

P
ME

3/2018

PRAWO

Mediów Elektronicznych

Badania kliniczne w świetle RODO

*Natalia Kalinowska, Bartłomiej Oręziak,
Marek Świerczyński*

Bezprawny dowód z korespondencji internetowej stron
w postępowaniu cywilnym

Błażej Gadek

Postanowienia dotyczące dziedziczenia profilu zawarte
w regulaminie portalu Facebook a prawo polskie

Patrycja Budrewicz

Prawnie uzasadnione interesy jako podstawa
przetwarzania danych *online*

Michał Czerniawski

Adjusting to change: how communication in mediation
is moving into digital environment in e-MEDIATION

Raya Tsvetkova, Sofia Nenova

Recenzja monografii: *Filip Radoniewicz*, Odpowiedzialność
karna za hacking i inne przestępstwa przeciwko
danym komputerowym i systemom informatycznym,
Warszawa 2016

dr Piotr Siemkowicz

RADA PROGRAMOWA:

r.pr. Włodzimierz Chróścik
SNSA Jacek Czaja
adw. Rafał Dębowski
prof. Włodzimierz Gromski
prof. Ryszard Jaworski
adw. Xawery Konarski
prof. Michele Angelo Lupoi
prof. dr hab. Jacek Mazurkiewicz
prof. Vytautas Nekrošius
dr Grzegorz Sibiga
prof. Grażyna Szpor
prof. Andreas Wiebe
dr Wojciech Wiewiórowski
prof. Krzysztof Wójtowicz

www.ksiegarnia.beck.pl



Cena 65 zł (w tym 5% VAT)



P ME

3/2018

Redakcja Kwartalnika Naukowego Prawo Mediów Elektronicznych

Redaktor naczelny: prof. dr hab. *Jacek Gołaczyński*, UWr
Sekretarz redakcji dr hab. prof. nadzw. UOp *Dariusz Szostek*
Członek redakcji dr hab. prof. nadzw. UOp *Piotr Stec*
Członek redakcji dr hab. *Marek Leśniak*, UWr
Członek redakcji dr *Aleksandra Klich*, USz

Rada programowa:

r.pr. *Włodzimierz Chróścik*
sędzia *Jacek Czaja*, NSA
adw. *Rafał Dębowski*
dr hab. prof. nadzw. UWr *Włodzimierz Gromski* (przewodniczący)
prof. dr hab. *Ryszard Jaworski*, UWr
adw. *Xawery Konarski*
prof. *Avv. Michele Angelo Lupoi*, Uniwersytet Boloński
prof. dr hab. *Jacek Mazurkiewicz*
prof. habil. dr *Vytautas Nekrošius*, Uniwersytet Wileński
dr *Grzegorz Sibiga*, INP PAN
dr hab. prof. nadzw. UKSW *Grażyna Szpor*
prof. dr *Andreas Wiebe*, University of Goettingen
dr *Wojciech Wiewiórowski*, UG
prof. dr hab. *Krzysztof Wójtowicz*, UWr

Recenzenci:

dr hab. prof. nadzw. UMK *Andrzej Adamski*
prof. *Zsolt Balogh*, Uniwersytet Corvinus Budapeszt
dr hab. prof. UŁ *Sławomir Cieślak*
dr hab. prof. nadzw. *Kinga Flaga-Gieruszyńska*, USz
prof. dr hab. *Jacek Górecki*, UŚ w Katowicach
prof. em. dr *Wolfgang Kilian*, University of Hannover
dr hab. prof. nadzw. UJ *Ryszard Markiewicz*
dr hab. *Marek Świerczyński*, UKSW
prof. *Richard Warner* Ph.D, Chicago – Kent College of Law
dr hab. prof. nadz. UŚ *Kazimierz Zgryzek*

Adres redakcji:

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych
Komunikacji Elektronicznej
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: pme@beck.pl



Wydawca:

Wydawnictwo C.H. Beck
ul. Bonifraterska 17
00-203 Warszawa

tel.: 22 33 77 600
fax: 22 33 77 602
www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Badania kliniczne w świetle RODO <i>Natalia Kalinowska, Bartłomiej Oręziak, Marek Świerczyński</i>	4
Bezprawny dowód z korespondencji internetowej stron w postępowaniu cywilnym <i>Błażej Gadek</i>	16
Postanowienia dotyczące dziedziczenia profilu zawarte w regulaminie portalu Facebook a prawo polskie <i>Patrycja Budrewicz</i>	24
Prawnie uzasadnione interesy jako podstawa przetwarzania danych online <i>Michał Czerniawski</i>	33
Adjusting to change: how communication in mediation is moving into digital environment in e-MEDIATION <i>Raya Tsvetkova, Sofia Nenova</i>	38
Recenzja monografii: <i>Filip Radoniewicz, Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warszawa 2016</i> <i>dr Piotr Siemkiewicz</i>	42

Contents

Clinical trials in the light of GDPR <i>Natalia Kalinowska, Bartłomiej Oręziak, Marek Świerczyński</i>	4
Unlawful evidence from the Internet correspondence of parties in civil proceedings <i>Błażej Gadek</i>	16
Regulations in regard to inheriting profile which are included on Facebook in the context of Polish law <i>Patrycja Budrewicz</i>	24
Legitimate interests as a basis for online data processing <i>Michał Czerniawski</i>	33
Adjusting to change: how communication in mediation is moving into digital environment in e-MEDIATION <i>Raya Tsvetkova, Sofia Nenova</i>	38
Monograph review: <i>Filip Radoniewicz, Criminal liability for hacking and other crimes against computer data and information systems, Warsaw 2016</i> <i>dr Piotr Siemkiewicz</i>	42



Szanowni Państwo,

z przyjemnością przedstawiam trzeci w 2018 r. numer kwartalnika naukowego Prawo Mediów Elektronicznych. Tradycyjnie został on poświęcony problematyce prawnej związanej z prawem nowych technologii. W bieżącym numerze znajdziecie Państwo artykuły dotyczące: ochrony danych osobowych w ramach badań klinicznych – *Natalii Kalinowskiej*, *Bartłomieja Oręziaka* i *Marka Świerczyńskiego*; dopuszczalności w procesie cywilnym dowodu bezprawnie uzyskanego z korespondencji internetowej – *Błażeja Gadka*; postanowień portalu Facebook o dziedziczeniu treści cyfrowych w kontekście prawa polskiego – *Patrycji Budrewicz* oraz recenzję monografii *Filipa Radoniewicza* pt. *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, *Piotra Siemkowicza*.

Zapraszam do publikacji w ramach Prawa Mediów Elektronicznych oraz do kontaktu z nami pod adresem: pme@beck.pl.

Z poważaniem
prof. dr hab. *Jacek Gołaczyński*

Badania kliniczne w świetle RODO

Natalia Kalinowska¹

Bartłomiej Oręziak²

Marek Świerczyński³

Stosowane w praktyce modele ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych w badaniach klinicznych budzą wiele wątpliwości prawnych. Kwestia ta wymaga wyjaśnienia w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE⁴. W niniejszej publikacji autorzy podejmują próbę uzasadnienia interpretacji przepisów RODO ułatwiającej prowadzenie badań klinicznych w Polsce⁵. Zwracają przy tym uwagę na problematykę profilowania uczestników badań klinicznych oraz badaczy i innych członków zespołu badawczego, ponieważ jest to jedno z zagadnień budzących obecnie najwięcej problemów praktycznych.

Uwagi wstępne

Mimo że w rozporządzeniu Parlamentu Europejskiego i Rady (UE) Nr 536/2014 z 16.4.2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE⁶ nie określono szczególnych zasad przetwarzania danych osobowych uczestników badań, to w art. 93 wskazano, że do przetwarzania danych osobowych, które odbywa się na podstawie tego rozporządzenia, stosuje się przepisy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych⁷. Natomiast zgodnie z art. 94 RODO, wszelkie odesłania do uchylonej dyrektywy należy traktować jako odesłania do RODO. Oznacza to, że przetwarzanie danych osobowych na podstawie rozporządzenia 536/2014 powinno w pełni odpowiadać wymogom wskazanym w RODO. Na tle art. 94 ust. 2 zd. 1 RODO pojawia się natomiast wątpliwość, jak traktować odesłania nie do całej treści dyrektywy 95/46/WE, lecz do poszczególnych jej przepisów⁸. W doktrynie niemieckiej⁹ zaproponowane zostały dwie możliwości wykładni:

- przyjęcie, że takie odesłania należy uznawać za nieistniejące, albo
- poszukiwanie przepisu RODO, który reguluje to samo zagadnienie co wskazany w odesłaniu przepis dyrektywy 95/46/WE.

W naszej ocenie należy podzielić ten drugi pogląd. W świetle art. 93 rozporządzenia UE o badaniach klinicznych należy zauważyć, że nowe przepisy mają wzmacniać prawa osób, których dane dotyczą. Prawa te obejmują prawo dostępu do danych, do ich poprawiania i wycofywania. W rozporządzeniu podkreślono jednak, że pewne ograniczenie tych praw jest niezbędne. Konieczne jest bowiem zapewnienie równowagi pomiędzy wiarygodnością danych z badań klinicznych wykorzystywanych do celów naukowych, jak też bezpieczeństwem

uczestników badań klinicznych. Jednym z kluczowych rozwiązań przyjętych w ww. rozporządzeniu jest zastrzeżenie, że wycofanie świadomej zgody nie może mieć wpływu na wyniki przeprowadzonych już działań, takich jak przechowywanie i wykorzystywanie danych uzyskanych na podstawie świadomej zgody przed wycofaniem. Stosowanie RODO w badaniach klinicznych wymaga więc uwzględnienia powyższej zasady zachowania równowagi pomiędzy wiarygodnością danych

¹ Autorka jest doktorantką w Katedrze Prawa Cywilnego i Prawa Prywatnego Międzynarodowego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

² Autor jest doktorantem w Katedrze Ochrony Praw Człowieka i Prawa Międzynarodowego Humanitarnego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

³ Autor jest profesorem w Katedrze Prawa Cywilnego i Prawa Prywatnego Międzynarodowego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

⁴ Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

⁵ Problemy ze stosowaniem przepisów o danych osobowych do badań klinicznych były wielokrotnie podnoszone w doktrynie, zob. m.in.: K. Forysiak, P. Zięcik, [w:] T. Brodniewicz (red.), *Badania kliniczne*, Warszawa 2015, s. 300–302; R. Stankiewicz, [w:] R. Stankiewicz (red.), *Instytucje rynku farmaceutycznego*, s. 99. Nie ulega wątpliwości, że archaiczna i często błędnie stosowana regulacja o ochronie danych osobowych w badaniach klinicznych stanowiła jedną z istotnych barier dla rozwoju badań klinicznych w Polsce. Mowa tutaj o przepisach ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm. – częściowo uchylona; dalej jako: ustawa z 1997 r.), rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 29.4.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 11.12.2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. Nr 229, poz. 1536), a także innych ustawach szczególnych zawierających postanowienia odnoszące się do zasad przetwarzania danych osobowych (np. ustawa z 6.11.2008 r. o prawach pacjenta i Rzecznik Praw Pacjenta, t.j. Dz.U. z 2017 r. poz. 1318 ze zm.).

⁶ Dz.Urz. UE L Nr 158, s. 1; dalej jako: rozporządzenie UE o badaniach klinicznych lub rozporządzenie Nr 536/2014.

⁷ Dz.Urz. UE L Nr 281, s. 31; dalej jako: dyrektywa 95/46/WE.

⁸ W. Chomiczewski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 1125.

⁹ C. Pilz, [w:] DS-GVO. Datenschutz-Grundverordnung VO (EU) 2016/679. Kommentar, C.H. Beck 2017, s. 802, za: W. Chomiczewski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie...*, s. 1125.

z badań klinicznych wykorzystywanych do celów naukowych, jak również bezpieczeństwem uczestników badań klinicznych.

Przetwarzanie danych osobowych uczestników badań klinicznych

Podstawą prawną legitymizującą udział w badaniu klinicznym jest świadoma zgoda, o której mowa w art. 29 rozporządzenia UE o badaniach klinicznych. Istnieją natomiast wątpliwości co do określenia właściwej podstawy prawnej przetwarzania danych osobowych (wrażliwych) uczestników takiego badania. Do tej pory powszechnie stosowaną praktyką było uzyskiwanie pisemnej zgody uczestników badań na przetwarzanie ich danych osobowych, czyli stosowanie art. 27 ust. 2 pkt 1 ustawy z 1997 r. o ochronie danych osobowych.

Wydaje się jednak, że w świetle przepisów RODO nie jest konieczne uzyskiwanie odrębnej zgody na przetwarzanie danych wrażliwych uczestników badań. Rozporządzenie to określa bowiem inne (bardziej odpowiednie w porównaniu do zgody) podstawy przetwarzania danych dotyczących zdrowia, które mogą znaleźć zastosowanie w przypadku badań klinicznych. W naszej ocenie kluczowa jest podstawa wskazana w art. 9 ust. 2 lit. j) RODO legitymizująca przetwarzanie szczególnych kategorii danych osobowych, które jest niezbędne do prowadzenia badań naukowych. Jak wskazano w motywie 53 RODO, przetwarzanie danych osobowych do celów naukowych powinno też być zgodne z innymi odpowiednimi przepisami, takimi jak przepisy o próbach klinicznych (tłumaczenie prawidłowe: badań klinicznych), co jednoznacznie wskazuje, że cele naukowe mogą obejmować także badania kliniczne. Dodatkowe potwierdzenie takiego podejścia można odnaleźć w motywie 157 RODO wskazującym, że „przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko, obejmując tym pojęciem na przykład (...), badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych [oraz] badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego”. Takie stwierdzenie nie tylko przesądza o dopuszczalności wskazania przesłanki niezbędności przetwarzania danych osobowych do celów badań naukowych, ale także sugeruje, że niezależnie od charakteru tych badań, komercyjnego czy niekomercyjnego, a nawet nieinterwencyjnego zastosowanie będą miały do nich przepisy RODO.

Otwarte pozostaje jednak pytanie o podstawę prawną przetwarzania (zwykłych) danych osobowych uczestników badań klinicznych. W naszej ocenie podstawą legalizującą będzie zgoda uczestnika badania z art. 6 ust. 1 lit. a) RODO. Z uwagi jednak na szczególny charakter tej przesłanki¹⁰, związany z zaostrzeniem wymagań dla zgody¹¹, administrator musi zadbać, aby zgoda spełniała wymóg „poinformowanej zgody” (*informed consent*)¹², ponieważ tylko w takim przypadku możliwe jest uznanie, że osoba, której dane dotyczą, ma świadomość konsekwencji związanych z wyrażeniem zgody.

W RODO uregulowano nie tylko kwestię wyrażenia zgody, ale także jej wycofania, wskazując, że musi ono być równie łatwe jak jej wyrażenie. Nie określono formy, w jakiej powinno nastąpić wycofanie zgody, jednakże ze względu na wymóg rozliczalności powinna być to forma możliwa do utrwalenia, np. pisemna, elektroniczna, ustna (pod warunkiem jej utrwalenia). Jeżeli więc uczestnik badania złożył ustne oświadczenie o wycofaniu się z badania i cofnięciu zgody na przetwarzanie jego danych osobowych w celu umożliwienia mu uczestnictwa w badaniu, należy tę okoliczność odnotować w CRF (dokumentacji badania klinicznego). Pojawia się tu pytanie o zakres, w jakim nastąpiło wycofanie zgody. Osoba, której dane dotyczą, może wyrazić zgodę w jednym lub w większej liczbie celów, ale także kilka niezależnych zgód. Dlatego każdorazowo administrator powinien zadbać o to, aby był w stanie określić, której ze zgód dotyczyło wycofanie. Uczestnik badania klinicznego może udzielać trzech zgód¹³:

- zgody na przetwarzanie danych (zwykłych) w celu umożliwienia mu uczestnictwa w badaniu;
- zgody na przetwarzanie danych w celu umożliwienia przeprowadzania badań diagnostycznych po wycofaniu się z badania;
- zgody na przetwarzanie danych w celu umożliwienia kontaktów z lekarzem prowadzącym badanie po wycofaniu się z badania.

W powyższej sytuacji cofnięcie każdej z tych zgód należy rozpatrywać niezależnie i podmiot danych powinien mieć wiedzę o możliwości niezależnego wycofania każdej ze zgód¹⁴.

¹⁰ RODO wskazuje na kilka wymogów dot. wyrażenia zgody, które są określone w art. 4 pkt 11 i w art. 7 oraz w motywie 32, 33, 42 i 43. Uwagę należy również zwrócić na wytyczne grupy roboczej art. 29 (wciąż w konsultacjach).

¹¹ P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer 2017, s. 93.

¹² Wymogi dla poinformowanej zgody zostały określone w wytycznych Grupy Roboczej art. 29 dot. zgody (WP 259). Zgodnie z nimi osoba, której dane dotyczą, powinna co najmniej mieć wiedzę o: (i) tożsamości administratora, (ii) celu każdej operacji przetwarzania, dla których zgoda jest wyrażana, (iii) danych lub kategoriach danych, które będą gromadzone i wykorzystywane, (iv) prawie do wycofania zgody, (v) informacji o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu na podstawie przetwarzanych danych, zgodnie z art. 22 ust. 2, oraz (vi) jeżeli ma to zastosowanie, transferze danych, w tym o możliwym ryzyku przekazywania danych do państw trzecich w przypadku braku decyzji w sprawie odpowiedniego stopnia ochrony i odpowiednich zabezpieczeń.

¹³ Uczestnik może udzielać także innych zgód, ale powyższe są zgodami na przetwarzanie danych osobowych i będą podlegały przepisom RODO.

¹⁴ Problematiczna wydaje się kwestia potencjalnego wyrażenia zgody na przetwarzanie danych dotyczących przeżywalności uzyskiwanych z rejestrów prowadzonych przez organy administracji publicznej po wycofaniu się z badania lub zaprzestaniu uczestnictwa w badaniu. Z uwagi na to, że RODO nie chroni danych osobowych osób zmarłych, taka zgoda w naszej ocenie nie powinna być pozyskiwana, chociaż z uwagi na zasadę transparentności za dobrą praktykę należy uznać poinformowanie uczestnika badań o przetwarzaniu jego danych osobowych także w tym celu. W naszej ocenie nie jest konieczne precyzyjne wskazywanie konkretnych rejestrów i baz danych, z których pozyskiwane będą te informacje, ale należy wskazać źródło pozyskiwania danych przez odwołanie się do ich kategorii (np. rejstry prowadzone przez NFZ, MZ, ZUS).

Rozporządzenie UE o badaniach klinicznych stawia wiele wymagań warunkujących ich przeprowadzenie. Jednym z nich jest przedstawienie rozbudowanego formularza świadomej zgody na udział w badaniu przekazywanego pacjentowi przez badacza¹⁵. Niemniej jednak wykorzystanie tego formularza nie powinno zwalniać badacza od spełnienia obowiązku informacyjnego wymaganego przepisami RODO. Należy zauważyć, że zakres informacji przekazywanych uczestnikowi badania w formularzu świadomej zgody i w ramach obowiązku informacyjnego nie są tożsame. W naszej ocenie rodzi to konieczność uzupełnienia formularza o te informacje, które są wymagane przez art. 13 RODO.

