przetwarzanie. Ta ocena może, w teorii, podlegać kontroli organu nadzorczego. Jednakże tak długo, jak kontrola ta nie nastąpi decyzja należy do przedsiębiorcy. Co więcej, jak wykazywano w literaturze empirycznej na temat praktyki wdrażania RODO w przedsiębiorstwach, podmioty prywatne dysponujące znacznymi środkami są w stanie tak sporządzić dokumentacje i ująć swoje analizy ryzyka, by wykazać, że niczyje prawa nie są zagrożone (Waldman, 2021).

III. Logika rynku

W świetle powyższych rozważań należy zwrócić uwagę na dwa miejsca, gdzie RODO nie zgadza się z logiką rynkową. Po pierwsze, przy braku regulacji konkretnych, poszczególnych celów przetwarzania prawem powszechnie obowiązującym, decyzja dotycząca dopuszczalności celów przetwarzania formalnie należy do osoby udostępniającej swoje dane, a realnie podejmowana jest przez administratora, który sam przeprowadza analizę ryzyka. Po drugie, nawet przy bardzo

protekcjonistycznym podejściu do pozycji osób, których dane dotyczą – w hipotetycznym świecie, w którym organy nadzorcze mają środki by każdorazowo poddawać ocenę ryzyka dokonaną przez administratora – szybko daje się zauważyć konflikt, pomiędzy dążeniem do minimalizacji danych a próbą osiągnięcia „informacji doskonałej".

1. Co nie jest zakazane, jest dozwolone

Sednem logiki rynkowej jest swoboda gospodarcza i swoboda umów (Niedośpiał, 2012; Sikorska-Lewandowska, 2019). Co do zasady przedsiębiorcom i konsumentom wolno robić wszystko, czego prawo im nie zabrania lub co nie godzi w prawa i wolności innych osób. W gospodarce regulowanej, jaką jest obecna gospodarka w Polsce i Unii Europejskiej, sytuacja jest bardziej skomplikowana. Na przykład, by wykonywać zawód regulowany (taki jak lekarz czy adwokat) należy zyskać odpowiednie kwalifikacje. By wprowadzać na rynek produkty konsumenckie, należy mieć na uwadze różne standardy (Nottage, 2018). Można jednak regulację rozumieć jako zestaw nakazów i zakazów „granicznych" (określających co podmioty prywatne muszą, a czego nie wolno im robić), w obrębie których to granic mają swobodę świadczenia i korzystania z usług.

W gospodarce cyfrowej, począwszy od lat 90. XX wieku, regulacji było stosunkowo niewiele (Cohen, 2019). Nawet obecna, szeroko zakrojona działalność legislacyjna Unii Europejskiej, nie wprowadza zbyt wielu zakazów, gdzie wyjątkiem mogą być trzy niedopuszczalne praktyki sztucznej inteligencji (Veale i Borgesius, 2021) lub, w niewielkim zakresie, tzw. *dark patterns* (Luguri i Strahilevitz, 2021). Niemniej zasadą jest wolność projektowania usług i modeli biznesowych, co sprzyjać miało innowacji (Ranchordas, 2014).

W pewnym sensie ten cel leseferystycznego podejścia – szeroko zakrojona innowacja – został osiągnięty. W artykułach dotyczących regulacji technologii z lat 90. czy wczesnych lat 2000., łatwo można zauważyć, że w zasadzie nikt nie przewidział powstania produktów, które dziś wydają nam się niezmiernie istotne: mediów społecznościowych, takich jak Facebook, platform streamingowych, takich jak YouTube, Spotify czy Netflix, serwisów randkowych, takich jak Tinder, czy platform tzw. *sharing economy,* jak Uber czy Airbnb. Co więcej, warto zauważyć – choć dziś niemodnym jest zwracać na to uwagę – że model biznesowy wielu z tych platform jest niezwykle egalitarny. Przy wszystkich mankamentach „kapitalizmu inwigilacji" – zagrożeniom dla prywatności, autonomii czy zdrowia psychicznego (Mik, 2016; Trzaskowski, 2021) – fakt, że każdy kto tylko ma dostęp do urządzenia połączonego z internetem może „za darmo" korzystać z wyszukiwarki, takiej jak Google (dającej dostęp do niemalże całej wiedzy zagregowanej przez ludzkość) czy narzędzi do komunikacji, takich jak Facebook (pozwalających, co do zasady, rozmawiać i koordynować działania z ludźmi na całym świcie) jest imponujący.

Stan ten udało się osiągnąć m.in. dlatego, że swoboda działalności gospodarczej i swoboda umów dotyczy nie tylko wolności w konstruowaniu usług (co wolno świadczyć przedsiębiorcom), lecz także wolności w konstruowaniu nowych modeli biznesowych (jak konsumentom wolno płacić za te usługi). Pojawiły się więc strategie oparte nie na pobieraniu płatności od konsumentów, lecz na zbieraniu ich danych i wykorzystywaniu tych danych do personalizacji reklam (Hwang, 2020). To reklamodawcy, nie konsumenci, płacą firmom takim jak Meta i Alphabet za to, że konsument korzysta z Facebooka lub Google'a. Ten model biznesowy został pośrednio zalegalizowany przez dyrektywę o treściach cyfrowych, wskazującą zakres swego stosowania również do umów, w których

„przedsiębiorca dostarcza lub zobowiązuje się dostarczyć konsumentowi treści cyfrowe lub usługę cyfrową, a konsument dostarcza lub zobowiązuje się dostarczyć przedsiębiorcy dane osobowe”[49].

Jaką rolę, w tym stanie rzeczy, odgrywa RODO? Rozporządzenie nie wypowiada się na temat tego, czy przedsiębiorcom wolno świadczyć usługi w zamian za dane osobowe użyte do personalizacji treści. RODO nakazuje jedynie spełnić szereg obowiązków w tym procesie. Ostatecznie jednak – w logice rynkowej – decyzja o tym, czy wolno zbierać dane konieczne do personalizacji reklam, należy do przedsiębiorcy (który musi ocenić czy nie wiąże się to z ryzykiem naruszenia praw osób, których dane dotyczą oraz konsumenta (tak długo jak przetwarzanie jest zgodne z prawem)). Nie zawsze będzie to „zgoda” rozumiana jako przesłanka legalizująca z art. 6; czasami będziemy mieć do czynienia z koniecznością wykonania umowy lub z uzasadnionym interesem administratora. Ostateczne słowo należy jednak, na papierze, do konsumenta.

Według RODO sytuacja ta powinna wyglądać następująco. Zanim konsument rozpocznie korzystanie z usługi, takiej jak Facebook, musi mieć możliwość zapoznania się z regulaminem i polityką prywatności[50]. Tam przedsiębiorca wyjaśnia, jakie dane będzie wykorzystywał, w jaki sposób i w jakim celu. Nie może wykorzystać więcej danych niż konieczne, ale ma swobodę w takim opisie celu, by konieczna do jego realizacji była znacząca liczba danych. Jeśli konsument na taki układ się godzi, wolno dane przetwarzać dopóty, dopóki sam cel nie jest niezgodny z prawem. Oczywiście, w tym procesie przedsiębiorca może naruszyć RODO, jeśli np. niewystarczająco jasno opisze swoje praktyki dotyczące danych (naruszając obowiązek informacyjny) lub będzie przetwarzał dane w sposób, którego nie zakomunikował konsumentowi. Jeśli jednak wystarczająco dobrze opisze swoje praktyki, w tym przeprowadzi ocenę ryzyka w przekonujący sposób, wewnętrznie i zewnętrznie, wolno mu robić wszystko, co konsument zaakceptuje.

W praktyce sytuacja formalnej decyzyjności konsumenta często oznacza, że „prawodawcą” jest tu przedsiębiorca (Sobczyk, 2019). Szereg badań empirycznych wykazuje, że konsumenci nie czytają polityk prywatności ani regulaminów, nawet jeśli zaznaczają pole, że to zrobili (Bakos i in., 2014; Obar i Oeldorf-Hirsch, 2018). Trudno jednak mieć o to pretensje do przedsiębiorców (którzy wszak spełniają obowiązek informacyjny) i do konsumentów (którzy, zajęci codziennymi sprawami, nie mają czasu tego wszystkiego czytać). W badaniach sprzed kilkunastu lat policzono, że przeczytanie wszystkich polityk prywatności usług i stron, z których korzysta konsument, zajęłoby mu pond 300 godzin rocznie (McDonald i Cranor, 2008). Biorąc pod uwagę coraz szersze korzystanie z technologii można założyć, że dziś byłoby to jeszcze więcej. Dodatkowo badania empiryczne dotyczące m.in. sposobów przeprowadzania oceny ryzyka przez przedsiębiorców wykazują, że są oni w stanie zainwestować znaczne środki w wygenerowanie opinii i analiz (tworzonych przez profesjonalne kancelarie i firmy consultingowe) zawierających skomplikowaną argumentację wykazującą, że ich cele przetwarzania nie tylko nie godzą w prawa osób, których dane dotyczą, ale wręcz te interesy realizują (Waldman, 2021).

Mamy więc do czynienia z sytuacją, w której o legalności celów przetwarzania, a więc i legalności potencjalnych negatywnych skutków przetwarzania, formalnie decyduje konsument, który realnie nie czyta na co się zgadza, a często tak naprawdę nie ma prawdziwego wyboru (Solove,

[49] Artykuł 3 ust. 1 dyrektywa Parlamentu Europejskiego i Rady 2019/770 z 20.05.2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz. Urz. L 136/1).