Administrator danych osobowych uczestników badań klinicznych

Właściwe określenie ról pełnionych przez sponsora i badacza w świetle przepisów o ochronie danych osobowych jest bardzo istotne¹⁶. Uczestnika należy bowiem poinformować m.in. o tym, kto jest administratorem jego danych (nie wykluczamy przy tym możliwości przyjęcia liberalnej interpretacji polegającej na tym, że wystarczające jest wyjaśnienie, kto jest sponsorem badania, uznając domyślnie, że to właśnie on jest administratorem danych), jak również o odbiorcach jego danych osobowych.

Zgodnie z RODO podmioty przetwarzające dane osobowe występują przeważnie w dwóch rolach: administratora danych lub podmiotu, któremu powierzono przetwarzanie danych osobowych (tzw. procesor). Rozporządzenie dopuszcza także możliwość istnienia strony trzeciej, tj. osoby fizycznej, osoby prawnej, organu publicznego lub jednostki, lub podmiotu innego niż:

- osoba, której dane dotyczą;
- administrator;
- podmiot przetwarzający;
- osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe.

Powyższe rozróżnienie ma podstawowe znaczenie dla wyznaczenia zakresu obowiązków określonych w przepisach chroniących dane osobowe, które powinien spełnić administrator, ponieważ głównym adresatem obowiązków określonych w RODO, a także decyzji wydawanych przez organ nadzorczy (Prezesa Urzędu Ochrony Danych Osobowych) jest administrator danych.

Przetwarzanie danych osobowych przez podmiot przetwarzający opiera się na umowie lub innym instrumencie prawnym, a jego odpowiedzialność jest ograniczona treścią tej umowy lub instrumentu prawnego¹⁷. Odpowiedzialność podmiotu przetwarzającego jest więc znacznie węższa niż odpowiedzialność spoczywająca na administratorze danych¹⁸.

Próba określenia zakresu odpowiedzialności strony trzeciej jest natomiast bezcelowa, ponieważ RODO poza zdefiniowaniem zakresu podmiotowego tego pojęcia nie wymienia jej praw i obowiązków. Jedynie art. 6 ust. 2 lit. f) RODO wskazuje na możliwość istnienia prawnie uzasadnionych interesów realizowanych przez tę stronę trzecią, ale nawet w tym zakresie poinformowanie o tych interesach, a także o tym, że strona trzecia jest odbiorcą danych osobowych, spoczywa na administratorze danych.

W rozporządzeniu ogólnym zawarta jest także definicja legalna administratora danych (art. 4 pkt 7 RODO). Jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W praktyce administratorem danych jest podmiot, który samodzielnie lub wspólnie z innym podmiotem, bądź za pomocą innych podmiotów, przetwarza dane osobowe na własne potrzeby.

Odpowiadając na pytanie o rolę sponsora, badacza i ośrodka badawczego w świetle przepisów RODO, należy rozważyć co najmniej trzy modele ochrony danych:

- 1) sponsor, badacz i ośrodek są współadministratorami danych osobowych;
- 2) sponsor jest administratorem danych, a badacz i ośrodek badawczy są podmiotami przetwarzającymi (procesorami);
- 3) sponsor jest stroną trzecią, badacz administratorem danych, a ośrodek badawczy procesorem.

1. Sponsor, badacz i ośrodek jako współadministratorzy danych osobowych

Zgodnie z RODO, jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami (art. 26 RODO). Z podanej definicji wynika, że aby mówić o współadministratorach, muszą być spełnione równocześnie trzy warunki:

- 1) podmiot lub podmioty muszą być administratorami danych osobowych w rozumieniu RODO;
- 2) muszą wspólnie ustalić cele przetwarzania danych;
- 3) muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych¹⁹.

¹⁵ M. Kasińska, [w:] M. Jagielski, M. Kasińska, P. Kawczyński, K. Wojsyk, A. Sieradzka, E. Bielak-Jomaa, K. Andres, *Ochrona danych osobowych medycznych*, Warszawa 2016, s. 41 i n.

¹⁶ Na temat ochrony danych osobowych pacjenta – uczestnika badania w prawie wspólnotowym i francuskim zob. I. de Lamberterie, H.J. Lucas, *Informatique, libertés et recherche médicale*, Paris 2001.

¹⁷ Szerzej na ten temat: B. Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, *Journal of Intellectual Property, Information Technology and E-Commerce Law* 2016, Nr 3, <https://www.jipitec.eu/issues/jipitec-7-3-2016/4506> (dostęp 21.4.2018 r.).

¹⁸ P. Litwiński, [w:] M. Jagielski, M. Kasińska, P. Kawczyński, K. Wojsyk, A. Sieradzka, E. Bielak-Jomaa, K. Andres, *Ochrona danych...*, s. 47 i n.

¹⁹ A. Buczyńska-Borowy, *Współadministratorzy i proces współadministrowania*, *ABI Expert* 2017, Nr 2, s. 44.

W RODO nie wskazuje się, co oznacza wspólne ustalanie takich celów. Nie jest jasne, czy stosunek współadministrowania będzie zachodził także wtedy, gdy dany podmiot, realizując proces przetwarzania, samodzielnie określi cele lub sposoby przetwarzania, na które zgodzą się pozostałe podmioty. W tym zakresie wypowiedziała się jednak Grupa Robocza²⁰, która w swojej opinii z 2010 r. wskazała, że sam fakt, że w procesie przetwarzania danych osobowych współpracują różne podmioty, np. w łańcuchu, nie oznacza, że są one wspólnymi administratorami we wszystkich przypadkach, ponieważ wymianę danych między dwiema stronami przy braku wspólnych celów lub sposobów przetwarzania w ramach wspólnej grupy operacji należy uważać wyłącznie za przekazywanie danych pomiędzy dwoma oddzielnymi administratorami danych. Trzeba zawsze badać skalę mikro i makro przetwarzania, ponieważ możliwe jest, że w skali mikro poszczególne operacje przetwarzania danych w łańcuchu wydają się niepowiązane, jako że każda z nich może mieć inny cel, ale już w skali makro możliwe byłoby uznanie operacji przetwarzania danych za „grupę operacji” służących jednemu celowi lub wykorzystujących wspólnie określone sposoby przetwarzania danych.

Przyjmując więc, że poszczególne cele przetwarzania danych osobowych w procesie w skali mikro realizowane przez sponsora, badacza i ośrodek badawczy, służą wspólnemu celowi całego procesu (w skali makro), w naszej ocenie możliwe jest przyjęcie, że między tymi podmiotami będzie zachodził stosunek współadministrowania. Ponadto uważamy, że każdy z celów realizowanych w skali mikro powinien być niezbędny do realizacji celu w skali makro oraz powinien być znany pozostałym współadministratorom.

2. Sponsor jest administratorem danych, a badacz i ośrodek badawczy są procesorami

Jeżeli natomiast przyjąć literalne brzmienie przepisu, które zakłada, że cele i sposoby przetwarzania muszą być ustalane wspólnie, należy uznać sponsora za administratora danych osobowych. Z kolei badacz i ośrodek badawczy będą podmiotami, które przetwarzają dane osobowe w imieniu administratora (art. 4 pkt 8 RODO). Należy zauważyć, że jest to pogląd dominujący, choć z uwagi na charakter danych, do których ma dostęp sponsor, może budzić wątpliwości. Za uznaniem go za administratora danych przemawia jednak, że to on zleca i finansuje badania, a także zapewnia udział w badaniu przez pracownika lub przedstawiciela firmy sponsorującej badania kliniczne (tzw. monitora, tj. osoby monitorującej badania) i audytora. Posiada więc uprawnienia o charakterze nadzorczym. Celem uporządkowania rozważań w dalszej części opracowania będziemy jednak, mówiąc o administratorze danych, odnosić się do sponsora.

3. Sponsor jest stroną trzecią, badacz administratorem a ośrodek badawczy procesorem

Za problematyczną z perspektywy oceny roli sponsora należy uznać zasadę, zgodnie z którą dane pacjentów są pozbawione funkcji identyfikacyjnej dla sponsora²¹ po dokonaniu pseudonimizacji lub anonimizacji danych pacjentów. Pseudonimizacja skutkuje niemożliwością przypisania informacji do konkretnej osoby, której dane dotyczą, bez użycia dodatkowych informacji, przy czym takie dodatkowe informacje są przechowywane osobno objętymi środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (w dokumentacji badania prowadzonej przez badacza). Informacje te nadal jednak stanowią dane osobowe w rozumieniu RODO. Natomiast po dokonaniu anonimizacji nie ma już możliwości, nawet przy użyciu dodatkowych informacji, zidentyfikowania poszczególnych uczestników badania. W takim układzie sponsor pozbawiony narzędzia pozwalającego na ponowną identyfikację uczestników badania w ogóle nie przetwarza danych osobowych²² i w związku z powyższym nie jest możliwe wykonywanie przez niego praw osób, których dane dotyczą, np. prawa dostępu do danych czy prawa do przenoszenia²³. W takim przypadku zasadne byłoby rozważenie uznania sponsora za stronę trzecią, która ma interes w przeprowadzaniu takich badań, ale nie w dostępie do danych osobowych. Dane osobowe są przetwarzane przede wszystkim przez badacza, który prowadzi badania kliniczne i ma faktyczny wpływ na cele i sposoby ich przetwarzania, mając jednocześnie bezpośredni kontakt z uczestnikiem badań (mimo że to sponsor zleca i finansuje badania kliniczne). Natomiast ośrodek badawczy stanowi miejsce, w którym badanie ma być przeprowadzone, i w ograniczonym zakresie może przetwarzać dane osobowe uczestników badań w celu określonym przez administratora danych. Mimo powyższych argumentów uważamy, że model ten budzi najwięcej wątpliwości prawnych.

²⁰ Opinia 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”, s. 20–24.

²¹ W. Wiewiórowski, Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych, Europejski Przegląd Sądowy 2017, Nr 5, s. 28.

²² Zgodnie z definicją z art. 4 pkt 7 RODO „administrator oznacza osobę (...) [która] samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych”. Skoro sponsor nie przetwarza danych osobowych, to nie spełnia wszystkich przesłanek z definicji pozwalających uznać go za administratora.

²³ W. Wiewiórowski, Prawo do przenoszenia..., s. 28.

Wymogi przetwarzania danych osobowych w badaniach klinicznych

RODO nakłada na podmioty przetwarzające dane osobowe wiele obowiązków. W kontekście badań klinicznych w szczególności jest istotne zachowanie zgodności z regułą minimalizacji przetwarzanych informacji (zapewnienie, że dane osobowe są przetwarzane jedynie w niezbędnym zakresie, nie dłużej niż przez czas wymagany do osiągnięcia celów, w związku z którymi są przetwarzane), regułą poufności informacji przetwarzanych (zapewnienie, że dane osobowe są udostępniane jedynie osobom upoważnionym i zabezpieczone przed dostępem osób nieupoważnionych²⁴), regułą rozliczalności (bazującą na prawnej odpowiedzialności za właściwe wypełnianie obowiązków wynikających z rozporządzenia²⁵ i nakładającą na administratora obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać) oraz regułą integralności przetwarzanych informacji (zapewnienie dokładności i kompletności danych osobowych, nienaruszalności danych, tj. ochrona przed nieuprawnionym ich zmienianiem bądź zniszczeniem). Szczególnie istotne jest uwzględnienie tych zasad w przypadku badań klinicznych, które są prowadzone w interesie publicznym. Jak wynika z RODO, przetwarzanie w tym celu odbywa się w zgodzie z przepisami prawa Unii lub prawa państwa członkowskiego, które powinno zapewnić odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową. Rodzi to pytanie o zasadność wykorzystania tej przesłanki, w przypadku gdy przepisy nie zapewniają takiej ochrony. Dodatkowym problemem jest trudność dokonania oceny, jakie środki są odpowiednie i konkretne. Nie wydaje się jednak, aby ocena ta miała spoczywać na administratorze danych osobowych.

W RODO zawarto zamknięty katalog przesłanek legalności przetwarzania danych osobowych zwykłych (art. 6) i szczególnych kategorii danych osobowych, zwanych także danymi wrażliwymi czy sensytywnymi (art. 9). Ten ostatni przepis, jako całość, został skonstruowany odmiennie niż art. 6 RODO określający podstawy prawne przetwarzania tzw. danych zwykłych. W art. 9 ust. 1 RODO ustanowiono bowiem generalny zakaz przetwarzania danych osobowych, które mogą być uznane za dane wrażliwe, natomiast ust. 2 tego przepisu określa sytuacje, w których zakaz ten został uchylony²⁶ (np. prowadzenie badań naukowych, do której to kategorii należą badania kliniczne). Spełnienie którejkolwiek z nich skutkuje dopuszczalnością przetwarzania danych.

W ramach danych osobowych przetwarzanych przy okazji prowadzenia badań klinicznych przetwarzane są przede wszystkim szczególne kategorie danych, a zwłaszcza dane dotyczące zdrowia. Przesłanek legalizujących ich przetwarzanie należy więc szukać w art. 9 RODO. W przypadku ba-

dań klinicznych zastosowanie znajdują przede wszystkim dwie przesłanki z art. 9 ust. 2 lit. i oraz j RODO, tj. niezbędność przetwarzania ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego oraz niezbędność przetwarzania do celów badań naukowych.

Oprócz konieczności wykazania podstawy do przetwarzania danych osobowych na administratorze ciąży ponadto liczne obowiązki informacyjne w stosunku do osób, których dane są zbierane. Informacje te powinny zostać przekazane na etapie zbierania danych osobowych. Zakres i sposób przekazywania tych informacji jest określony odpowiednio w art. 12 i n. RODO. Artykuł 13 RODO wskazuje informacje przekazywane przez administratora danych, w przypadku gdy ten pozyskał dane bezpośrednio od podmiotu danych osobowych, natomiast art. 14 RODO odnosi się do pozyskiwania danych z innych źródeł.

W przypadku pozyskiwania danych od podmiotu danych administrator podaje osobie, której dane dotyczą, następujące informacje:

- swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
- gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
- cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Ponadto aby przetwarzanie było rzetelne i przejrzyste dla osoby, której dane dotyczą, administrator podaje:

- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

²⁴ P. Barta, M. Kawecki, [w:] P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Legalis/el. 2018.

²⁵ P. Drobek, [w:] E. Bielak-Jomaa, D. Lubasz (red.), RODO. Ogólne rozporządzenie..., s. 342.

²⁶ P. Barta, M. Kawecki, [w:] P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony..., Legalis/el. 2018.

- informacje o prawie wniesienia skargi do organu nadzorczego;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Zakres informacji podawanych w przypadku pozyskiwania danych z innych źródeł obejmuje dodatkowo kategorie przetwarzanych o tej osobie danych osobowych oraz informacje o źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

Przetwarzanie danych osobowych badaczy i innych członków zespołu badawczego

Niezależnie od faktu przetwarzania danych osobowych uczestników badania klinicznego należy także rozważyć zagadnienie przetwarzania danych osobowych członków zespołu badawczego. W tym zakresie na podstawie umowy o przeprowadzenie badania klinicznego sponsor jest administratorem danych osobowych badaczy, a przesłanką przetwarzania ich danych jest niezbędność do wykonania tej umowy (art. 6 ust. 1 pkt b RODO). Powstaje pytanie, czy współbadacze oraz inne osoby wchodzące w skład zespołu powinni udzielać zgody na przetwarzanie ich danych osobowych w odrębnym formularzu, w sytuacji gdy sponsor nie zawrze z nimi odrębnych umów. Nie podzielamy opinii, że zgoda powinna stanowić podstawę przetwarzania tych danych. W naszej ocenie znacznie bardziej właściwa byłaby przesłanka prawnie uzasadnionego interesu administratora danych. Zastosowanie tej przesłanki jest możliwe, jeśli nadrzędne wobec tych interesów okazałyby się prawa i wolności tych osób, co w przypadku członków zespołu badawczego nie ma miejsca. Ponadto jak wskazano w motywie 47 RODO, taki prawnie uzasadniony interes może istnieć w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Właśnie taka sytuacja zachodzi w przypadku prowadzenia badań klinicznych, gdyż badacze działają na rzecz sponsora zlecającego te badania. Zgoda na przetwarzanie danych osobowych w powyższym celu nie wydaje się więc ani potrzebna, ani celowa. Zdajemy sobie jednak sprawę, że propozycja ta stanowi istotne *novum*, gdy chodzi o polską praktykę realizacji badań klinicznych.

W tym zakresie wątpliwości może budzić kwestia przetwarzania danych osobowych badaczy i innych członków zespołu badawczego, wykraczających poza zakres tzw. danych

służbowych (np. adres prywatny, numer dowodu osobistego), które jednak są wykorzystywane (przetwarzane) w związku z realizacją umowy łączącej sponsora z badaczem (np. prawidłowe dokonanie rozliczeń). Wydaje się, że z uwagi na wskazanie dokonane w motywie 47 RODO podstawą przetwarzania tych danych także będzie prawnie uzasadniony cel administratora danych.

Powierzenie przetwarzania danych osobowych w badaniach klinicznych

W art. 28 RODO określono zasady umownego powierzenia danych osobowych. Dane mogą zostać powierzone na mocy umowy lub innego instrumentu prawnego. Ta umowa lub inny instrument prawny mogą mieć formę pisemną lub elektroniczną. Umowa ta musi określać przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora i podmiotu przetwarzającego. Obowiązki administratora zostały określone w art. 24 RODO. Podmiot przetwarzający pomaga w spełnieniu tych obowiązków oraz wypełnia obowiązki z art. 28 ust. 3 RODO zgodnie z umową, w której wszystkie te obowiązki powinny być określone.

Jeśli uznać, że sponsor jest administratorem danych, to ośrodek badawczy oraz badacza należy uznać za podmioty przetwarzające, które będą przetwarzały dane na udokumentowane polecenie sponsora. Pewne trudności przy tej konstrukcji może rodzić kwestia obowiązku korzystania przez sponsora tylko z takich badaczy i takiego ośrodka badawczego, którzy zapewniają odpowiednie gwarancje spełnienia wymogów wynikających z RODO. W doktrynie wskazuje się, że wybór takiego procesora przez administratora powinien być uważny, a współpraca z podmiotami niedającymi odpowiednich gwarancji jest wykluczona²⁷.

Procesor odpowiada wyłącznie w zakresie określonym umową powierzenia²⁸. W szczególności podejmuje wszelkie środki dotyczące bezpieczeństwa przetwarzania wymagane na mocy art. 32 RODO, przestrzega warunków dotyczących podpowierzenia danych innemu podmiotowi, pomaga sponsorowi wywiązać się z obowiązku odpowiadania na żądania podmiotów danych (uczestników badań) oraz wywiązać się z obowiązków w zakresie bezpieczeństwa przetwarzania zgłaszania naruszeń ochrony danych, zawiadamiania osoby, której dane dotyczą, o takim naruszeniu oraz wspiera administratora w zakresie dokonywania oceny skutków dla ochrony danych, a także w ramach procedury uprzednich konsultacji. Ponadto badacz/ośrodek badawczy występujący

²⁷ K. Witkowska-Nowakowska, [w:] E. Bielak-Jomaa, D. Lubasz (red.), RODO. Ogólne rozporządzenie..., s. 635.

²⁸ P. Litwiński, [w:] M. Jagielski, M. Krasińska, P. Kawczyński, K. Wojsyk, A. Sieradzka, E. Bielak-Jomaa, K. Andres, Ochrona danych..., s. 47 i n.

w roli procesorów powinni udostępniać administratorowi wszelkie informacje niezbędne do wykazania spełnienia jego obowiązków określonych w art. 32 RODO oraz umożliwiać administratorowi danych lub upoważnionemu przez niego audytorowi przeprowadzanie audytów – w naszej ocenie, może to obejmować także umożliwianie udziału w badaniu przez monitora i audytora.