[50] Artykuł 12–14 RODO.

2012). Organ nadzorczy, badający czy Meta lub Alphabet narusza RODO, sprawdzi czy dochowano obowiązku informacyjnego, czy zachowana jest zasada ograniczenia przetwarzania itd., ale oprze się o decyzję konsumenta, jeśli chodzi o legalność samego celu przetwarzania. Tu decyzję prawodawca pozostawił mechanizmom rynkowym (tak długo, jak cel przetwarzania wprost nie narusza prawa ani wprost nie godzi w prawa osób udostępniających swoje dane). Tym samym, jeśli tylko administratorzy wystarczająco dobrze wykonają wewnętrzną i zewnętrzną dokumentację, okazać się może, że wiele elementów „kapitalizmu inwigilacji" nie jest sprzecznych z przepisami RODO, ale przeciwnie – jest zalegalizowanych przez RODO w połączeniu z decyzją konsumenta.

2. Konkurencja doskonała i pełnia informacji o preferencjach

W teorii ekonomii kapitalizmu istnieje pojęcie tzw. konkurencji doskonałej (Gretsky i in., 1997; Stigler, 1957). Jest to wyidealizowany konstrukt, którego nie uda się nigdy w praktyce zrealizować, ale który – jako cel regulacyjny – wpływa na działania prawodawcy chcącego jak najbardziej zbliżyć świat realny do tego celu idealnego (Varian, 2009). Elementem „konkurencji doskonałej" (zakładającej m.in. niski koszt wejścia i wyjścia z rynku, brak monopoli itd.) jest założenie „informacji doskonałej" (Samet, 1996). W tym założeniu każdy konsument miałby pełnię informacji o dostępnych dobrach i usługach, a każdy przedsiębiorca – pełnię informacji o dostępnych środkach produkcji oraz o preferencjach wszystkich konsumentów.

Pierwszy element bezpośrednio przełożył się na wiele regulacji, których celem jest zapewnienie konsumentom dostępu do informacji. Z jednej strony, ustawodawca wprowadza listę obowiązków informacyjnych (Ben-Shahar i Schneider, 2014; Namysłowska i Jabłonowska, 2019; Wagner i Walker, 2019) mających przeciwdziałać asymetrii informacji między przedsiębiorcami a konsumentami (Akerlof, 1970). Z drugiej – mnogość przepisów jest źródłem m.in. zakazów wprowadzania do obrotu informacji nieprawdziwych czy wprowadzających w błąd, wyrażonych w przepisach dotyczących tzw. nieuczciwych praktyk rynkowych (Boom i Garde, 2016; Herrine, 2021; Howells i in., 2016). Celem tych regulacji jest, by konsument jak najlepiej orientował się w wyborach dostępnych na rynku.

Drugi element, mniej oczywisty, dotyczy właśnie dostępu przedsiębiorców do informacji o preferencjach konsumentów. Co do zasady prawo prywatne nie zabrania ani zbierania danych o potrzebach konsumentów, ani działania w oparciu o te dane. Przeciwnie, poprzez brak wprowadzenia jakiejkolwiek „własności" informacji (Cofone, 2021) zachęca przedsiębiorców do badań rynku, obserwacji i innowacji. Ciekawe, acz wykraczającym poza ramy niniejszego artykułu, byłoby pytanie, czy w porządku prawnym, w którym nie ma prawa ochrony danych osobowych (RODO, wcześniej dyrektywa 96/46) istniałby prywatnoprawny wymóg uzyskania zgody konsumenta na zbieranie i wykorzystywanie danych go dotyczących w celach marketingu internetowego.

To właśnie tutaj RODO, z zasadami ograniczenia przetwarzania i minimalizacji danych, idzie wbrew logice rynkowej, według której przedsiębiorca nie tylko może, lecz także powinien dążyć do zdobycia wiedzy o preferencjach konsumentów i wykorzystania jej w decyzjach dotyczących produkcji i marketingu. Szeroki dostęp do tej wiedzy, wynikający z technologicznej możliwości śledzenia poczynań użytkowników usług internetowych, stał się spełnieniem marzeń ekonomistów próbujących zbliżyć nas do konkurencji doskonałej (Mayer-Schönberger i Ramge, 2018). Tym samym organ nadzorczy zabraniający korporacjom zbierania danych – nawet pomimo faktu, że

konsument na takie zbieranie się zgodził, a przetwarzanie nie jest wprost niezgodne z prawem obowiązującym lub nie godzi w sposób oczywisty w prawa osób, których dane dotyczą – szedłby wbrew zarówno interesom graczy rynkowych, jak i głęboko zakorzenionym zasadom kapitalistycznego ustroju społeczno-gospodarczego.

Czy to oznacza, że w gospodarce rynkowej konsumenci skazani są na życie w „kapitalizmie inwigilacji", a ich prawo do prywatności jest immanentnie zagrożone? Bynajmniej. Jednakże to nie bardziej agresywna egzekucja RODO, a konkretna (nowa) regulacja jest ścieżką wyjścia z tego problemu.

IV. Możliwe ścieżki reformy

RODO w połączeniu z logiką rynkową (swoboda umów i dążenie do informacji doskonałej) i realiami rynkowymi (wielu quasi-monopolistycznych graczy, konsumenci niemający czasu ani ochoty studiować polityk prywatności) doprowadziły do obecnego stanu rzeczy, w którym to wielkie przedsiębiorstwa faktycznie decydują o dopuszczalności poszczególnych celów przetwarzania. Licząca setki stron dokumentacja sprawia, że ich praktyki często nie są niezgodne z RODO, a wręcz są przez RODO – w połączeniu z decyzjami konsumentów – legalizowane. By wyjść z tego impasu, szanując jednocześnie zarówno prawo podstawowe do ochrony danych (Lynskey, 2014), jak i głęboką logikę gospodarki rynkowej, ustawodawca powinien zadziałać w innym miejscu niż ochrona danych – bezpośrednio wypowiadając się na temat legalności poszczególnych celów przetwarzania. W ostatniej części artykułu na początku zaproponowano normatywny argument za takim rozwiązaniem, a następnie – na kilku przykładach dotyczących szkód ponoszonych przez konsumentów i społeczeństwo w „kapitalizmie inwigilacji" – zaproponowano kilka możliwych podejść legislacyjnych.

1. Efekty zewnętrzne przetwarzania danych osobowych

Najmocniejszy argument przeciwko twardej regulacji celów przetwarzania przez prawodawcę sprowadza się do stwierdzenia, że byłoby to zbyt paternalistyczne podejście do konsumentów. Jeśli konsument, który rozumie możliwe konsekwencje przetwarzania jego danych przez Facebooka, godzi się na nie w zamian za dostęp do usługi, dlaczego państwo miałoby mu tego zabraniać? Istnieją oczywiście argumenty praktyczne, wskazujące że kontrfaktycznym jest założenie o zrozumieniu konsekwencji przez konsumentów, którzy nie mają czasu ani ochoty czytać polityk prywatności (Bakos i in., 2014; McDonald i Cranor, 2008; Obar i Oeldorf-Hirsch, 2018; Solove, 2012). Jednakże, na potrzeby argumentu normatywnego, warto poczynić założenie, że byłoby to możliwe.

By zrozumieć w pełni niesprawiedliwość „kapitalizmu inwigilacji" należy bliżej przyjrzeć się temu, w jaki sposób przedsiębiorcy zbierający i analizujący dane je monetyzują. Istnieje bowiem w publicznym dyskursie mit, zgodnie z którym reklamy, które widzi konkretny konsument są oparte na danych tylko i wyłącznie jego dotyczących. Pojawią się sytuacje, w których jest to prawda. Przykładowo konsument, który szukał pewnej książki w internecie może później zobaczyć reklamę księgarni internetowej z tą książką właśnie. Jednakże znacznie częściej analiza danych ma zupełnie inny charakter.

Dzięki technologiom, takim jak uczenie maszynowe, przedsiębiorcy monetyzujący dane patrzą na nie jako zbiory big data, pozwalające dowiedzieć się czegoś (na poziomie probabilistycznym) o konsumencie, na podstawie danych dotyczących milionów innych konsumentów (Alpaydin, 2016; Igual i Seguí, 2017). Na przykład, konsument korzystający z Facebooka, na którym podaje swoje dane demograficzne oraz śledzi wiele niepozornych stron, może zakomunikować coś na temat swoich poglądów politycznych, religijnych, orientacji seksualnej i ogólnie stylu życia. Jeśli inny konsument, który nigdy nie dzielił się takimi danymi, wskaże podobne dane demograficzne i śledzi te same strony, platforma – patrząc na tego konsumenta przez pryzmat milionów innych użytkowników – jest w stanie oszacować prawdopodobieństwo, że ten inny konsument ma konkretne przekonania i preferencje. Nie musi ich nawet nazywać wprost – religia czy polityka nigdy nie będzie treścią danych bezpośrednio przetwarzanych o danej osobie – wystarczy, że pojawi się informacja „konsument X ma 68% szans bycia zainteresowanym tą reklamą, wyświetloną o tej godzinie, ponieważ tak właśnie zachowują się ludzie o zbliżonym do niego profilu".

W tej sytuacji, udostępniając dane na swój temat konsument pośrednio dostarcza przedsiębiorcy wiedzy na temat tysięcy innych użytkowników, podobnych do niego lub różnych ode niego. Nagle, „zgadzając się" na przetwarzanie dotyczących go danych, konsument wypowiada się nie tylko w swoim imieniu, lecz także tysięcy innych ludzi (Pałka, 2020; Viljoen, 2021).