Podstawowym zadaniem podmiotu, któremu powierzono przetwarzanie danych osobowych, jest więc zabezpieczenie ich przetwarzania. W tym zakresie należy zauważyć, że RODO nie przesądza, jakie środki powinny zostać zastosowane przez procesora. Jest to wynikiem podejścia opartego na ryzyku, tj. konstrukcji bazującej na kształtowaniu obowiązków, których zakres określany jest przez pryzmat oceny ryzyka²⁹. Wątpliwa jest możliwość realizacji tego wymogu przez badaczy i ośrodki, które nie przeprowadziły stosownego wdrożenia RODO w swoich organizacjach (działalności).

Przez umowy powierzenia przetwarzania danych osobowych należy rozumieć wszelkie umowy, do wykonania których zleciobiorca przetwarza dane osobowe administratora (bez względu na to, czy przetwarzanie danych stanowi jej istotę, czy też następuje tylko „przy okazji”). Ponadto brak zawarcia takiej umowy między administratorem danych a podmiotem przetwarzającym (niezależnie czy za administratora danych uznajemy sponsora czy badacza) nie powoduje, że do powierzenia danych faktycznie nie dochodzi³⁰.

Problematyczne wydaje się natomiast określenie, jak należy dokonywać powierzenia przetwarzania danych, w sytuacji gdy założy się, że między sponsorem, badaczem i ośrodkiem badawczym dochodzi do współadministrowania przetwarzanymi danymi osobowymi. Jak wskazuje się w literaturze³¹, w takim przypadku każdy ze współadministratorów powinien zawierać umowy powierzenia w zakresie przypisanych mu celów i sposób przetwarzania, chyba że wspólne uzgodnienia w ogóle wyłączały możliwość umownego powierzenia.

Niedopełnienie wymogów z art. 28 RODO wiąże się z ryzykiem nałożenia administracyjnej kary pieniężnej w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Jeśli jednak administrator danych lub podmiot przetwarzający naruszą podstawowe zasady przetwarzania szczególnych kategorii danych osobowych (w tym danych dotyczących zdrowia), to kara pieniężna może wynieść do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Jeśli więc w wyniku prowadzonych badań klinicznych doszłoby do naruszenia obejmującego zarówno niedopełnienie obowiązków określonych w art. 28 RODO, jak i przetwarzanie szczególnych kategorii danych, to z uwagi na to, że do naruszeń doszło w ramach tych samych lub powiązanych operacji przetwarzania danych, kara wyniosłaby maksymal-

nie do 20 000 000 euro lub do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Jeśli jednak do obu naruszeń doszłoby w ramach niepowiązanych ze sobą badań klinicznych (operacji przetwarzania danych), procesor lub administrator danych odpowiadałby za każde naruszenie z osobna.

Poza odpowiedzialnością pieniężną, w nowej polskiej ustawie z 10.5.2018 r. o ochronie danych osobowych³², mając na względzie dobro podmiotów danych oraz wagę naruszenia, jakim jest przetwarzanie danych osobowych, uznano, że przetwarzanie danych bez podstawy prawnej, a więc nieuprawnione i umyślne przetwarzanie, powinno być zagrożone karą grzywny, ograniczenia wolności albo pozbawienia wolności³³. W zakresie maksymalnej kary (pozbawienia wolności) ustawodawca dokonał rozróżnienia i w zależności od kategorii danych – wskazał ją na poziomie dwóch lat pozbawienia wolności w przypadku naruszenia zasad ochrony danych zwykłych oraz trzech lat pozbawienia wolności w przypadku naruszenia zasad ochrony danych wrażliwych.

Profilowanie w badaniach klinicznych

1. Profilowanie w świetle wytycznych Grupy Roboczej art. 29

Grupa Robocza art. 29³⁴ w swoich wytycznych dot. profilowania i automatyzowanego podejmowania decyzji³⁵ wyróżnia profilowanie ogólne, podejmowanie decyzji oparte na profilowaniu oraz wyłącznie zautomatyzowane podejmowanie decyzji oparte na profilowaniu³⁶.

W ocenie Grupy Roboczej profilowanie składa się z trzech elementów:

- 1) musi stanowić formę zautomatyzowanego przetwarzania;
- 2) musi być przeprowadzane na danych osobowych i
- 3) celem profilowania musi być ocena osobistych aspektów dotyczących osoby fizycznej³⁷.

²⁹ D. Lubasz, [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO. Ogólne rozporządzenie..., s. 692.

³⁰ K. Witkowska-Nowakowska, [w:] E. Bielak-Jomaa (red.), D. Lubasz (red.), RODO. Ogólne rozporządzenie..., s. 634.

³¹ J. Byrski, Umowne powierzenie do przetwarzania danych osobowych w ustawie o ochronie danych osobowych, dyrektywie 95/46 i w ogólnym rozporządzeniu o ochronie danych, MoP 2016, Nr 20, s. 39.

³² Dz.U. poz. 1000 ze zm.

³³ Uzasadnienie do projektu nowej ustawy o ochronie danych osobowych, s. 40–41; <https://legislacja.rcl.gov.pl/docs//2/12302950/12457690/12457691/dokument334234.pdf> (dostęp z 20.3.2018 r.).

³⁴ Grupa Robocza Art. 29 została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności.

³⁵ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251).

³⁶ *Ibidem*, s. 8.

³⁷ *Ibidem*, s. 6.

Na bardzo ogólnym poziomie profilowanie wiąże się z kategoryzowaniem osób według ich cech „niezmiennych” (takich jak płeć, wiek, pochodzenie etniczne, wzrost) czy „zmiennych” (takich jak zwyczaje, preferencje i inne elementy zachowania)³⁸. Zazwyczaj profile tworzy się za pomocą techniki zwanej „analizą behawioralną”. Polega ona na dopasowaniu i korelacji określonego zachowania (np. wyborów konsumenckich) z cechami (np. wiek)³⁹.

Profilowanie może również wykorzystywać inne dane niż pochodzące i powiązane z podmiotem danych, np. dane statystyczne. Profile tego rodzaju opierają się na prognozowaniu różnych postaw ludzkich na podstawie zestawiania danych wielu osób i następnie określaniu statystycznego prawdopodobieństwa tych zachowań. Do uprzednio przygotowanych modeli „dopasowywane” są więc konkretne osoby. Rodzi to ryzyko przypisania im cech, których w istocie one nie mają, co z kolei prowadzić może do nieusprawiedliwionego pozbawienia ich dostępu do pewnych dóbr i usług⁴⁰. Dlatego często jest wykorzystywane do przewidywania ludzkich zachowań przy użyciu danych z różnych źródeł w celu sformułowania wniosków o danej osobie, na podstawie cech innych osób, które wyglądają statystycznie podobnie⁴¹. W takim przypadku ryzyko dyskryminacji jest znacznie wyższe.

Opinia Grupy Roboczej art. 29 dotycząca profilowania⁴² początkowo była bardzo restrykcyjna – zdaniem Grupy nawet proste ocenianie czy klasyfikacja osób na podstawie cech takie jak wiek, płeć i wzrost mogło być uznane za profilowanie, niezależnie od tego, czy było skorelowane z jakimkolwiek celem predykcyjnym⁴³. Rewizja wytycznych⁴⁴ przyniosła złagodzenie tego stanowiska. Grupa wskazała, że prosta klasyfikacja osób na podstawie znanych cech, takich jak wiek, płeć i wzrost, niekoniecznie musi prowadzić do profilowania. Zasadniczo będzie to zależeć od celu klasyfikacji⁴⁵. Takie podejście należy ocenić pozytywnie, ponieważ nie wydaje się, aby prosta klasyfikacja, przy której podmiot danych łatwo może ocenić jej zasady, miała być objęta ochroną równoważną ze skomplikowanymi procesami przetwarzania, dokonywanymi z wykorzystaniem np. bardzo dużej ilości zmiennych, algorytmów czy danych o tej osobie, niepochodzących bezpośrednio od niej albo zestawiania jej danych z danymi statystycznymi dla profilu, który powstał w oparciu o dane pochodzące od tej osoby. Z uwagi na to, że ludzie mają różne poziomy zrozumienia złożonej techniki związanej z profilowaniem i automatycznymi procesami decyzyjnymi to działania te mogą być dla nich wyzwaniem⁴⁶. Osoby, których dane są przetwarzane w taki sposób, mogą nie tylko nie rozumieć przyczyn i przebiegu samego procesu przetwarzania, ale wręcz nie mieć wiedzy o tym, że w ogóle się ono odbywa⁴⁷.

Należy także podzielić opinię Grupy Roboczej, zgodnie z którą zautomatyzowanym podejmowaniem decyzji obejmującym przetwarzanie nie jest prosta klasyfikacja służąca

uzyskaniu zbiorczego przeglądu np. swoich klientów bez dokonywania jakichkolwiek prognoz ani wyciągania wniosków na temat konkretnej osoby. W takim przypadku nie dochodzi do profilowania, ponieważ celem nie jest ocena indywidualnych cech⁴⁸.

2. Profilowanie w świetle RODO

Zgodnie z art. 4 pkt 4 RODO profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, przeznaczoną do analizowania lub prognozowania osobowości bądź niektórych czynników osobowych osoby fizycznej, w szczególności analizy i prognozy jej zdrowia, sytuacji ekonomicznej, efektów jej pracy, osobistych preferencji lub zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się⁴⁹. Z tej definicji wynika, że profilowanie nie dotyczy przypadków niezautomatyzowanego (ręcznego) przetwarzania danych.

Wyróżnia się dwa rodzaje profilowania:

- 1) profilowanie zwykłe,
- 2) profilowanie kwalifikowane.

³⁸ Agencja Praw Podstawowych, Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu. http://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_PL.pdf (dostęp z 16.12.2017 r.).

³⁹ J. Niklas, Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji, http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekście_ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf (dostęp z 16.12.2017 r.).

⁴⁰ X. Konarski, Profilowanie danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych osobowych – dotychczasowy i przyszły stan prawny w UE oraz w Polsce, MoP 2016, Nr 20, s. 49, za: Rekomendacja CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili, s. 2.

⁴¹ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP 251), s. 7.

⁴² *Ibidem*.

⁴³ *Ibidem*.

⁴⁴ *Ibidem*.

⁴⁵ *Ibidem*.

⁴⁶ Szczególnie zautomatyzowane decyzje podejmowane z wykorzystaniem sztucznej inteligencji (*artificial intelligence*, AI) czy systemów samouczących (*machine learning*, ML) stwarzają ryzyko niezrozumienia motywów podjęcia takiej decyzji i w efekcie zagrażają autonomii informacyjnej. Podobnie w tym zakresie wypowiada się: M. Hildebrandt, The Dawn of a Critical Transparency Right for the Profiling Era, https://works.bepress.com/mireille_hildebrandt/40/download/ (dostęp z 21.4.2018 r.); M.L. Jones, Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood, Soc Stud Sci 2017, Nr 47.

⁴⁷ Guidelines on Automated individual..., s. 17.

⁴⁸ *Ibidem*, s. 7.

⁴⁹ „Profiling” means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements.

Profilowanie zwykłe	Profilowanie kwalifikowane
Art. 4 pkt 4 RODO	Art. 22 RODO
Dowolna forma zautomatyzowanego przetwarzania ⁵⁰	Forma wyłącznie zautomatyzowanego przetwarzania ⁵¹
Brak decyzji lub decyzja: – niewywołująca skutków prawnych. – niewpływająca na osobę, której dane dotyczą. – niewpływająca istotnie na osobę, której dane dotyczą	Decyzja wywołująca skutki prawne lub w podobny sposób istotnie wpływająca na osobę, której dane dotyczą

Źródło: N. Kalinowska – opracowanie własne.

Rozporządzenie o ochronie danych osobowych wielokrotnie odnosi się do profilowania osoby fizycznej. Słowo profilowanie w samym rozporządzeniu pojawia się 23 razy. Jak wskazano powyżej, przetwarzanie danych osobowych z wykorzystaniem profilowania zwykłego i profilowania kwalifikowanego jest objęte zupełnie innym reżimem ochronnym. Wymagany poziom ochrony jest zależny od ryzyka dla ochrony praw i wolności osób, których dane dotyczą. RODO stanowi, że im ryzyko związane z przetwarzaniem danych osobowych jest większe, tym większy powinien być zakres obowiązków ciążących na administratorze danych⁵².

3. Zautomatyzowane podejmowanie decyzji obejmujące profilowanie

Na gruncie RODO wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, istnieje zwłaszcza w tych sytuacjach, gdy profilowanie jest elementem przetwarzania, o którym mowa w art. 22 RODO. Jak wskazuje motyw 71 RODO, do takiego przetwarzania zalicza się „profilowanie”, ale tylko wtedy, gdy wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. W doktrynie wskazuje się na trudność z ustaleniem, jakie decyzje można uznać za wpływające na osobę w podobny sposób, jak decyzje o skutkach prawnych⁵³. Wskazuje się, że może być decyzja prowadząca do niezawarcia umowy. W takim przypadku nie powstają bowiem skutki prawne, a zatem konieczne jest – w interesie podmiotów danych – posłużenie się dodatkowym kryterium „istotnego wpływu”⁵⁴. Również wytyczne Grupy Roboczej art. 29 wskazują, że aby przetwarzanie danych znacząco wpłynęło na podmiot danych, efekty przetwarzania muszą być wystarczająco duże lub ważne, aby być godnym uwagi. Innymi słowy, decyzja musi potencjalnie:

- znacząco wpłynąć na okoliczności, zachowania lub wybory osoby, której dane dotyczą;
- mieć długotrwały lub trwały wpływ na osobę, której dane dotyczą lub
- w najbardziej skrajnym przypadku prowadzić do wykluczenia lub dyskryminacji osób.

Dodatkowo Grupa Robocza uznaje, że wystarczająco istotnym skutkiem są m.in. decyzje wpływające na dostęp do usług zdrowotnych. Wydaje się więc, że profilowanie wykorzystywane w badaniach klinicznych w rozumieniu RODO może powodować takiego rodzaju istotne skutki dla osoby, której dane dotyczą, ponieważ niemożność wzięcia udziału w badaniu klinicznym pozbawia pacjenta dostępu do leku i terapii z nią związanej, która potencjalnie mogłaby poprawić jego stan zdrowia.

Warto zauważyć, że jeśli zautomatyzowane podejmowanie decyzji, o którym mowa w art. 22 RODO, będzie obejmowało przetwarzanie szczególnych kategorii danych, administrator będzie mógł je zastosować tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na nie wyraźną zgodę lub gdy będzie ono niezbędne ze względów związanych z ważnym interesem publicznym. RODO wymaga, aby poza istnieniem jednej z dwóch przesłanek legalizujących dodatkowo istniały właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, nie wskazując jednak, kto ma je zapewnić. W przypadku przesłanki z art. 9 ust. 2 lit. g) RODO, która mówi o ważnym interesie publicznym wprost wskazano, że w przepisach prawa Unii lub państwa członkowskiego mają być przewidziane odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Wydaje się więc, że przy oparciu przetwarzania danych dotyczących zdrowia w ramach badań klinicznych na przesłance z art. 9 ust. 2 lit. g) RODO administrator nie będzie zobligowany do podejmowania dodatkowych działań na rzecz zapewnienia takich środków ochrony. Taki pogląd jest jednak

⁵⁰ W wersji angielskiej rozporządzenie posługuje się wyrażeniem dowolnej/jakiegokolwiek formy (*any form*).

⁵¹ W angielskiej wersji rozporządzenia wprost wskazano, że taka decyzja opiera się wyłącznie (*solely*) na zautomatyzowanym przetwarzaniu.

⁵² M. Byczkowski, Znaczenie norm ISO we wdrażaniu bezpieczeństwa technicznego i organizacyjnego wymaganego w RODO, MoP 2017, Nr 20, s. 17.

⁵³ S. Wachter, B. Mittelstadt, L. Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law* 2017, Nr 2, s. 93.

⁵⁴ X. Konarski, Profilowanie danych osobowych..., s. 50.

możliwy do zaakceptowania jedynie w przypadku uznania, że pojęcie „właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą” jest tożsame z pojęciem „odpowiednich i konkretnych środków ochrony praw podstawowych i interesów osoby, której dane dotyczą”. Odnosząc się do art. 22 ust. 3 RODO, można uznać, że właściwe środki ochrony obejmują co najmniej prawo do uzyskania interwencji ludzkiej ze strony administratora do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Jeśli więc przepisy prawa będą gwarantować przynajmniej taki zakres ochrony, to należy uznać, że podejmowanie dodatkowych działań przez administratora nie jest wymagane.

Z drugiej strony, w kontekście przeprowadzania badań klinicznych należy mieć na uwadze treść motywu 71 RODO, zgodnie z którym administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające, w szczególności korektę powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą. Ma to na celu ograniczenie negatywnych skutków:

- 1) w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną lub
- 2) skutkujący środkami mającymi taki efekt.

Mimo że zalecenie to wynika z motywu, w naszej ocenie, z uwagi na kontekst przetwarzania danych uczestników badań klinicznych jednym z działań, które powinny zostać podjęte przez administratora, jest wdrożenie i stosowanie takich procedur i środków. Aby zapewnić należytą ochronę szczególnym kategoriom danych osobowych zautomatyzowane podejmowanie decyzji i profilowanie na nich oparte powinno być dozwolone wyłącznie przy zachowaniu powyżej opisanych warunków.

Profilowanie skutkujące zautomatyzowanym podejmowaniem decyzji zawiera w sobie zarówno element tzw. prawa pozytywnego, jak i negatywnego. Osoba, której dane dotyczą, ma bowiem prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu jej danych, których skutkiem jest podjęcie decyzji o skutku prawnym lub podobnie istotnym (prawo negatywne), ale ma również prawo do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji (prawo pozytywne), co jest przejawem woli ustawodawcy unijnego, aby osoby, których dane dotyczą, miały wiedzę o takim przetwarzaniu i aby było ono dla nich transparentne⁵⁵.

Warto w tym miejscu przypomnieć, że rozporządzenie UE w sprawie badań klinicznych produktów leczniczych wprowadza definicję legalną badań klinicznych. Zgodnie z jej treścią „badanie kliniczne” oznacza badanie biomedyczne⁵⁶ spełniające którykolwiek z następujących warunków:

- a) przydział uczestnika do danej strategii terapeutycznej ustalany jest z góry i odbywa się w sposób niestanowiący standardowej praktyki klinicznej zainteresowanego państwa członkowskiego;
- b) decyzja o przepisaniu badanego produktu leczniczego jest podejmowana łącznie z decyzją o włączeniu uczestnika do badania biomedycznego lub
- c) oprócz standardowej praktyki klinicznej u uczestników wykonuje się dodatkowe procedury diagnostyczne lub procedury monitorowania.

W ramach przydziału uczestnika, o którym mowa w punkcie a), może dochodzić do zautomatyzowanego podejmowania decyzji o skutku prawnym lub w podobnie istotny sposób wpływającym na osobę, której dane dotyczą. W takim przypadku, aby móc przetwarzać te dane, administrator musi pozyskać wyraźną zgodę lub wykazać, że przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym.

4. Obowiązki administratora wynikające z wykorzystywania profilowania obejmującego zautomatyzowane podejmowanie decyzji w badaniach klinicznych

Uznając, że badania kliniczne obejmują przetwarzanie, o którym mowa w art. 22 RODO, administrator danych powinien:

- poinformować o profilowaniu i zasadach zautomatyzowanych decyzji podejmowanych na jego podstawie (art. 13–15);
- poinformować o możliwości wyrażenia sprzeciwu na profilowanie (art. 21);
- poinformować o możliwości kwestionowania automatycznych decyzji wydanych w oparciu na profilowaniu (art. 22);
- przeprowadzić ocenę skutków profilowania dla ochrony danych osobowych (art. 35 ust. 3 lit. a)⁵⁷.

⁵⁵ M. Hildebrandt, *The Dawn...*, s. 47.

⁵⁶ Zgodnie z rozporządzeniem 536/2014 badanie biomedyczne „oznacza każde badanie dotyczące ludzi, mające na celu:

a) odkrycie lub potwierdzenie klinicznych, farmakologicznych lub innych farmakodynamicznych skutków jednego lub większej liczby produktów leczniczych;

b) stwierdzenie wszelkich działań niepożądanych jednego lub większej liczby produktów leczniczych; lub

c) zbadanie wchłaniania, dystrybucji, metabolizmu i wydalania jednego lub większej liczby produktów leczniczych; mające na celu upewnienie się co do bezpieczeństwa lub skuteczności tych produktów leczniczych”.

⁵⁷ X. Konarski, *Profilowanie danych osobowych...*, s. 50.

Jednym z najbardziej rozbudowanych obowiązków wynikających z RODO w stosunku do polskiej ustawy o ochronie danych osobowych jest obowiązek informacyjny, który administrator powinien spełnić zarówno, jeśli pozyskuje je od osoby, której dane dotyczą (art. 13 RODO), jak i jeśli pozyskuje je w sposób inny niż od osoby, której dane dotyczą (art. 14 RODO). W ramach obowiązku informacyjnego administrator jest zobligowany poinformować m.in. o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu⁵⁸. Ponadto powinien wskazać istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą⁵⁹. Ponadto mimo że nie zostało to wprost wskazane, to w przypadku profilowania kwalifikowanego, administrator powinien poinformować o możliwości kwestionowania decyzji wydanej na podstawie zautomatyzowanego przetwarzania, o którym mowa w art. 22 RODO.

Kwestią dyskusyjną pozostaje, czy należy informować o profilowaniu zwykłym, skoro RODO nie nakłada takiego obowiązku. W art. 13 oraz 14 RODO w zakresie informowania o profilowaniu z art. 4 pkt 4 RODO nie przewidziano analogicznego obowiązku, aczkolwiek motyw 60 RODO wskazuje, że zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania. Motyw nie wskazuje, czy chodzi o profilowanie zwykłe czy kwalifikowane. Jednakże przekazywanie w ramach obowiązku informacyjnego, że przetwarzanie obejmuje profilowanie zwykłe, należy uznać to za dobrą praktykę przyczyniającą się, do pełniejszej realizacji zasady transparentności przetwarzania danych osobowych, zwłaszcza że w przypadku badań klinicznych profilowaniu podlegają szczególne kategorie danych, co ma wpływ na wzrost ryzyka takiego przetwarzania dla praw i wolności osób, których dane dotyczą.

Artykuł 21 ust. 1 RODO stanowi, że osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, tym profilowania na podstawie tych przepisów. Sprzeciw ten ma charakter względnie skuteczny, gdyż administrator może go zakwestionować, jeśli wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Jedyną sytuacją, w której

administrator musi bezwzględnie respektować sprzeciw podmiotu danych, jest ta, gdy dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego. Rozporządzenie wprost wskazuje, że jeżeli osoba, której dane dotyczą, wnieśnie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Należy zauważyć, że zgodnie z art. 21 RODO sprzeciw dotyczy przetwarzania na podstawie art. 6 ust. 1 lit. e) lub f). Wobec czego nie będzie miał zastosowania w przypadku profilowania (zwykłego oraz kwalifikowanego) obejmującego dane wrażliwe. Jedynie sprzeciw na przetwarzanie danych wrażliwych na potrzeby marketingu bezpośredniego będzie mógł zostać skutecznie wniesiony i bezwzględnie respektowany przez administratora danych. Jeśli jednak sponsor będzie przetwarzał dane zwykłe na podstawie art. 6 ust. 1 lit. d) lub f) RODO, wtedy zarówno sprzeciw z art. 21 ust. 1, jak i z ust. 2 RODO będzie przysługiwał osobom, których dane dotyczą.

Ocena skutków dla ochrony danych na gruncie RODO jest wymagana w ściśle określonych przypadkach. W wytycznych Grupy Roboczej dotyczących oceny skutków dla ochrony danych wskazuje się na dziewięć kryteriów, które należy brać pod uwagę, badając, czy dane rodzaj przetwarzania może powodować wysokie ryzyko dla ochrony praw i wolności podmiotu danych. Wśród tych kryteriów znajdują się m.in. dokonywanie oceny lub punktacji, automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku, przetwarzanie danych wrażliwych, przetwarzanie danych na dużą skalę, łączenie lub dopasowywanie zbiorów danych czy przetwarzanie danych dotyczących osób wymagających szczególnej opieki⁶⁰.

Z uwagi na to, że w ramach badań klinicznych dochodzi do przetwarzania spełniającego co najmniej dwa z powyższych kryteriów, np. przetwarzania szczególnych kategorii danych na dużą skalę, administrator przed przeprowadzeniem takich badań będzie zobligowany do dokonania oceny skutków dla ochrony danych osobowych. Takie stanowisko dotyczące przeprowadzania oceny skutków w odniesieniu do badań klinicznych zostało dodatkowo poparte przez GIODO w opublikowanym 28.3.2018 r. dokumencie „Proponowany

⁵⁸ Jak słusznie zauważa *Mireille Hildebrandt*, dopóki osoba, której dane dotyczą, nie jest świadoma, że została poddana takiej decyzji, nie ma również świadomości o prawach jej przysługujących, np. prawie do zakwestionowania takiej decyzji: *M. Hildebrandt*, Profiling and the rule of law, <https://link.springer.com/content/pdf/10.1007%2Fs12394-008-0003-1.pdf>, s. 65 (dostęp z 21.4.2018 r.).

⁵⁹ *G. Comandè, G. Malignieri*, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law* 2017 Nr 4, s. 264–265.

⁶⁰ Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679 (WP 248 rev.01), s. 11–12.

wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków”. Organ wskazał w nim, że w jednym z potencjalnych obszarów wystąpienia konieczności takiej oceny będzie prowadzenie badań klinicznych przez szpitale lub inne organizacje⁶¹.

Podsumowanie

Analizując wpływ przepisów RODO na prowadzenie badań klinicznych, należy zauważyć, że akt ten wprowadza inne niż zgoda podstawy przetwarzania danych osobowych uczestników badań klinicznych, np. art. 9 ust. 2 lit. i) RODO legalizujący przetwarzanie niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, czy też art. 9 ust. 2 lit. j) RODO wskazujący na niezbędność przetwarzania danych wrażliwych do celów prowadzenia badań naukowych. Ponadto RODO wprowadza wiele nowych praw i obowiąz-

ków, w tym rozbudowany obowiązek informacyjny, ocenę skutków dla ochrony danych, uprzednie konsultacje i inne, z którymi będą mierzyć się administratorzy danych osobowych. Dodatkowo niektóre z praw przysługujących podmiotom danych, np. prawo do przenoszenia danych osobowych, otwierają dyskusję o aktualności dotychczasowego określania ról podmiotów przetwarzających dane osobowe pacjentów (np. koncepcja uznania sponsora za stronę trzecią – co jest jednak dyskusyjne), w tym rozszerza ją o nowe możliwości (np. współadministrowania danymi osobowymi przez sponsora, badacza i ośrodek badawczy). Niewątpliwie konieczność dostosowania się do nowych przepisów przez sponsorów, badaczy i ośrodki, jak też inne podmioty uczestniczące w badaniach klinicznych (np. CRO) wymusi uporządkowanie zasad i procedur przetwarzania danych osobowych w ramach prowadzenia badań klinicznych, tak aby zapewnić realizację praw podmiotów danych i właściwe spełnienie obowiązków przez podmioty przetwarzające dane osobowe.

⁶¹ Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych, <https://giudo.gov.pl/pl/file/13366>, s. 2 (dostęp z 21.4.2018 r.).

Słowa kluczowe: ochrona danych osobowych, RODO, profilowanie, badania kliniczne, prawo.

Clinical trials in the light of GDPR

Applied in practice models of protection of natural persons in regard to processing of their personal data in clinical trials raise many legal doubts. The issue requires explanation in the light of regulation from the European Parliament and of the Council 2016/679 of 27.4.2016, in the matter of free movement of such data and repealing the directive 95/46/EC. In the present publication the authors attempt to justify interpretation of GDPR regulations which allows to conduct clinical trials in Poland. They point out issues of profiling participants of clinical trials and researchers and other members of a research group, because it is one of the issues that currently raises the most practical problems.

Keywords: personal data protection, GDPR, profiling, clinical trials, law.

Monografie Prawnicze

Zamów:
tel. 22 31 12 222
www.ksiegarnia.beck.pl

MONOGRAFIE PRAWNICZE

OCHRONA KLIENTA NA RYNKU
USŁUG FINANSOWYCH
W ŚWIELE AKTUALNYCH
PROBLEMÓW
I REGULACJI PRAWNYCH

Pod redakcją
EDYTY RUTKOWSKIEJ-TOMASZEWSKIEJ

Bezprawny dowód z korespondencji internetowej stron w postępowaniu cywilnym

Błażej Gadek¹

Celem niniejszego opracowania jest analiza dopuszczalności wprowadzenia do procesu cywilnego dowodów z korespondencji internetowej, które zostały pozyskane w sposób bezprawny. W obliczu braku stosownej normy prawnej w Kodeksie postępowania cywilnego, która wprost określałaby (nie)dopuszczalność takiego zjawiska, konieczna staje się prawna komparatystyka regulacji konstytucyjnych, a także odniesienie się do aktów prawa międzynarodowego. Jednocześnie autor dokonuje przeglądu tendencji pojawiających się w literaturze oraz orzecznictwie sądowym, w zakresie możliwości posługiwania się dowodem nielegalnym w procesie cywilnym.

Uwagi wstępne

Zgodnie z obowiązującą w polskim procesie cywilnym zasadą kontrydiktoryjności, odpowiedzialność za wynik procesu spoczywa na stronach, podobnie jak idąca za tym powinność zbierania oraz przedstawiania dowodów, celem poparcia podejmowanych przez siebie akcji procesowych. Jedynie wyjątkowo dopuszczalna jest sytuacja, w której sąd podejmuje czynności z urzędu, korzystając ze swego dyskrejonalnego uprawnienia do przeprowadzenia dowodów².

W praktyce sądowej strony uciekają się do korzystania z różnych źródeł dowodowych, a duża popularność form komunikacji internetowej będzie powodować, że liczba wniosków dowodowych, obejmujących dowód z treści korespondencji internetowej, będzie tylko rosła. Niewątpliwa przydatność użycia tego rodzaju dowodów wynika z tego, że około 40% Polaków korzystających z Internetu prowadzi także korespondencję przy użyciu komunikatorów internetowych³.

Problematyka ujęcia dowodu

W Kodeksie postępowania cywilnego ustawodawca nie zdecydował się na zamknięty katalog środków dowodowych, stąd wymienione w nim źródła dowodu mają charakter li tylko egzemplifikacyjny⁴. Dowód z korespondencji internetowej stron stanowi tak zwany dowód elektroniczny – niewymieniony *explicite* w ustawie. Wciąż jednak może być to dowód użyteczny, celowo przez strony wnioskowany, a pozwalający dokonać rzetelnego odtworzenia stanu faktycznego przez sąd. Jakkolwiek należy wziąć pod uwagę możliwość dokonania przez stronę fałszu intelektualnego na przedstawianej korespondencji tudzież próbę manipulowania wyrwanym z kontekstu fragmentem rozmowy, niemniej jednak ocena takiego dowodu, podobnie zresztą jak każdego innego przedstawionego przez strony w procesie cywilnym, jego wiarygodności oraz mocy, leży w gestii sądu.

Brak legalnej definicji dowodu, jednak w art. 227 KPC ustawodawca stanowi, iż dowód mogą stanowić jedynie okoliczności faktyczne mające istotne znaczenie dla rozstrzygnięcia sprawy. Przedmiotem dowodu stają się zatem fakty, które należy rozumieć bardzo szeroko jako te wszystkie elementy stanu faktycznego, które mogą ulec sprawdzeniu w drodze postępowania dowodowego⁵. Wieloznaczność pojęcia „dowód” wywołuje konieczność kontekstowego posługiwania się tym sformułowaniem, może ono bowiem odnosić się zarówno do źródła dowodu, czyli nośnika informacji o faktach, jak i do środka dowodowego⁶. Brak jest przepisu w Kodeksie postępowania cywilnego, który formalnie zabraniałby dopuszczenia dowodu bezprawnego, co wywołuje pytanie o dopuszczalność wprowadzania do procesu cywilnego dowodu nielegalnego, w tym dowodu z korespondencji internetowej uzyskanego za pomocą przestępstwa, typizowanego w art. 267 KK⁷. Pojęcia dowodu bezprawnego oraz dowodu nielegalnego w niniejszym artykule występują zamiennie. Samo zagadnienie jest o tyleż kontrowersyjne, że z jednej strony, dotyka gwarantowanych konstytucyjnie wolności, w szczególności ochrony prywatności i tajemnicy komunikowania, z drugiej zaś strony, nieuwzględnienie dowodu uzyskanego bezprawnie, w postaci wykradzionej korespondencji internetowej, może uniemożliwić wydanie rozstrzygnięcia opartego na prawdzie materialnej, a co za tym idzie – naruszyć gwarantowane konstytucyjnie prawo jednostki

¹ Autor jest studentem V roku studiów stacjonarnych prawa na WPAiE Uniwersytetu Wrocławskiego.

² L. Błaszczak, K. Markiewicz, E. Rudkowska-Ząbczyk (red.), *Dowody w postępowaniu cywilnym*, Warszawa 2010, s. 141.

³ Komunikat z badań CBOS Korzystanie z Internetu 2017, Nr 49, s. 12.

⁴ L. Błaszczak, K. Markiewicz, E. Rudkowska-Ząbczyk (red.), *Dowody...*, s. 9.

⁵ J. Klich-Rump, *Podstawa faktyczna rozstrzygnięcia sądowego w procesie cywilnym*, Warszawa 1977, s. 12.

⁶ L. Błaszczak, K. Markiewicz, E. Rudkowska-Ząbczyk (red.), *Dowody...*, s. 14.

⁷ J. Gołaczyński, *Dowody pozyskane bezprawnie w sprawach o rozwód*, [w] J. Łukasiewicz (red.), *Prawo rodzinne i spadkowe wobec współczesnych zjawisk technologicznych i społecznych*, Rzeszów 2018.

do rzetelnego procesu, chronione także na gruncie Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności. Jednocześnie powstaje pytanie, czy wprowadzenie dowodu bezprawnego do procesu cywilnego nie narusza zarazem prawa do sprawiedliwego (rzetelnego) procesu sądowego, jeżeli fundament takiego postępowania oparty będzie na ustaleniach faktycznych dokonanych na podstawie dowodów, które zostały uzyskane w drodze przestępstwa.

Doktryna owoców zatrutego drzewa w procedurze cywilnej w zestawieniu z Kodeksem postępowania administracyjnego oraz Kodeksem postępowania karnego

Niniejszy artykuł porusza problematykę dopuszczalności przeprowadzenia dowodu tzw. owocu zatrutego drzewa w procesie cywilnym i umiejscawia to zagadnienie w następujących kontekstach: z jednej strony, brak w polskim porządku prawnym normy zabraniającej wykorzystania takich dowodów w procesie cywilnym, a z drugiej strony, celem postępowania, ale i warunkiem wydania sprawiedliwego orzeczenia jest prawda materialna. Jednocześnie dochodzi do pewnego rodzaju ścierania się konstytucyjnie chronionych praw: do swobody komunikowania się, do prywatności z zasadą rzetelnego (sprawiedliwego) procesu, co wszak wymaga dotarcia do prawdziwych ustaleń faktycznych.

Wyżej wspomniana doktryna owoców zatrutego drzewa jest wywodzącą się z amerykańskiego systemu *common law* koncepcją, która zabrania wprowadzania do procesu dowodów zebranych w niewłaściwy sposób, a nawet pochodzących ze skażonego źródła⁸. Koncepcja ta, jak zresztą wynika ze wstępu do niniejszego artykułu, nie została bezpośrednio wyartykułowana w polskim prawie procesowym cywilnym. Zastanawiające, czy można to uznać za przeoczenie legislatora, jeśli wspomni się, że art. 75 KPA przewiduje, iż jako dowód można dopuścić wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem. Obecnie obowiązujące przepisy polskiego Kodeksu postępowania karnego, będące następstwem nowelizacji z 11.3.2016 r., która weszła w życie 15.4.2016 r., nie przewidują niedopuszczalności wprowadzenia do procesu karnego dowodów bezprawnych⁹. Taki sposób ujęcia przedmiotowego zagadnienia, niezależnie od licznych wątpliwości doktryny, stanowi wyraz jednoznacznego opowiedzenia się ustawodawcy, za określoną koncepcją prowadzenia procesu karnego. Pomijając już ocenę takiego zabiegu normatywnego, jak również nie podejmując się oceny legislacyjnej precyzji przy konstruowaniu aktualnego brzmienia art. 168a KPK, okolicznością szczególnie istotną dla problematyki niniejszego artykułu jest sama bezpośrednia regulacja w ustawie procesowej zakresu dopuszczalności

przeprowadzenia dowodu uzyskanego w sposób sprzeczny z prawem. Ustawodawca zatem stanowi wprost, iż w polskiej procedurze karnej taki dowód jest dopuszczalny (z wyjątkami), natomiast regulacji takiej nie przewiduje dla procedury cywilnej. Wydaje się jednak, że wnioskowanie na tej podstawie, iż prowadzić to powinno do automatycznego uznania niedopuszczalności przeprowadzania dowodów bezprawnych w procesie cywilnym, w tym także dowodów uzyskanych za pomocą przestępstwa, stanowiłoby rażące uproszczenie problemu zasługującego na poważniejsze rozpoznanie.

Brak wyraźnej normy prawnej nie przesądza wszak o (nie)dopuszczalności wprowadzenia dowodu bezprawnego do procesu cywilnego, gdyż ocena tego zagadnienia wymaga uwzględnienia, oprócz (braku) stosownych przepisów Kodeksu postępowania cywilnego, także regulacji ujętych w aktach normatywnych hierarchicznie równego rzędu ustawie procesowej. Przede wszystkim należy tutaj wziąć pod uwagę kodeksową ochronę dóbr osobistych, ale też rozważyć regulacje przewidziane przez akty normatywne wyższego rzędu – Konstytucję RP oraz ratyfikowane umowy międzynarodowe, a głównie Europejską Konwencję o ochronie praw człowieka i podstawowych wolności, konstytuującą pojęcie rzetelnego procesu sądowego.