Szkody wynikające z przetwarzania danych w zbiorach big data mają różnoraki charakter. Badacze wskazują na niebezpieczeństwo manipulacji w sferze rynkowej i politycznej, będącej konsekwencją bardzo dokładnego targetowania treści (Helberger, Dobber i in., 2021; Helberger, Lynskey i in., 2021; Mik, 2016; Susser i in., 2019). Możliwa jest dyskryminacja w wyświetlanych reklamach (Ali i in., 2019; Sweeney, 2013) na poziomie, na którym prawo nie jest w stanie jej przeciwdziałać (Xenidis, 2020). Coraz częściej pojawiają się głosy dotyczące negatywnego wpływu przetwarzania danych na zdrowie psychiczne użytkowników, np. w zakresie uzależnienia wywoływanego spersonalizowanymi treściami (Citron i Solove, 2022; Pałka, 2021; Zakon, 2020). Dopuszczalność sposobów przetwarzania prowadzących do tych szkód wynika obecnie z zagregowanych zgód poszczególnych podmiotów danych, oczywiście tak długo, jak nie jest niezgodna z obowiązującym prawem.

Właśnie to istnienie efektów zewnętrznych jest najmocniejszym argumentem za regulacją poszczególnych celów przetwarzania. Ustawodawca powinien „wyjąć" z rynku działania, którym mechanizm rynkowy – ze względu na swój indywidualistyczny charakter – nie jest w stanie przeciwdziałać. Nie na poziomie prawa ochrony danych, a na poziomie konkretnych regulacji rządzących poszczególnymi sferami życia społeczno-gospodarczego.

2. Ustawowa regulacja konkretnych celów przetwarzania

Przypomnijmy, że zgodnie z art. 5 RODO cel przetwarzania danych musi być zgodny z prawem. Najprostszym i w państwie demokratycznym najbardziej właściwym sposobem ukrócenia „kapitalizmu inwigilacji" jest więc uregulowanie konkretnych celów przetwarzania.

Przykładowo, w stosunku do reklam personalizowanych za pomocą big data prawo konsumenckie mogłoby wprost wypowiedzieć się na temat tego, jak dane zbierane w tym celu mogą być wykorzystywane. Można to uczynić od strony technologii – przyglądając się algorytmom – lub od strony życia społecznego. Za nieuczciwą praktykę rynkową można by uznać nie tylko reklamę

wprowadzającą w błąd, lecz także targetowaną informację wyświetlaną między 22 a 7 rano (gdy konsumenci są zmęczeni), reklamę konkretnego produktu kierowaną do dzieci lub osób starszych itd. Nagle, nawet jeśli konsument zgodzi się na takie a nie inne wykorzystanie danych go dotyczących, zgoda ta nie ma mocy legalizującej, gdyż sam cel jest niezgodny z prawem (konsumenckim, nie prawem ochrony danych). Nie można oczekiwać, by to administrator, w procesie „oceny ryzyka", którą sam przeprowadza, doszedł do takiego wniosku; nie ma potrzeby delegować weryfikacji tej oceny na organ nadzorczy. Prawodawca, mając polityczny mandat i działając w ramach istniejących struktur kontroli konstytucyjnej, może dokonać tej oceny bezpośrednio.

Podobne interwencje można sobie wyobrazić także w stosunku do innych szkód. Przykładowo, podobnie jak prawu konsumenckiemu znane są standardy mające chronić zdrowie fizyczne konsumentów, ustawodawca mógłby wprowadzić standardy dotyczące zdrowia psychicznego. Konsument, który zaakceptuje politykę prywatności, zgodnie z którą dane wykorzystywane będą do uczynienia usługi jak najbardziej angażującą i zachęcającą użytkowników do spędzania jak najwięcej czasu na platformie, nie zalegalizuje już takiej praktyki. Nie będzie mieć również znaczenia fakt, że administrator „ocenił", iż spędzanie dużej ilości czasu na platformie nie godzi w prawa konsumentów, a je realizuje. Taka ocena administratora i taka decyzja konsumenta będą bowiem niezgodne z prawem powszechnie obowiązującym, tak jak nielegalna jest sprzedaż różnych uzależniających substancji psychoaktywnych.

W jaki sposób najlepiej sformułować takie regulacje zależeć będzie od konkretnych okoliczności i celów ustawodawczych. Nie jest celem niniejszego artykułu zgłaszanie takich propozycji. Istotą proponowanego podejścia jest wprowadzenie szeregu interwencji punktowych, w precyzyjny sposób ograniczających swobodę gospodarczą o działania społecznie szkodliwe. Jak w polskim porządku prawnym nie ma jednej ustawy o niedozwolonych reklamach – osobno ustawodawca uregulował komunikaty wprowadzające w błąd, reklamy leków, alkoholu itd. – tak nie ma potrzeby dążyć do wprowadzenia jednej ustawy o wykorzystaniu danych do personalizacji reklam. Przeciwnie, po wielu ogólnych i horyzontalnych aktów, przyszedł czas na interwencje bardzo konkretne.