Bezprawny dowód z korespondencji internetowej stron jako owoc typizowanego przez Kodeks karny przestępstwa

Zgodnie z brzmieniem art. 267 § 1 KK: „Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch”. Dyspozycja tego artykułu określa znamiona przestępstwa, w efekcie popełnienia którego uzyskuje się dostęp do treści korespondencji przeciwnika procesowego z osobą trzecią. Relacja pomiędzy tak uzyskanym materiałem procesowym, w postaci cudzej korespondencji, a oceną wniosku dowodowego obejmującego przeprowadzenie dowodu z jej treści stanowi główną oś niniejszego artykułu.

Jak podkreśla się w literaturze przedmiotu, przedmiotem ochrony przez wyżej stypizowane przestępstwo jest szeroko rozumiane prawo do dysponowania informacją¹⁰, a stano-

⁸ A. Mariański, Glosa do wyroku NSA z 22.2.2006 r., I FSK 1077/05, MoPod 2006, Nr 12, s. 50.

⁹ Art. 168a KPK.

¹⁰ W. Wróbel, Przestępstwa przeciwko ochronie informacji, [w:] A. Zoll (red.), Kodeks karny, t. II, Warszawa 2008, s. 1278.

wisko to poparł także SN w uchwale z 22.1.2003 r.¹¹, choć w doktrynie pojawia się również pogląd, iż przedmiotem ochrony są: tajemnica komunikowania się oraz prawo do prywatności¹². Niezależnie jednak od sposobu ujęcia węzłowego zagadnienia, zgodzić się należy, że ustawodawca w ten sposób penalizuje zachowania polegające na bezprawnym uzyskaniu dostępu do informacji objętych ochroną oraz do systemu informatycznego, co wpisuje się w naruszenie konstytucyjnie gwarantowanej „tajemnicy komunikowania się”, a co Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności w art. 8 ust. 1 traktuje jako „pożądanie korespondencji”¹³.

Taki czyn przestępny w szczególności będzie polegać na przełamaniu lub ominięciu zabezpieczeń, natomiast wątpliwe jest, z uwagi na konieczność ścisłej wykładni przepisów prawa karnego, wywodzonej z samego faktu zagrożenia karą za popełniony czyn i pryncypiów tej gałęzi prawa, wyrażonej sentencją *nullum crimen sine lege*, czy pozostawianie na ekranie komputera otwartej korespondencji internetowej, umożliwiające zrobienie tzw. zrzutów ekranu czy też sfotografowanie tejże, może być penalizowane. Za szerokim ujęciem i karalnością także takich zachowań wydaje się opowiadać P. Kardas, który podkreśla, że zwrot „bez uprawnienia” ma charakter klauzuli normatywnej¹⁴. Podobnie zresztą stwierdził SN w wyroku z 3.2.2004 r.: „Wprawdzie art. 267 KK za przestępcze naruszenie tajemnicy korespondencji traktuje jedynie otwieranie »zamkniętych pism«, to jednak przepisy te (...) wyznaczają aksjologiczny kierunek postępowania z wszelką korespondencją. W kategoriach etycznych powszechnie stosowana i społecznie akceptowana (...) jest zasada nieczytania cudzej korespondencji, nawet jeśli ma ona postać karty pocztowej”¹⁵.

Stanowiska zajmowane przez doktrynę i judykaturę

Pierwszą, w powojennej literaturze, próbą zmierzenia się z problematyką dowodu bezprawnego w procesie cywilnym był artykuł E. Wengerka, w którym autor opowiadał się za niedopuszczalnością wprowadzenia do procesu dowodów bezprawnych. W szczególności wskazywał on, że dopuszczalność stosowania dowodów bezprawnych w procesie karnym nie przesądza automatycznie o dopuszczalności wprowadzenia tego rodzaju dowodów do procesu cywilnego, z uwagi na daleko idące różnice pomiędzy procesem karnym a cywilnym. Podkreślał, iż proces karny ma na celu wykrycie przestępcy i ukaranie go, a celem postępowania cywilnego jest realizacja norm prawa materialnego¹⁶. Wówczas, podobnie jak dzisiaj, Kodeks postępowania cywilnego nie był wyposażony w normę, która bezpośrednio regulowałaby tę tematykę. Stało się to przyczynkiem coraz bardziej ożywionych dyskusji w li-

teraturze przedmiotu ostatnich lat. Zapoczątkowany przez E. Wengerka trend do odmowy dopuszczalności przeprowadzenia dowodu nielegalnego w procesie cywilnym jest obecnie najbardziej dominującym w literaturze.

D. Korszeń stwierdził z kolei, że wprowadzenie dowodów nielegalnych do procesu cywilnego byłoby nie do pogodzenia z wieloma przepisami rangi konstytucyjnej, ustawowej oraz nieskodyfikowanymi normami etycznymi, nawet pomimo braku wyrażonej normy zabraniającej przeprowadzenia tego typu dowodów w procesie cywilnym¹⁷. Stoi on na stanowisku, że w przedstawieniu dowodu z korespondencji stron w oczywisty sposób wyraża się realizowanie przez stronę konstytucyjnie gwarantowanego prawa do sądu, niemniej jednak nie można tego samego powiedzieć o wykorzystaniu dowodu z korespondencji osób trzecich. Takie stanowisko, w dużej mierze, zdaje się dominować w literaturze przedmiotu, a poszczególni autorzy, roztrząsając to zagadnienie, skupiają się przede wszystkim na konflikcie wartości, który istnieje pomiędzy prawem do sądu a ochroną tajemnicy korespondencji czy szerzej prawa do prywatności. Nienaruszalność prywatności i tajemnicy korespondencji jednostki w inny sposób niż za jej uprzednią zgodą ma ich zdaniem prymat nad realizacją roszczeń procesowych przeciwnika w procesie nawet tych najbardziej uzasadnionych.

Kategorycznie tezę tę wygłosił T. Wiśniewski – jego zdaniem należy bowiem z góry dyskwalifikować dowody uzyskane w sposób sprzeczny z prawem, a prowadzi do tego analiza przepisów Kodeksu postępowania cywilnego oraz Kodeksu cywilnego¹⁸. Pogląd przyjęty przez autora, jakkolwiek klarowny, razi pewnego rodzaju restrykcyjnością, nietrudno bowiem wyobrazić sobie sytuację, w której aprioryczna odmowa dopuszczenia dowodu pochodzącego „z zatrutego drzewa”, wywołuje daleko idące konsekwencje w postaci upadku roszczenia. Wydawać by się mogło, iż sądy, zapewniając pełną realizację konstytucyjnie gwarantowanego prawa do rzetelnego i sprawiedliwego procesu, dysponują instrumentami, w postaci swobodnej oceny dowodów, pozwalającej ważyć *in concreto* zasadność dopuszczenia dowodu uzyskanego w sposób sprzeczny z prawem. Oczywiście jest jednak, że wprowadzenie

¹¹ I KZP 43/02, OSNKW 2003, Nr 1–2, poz. 5.

¹² J. Piórkowska-Flieger, [w:] T. Bojarski (red.), Kodeks karny, Warszawa 2012, s. 101.

¹³ S. Hoc, [w:] R. Stefański (red.), Kodeks Karny. Komentarz, Warszawa 2018, s. 1607–1622.

¹⁴ P. Kardas, Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego, Czasopismo Prawa Karnego i Nauk Penalnych 2000, Nr 1, s. 68.

¹⁵ II KK 388/02, Prok. i Pr. – wkł. 2004, Nr 9, s. 4.

¹⁶ E. Wengerek, Korzystanie w postępowaniu cywilnym ze środków dowodowych uzyskanych sprzecznie z prawem, PiP 1977, Nr 2, s. 39.

¹⁷ D. Korszeń, Zakres zakazu przeprowadzania w postępowaniu cywilnym dowodów nielegalnych (bezpprawnych), MoP 2013, Nr 1, s. 18 i n.

¹⁸ T. Wiśniewski, Przebieg procesu cywilnego, Warszawa 2013, s. 79.

dowodu nielegalnego do procesu cywilnego może z drugiej strony wywoływać pytanie o generalną rzetelność tak prowadzonego postępowania, co wszak jest fundamentalnym pytaniem w zakresie analizowanego problemu.

Pewną dywersyfikację dowodów przyjmuje z kolei *T. Zembrzusi*, który bardzo wyraźnie rozróżnia dowód uzyskany za pomocą przestępstwa, niemogący być dowodem w procesie cywilnym, od dowodu naruszającego dobra osobiste przeciwnika procesowego, który już może zostać wprowadzony do procesu¹⁹. Inne ujęcie tego zagadnienia, zdaniem tego autora, naruszałoby zasadę swobodnej oceny dowodów. Formuluje on stanowisko, które można określić mianem „warunkowej dopuszczalności dowodów sprzecznych z prawem” – sprzeciwia się arbitralnej normie, zabraniającej korzystania z dowodu uzyskanego w sposób sprzeczny z prawem w jakiegokolwiek sprawie. Pogląd ten, jakkolwiek interesujący, w odniesieniu do tematu niniejszej pracy ma o tyle mniejsze zastosowanie, iż w zasadzie uzyskanie dostępu do korespondencji internetowej przeciwnika procesowego „za pomocą” przestępstwa, zawsze będzie kwalifikowane jako dowód uzyskany w wyniku przestępstwa, co uniemożliwia zastosowanie wzmiankowanej dystynkcji. W związku z powyższym pogląd *T. Zembrzuskiego*, jakkolwiek zakładający pewnego rodzaju elastyczność przy rozróżnianiu rodzajów wniosków dowodowych, przekreśla automatycznie zastosowanie w procesie dowodu z korespondencji internetowej, która uzyskana była w wyniku przestępstwa.

Z kolei pogląd zbliżony do *D. Korszenia* wyraziła *A. Laskowska*, również powołując się na konstytucyjne unormowania, ale z kolei w przeciwieństwie do stanowiska wyrażonego przez *T. Zembrzuskiego*, uzasadniając zakaz przeprowadzenia tego rodzaju dowodów także ochroną dóbr osobistych, powołuje się na brzmienie art. 23 KC²⁰. Założeniem ustawodawcy, konstruującego instytucję dóbr osobistych oraz form ich ochrony, było zapewnienie skutecznej ochrony wartościom niemajątkowym, ściśle związanym z osobowością człowieka, wywodzonym z przyrodzonej godności człowieka, objętej wszak konstytucyjną ochroną przez art. 31 Konstytucji RP²¹. Ustawodawca kreuje domniemanie, że każde naruszenie dóbr osobistych jest bezprawne, a ocena tego naruszenia dokonywana jest z punktu widzenia obiektywnego obserwatora, a nie biorąc pod uwagę subiektywną wrażliwość skarżącego, co stanowi jednocześnie tamę dla pieniactwa procesowego²². Bezprawność w szczególności będzie polegać na naruszeniu tekstu ustawy, a co za tym idzie, bez wątpienia taka sytuacja zachodzi w przypadku popełnienia przestępstwa. *D. Korszeń* jednak wskazuje, przywołując doktrynę i orzecznictwo, że istnieją okoliczności egzoneracyjne, takie jak: zgoda uprawnionego i działanie na własne ryzyko, wykonywanie własnego prawa podmiotowego, obrona konieczna, działanie w ramach porządku prawnego²³.

Z pewnością gdy w toku procesu jedna ze stron wnosi o dopuszczenie dowodu bezprawnego, przedstawiając korespondencję przeciwnika procesowego z osobą trzecią, już doszło do naruszenia dobra osobistego, w związku z czym uprawnionemu, z punktu widzenia ochrony dóbr osobistych, przysługuje roszczenie o dopełnienie czynności potrzebnych do usunięcia jego skutków. Powstaje zatem pytanie, czy bezwzględnie skuteczny powinien być wniosek uprawnionego o oddalenie takiego wniosku dowodowego przez sąd, powołując się na wyżej wymienione roszczenie, tudzież czy sąd taki wniosek powinien oddalić z urzędu. Jednocześnie w doktrynie i orzecznictwie mocno wybrzmiewa, kontrowersyjny skądinąd pogląd, iż uchyla bezprawność działanie w obronie uzasadnionego interesu prywatnego²⁴.

Natomiast SN, na kanwie analizy przepisów zezwalających na stosowanie podsłuchu operacyjnego w sprawach karnych, doszedł do przekonania²⁵, iż dopuszczalność tego rodzaju dowodów ograniczonych tylko do najcięższych przestępstw nie usprawiedliwia stosowania prywatnego podsłuchu i nagrań ze względu na interes prywatny do celów procesowych. W celu zachowania spójności wyводу SN ów wniosek należałoby rozciągnąć także na pozyskany nielegalnie dowód z korespondencji osób trzecich. Sąd stoi na stanowisku, że interes rozumiany jako poszukiwanie ochrony prawnej w procesie, a traktowany jako przesłanka wyłączająca bezprawność, powodowałby zbyt daleko idące ograniczenie tajemnicy komunikowania się.

Sąd Najwyższy w swej linii orzeczniczej nie jest jednak konsekwentny, gdyż w wyroku z 25.4.2003 r. wykazał się bardziej liberalnym stanowiskiem, uznając możliwość dopuszczenia dowodu nielegalnego, choć dotyczył on przeprowadzenia dowodu z potajemnie nagranej rozmowy stron²⁶. W tej sprawie wypowiedział się *T. Zembrzusi*, który wska-

¹⁹ *T. Zembrzusi*, [w:] *Ł. Błaszczak, K. Markiewicz, E. Rudkowska-Ząbczyk* (red.), *Dowody w postępowaniu cywilnym*, Warszawa 2010, s. 72–75.

²⁰ *A. Laskowska*, *Dowody w postępowaniu cywilnym* uzyskane w sposób sprzeczny z prawem, *PiP* 2003, Nr 12, s. 96.

²¹ *B. Gawlik*, *Ochrona dóbr osobistych. Sens i nonsens tzw. praw podmiotowych osobistych*, *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Wynalazczości i Ochrony Własności Intelektualnej* 1985, Nr 4, s. 124.

²² Zob. m.in. wyrok SN z 16.1.1976 r., II CR 692/75, OSNC 1976, Nr 11, poz. 251, z glosą *J. Piętowskiego*, NP 1977, Nr 7–8, s. 1144; wyrok SN z 11.3.1997 r., III CKN 33/97, OSNC 1997, Nr 6–7, poz. 93; wyrok SN z 25.4.1989 r., I CR 143/89, z glosą aprobowującą *A. Szpunara*, OSP 1990, Nr 9, poz. 330.

²³ *D. Korszeń*, *Zakres zakazu...*, s. 5.

²⁴ *A. Szpunar*, *Ochrona dóbr osobistych*, Warszawa 1979, s. 161; *tenże*, *Zgoda uprawnionego w zakresie ochrony dóbr osobistych*, *Ruch Prawniczy, Ekonomiczny i Socjologiczny* 1990, Warszawa, s. 55; *K. Piasecki*, *Kodeks cywilny. Księga pierwsza*, Warszawa 2003, s. 191; *J. Sadowski*, *Naruszenie dóbr osobistych przez media. Analiza praktyki sądowej*, Warszawa 2003, s. 50, a w orzecznictwie wyroki SN: z 19.9.1968 r., II CR 291/68, OSN 1969, Nr 11, poz. 200; z 29.10.1971 r., II CR 455/71, OSN 1972, Nr 4, poz. 77; z 14.11.1986 r., II CR 295/86, OSN 1988, Nr 2–3, poz. 40; z 19.10.1989 r., II CR 419/89, OSPiKA 1990, Nr 11, poz. 377.

²⁵ Zob. wyrok SN z 13.11.2002 r., I CKN 1150/00, *Legalis*.

²⁶ Zob. wyrok SN z 25.4.2003 r., IV CKN 94/01, PS 2004, Nr 12, s. 156.

zał, iż wyrażona w art. 3 KPC klauzula dobrych obyczajów obowiązuje strony do dokonywania czynności procesowych zgodnie z dobrymi obyczajami oraz dawania wyjaśnień co do okoliczności sprawy zgodnie z prawdą i bez zatajania czegokolwiek, a powoływanie się przez jedną ze stron na niedopuszczalność przeprowadzenia dowodu, z uwagi na naruszenie art. 23 i 24 KC kwalifikuje z kolei jako naruszenie art. 3 KPC²⁷. Sama klauzula dobrych obyczajów, podobnie jak zasady współżycia społecznego, jest klauzulą generalną, zawierającą zwroty nieostre, a zatem indywidualizacja normy prawnej następuje dopiero w konkretnych sytuacjach²⁸. W szczególności należy mieć baczenie, jaki skutek miałyby praktyka sądów zezwalająca na wprowadzenie do procesu nielegalnie pozyskanej korespondencji internetowej stron, a stanowiąca w istocie przyzwolenie na popełnianie przestępstwa typizowanego w art. 267 KK, celem zdobycia dowodów, czego konsekwencją mogłoby być rozpowszechnienie się takich zachowań. Słusznie jednak wskazywał *T. Zembrzusi*, że niedopuszczenie takiego dowodu, naruszającego dobra osobiste, może uniemożliwić ustalenie faktów związanych np. z rozkładem pożycia małżeńskiego, gdyż niemożliwe byłoby przedstawienie nagrania dokumentującego zdradę małżeńską, analogicznie niemożliwe byłoby przedstawienie dowodu z korespondencji jednej ze stron, stanowiącej dowód rozkładu pożycia małżeńskiego²⁹.

Interesująco, na tle powyższych rozważań, przedstawia się stanowisko zaprezentowane przez SA w Białymstoku w wyroku z 31.12.2012 r., którego teza zakłada, że naruszenie prawa do prywatności lub innych praw o charakterze bezwzględnym, nie ma charakteru bezprawnego, gdyż uchylona zostaje poprzez realizowanie przez jednostkę prawa do sądu, gwarantowanego przez art. 45 Konstytucji RP³⁰. Jest to zatem konflikt wartości konstytucyjnych, a przeto od okoliczności indywidualnych, konkretnych dla danej sprawy, zależeć powinna decyzja procesowa sądu o dopuszczeniu bądź oddaleniu wniosku dowodowego. Podsumowując to rozstrzygnięcie, *Ł. Czarnecki* puentuje, że: „Bardziej rygorystyczne stanowisko należałoby stosować do nielegalnych podsłuchów rozmów prowadzonych przez osoby trzecie, czy tego typu nielegalnych działań, jak przejmowanie cudzej korespondencji czy hakerskie włamanie do skrzynki odbiorczej poczty elektronicznej, zaś mniej stanowcze do nagrywania rozmowy w sytuacji, gdy osoba nagrywająca jest jednocześnie odbiorcą informacji, a więc w tych przypadkach, w których jeden z uczestników dokumentuje w ten sposób treść ich wypowiedzi”³¹. Przytoczone stanowisko zarówno judykatury, jak i doktryny, stanowi próbę pogodzenia przeciwstawnych wartości przy zastosowaniu swoistego testu konstytucyjności. W celu oceny dopuszczalności wprowadzenia dowodu pochodzącego „z zatrutego drzewa” konieczna staje się odpowiedź na pytanie, czy w okolicznościach danej sprawy interes wnioskującego ma prymat, z uwagi na konieczność

zapewnienia stronom procesu, którego wynik zostanie oparty na prawdzie materialnej i rzeczywistym przebiegu zdarzeń, nad konstytucyjną ochroną tajemnicy korespondencji.

Jak zauważa *A. Łazarska*, prawo do sądu realizowane jest przez zespół uprawnień składających się na regułę rzetelnego procesu, do których należy zaliczyć także prawo do obrony, rozumiane możliwie szeroko, jako „wszystkie sytuacje obrony praw i interesów jednostki w postępowaniach jurysdykcyjnych”³². Autorka ta wskazuje jednak na granice obrony swych praw, które są wyznaczone przez sferę życia prywatnego innych uczestników postępowania, a wprowadzające, jak dalej konstatuje, pierwiastek humanizmu do procesu, ograniczając chociażby wykorzystywanie w procesie cywilnym dowodów sprzecznych z prawem. Budzi pewną wątpliwość stanowisko zajmowane przez autorkę, która twierdzi, iż niedopuszczalne jest przeprowadzenie dowodu naruszającego sferę intymną człowieka, a zwłaszcza jego dóbr osobistych. W kontekście spraw rodzinnych takie wnioski są zdecydowanie za daleko idące, ponieważ istotą takich postępowań jest roztrząsanie spraw prywatnych wkraczających czy wręcz osadzonych w sferze intymnej. Co za tym idzie, nie wydaje się przekonujące stanowisko *A. Łazarskiej* w tym zakresie, w jakim odmawia ona dopuszczenia tego rodzaju dowodów li tylko ze względu na wkroczenie sądu w sferę intymną jednostki. Poddanie pod rozstrzygnięcie sądu spraw związanych z władzą rodzicielską nad dzieckiem lub spraw małżeńskich niechybnie doprowadzi bowiem do rozpoznania przez sąd szczegółów życia intymnego rodziny, jest to wręcz istota tego rodzaju spraw. Stąd też zaprezentowany przez *A. Łaskowską* pogląd w głosie do wyroku SN z 25.4.2003 r. należy uznać za niedotykający istoty problemu, gdyż autorka koncentruje się na samym subiektywnym przekonaniu współmałżonka o naruszeniu jego dóbr osobistych, jako nieuzasadniającym odmowy przeprowadzenia dowodu, tylko z tego powodu, natomiast nacisk należałoby położyć na powinność wszechstronnego zbadania materiału dowodowego w sprawie, w celu rozstrzygnięcia, czy doszło do zupełnego i trwałego rozkładu pożycia³³.

Szczególną uwagę należy zwrócić na stanowisko przyjęte przez Europejski Trybunał Praw Człowieka podejmujące problematykę relacji dowodów o charakterze bezprawnym i zachowania standardu rzetelnego procesu, umiejscawiając

²⁷ *T. Zembrzusi*, [w:] *Ł. Błaszczak, K. Markiewicz, E. Rudkowska-Ząbczyk* (red.), *Dowody...*, s. 72–75.

²⁸ *E. Marszałkowska-Krześ* (red.), *Meritum Postępowanie cywilne*, Warszawa 2017, s. 33.

²⁹ *T. Zembrzusi*, [w:] *Ł. Błaszczak, K. Markiewicz, E. Rudkowska-Ząbczyk* (red.), *Dowody...*, s. 72–75.

³⁰ I ACa 504/11, OSAB 2013, Nr 1, s. 17.

³¹ *Ł. Czarnecki*, *Dopuszczalność tzw. dowodu bezprawnego (nielegalnego, sprzecznego z prawem) w procesie cywilnym*, MoP 2016, Nr 16, s. 7.

³² *A. Łazarska*, *Rzetelny proces cywilny*, Warszawa 2012, s. 317 i n.

³³ *A. Łaskowska*, *Głosa do wyr. SN z 25.4.2003 r., IV KKN 94/01, PS 2004, Nr 11–12, poz. 156, teza 2.*

to na płaszczyźnie relacji art. 8 z art. 6 EKPCz. W pierwszej kolejności należy zauważyć, że odnośnie do oceny rzetelności czy sprawiedliwości przeprowadzenia procesu – te terminy funkcjonują bowiem zamiennie – niezbędna jest ocena całości kształtu okoliczności sprawy, jak przyjął Europejski Trybunał Praw Człowieka w wyroku z 19.4.1993 r.³⁴. Podkreślić należy także, iż rolą sądu konwencyjnego jest badanie, czy proces nosił znamiona rzetelnego, a nie wtórnego rozpoznawania sprawy, w charakterze sądu trzeciej instancji. Trybunał bowiem stwierdza, czy interpretacja przepisów zastosowana przez sąd krajowy jest zbieżna ze standardami konwencyjnymi³⁵. Jednak wyłącznie prawu krajowemu pozostawiono do rozstrzygnięcia kwestię dopuszczalności poszczególnych dowodów, ponieważ Konwencja nie zawiera katalogu dopuszczalnych dowodów. Ocena, czy wprowadzenie danego dowodu uzyskanego w sposób bezprawny narusza standard konwencyjny, odnosić powinna się do całości przebiegu procesu, a samo uzyskanie i wykorzystanie takiego dowodu nie dyskwalifikuje automatycznie postępowania. Niejednokrotnie dowód uzyskany w sposób bezprawny może stanowić jedyne źródło dowodowe, stanowiąc poparcie dla wysuwanych tez, w szczególności w sprawach z zakresu prawa rodzinnego, w tym sprawach rozwodowych, gdzie obligatoryjną przesłanką pozytywną dla orzeczenia o rozwiązaniu małżeństwa jest trwały i zupełny rozkład pożycia małżeńskiego, a to, jak trafnie zauważa *J. Gołaczyński*, bardzo często może zostać udowodnione jedynie po przeprowadzeniu dowodu bezprawnego, gdyż dotyczy sytuacji i relacji intymnych, odbywających się niepublicznie, a co za tym idzie – samo przesłuchanie świadków i stron, na przykład na okoliczność zdrady małżeńskiej, może nie rozwiązać wszelkich wątpliwości dotyczących takiej sytuacji³⁶.

Istotną dystynkcję w kategorii tak zwanych dowodów nielegalnych zauważa *L. Czarnecki*, ponieważ zadaje on pytanie, czy sąd cywilny powinien z góry dyskwalifikować każdy dowód uzyskany w wyniku przestępstwa³⁷. Rozróżnia bowiem środki dowodowe zawierające fałsz intelektualny, a zatem oparte na dokumencie podrobionym lub przerobionym, tudzież uzyskane w wyniku groźby lub przymusu, a środki dowodowe, uzyskane bez zgody, a nawet wiedzy innych osób, zwłaszcza w kontekście wypełnienia dyspozycji art. 267 KK. Przedmiotem dowodu, zgodnie z przywoływanym już brzmieniem art. 227 KPC, są fakty mające istotne znaczenie dla rozstrzygnięcia. Środek dowodowy, który zawiera fałsz intelektualny, nie może stanowić podstawy rozstrzygnięć faktycznych, gdyż uniemożliwiałoby to wydanie sprawiedliwego rozstrzygnięcia, opartego na faktach. Stąd też art. 401¹ KPC jako jedną z podstaw wznowienia postępowania uczynił oparcie wyroku na dokumencie podrobionym lub przerobionym. Nie dotyczy to jednak sytuacji, w której nielegalne było samo pozyskanie środka dowodowego, natomiast środek dowodowy nie zawiera fałszu intelektualnego.

Odminną kwestią jest natomiast sama ocena takiego dowodu w świetle zasad wynikających z art. 233 KPC, który mówi o swobodnej ocenie wiarygodności i mocy dowodu, na podstawie wszechstronnego rozważenia zebranego materiału. *Ł. Czarnecki* podnosi, iż sąd samodzielnie może uznać, które dowody są niewiarygodne, nie czekając na orzeczenie sądu karnego w tym zakresie³⁸.

Wśród możliwych sposobów rozwiązania tego węzłowego zagadnienia leżeć może brzmienie art. 3 KPC. Jak zauważa bowiem *J. Gołaczyński*, w sprawach chociażby rozwodowych, następuje konflikt pomiędzy prawem do ochrony rodziny a wolnością komunikowania się i prawem do autonomii informacyjnej oraz prawem do sądu³⁹. W takim sporze któreś z tych wartości muszą w konkretnej sprawie ustąpić pozostałym. Co za tym idzie, skoro klauzula dobrych obyczajów nakłada na strony i uczestników postępowania obowiązek dokonywania czynności procesowych zgodnie z dobrymi obyczajami, dawać wyjaśnienia co do okoliczności sprawy zgodnie z prawdą i bez zatajania czegokolwiek oraz przedstawiać dowody, to tym bardziej sąd może oceniać ich zachowania (a także podejmowane akcje procesowe) przez pryzmat klauzuli dobrych obyczajów. Z punktu widzenia dobrych obyczajów, będących wszak płaszczyzną ocenną, równie naganne może być zachowanie strony ukrywającej fakty i zatajającej fakty procesowo dla niej niekorzystne, jak też zachowanie drugiej strony, która w sposób sprzeczny z prawem pozyskuje dowody takich niekorzystnych okoliczności.

Rozstrzygając sprawę cywilną, sąd związany jest zasadą swobodnej oceny dowodów, co nakłada na niego następujące obowiązki: po pierwsze – wszechstronnego rozważenia zebranego w sprawie materiału, po drugie – uwzględnienia wszystkich dowodów przeprowadzonych w sprawie, po trzecie – skonkretyzowania okoliczności towarzyszących przeprowadzeniu poszczególnych dowodów mających znaczenie dla oceny ich mocy i wiarygodności, a wreszcie po czwarte – wskazania jednoznacznego kryterium oraz argumentacji pozwalającej wyższej instancji i skarżącemu na weryfikację dokonanej oceny w przedmiocie uznania dowodu za wiarygodny bądź też jego zdyskwalifikowanie⁴⁰. W przypadku dopuszczenia dowodu z korespondencji internetowej, który został uzyskany z naruszeniem przepisów prawa, sąd

³⁴ Zob. wyrok ETPCz z 19.4.1993 r., 13942/88, w sprawie *Kraska* przeciwko Szwajcarii, par. 30

³⁵ *L. Garlicki, P. Hofmański, A. Wróbel*, Konwencja o ochronie praw człowieka i podstawowych wolności. T. I, Komentarz do artykułów 1–18, Warszawa 2010, s. 45.

³⁶ *J. Gołaczyński*, Dowody....

³⁷ *Ł. Czarnecki*, Dopuszczalność..., s. 8.

³⁸ *Ibidem*, s. 10.

³⁹ *J. Gołaczyński*, Dowody....

⁴⁰ *K. Flaga Gieruszyńska*, [w:] *A. Zieliński* (red.), Kodeks postępowania cywilnego. Komentarz, Legalis/el. 2016. komentarz do art. 233.

obowiązany jest potraktować taki dowód jak każdy inny dowód w sprawie. W szczególności zatem powinien zbadać jego treść, odnosząc ją do pozostałych dowodów w sprawie, a także wziąć pod uwagę reakcję stron i świadków na taki dowód. Komunikacja internetowa, charakteryzująca się często mnogością wątków oraz chaotycznością, stanowić może przedmiot manipulacji i tendencyjnego przedstawienia faktów, więc sąd, dopuszczając taki dowód, powinien w szczególności mieć to na uwadze zaraz obok możliwości popełnienia fałszu intelektualnego na nim⁴¹. Z uwagi na podniesione wątpliwości stosowne byłoby uwiarygodnienie treści korespondencji internetowej stron przez notariusza poprzez sporządzenie protokołu otwarcia komunikatora internetowego. Niewątpliwym minusem takiego rozwiązania byłaby konieczność ominięcia zabezpieczeń w obecności notariusza celem sporządzenia przez niego protokołu, co narażałoby go na odpowiedzialność karną oraz dyscyplinarną. Przedstawienie dowodów w postaci przedstawienia wydruków z komunikatora internetowego w postaci tzw. zrzutów ekranu może jednak zostać łatwo zakwestionowane przez stronę jako dowód podatny na manipulacje w nawet najprostszych programach graficznych.

Omawiając dopuszczalność wprowadzenia tego rodzaju dowodu, należy odnieść się do formułowanych *de lege lata* poglądów doktryny o konieczności uwzględnienia przez sąd w konkretnych sprawach konfliktu wartości konstytucyjnych, idąc chociażby za A. Laskowską⁴² czy D. Korszeniem⁴³, zwłaszcza iż art. 8 ust. 2 Konstytucji RP przyznaje sądom uprawnienie do bezpośredniego stosowania Konstytucji. W szczególności, idąc za P. Tuleją, sądy wyjątkowo uprawnione są do bezpośredniego stosowania norm konstytucyjnych, opierając swe rozstrzygnięcie (dopuszczenie lub odmowa dopuszczenia wniosku dowodowego jest orzeczeniem) wyłącznie na tekście ustawy zasadniczej, co w konkretnej sprawie powinno się przełożyć na odmowę dopuszczenia wniosku dowodowego lub dopuszczeniu dowodu, poprzez przyznanie prymatu w danym wypadku art. 45 Konstytucji albo art. 47 Konstytucji⁴⁴. Co do zasady, wydaje się jednak, iż stanowisko zaproponowane przez Ł. Czarneckiego zasługuje na uznanie, wskazuje on bowiem na powinność dopuszczenia przez sąd każdego dowodu, który przyczyni się do rozstrzygnięcia sprawy, zgodnie z treścią art. 227 KPC⁴⁵. Ewentualna odmowa rozstrzygnięcia sprawy, na podstawie takiego nielegalnego dowodu, powinna nastąpić dopiero po merytorycznym rozpoznaniu jego przydatności⁴⁶. Wnioskujący o przeprowadzenie dowodu nielegalnie zdobytego jest już bowiem narażony na odpowiedzialność karną, a odmowa dopuszczenia takiego dowodu może zarazem doprowadzić do przegranej przez niego sprawy cywilnej, gdyż pozbawiony będzie przy takim rozstrzygnięciu sądu być może jedynej możliwości udowodnienia swojego roszczenia. Zastanowić się zatem należy, czy z takiego holistycznego punktu widzenia sankcja karna nie

jest już, sama w sobie, wystarczająco ujemną konsekwencją zachowania wnioskującego o dopuszczenie podobnego dowodu. Przyjmując pogląd, który został wyrażony przez Ł. Czarneckiego, przegrana w procesie cywilnym, wynikająca z niemożności udowodnienia swych racji, nie stanowiłaby już negatywnie kwalifikowanego następstwa posłużenia się dowodem uzyskanym nielegalnie, gdyż sąd o jego przydatności decydowałby w drodze rozstrzygnięcia opartego na zasadzie swobodnej oceny dowodów.

Podsumowanie

Ł. Czarnecki słusznie wprowadza dystynkcję pomiędzy odpowiedzialnością karną, jako konsekwencją przedstawienia dowodu zdobytego w sposób nielegalny, a ryzykiem przegranej procesu cywilnego, z uwagi na brak potencjalnie innych dowodów mogących przyczynić się do rozstrzygnięcia sprawy zgodnie z prawdą, jak nakazuje treść art. 3 KPC. W związku z powyższym należałoby, co do zasady, opowiadać się za dopuszczalnością przeprowadzenia tego rodzaju dowodów w sprawach cywilnych. W moim przekonaniu bowiem tak długo, jak Kodeks postępowania cywilnego nie będzie wprost regulował tej kwestii, to sądy będą musiały dokonywać *in concreto* ważenia konstytucyjnych wartości, rozstrzygając, czy w konkretnej sprawie bezwzględna realizacja zasady prawdy materialnej oraz prawa jednostki do sądu pochłania konstytucyjną ochronę korespondencji, a nawet szerzej – prywatności. Błędne zdawałoby się założenie, iż skoro procedura karna i administracyjna posiadają swoiste regulacje, odnoszące się do dowodów bezprawnych, należałoby analogicznie rozstrzygać próbę przedstawienia wniosków dowodowych uzyskanych nielegalnie w procedurze cywilnej. Wykładnia systemowa powinna jednak uwzględniać zasadnicze różnice między procedurą w sprawach cywilnych, w których występują, przynajmniej teoretycznie, podmioty równe sobie, z procedurą w sprawach publicznoprawnych, gdzie o równości stron przy zderzeniu obywatela z *imperium* trudno mówić. Tym samym specyfika niektórych spraw, w szczególności spraw rodzinnych, gdzie ich istotą jest roztrząsanie szczegółów życia intymnego, z uwagi na praktyczną trudność w udowodnieniu pewnych twierdzeń i faktów, wymagać może, w okolicznościach konkretnej sprawy, uwzględnienia także dowodów o nielegalnej proveniencji.

⁴¹ *Ibidem*.

⁴² A. Laskowska, Dowody w postępowaniu..., s. 96.

⁴³ D. Korszeń, Zakres zakazu..., s. 18 i n.

⁴⁴ P. Tuleja, [w:] M. Saffan, L. Bosek (red.), Konstytucja RP. T. I. Komentarz do art. 1–86, Warszawa 2016, komentarz do art. 8.

⁴⁵ Ł. Czarnecki, Dopuszczalność..., s. 10.

⁴⁶ *Ibidem*.

Ta sama wykładnia systemowa nakazuje jednak, by proces stosowania prawa pozostawał w zgodności z aktami hierarchicznie wyższego rzędu. Stąd też wyrażony wyżej postulat, aby każdorazowo sądy dokonywały oceny przydatności danego wniosku dowodowego dla sprawiedliwego rozstrzygnięcia sprawy, powinien głośno wybrzmieć, ponieważ to na sądach spoczywać będzie odpowiedzialność

za kształtowanie przejrzystej linii orzeczniczej. Tym samym w każdej sprawie, w której dochodzi do ważenia wartości konstytucyjnych, sąd nie automatycznie, a dogłębnie analizując stan faktyczny sprawy, powinien zdecydować się na dopuszczenie lub oddalenie wniosku dowodowego dotkniętego bezprawnością.

Słowa kluczowe: dowód nielegalny, dowód bezprawny, komunikacja internetowa, proces cywilny, doktryna owoców zatrutego drzewa.

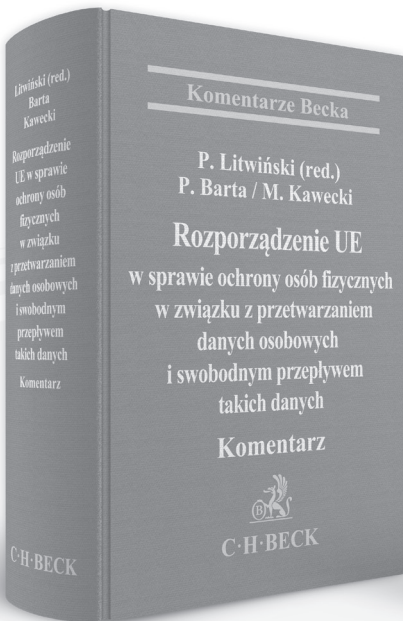
Unlawful evidence from the Internet correspondence of parties in civil proceedings

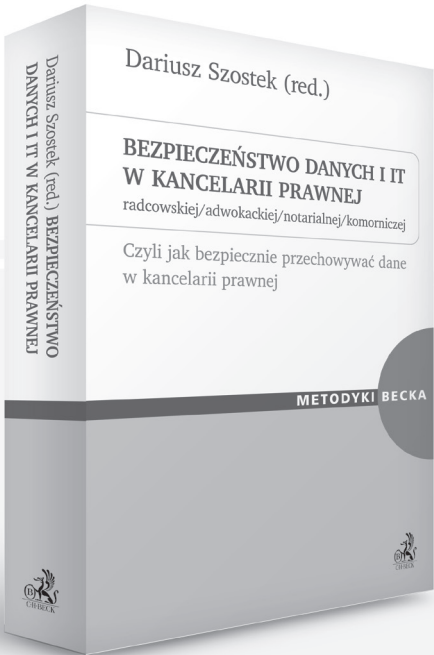
The aim of the present study is the analysis of admissibility of introducing illegally obtained evidence from the Internet correspondence into civil proceedings. In the absence of an appropriate legal norm in the Civil Procedure Rules (CPR), which would directly define the (in)admissibility of the relevant phenomenon, it becomes necessary to make legal comparative studies of constitutional regulations, as well as refer to acts of international law. At the same time, the author reviews tendencies appearing in literature and judicial decisions within the scope of possibility of using the above-mentioned illegal evidence in civil proceedings.