Właśnie takie podejście – delegalizujące lub regulujące bardzo konkretne cele przetwarzania danych – jest w stanie pogodzić ze sobą indywidualistyczne logiki rynku i RODO, które jednak dążą do przeciwnych celów (pełnej informacji kontra minimalizacji danych). Przedsiębiorcy zachowują swobodę działalności, konsumenci autonomię informacyjną, a jednocześnie publiczny interes – taki jak brak manipulacji, dyskryminacji czy szkód dla zdrowia psychicznego – mógłby być realizowany.

V. Konkluzje

Celem niniejszego artykułu było wykazanie, że szkody ponoszone przez konsumentów i społeczeństwo w systemie „kapitalizmu inwigilacji" nie wynikają przede wszystkim z niewystarczającej egzekucji przepisów RODO, a z faktu, że akt ten nie jest najlepszym narzędziem do przeciwdziałania tego typu szkodom. Problemem nie jest bowiem naruszenie zasad RODO przed administratorów (choć czasami można tak argumentować), a fakt, że rozporządzenie nie wypowiada się na temat dopuszczalności poszczególnych, konkretnych celów przetwarzania. W gospodarce rynkowej przy braku regulacji faktycznie decyzje na temat dopuszczalności celów przetwarzania podejmowane

są przez przedsiębiorców (oczywiście działających w ramach istniejącego porządku prawnego), nawet jeśli formalnie jest to domena konsumentów.

Jednakże, jak wykazano, nawet gdyby konsumenci mieli realne zdolności do oceny skutków przetwarzania danych ich dotyczących, ze względu na istnienie efektów zewnętrznych nie są oni – z normatywnego punktu widzenia – umocowani, by decyzje takie podejmować. Nie jest to również rolą, w państwie demokratycznym, organów nadzorczych. By zachować swobodę gospodarczą i jednocześnie uszanować prawo podstawowe do ochrony danych, ustawodawca powinien wypowiedzieć się na temat dopuszczalności poszczególnych celów przetwarzania.

Bibliografia

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431.

Ali, M., Sapiezynski, P., Bogen, M., Korolova, A., Mislove, A. i Rieke, A. (2019). Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 199:1–199:30. https://doi.org/10.1145/3359301.

Alpaydin, E. (2016). *Machine Learning: The New AI*. The MIT Press.

Andrew, J. i Baker, M. (2021). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*, *168*(3), 565–578. https://doi.org/10.1007/s10551-019-04239-z.

Bakos, Y., Marotta-Wurgler, F. i Trossen, D. R. (2014). Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts. *The Journal of Legal Studies*, *43*(1), 1–35. JSTOR. https://doi.org/10.1086/674424.

Ben-Shahar, O. i Schneider, C. E. (2014). *More Than You Wanted to Know: The Failure of Mandated Disclosure*. Princeton University Press.

Bhargava, V. R. i Velasquez, M. (2021). Ethics of the Attention Economy: The Problem of Social Media Addiction. *Business Ethics Quarterly*, *31*(3), 321–359. https://doi.org/10.1017/beq.2020.32.

Boom, W. van i Garde, A. (2016). *The European Unfair Commercial Practices Directive: Impact, Enforcement Strategies and National Legal Systems*. Routledge. https://doi.org/10.4324/9781315616391.

Breen, S., Ouazzane, K. i Patel, P. (2020). GDPR: Is your consent valid? *Business Information Review*, *37*(1), 19–24. https://doi.org/10.1177/0266382120903254.

Citron, D. i Solove, D. J. (2022). Privacy Harms. *Boston University Law Review*, *102*(3), 793–864.

Cofone, I. (2021). Beyond Data Ownership. *Cardozo Law Review*, *43*, 501.

Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.

Contissa, G., Docter, K., Lagioia, F., Lippi, M., Micklitz, H.-W., Pałka, P., Sartor, G. i Torroni, P. (2018). *CLAUDETTE meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence* [Working Paper]. http://cadmus.eui.eu//handle/1814/60795.

Dunn, P. i Gregorio, G. D. (2022). The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review*, *59*(2). https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\COLA\COLA2022032.pdf.

Fajgielski, P. (2018). *Ogólne Rozporządzenie o ochornione danych osobowych. Ustawa o Ochronie Danych Osobobowych. Komentarz.* Wolters Kluwer Polska.

Gellert, R. (2020). *The Risk-Based Approach to Data Protection*. Oxford University Press.