Keywords: illegal evidence, unlawful evidence, Internet correspondence, civil trial, fruit of the poisonous tree doctrine.



RODO





Zamów: **tel. 22 31 12 222** www.ksiegarnia.beck.pl

Postanowienia dotyczące dziedziczenia profilu zawarte w regulaminie portalu Facebook a prawo polskie

Patrycja Budrewicz¹

W niniejszym opracowaniu autorka, w związku z rosnącą popularnością portali społecznościowych, w szczególności serwisu Facebook, zwraca uwagę na ujawniającą się potrzebę uregulowania sytuacji treści cyfrowych po śmierci ich właściciela. W swojej pracy, definiując treści cyfrowe, wskazuje na możliwość dziedziczenia treści powiązanych z kontem na portalu Facebook, a także porusza kwestię prawa właściwego w sprawach pomiędzy użytkownikami serwisu a operatorem. Celem autorki jest przede wszystkim analiza rozwiązań zaproponowanych przez operatora Facebooka w przypadku śmierci użytkownika w kontekście krajowych regulacji prawa spadkowego.

Uwagi wstępne

Facebook to największy – z ponad miliardem użytkowników², i prawdopodobnie najbardziej znany serwis społecznościowy, który początkowo miał służyć tylko studentom Uniwersytetu Harvarda, w celach komunikacyjnych. Rozważania nad prawnymi uregulowaniami po śmierci użytkowników Facebooka trzeba rozpocząć od wytłumaczenia, czym jest ten serwis społecznościowy. Mimo że portali, takich jak Facebook, jest na świecie coraz więcej, to polski ustawodawca jeszcze nie stworzył dla nich definicji legalnej. Jak podaje Słownik języka polskiego PWN, pojęcie serwis społecznościowy może być używane zamiennie z pojęciem portalu społecznościowego i jest to witryna współtworzona przez społeczność internautów o podobnych zainteresowaniach, w celu interakcji między nimi³. Sięgając do źródeł zagranicznych, a dokładnie do Opinii Grupy Roboczej Artykułu 29 ds. ochrony danych Nr 5/2009 z 12.6.2009 r. w sprawie portali społecznościowych, odnajdziemy tam definicję portalu społecznościowego. Portale zostały określone jako sieciowe serwisy społecznościowe oraz zdefiniowane jako platformy komunikacyjne on-line, oferujące użytkownikom, będącym osobami fizycznymi, przyłączanie się do istniejących już grup bądź tworzenie nowych, podobnych sieci⁴. Można wyróżnić wiele cech charakterystycznych dla sieciowych serwisów społecznościowych, ale trzy z nich są fundamentalne, tj.:

- 1) możliwość tworzenia własnego, indywidualnego „profilu” na portalu przez przekazanie swoich danych osobowych;
- 2) publikowanie, za pomocą tego profilu, informacji o sobie samym i innych własnych materiałów w postaci danych cyfrowych, jak np. zdjęć, filmów wideo czy linków do stron internetowych, oraz
- 3) wyszukiwanie i tworzenie grupy znajomych, w postaci bazy kontaktów, w celu komunikacji z poszczególnymi użytkownikami portalu.

Podsumowując, można powiedzieć, że serwisy (portale) społecznościowe są swojego rodzaju stroną internetową, skupiającą grupę ludzi o podobnych zainteresowaniach, oferującą usługi w postaci nawiązywania nowych kontaktów oraz utrzymywania znajomości, a także prezentowania siebie, poprzez m.in. udostępnianie swoich materiałów dla szerszego grona odbiorców, dzięki spersonalizowanym profilom.

Mając już definicję serwisu, warto przyjrzeć się znaczeniu samego profilu na portalu społecznościowym. Słownik PWN traktuje go po prostu jako część serwisu, która zawiera informacje o użytkowniku⁵. Profil (jak też tzw. tablice) na Facebooku, na którym dana osoba może publikować zdjęcia, posty itp., jest przynależny tylko do osoby prywatnej, więc tworzy jej tożsamość internetową. Można powiedzieć, że profil jest krótkim opisem czyjegoś życia, pracy, charakteru itp., zawierającym informacje o zainteresowaniach⁶.

Pojęcie dziedziczenia i spadku

W tym miejscu konieczne jest wstępne omówienie polskiej regulacji dotyczącej dziedziczenia, inaczej sukcesji uniwersalnej po spadkodawcy, której przedmiotem jest spadek. Ustawodawca nie uregulował wyraźnie definicji spadku, jednak można ją odtworzyć z art. 922 § 1 KC, na podstawie

¹ Autorka jest studentką IV roku prawa na Uniwersytecie Wrocławskim na Wydziale Prawa, Administracji i Ekonomii.

² O. Smith, Facebook terms and conditions: why you don't own your online life, <https://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html> (dostęp z 24.3.2018 r.).

³ Zob. <https://sjp.pwn.pl/sjp/serwis-spoecznościowy;5579205.html> (dostęp z 22.3.2018 r.).

⁴ Zob. http://www.memex.pl/doc/Portale_spoecznościowe_GR_ART_29.pdf (dostęp z 22.3.2018 r.).

⁵ Zob. <https://sjp.pwn.pl/sjp/serwis-spoecznościowy;5579205.html> (dostęp z 22.3.2018 r.).

⁶ Zob. <https://dictionary.cambridge.org/dictionary/english/profile> (dostęp z 22.3.2018 r.).

którego do spadku zalicza się cywilnoprawne (czyli wynikające ze stosunków cywilnoprawnych) prawa i obowiązki majątkowe zmarłego, które w chwili śmierci przechodzą na jedną lub kilka osób⁷, jeśli nie zostały wyłączone ze spadku na mocy przepisów szczególnych bądź nie są ściśle związane z osobą zmarłego⁸. Podział na prawa majątkowe i niemajątkowe ulega zatarciu, co potwierdza orzecznictwo SN⁹. Rozróżnienie to jest jednak bardzo istotne, ponieważ niemajątkowe prawa i obowiązki, co do zasady, wygasają z chwilą śmierci podmiotu zobowiązanego lub uprawnionego, a zatem są niedziedziczne (np. prawo osobistości)¹⁰. Nauka dzieli wyłączenia ze spadku na cztery grupy:

- 1) prawa, które zaspokajają indywidualny ekonomiczny interes uprawnionego, gdzie śmierć podmiotu powoduje wygaśnięcie prawa, przez brak interesu (np. służebność osobista)¹¹;
- 2) prawa, których treść zależna jest od osobistych potrzeb uprawnionego (np. prawo do renty przy rozstroju zdrowia);
- 3) prawa i obowiązki ze stosunków prawnych, w których niezbędna do właściwego spełnienia świadczenia jest osobista zdolność bądź szczególne kwalifikacje zmarłego dłużnika (np. umowa o świadczenie usług, w której zastrzeżono osobisty charakter świadczenia zobowiązanego);
- 4) prawa i obowiązki wynikające ze stosunków prawnych opartych na zaufaniu (np. umowa zlecenia).

Jak wynika z powyższego, spadek obejmuje praktycznie całą sytuację majątkową zmarłego i wyliczenie wszystkich składników majątku jest w zasadzie niemożliwe.

Dodatkowo, w normach szczególnych Kodeksu cywilnego (katalog zamknięty), zostały przewidziane regulacje dotyczące poszczególnych przedmiotów, które z chwilą śmierci przechodzą na oznaczone w ustawie lub przez spadkodawcę osoby, niezależnie od tego, czy są one spadkobiercami¹² (tzw. sukcesja singularna). Stanowią one wyjątki od ogólnej zasady prawa spadkowego, jakim jest dziedziczenie, a najbardziej znanym spośród nich jest zapis windykacyjny.

Pojęcie i dziedziczenie treści cyfrowych

Profil na Facebooku, jak też materiały na nim publikowane należą do zakresu pojęcia treści cyfrowych. Ustawa z 30.5.2014 r. o prawach konsumenta¹³, która wdrożyła dyrektywę Parlamentu Europejskiego i Rady 2011/83/UE z 25.10.2011 r. w sprawie praw konsumentów¹⁴, w art. 2 pkt 5 definiuje pojęcie treści cyfrowej, jako dane wytwarzane i dostarczane w postaci cyfrowej. Dane cyfrowe (ang. *digital assets*) mogą mieć wiele form, np. pliki wideo, muzycz-

ne, zdjęcia przechowywane na stronach internetowych czy tzw. internetowych chmurach, a nawet same portale.

Po wielu próbach stworzenia odpowiedniej definicji, w USA w lipcu 2014 r. uchwalono *Fiduciary Access To Digital Assets Act*¹⁵, w którym treści cyfrowe zostały zdefiniowane jako zapisy elektroniczne, do których jednostki mają prawo lub które służą jej interesom, co obejmuje swym zakresem zapisy istniejące (jak informacje przechowywane na komputerze użytkownika, materiał przesłany na strony internetowe czy zapisy komunikacji elektronicznej), a także te, które dopiero powstaną.

Mając na względzie powyższe definicje „treści cyfrowych”, można powiedzieć, że konto na Facebooku wraz z zawartością mieści się w tym zakresie, ponieważ korzystanie z niego zakłada przesyłanie zdjęć, filmów, wiadomości, publikowane są posty i komentarze, co jest niczym innym jak przesyłaniem wytworzonych przez użytkownika danych cyfrowych i dostarczaniem ich na serwery administratora portalu. Konto jest nośnikiem, na którym zapisane są dane cyfrowe, a tym samym treścią cyfrową. Aby uznać, że treści cyfrowe mogą być przedmiotem obrotu *mortis causa*, należy sprawdzić, czy spełniają cechy pozwalające na zaliczenie ich do masy spadkowej według Kodeksu cywilnego. Skupiając się na samym profilu na Facebooku, po pierwsze, możliwość korzystania z tego serwisu wiąże się z zawarciem adhezyjnej umowy elektronicznej z dostawcą usług internetowych typu *click-wrap*, czyli zaakceptowaniem z góry narzuconych zasad korzystania¹⁶. Umowa, którą zawieramy z dostawcą usługi, jest umową obligacyjną oraz wzajemną, i z racji zaliczenia praw i obowiązków obligacyjnych (z wyjątkami) do spadku nie ulega wątpliwości, że na jej podstawie powstaje stosunek cywilnoprawny (zobowiązaniowy). Bardziej problematyczna jest kwestia przesłanki majątkowego charakteru. Jeśli by przyjąć, że spośród treści cyfrowych można wyróżnić takie, które mają charakter osobisty, np. zdjęcia, dane osobiste poczty e-mail, takie, które można zaliczyć do treści społecznościowych, np. właśnie te na portalu Facebook, te związane z prowadzeniem działalności gospodarczej, np. domena internetowa, oraz te służące realizacji bieżących potrzeb codziennych, np. związane z obsługą serwisu *PayPal*, to już poprzez różnorodność treści można zobaczyć, że nie wszystkie

⁷ Zob. art. 922 § 1 KC.

⁸ Zob. art. 922 § 2 KC.

⁹ Zob. postanowienie SN z 10.4.2002 r., IV CZ 29/02, OSP 2003, z. 4, poz. 52.

¹⁰ Szerzej zob. P. Księżak, *Prawo spadkowe*, Warszawa 2017, s. 49.

¹¹ *Ibidem*, s. 50.

¹² Zob. art. 922 § 2 KC.

¹³ Tj. Dz.U. z 2017 r. poz. 683 ze zm.

¹⁴ Dz.Urz. UE L Nr 304, s. 64.

¹⁵ *Fiduciary Access to Digital Assets Act* z 22.7.2014 r., Section 2(10).

¹⁶ M. Załucki, „Facebook”, „Twitter”, „My Space”... wirtualny świat serwisów społecznościowych *mortis causa*. Zarys problematyki, Wrocławskie Studia Sądowe 2014, Nr 4, s. 234.

z nich będą mogły być zakwalifikowane do masy spadkowej¹⁷. Powstaje pytanie, czy konto na Facebooku ma jakąś wartość. Trzeba mieć na uwadze, że wiele czynników wpływa na wartość konta, np. liczba znajomych, fanów, aktywność użytkownika czy ilość udostępnianych danych cyfrowych¹⁸. Nie wolno też zapominać o najważniejszym czynniku wpływającym na wartość konta, tj. byciu osobą publicznie znaną. W takim wypadku charakter majątkowy nie powinien budzić wątpliwości. Co do kont pozostałych osób wskazuje się, że zostało ono wycenione na około 14\$ za użytkownika, a wartość z każdym rokiem wzrasta¹⁹. Przyjąć należy, iż konta na portalach społecznościowych, w całości bądź w części, mogą mieć wartość majątkową, podobnie zresztą jak zgromadzone na nich dane, przy czym kategoryczne rozstrzygnięcie tego, ze względu na różnorodność treści cyfrowych, jest niemożliwe.

Przyglądając się wyłączeniom z masy spadkowej w kontekście treści cyfrowych, a na wstępie pierwszemu z nich, nie można z całą pewnością stwierdzić, że samo konto na Facebooku będzie zaspokajało osobisty interes spadkodawcy, mimo że konta te taki osobisty charakter mają. Często bowiem nie są one przeznaczone do zaspokojenia tylko indywidualnych interesów posiadacza konta, ale także służą potrzebom innych użytkowników portalu, m.in. przez przeglądanie udostępnionych przez użytkownika treści czy kontakt z nim²⁰. Sprawę należałoby zbadać *ad casum*. Nie ulega za to wątpliwości, że przez korzystanie z tego konta użytkownik może realizować swoje indywidualne potrzeby (m.in. potrzebę kontaktu z innymi osobami), a wtedy prawo do dostępu do konta wygasa wraz ze śmiercią użytkownika, ze względu na to, iż ustaje cel. Trzeba tutaj rozgraniczyć możliwość dziedziczenia całego konta od dziedziczenia tylko niektórych treści na nim rozpowszechnionych, choć bez dostępu do całego konta trudno jest uzyskać dostęp do konkretnych treści cyfrowych, które podlegałyby dziedziczeniu²¹. Zważając na cele niniejszego artykułu, wydaje się zbędne omawianie wyłączenia trzeciego, ponieważ użytkownik, wybierając dostawcę Facebooka, raczej nie kieruje się jego szczególnymi kwalifikacjami, a właśnie funkcjonalnością portalu. Trudno sobie jednak wyobrazić stosunek prawny powstający po zawiązaniu umowy z usługodawcą, nieoparty na zaufaniu. Mimo że zaufanie nie jest pierwszą kwestią braną pod uwagę przy wyborze dostawcy usług i raczej chodzi o jego popularność, to dopuszczenie spadkobierców do konta rodzi wątpliwości w kwestii ochrony prywatności użytkowników, z którymi zmarły się kontaktował, oraz umożliwia podszywanie się pod zmarłego. Usługodawca, nie chcąc tracić zaufania innych użytkowników, wprowadził regulację zabraniającą przekazywania swojego konta komukolwiek, bez jego pisemnego zezwolenia²². Podsumowując, trudno jest jednoznacznie stwierdzić, że konto na Facebooku podlega dziedziczeniu, szczególnie ze względu na wzajemne zaufanie stron umowy oraz osobisty charakter konta, jednak nie jest to wykluczone.

Należałoby też w tym momencie dokonać rozgraniczenia na możliwość dziedziczenia samego konta oraz jedynie niektórych treści cyfrowych z nim powiązanych, wytworzonych i dostarczonych na podstawie umowy o świadczenie usług drogą elektroniczną, które to w większości można zaliczyć do masy spadkowej.

Śmierć użytkownika Facebooka a regulamin portalu

Przechodząc do postanowień portalu dotyczących sytuacji danych cyfrowych po śmierci użytkownika, należy podkreślić, iż dostęp do danych na koncie chroniony jest poprzez hasło i login, co stwarza przeróżne problemy w zakresie ich dziedziczenia. Na przeszkodzie sukcesji treści cyfrowych w poszczególnych serwisach stoją często regulaminy tych serwisów, na które użytkownicy musieli wyrazić swoją zgodę.

Za życia użytkownik Facebooka może dysponować swoim kontem w zasadzie w sposób dowolny, nienaruszający umowy, czyli może z niego korzystać, usunąć go, dezaktywować, jednak jego los po śmierci użytkownika nie jest jasny. Facebook, z racji tego, że został stworzony przez studentów dla studentów, początkowo nie posiadał rozwiązań, jak sobie radzić w przypadku śmierci któregoś z użytkowników. Jednak musiało to zostać rozwiązane, z uwzględnieniem ochrony prywatności i zaufania obecnych oraz przyszłych użytkowników, jak też potrzeby rodziny zmarłego.

Nie można niestety powiedzieć, że dzisiejsze rozwiązania stosowane przez Facebooka rozwiązują wszelkie problemy, ale trzeba przeanalizować sposób, w jaki się one wykształciły.

Początkowo konta zmarłych użytkowników były po prostu usuwane po 30 dniach²³. Ten 30-dniowy okres (ang. *30-day window*), w którym znajomi użytkownika mogli dalej publikować na jego tablicy posty, był zwany upamiętnianiem (ang. *memorialization*). Jednak ta regulacja się nie sprawdziła, na co wskazuje głośna sprawa *B. Foughta* zamordowanego w marcu 2007 r. Pomimo ponad 100 próśb od jego rodziny i przyjaciół o zachowanie jego profilu, ten został usunięty²⁴.

¹⁷ M. Załucki, Facebook..., s. 238–239.

¹⁸ M. Mądel, Następstwo prawne treści cyfrowych na wypadek śmierci, Kraków 2017, s. 170.

¹⁹ K. Close, Your Existence Is Worth About \$14 to Facebook, <http://time.com/money/4197920/facebook-what-user-views-worth/> (dostęp z 26.3.2018 r.).

²⁰ Zob. M. Mądel, Następstwo prawne..., s. 178–179.

²¹ Szerzej *ibidem*, s. 183–184.

²² Zob. Regulamin pkt 3.1, https://www.facebook.com/legal/terms/update?ref=old_policy (dostęp z 9.5.2018 r.).

²³ D. McCallig, Facebook after death: an evolving policy in a social network, *International Journal of Law and Information Technology* 2014, Vol. 22, No. 2, s. 117.

²⁴ Szerzej zob. komentarz A. Johnson *Fought* z 7.5.2007 r. w grupie Facebook Memorialization Is Misguided: Dead Friends Are Still People, <https://www.facebook.com/groups/2785485042/search/?query=fought> (dostęp z 24.3.2018 r. –wymagane jest posiadanie konta).