Gentile, G. i Lynskey, O. (2022). DEFICIENT BY DESIGN? THE TRANSNATIONAL ENFORCEMENT OF THE GDPR. *International & Comparative Law Quarterly*, *71*(4), 799–830. https://doi.org/10.1017/S0020589322000355.

Gretsky, N. E., Ostroy, J. M. i Zame, W. R. (1997). An Application of Measure Theory to Perfect Competition. In *Stochastic processes and functional analysis*. CRC Press.

Hacker, P. (2021). Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law. *European Law Journal*. https://doi.org/10.1111/eulj.12389.

Helberger, N., Dobber, T. i de Vreese, C. (2021). Towards Unfair Political Practices Law: Learning lessons from the regulation of unfair commercial practices for online political advertising. *JIPITEC*, *12*(3). http://www.jipitec.eu/issues/jipitec-12-3-2021/5338.

Helberger, N., Lynskey, O., Micklitz, H.-W., Rott, P., Sax, M. i Strycharz, J. (2021). *EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets.* https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf.

Herrine, L. (2021). The Folklore of Unfairness. *New York University Law Review*, *96*, 431.

Hijmans, H. (2020). Article 1 Subject-matter and objectives. W: C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler (red.), *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press. https://doi.org/10.1093/oso/9780198826491.003.0003.

Howells, G., Micklitz, H.-W. i Wilhelmsson, T. (2016). *European Fair Trading Law: The Unfair Commercial Practices Directive*. Routledge. https://doi.org/10.4324/9781315580890.

Hwang, T. (2020). *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*. FSG Originals.

ICCL. (2022). *The Biggest Data Breach: ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe*. https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/.

Igual, L. i Seguí, S. (2017). *Introduction to Data Science*. Springer International Publishing. https://doi.org/10.1007/978-3-319-50017-1.

Jabłońska, P. (2020). Konstytucyjne podstawy rozproszonej kontroli konstytucyjności prawa. *Przegląd Sądowy*, *11–12*. https://ruj.uj.edu.pl/xmlui/handle/item/300970.

Kamara, I. i De Hert, P. (2018). Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach. W: E. Selinger, J. Polonetsky, O. Tene (red.), *Cambridge Handbook of Consumer Privacy* (pp. 321–352). Cambridge University Press.

Krasuski, A. (2018). *Ochrona danych osobowych na podstawie RODO*. Wolters Kluwer Polska.

Krasuski, A. i Siembida, P. (2022). *Analiza ryzyka w ochronie danych osobowych*. Wolters Kluwer Polska.

Liepiņa, R., Contissa, G., Drazewski, K., Lagioia, F., Lippi, M., Micklitz, H., Pałka, P., Sartor, G. i Torroni, P. (2019). GDPR Privacy Policies in CLAUDETTE: Challenges of Omission, Context and Multilingualism. *Proceedings of the Third Workshop on Automated Semantic Analysis of Information in Legal Text (ASAIL 2019)*, 7. http://ceur-ws.org/Vol-2385/paper9.pdf.

Litwiński, P., Barta, P. i Kawecki, M. (2018). *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz* (P. Litwiński, red.). C.H. Beck.

Luguri, J. i Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, *13*(1), 43–109. https://doi.org/10.1093/jla/laaa006.

Lynskey, O. (2014). Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order. *International & Comparative Law Quarterly*, *63*(3), 569–597. https://doi.org/10.1017/S0020589314000244.

Matczak, M. (2010). Kompetencja w prawie administracyjnym. W: R. Hauser, Z. Niewiadomski, A. Wróbel, *System Prawa Admistracyjnego. Tom I. Instytucje Prawa Adminsitracyjnego.* C.H. Beck.

Mayer-Schönberger, V. i Ramge, T. (2018). *Reinventing Capitalism in the Age of Big Data*. Basic Books.

McDonald, A. M. i Cranor, L. F. (2008). The Cost of Reading Privacy Policies 2008 Privacy Year in Review. *I/S: A Journal of Law and Policy for the Information Society*, *4*(3), 543–568.

Mik, E. (2016). The erosion of autonomy in online consumer transactions. *Law, Innovation and Technology*, *8*(1), 1–38. https://doi.org/10.1080/17579961.2016.1161893.

Namysłowska, M. i Jabłonowska, A. (2019). Information Obligations and Disinformation of Consumers: Polish Law Report. W: G. Straetmans (red.), *Information Obligations and Disinformation of Consumers* (ss. 301–337). Springer International Publishing. https://doi.org/10.1007/978-3-030-18054-6_8.

Niedośpiał, M. (2012). *Swoboda umów: Synteza*. Warszawa. https://ruj.uj.edu.pl/xmlui/handle/item/80675.

Niewiadomski, Z. (2010). Pojęcie administracji publicznej. W: R. Hauser, Z. Niewiadomski, A. Wróbel, *System Prawa Admistracyjnego. Tom I. Instytucje Prawa Adminsitracyjnego.* C.H. Beck.

Nottage, L. (2018). Product safety regulation. *Handbook of Research on International Consumer Law, Second Edition*. Pozyskano z: https://www.elgaronline.com/view/edcoll/9781785368202/9781785368202.00015.xml.

Obar, J. A. i Oeldorf-Hirsch, A. (2018). The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870.

Padden, M. i Öjehag-Pettersson, A. (2021). Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR). *Critical Policy Studies*, *15*(4), 486–503. https://doi.org/10.1080/19460171.2021.1927776.

Pałka, P. (2020). Data Management Law for the 2020s: The Lost Origins and the New Needs. *Buffalo Law Review*, *68*(2), 559–640.

Pałka, P. (2021). The World of Fifty (Interoperable) Facebooks. *Seton Hall Law Review*. https://doi.org/10.2139/ssrn.3539792.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176.

Ranchordas, S. (2014). Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation Symposium – Governance of Emerging Technologies: Law, Policy, and Ethics. *Jurimetrics*, *55*(2), 201–224.

Sadurski, W. (2002). Judicial Review and the Protection of Constitutional Rights. *Oxford Journal of Legal Studies*, *22*(2), 275–299. https://doi.org/10.1093/ojls/22.2.275.

Safjan, M. (2012). Zasady prawa prywatnego. In M. Safjan, *System Prawa Prywatnego. Tom 1. Prawo cywilne – Część ogólna* (2nd ed.). C.H. Beck.

Samet, D. (1996). Hypothetical Knowledge and Games with Perfect Information. *Games and Economic Behavior*, *17*(2), 230–251. https://doi.org/10.1006/game.1996.0104.

Sikorska-Lewandowska, A. (2019). Zasady prowadzenia działalności gospodarczej w świetle ustawy – Prawo przedsiębiorców. *Przegląd Prawa Handlowego*, (1), 52–58.

Sobczyk, A. (2019). *RODO. Rozproszona władza publiczna*. Wydawnictwo Uniwersytetu Jagiellońskiego.

Solove, D. J. (2012). Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*(7), 1880–1903.

Solove, D. J. i Schwartz, P. M. (2018). *Information Privacy Law* (6th ed.). Wolters Kluwer Law & Business.

Stigler, G. J. (1957). Perfect Competition, Historically Contemplated. *Journal of Political Economy*, *65*(1), 1–17.

Susser, D., Roessler, B., Nissenbaum, H. (2019). Online Manipulation: Hidden Influences in a Digital World. *Georgetown Law Technology Review*, *4*, 1–45.

Sweeney, L. (2013). Discrimination in Online Ad Delivery. *ArXiv:1301.6822 [Cs]*. http://arxiv.org/abs/1301.6822.

Tamò-Larrieux, A. (2018). *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things* (1st ed. 2018 edition). Springer.

Trzaskowski, J. (2021). *Your Privacy Is Important to Us! – Restoring Human Dignity in Data-Driven Marketing*. ExTuto.

Trzaskowski, J. (2022). Data-driven value extraction and human well-being under EU law. *Electronic Markets*. https://doi.org/10.1007/s12525-022-00528-0.

Varian, H. R. (2009). *Intermediate Microeconomics: A Modern Approach* (Eighth edition). W. W. Norton & Company.

Veale, M. i Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402.

Viljoen, S. (2021). A Relational Theory of Data Governance. *Yale Law Journal*, *131*, 573.

Wagner, W. i Walker, W. (2019). *Incomprehensible!: A Study of How Our Legal System Encourages Incomprehensibility, Why It Matters, and What We Can Do About It*. Cambridge University Press. https://doi.org/10.1017/9781139051774.

Waldman, A. (2020). Data Protection by Design? A Critique of Article 25 of the GDPR. *Cornell International Law Journal*, *53*(1), i–168.

Waldman, A. E. (2021). *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. Cambridge University Press.

Waldron, J. (2021). The rule of law and the role of courts. *Global Constitutionalism*, *10*(1), 91–105. https://doi.org/10.1017/S2045381720000283.

Witkowska-Nowakowska, K. (2018). Zasady przetwarzania. W: D. Lubasz, *RODO dla małych i średnich przedsiębiorstw*. Wolters Kluwer.

Xenidis, R. (2020). Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. *Maastricht Journal of European and Comparative Law*, *27*(6), 736–758. https://doi.org/10.1177/1023263X20982173.

Zakon, A. (2020). Optimized for Addiction: Extending Product Liability Concepts to Defectively Designed Social Media Algorithms and Overcoming the Communications Decency Act. *Wisconsin Law Review*, *2020*, 1107.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (First edition). PublicAffairs.