Zmiana polityki Facebooka i w efekcie umożliwienie tworzenia permanentnych ksiąg pamiątkowych, dzięki czemu przywrócono profil *B. Foughta*, została wprowadzona na skutek kampanii studentów colleg'u opowiadającej się za nieusuwaniami profili studentów zamordowanych w strzelaninie w Virginia Tech w kwietniu 2007 r. W tamtym okresie konta ofiar stały się szeroko znanymi miejscami pamięci (ang. *high-profile memorials*), gdzie ludzie publikowali słowa otuchy²⁵. Warto sobie uświadomić, że przecież profil na Facebooku nie tylko odzwierciedla samych użytkowników i stanowi historyczny zapis, ale jest także przechowalną materiałów, której autorami są inne jednostki pozostające ze sobą w relacji bądź współpracy²⁶. Naturalne wydaje się więc, że strata nawet części opublikowanych czy wspólnie wypracowanych danych spotka się z oporem.

Obecnie na wypadek śmierci użytkownika Facebook – w Centrum pomocy on-line²⁷ – przewiduje dwie opcje. Po pierwsze, użytkownik może wyznaczyć opiekuna konta, które uzyska status *In memoriam* po tym, jak Facebook otrzyma informację o jego śmierci (usługa Legacy Contacts). Po drugie, można wybrać opcję trwałego usunięcia konta.

Tylko częściowo kwestia konta po śmierci jego użytkownika została uregulowana w nowym Regulaminie serwisu z 19.4.2018 r.²⁸. Ponadto biorąc pod uwagę informacje uzyskane z Centrum pomocy i formularzy, obecnie wydaje się, że Facebook zaleca wybór opcji pierwszej, ponieważ zabezpiecza ona materiały związane z kontem osoby zmarłej i tworzy swego rodzaju księgę pamiątkową, w której znajomi dzielą się wspomnieniami o zmarłym²⁹. Niektóre z funkcji dostępnych dla kont aktywnych pozostają wtedy ograniczone, ale znajomi dalej mogą udostępniać posty na tablicy użytkownika (jeśli ustawienia konta na to zezwalają), a nawet wysyłać prywatne wiadomości. Wszelkie dotychczasowe aktywności, materiały udostępnione za życia, jak np. zdjęcia, nie są kasowane. Wyłącznikiem tego konta jest jego wyraźne oznakowanie, przez słowa *In memoriam* obok imienia i nazwiska, oraz usunięcie wrażliwych informacji, danych kontaktowych oraz statusu. Plusem jest też fakt, że sam profil nie pojawi się w „sugerowanych znajomych”, we wbudowanej w serwis wyszukiwarce czy w przypomnieniach o urodzinach. Do konta nie można się zalogować (nawet w przypadku znajomości hasła), a jego modyfikacje (jak napisanie przypiętego posta np. wiadomości pożegnalnej w imieniu zmarłego, odpowiedzenie na zaproszenie do grona znajomych m.in. od członków rodziny, którzy wcześniej nie posiadali konta na Facebooku, zmiana zdjęcia profilowego) są możliwe, tylko jeśli został ustanowiony opiekun konta, czyli tzw. pełnomocnik do spraw dorobku. Jedynie użytkownik, który ukończył 18 lat, może w każdym momencie ustanowić opiekuna konta (o czym osoba ta zostanie poinformowana automatycznie), a także go zmienić bądź usunąć, wchodząc w ustawienia ogólne swojego konta. Co ważne, osoba taka musi należeć do grona naszych znajomych

na Facebooku. Opiekun konta będzie mógł złożyć prośbę o jego usunięcie, ale sam nie będzie mógł modyfikować starych postów ani usuwać ich i znajomych, wysyłać nowych zaproszeń czy odczytać wiadomości, a nawet zalogować się do konta i dodać nowego opiekuna. Można również rozszerzyć jego zakres uprawnień o pobranie kopii materiałów udostępnionych przez zmarłego na Facebooku. W regulaminie podkreśla się, iż z wnioskiem o udzielenie dostępu do tego typu treści może wystąpić jedynie opiekun konta lub osoba wskazana przez użytkownika w ważnym testamencie lub innym podobnym dokumencie zawierającym wyraźną wolę ujawnienia treści w momencie jego śmierci.

Użytkownik, który nie chce, aby konto było dostępne na Facebooku po jego śmierci, może wybrać opcję jego trwałego usunięcia³⁰. W takim przypadku, wchodząc w ustawienia ogólne, w polecenie „zarządzaj kontem”, trzeba kliknąć w opcję „poproś o usunięcie konta”, a następnie postępować zgodnie z instrukcjami wyświetlanymi na ekranie. Ta opcja uniemożliwia ponowną aktywację konta oraz odzyskanie jakichkolwiek dodanych materiałów, a użytkownicy Facebooka nie będą mogli wtedy wyświetlić tego konta. Jednakże nie wszystkie dane pozostaną usunięte, ponieważ nie dotyczy to np. wiadomości wysyłanych do innych użytkowników. Facebook, w przypadku wybrania opcji usunięcia konta po śmierci, zaleca utworzenie grupy dla znajomych i rodziny, w której będą mogli oni dzielić się wspomnieniami związanymi z osobą zmarłego.

Pojawia się jednak pytanie, co dzieje się, gdy użytkownik nie podejmie żadnej decyzji w tej kwestii. Okazuje się, że w takim przypadku Facebook może na prośbę bliskiego znajomego lub członka rodziny nadać status *In memoriam* kontu (czyli utworzyć tzw. *Memorial Page*). Decyzja w tym zakresie należy jednak wyłącznie do Facebooka. Ważne jest, że jeśli osoba zmarła wcześniej nie ustaliła opiekuna konta, to nikt aktywnie nie będzie mógł nim zarządzać po wysłaniu wniosku o nadanie statusu *In memoriam*³¹. Aby skutecznie złożyć wniosek, administrator portalu wymaga podania danych osoby zmarłej, w tym daty śmierci, a opcjonalnie można załączyć

²⁵ D. McCallig, Facebook..., s. 118.

²⁶ E. Kasket, Access to the Digital Self in Life and Death: Privacy in the Context of Posthumously Persistent Facebook Profiles, scripted, A Journal of Law, Technology & Society 2013.

²⁷ Centrum Pomocy Facebooka, <https://www.facebook.com/help/103897939701143?helpref=search&sr=1&query=Co%20si%C4%99%20stanie%20z%20moim%20kontem%20na%20Facebooku%2C%20kiedy%20umr%C4%99%3F> (dostęp z 24.3.2018 r.).

²⁸ Regulamin pkt 4.5.5, https://www.facebook.com/legal/terms/update?ref=old_policy (dostęp z 9.5.2018 r.).

²⁹ M. Mądel, Następstwo prawne..., s. 105.

³⁰ Szerzej zob. w Centrum pomocy „Jak trwale usunąć konto?”, https://www.facebook.com/help/224562897555674?helpref=faq_content (dostęp z 24.3.2018 r.).

³¹ Zob. Prośba o nadanie statusu *In memoriam*, <https://www.facebook.com/help/contact/651319028315841> (dostęp z 24.3.2018 r.).

akt zgonu i podać link do nekrologu lub innych dokumentów związanych ze śmiercią tej osoby. Podobnie jest w przypadku drugiej możliwości, ponieważ z wnioskiem o usunięcie konta mogą zgłosić się, po weryfikacji pokrewieństwa, członkowie najbliższej rodziny (np. rodzice, współmałżonek) bądź wykonawca testamentu (należy to udowodnić). We wniosku powinno się podać dane osoby zgłaszającej i osoby zmarłej, adres jego osi czasu i e-mail powiązany z kontem tej osoby³².

Oczywiste jest, że Facebook musi mieć dowody śmierci danej osoby, by nie usunąć trwale konta osobie żyjącej. Aby zatem uchronić się np. przed przykrymi żartami ze strony innych osób, Facebook żąda załączenia skanu lub świadectwa zgonu takiej bliskiej osoby albo chociaż dokumentu potwierdzającego, że ma do czynienia z prawomocnym przedstawicielem zmarłej osoby (np. pełnomocnictwo, zaświadczenie o powołaniu na zarządcę majątku spadkowego, testament)³³.

Facebook dopuszcza jeszcze jedną, rzadką sytuację, kiedy dana osoba chciałaby uzyskać dostęp do dodatkowych informacji o koncie zmarłego lub jego zawartości³⁴. W takiej sytuacji można złożyć wniosek, do którego należy dołączyć dowód wskazujący na bycie do tego upoważnionym (np. członek rodziny), kserokopię dowodu tożsamości, dokumentu potwierdzającego związek prawny ze zmarłym, jak też kopię aktu zgonu oraz nakaz sądowy³⁵. Facebook jednak zastrzega, że nie gwarantuje udostępnienia zawartości takiego konta, na co wskazuje sprawa *S. Daftary*³⁶, zmarłej tragicznie w 2008 r., której matka żądała ujawnienia zawartości jej konta z ostatnich 20 dni jej życia, wierząc, że mogły zawierać dowody wskazujące na jej stan umysłu w dniach poprzedzających jej śmierć. Dane te miały zostać przekazane Coroner's Inquest w UK. Serwis stwierdził jednak, że ujawnienie danych przez usługodawcę jest dobrowolne i mimo iż matka *S. Daftary* jest administratorem dóbr córki, nawet sąd nie może mu tego nakazać. W orzeczeniu dotyczącym tej sprawy rację przyznano Facebookowi. Stwierdzono, że prawo precedensowe potwierdza, że pozwy cywilne nie mogą wymuszać na dostawcach, takich jak Facebook, produkcji zapisów, ponieważ byłoby to sprzeczne z ustawą o przechowywaniu informacji (the Stored Communications Act), a sądowi nie przysługuje jurysdykcja w zakresie rozpatrywania, czy wnioskodawcy mogą wyrazić zgodę w imieniu *S. Daftary* na ujawnienie tych treści. To jednak nie wyłącza możliwości dobrowolnego dostarczenia przez Facebooka żądanych materiałów, jeśli uznałby, że wnioskodawcy mają prawo wyrażenia zgody w imieniu zmarłej³⁷.

Podsumowując, Facebook – w przeciwieństwie do niektórych dostawców usług – nie ma w umowie użytkownika z portalem klauzuli, która pozwala na zakończenie obowiązywania kontraktu w przypadku śmierci bądź dezaktywacji konta po upływie konkretnego okresu nieaktywności³⁸. Facebook proces powiadomienia o śmierci użytkownika przekazał bowiem w ręce użytkownika konta, innych użytkowników, a nawet osób spoza tego grona, co pomimo wielu zalet, nie

pozwała na uniknięcie błędnych zgłoszeń mogących doprowadzić do usunięcia konta lub zablokowania możliwości logowania. Uzyskanie dostępu do treści cyfrowych w pewnych przypadkach zależy także wyłącznie od uznania usługodawcy – następcy prawni nie mają na to wpływu³⁹.

Wybór prawa właściwego

Rozpatrując kwestię, jak się ma Regulamin portalu Facebook do polskiego prawa spadkowego, nie można pominąć sprawdzenia, czy krajowe prawo spadkowe będzie w tej sytuacji właściwe. Ponieważ Facebook nie jest polskim portalem, nasuwa się pytanie, czy do sprawy spadkowej po obywatelu polskim zastosowanie mogłyby znaleźć przepisy prawa obcego. W tym przypadku należy udzielić odpowiedzi twierdzącej. Przemawia za tym analiza trzech reguł dotyczących jurysdykcji sądów przy rozpatrywaniu ogółu spraw dotyczących spadku w rozporządzeniu Parlamentu Europejskiego i Rady (UE) Nr 650/2012 z 4.7.2012 r. w sprawie jurysdykcji, prawa właściwego, uznawania i wykonywania orzeczeń, przyjmowania i wykonywania dokumentów urzędowych dotyczących dziedziczenia oraz w sprawie ustanowienia europejskiego poświadczenia spadkowego⁴⁰, które kształtuje ponadto uprawnienie spadkodawcy do wyboru jurysdykcji sądu w umowie prorogacyjnej⁴¹. W razie nieskorzystania z uprawnienia prawem właściwym będzie prawo państwa, w którym zmarły miał miejsce zwykłego pobytu w chwili śmierci⁴². Kwestie wyboru prawa właściwego dla spraw nie tylko pomiędzy podmiotami z UE, ale także państwami trzecimi, uściśla rozporządzenie Rzym I⁴³, statuując, iż wybór dokonany przez strony (także umów elektronicznych)⁴⁴ nie

³² Zob. Wniosek specjalny dotyczący konta ubezwłasnowolnionej lub zmarłej osoby, <https://www.facebook.com/help/contact/228813257197480> (dostęp z 24.3.2018 r.).

³³ Zob. Jak mogę poprosić o usunięcie konta na Facebooku należącego do zmarłego członka rodziny?, <https://www.facebook.com/help/1518259735093203?helpref=related&ref=related> (dostęp z 24.3.2018 r.).

³⁴ Zob. Jak mogę poprosić o dostęp do zawartości konta na Facebooku należącego do osoby zmarłej?, <https://www.facebook.com/help/123355624495297?helpref=related&ref=related> (dostęp z 24.3.2018 r.).

³⁵ Szerzej zob. Wniosek dotyczący udostępnienia zawartości konta zmarłej osoby, <https://www.facebook.com/help/contact/398036060275245> (dostęp z 24.3.2018 r.).

³⁶ In re Request for Order Requiring Facebook, Inc. to Produce Documents and Things, Case No C 12-80171 LHK (PSG) (N.D. California, 20 September 2012), <http://www.digitalpassing.com/wordpress/wp-content/uploads/2012/10/Daftary-Facebook-Order-9-20-2012.pdf> (dostęp z 24.3.2018 r.).

³⁷ In re Request..., s. 3

³⁸ D. McCallig, Facebook..., s. 113

³⁹ M. Mqdel, *op.cit.*, s. 107

⁴⁰ OJ L 201, p. 107.

⁴¹ Zob. art. 5 ust. 1 oraz art. 22 *ibidem*.

⁴² Zob. więcej art. 21 i 23 *ibidem*.

⁴³ Rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 593/2008 z 17.6.2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I), Dz.Urz. UE L 177, s. 6.

⁴⁴ Zob. art. 3 *ibidem*.

może prowadzić do pozbawienia konsumenta ochrony wynikającej z norm bezwzględnie obowiązujących w państwie miejsca zwykłego pobytu konsumenta (art. 6). W takiej sytuacji sąd powinien, porównując standardy ochrony konsumenta, zastosować regulację korzystniejszą⁴⁵.

W przypadku umów obligacyjnych, gdy konsument ma miejsce zwykłego pobytu w Polsce, stosuje się więc prawo polskie, przy czym trzeba rozważyć, jak ma się to do postanowień umownych we wzorcach umów stosowanych przez dostawców usług elektronicznych? Konsument nie ma realnej możliwości negocjacji takiego postanowienia, co od razu nasuwa na myśl art. 385¹ KC (definicja klauzuli abuzywnej)⁴⁶, i co potwierdza teza SN w wyroku z 17.9.2014 r.⁴⁷ mówiąca, iż zamieszczenie we wzorcu umowy konsumenckiej postanowienia przewidującego zastosowanie prawa obcego dla konsumenta, a właściwego dla twórcy wzorca stanowi klauzulę niedozwoloną, ponieważ godzi w równowagę kontraktową na niekorzyść konsumenta. Wyrok ten został mocno skrytykowany przez przedstawicieli nauki prawa, a TS nieco odmiennie tę kwestię potraktował w wyroku z 28.7.2016 r. w sprawie Amazon⁴⁸. Stwierdził mianowicie, że właściwość prawa obcego jest dopuszczalna, jednak należy poinformować konsumenta, iż może skorzystać z odpowiednich regulacji korygujących z rozporządzenia Rzym I, pozwalających na zastosowanie korzystniejszych dla niego przepisów państwa, w którym ma miejsce zwykłego pobytu. Sąd berliński⁴⁹ przychylił się do decyzji, uznając, iż w sprawie dotyczącej dziedziczenia konta na portalu Facebook będzie miało zastosowanie prawo miejsca zwykłego pobytu konsumenta, tj. niemieckie. Ponadto rozporządzenie Bruksela I bis⁵⁰ stwarza dodatkowe warunki przy narzucaniu konsumentowi umowy prorogacyjnej dotyczącej jurysdykcji, z których interesuje nas drugi (pozostałe dwa nie mają tutaj zastosowania), czyli jeśli umowa przyznaje konsumentowi uprawnienie do wytaczania powództwa przed sądy inne niż sądy określone w sekcji 4 rozporządzenia⁵¹.

W poprzednio obowiązującej (do 19.4.2018 r.) wersji Oświadczenia dotyczącego praw i obowiązków (z 31.1.2018 r.) wszelkie spory w ramach portalu społecznościowego podlegały przepisom prawa stanu Kalifornia, a sądem właściwym do ich rozpatrzenia był wyłącznie sąd okręgowy Północnego Dystryktu Kalifornii lub sąd stanowy hrabstwa San Mateo⁵². Akceptując zasady funkcjonowania Facebooka (co dzieje się automatycznie poprzez kliknięcie przycisku „Rejestracja”), użytkownik wyraża zgodę na obowiązywanie jurysdykcji powyższych sądów. Pojawia się więc ryzyko, że roszczenia spadkobierców o uzyskanie dostępu do treści cyfrowych zmarłego nie byłyby rozstrzygane w Polsce.

Aktualizacją z 19.4.2018 r. wszedł w życie nowy Regulamin⁵³, który zastąpił poprzednią wersję Oświadczenia dotyczącego praw i obowiązków, na mocy którego co do roszczeń i sporów niezwiązanych z powyższym Regulaminem

lub produktami Facebooka sądem właściwym jest właściwy sąd w Republice Irlandii, co stanowi spore ułatwienie dla użytkowników w stosunku do poprzedniej regulacji wskazującej jako właściwy sąd stanu Kalifornia. Ponadto dla użytkowników-konsumentów mających miejsce zamieszkania w państwie członkowskim UE przy sporze z Facebookiem zastosowanie znajdą przepisy obowiązujące w tym państwie członkowskim, a sprawę może rozstrzygnąć dowolny właściwy sąd tego państwa członkowskiego, jeśli posiada w zakresie sporu jurysdykcję⁵⁴. Zapis ten stwierdza więc właściwość prawa polskiego w stosunku do Polaków zamieszkujących w Polsce. W przypadku ewentualnych dalszych sporów co do prawa właściwego dla polskich użytkowników w Polsce i tak na podstawie analizy unijnych rozporządzeń prawem właściwym będzie co do zasady prawo polskie, a spór rozstrzygać będzie sąd polski.

Polские rozwiązania prawa spadkowego wobec regulaminu Facebooka

Ocena zgodności z prawem postanowień przyjętych przez Facebooka dotyczących dziedziczenia profilu, jak też treści z nim powiązanych wymaga przyjrzenia się krajowym rozwiązaniom ustawowym. W przypadku braku umowy to sam spadkodawca decyduje o dalszym losie tych treści, a zatem trzeba rozważyć, czy może to uczynić w drodze sporządzenia testamentu, skoro na gruncie prawa polskiego przyjęto za zasadę swobodę decydowania o losach majątku po śmierci. Wolność testowania została ograniczona przez przepisy ustawowe dotyczące wymogów testamentu, możliwości odwołania go (ograniczenia formalne), a także instytucję zachowku (ograniczenie materialne)⁵⁵. Pojęcie testamentu można wy prowadzić z kilku przepisów Kodeksu cywilnego⁵⁶, z których

⁴⁵ Zob. D. Szostek, M. Świerczyński, Problem prawa właściwego oraz sądów właściwych w zakresie umów dotyczących treści cyfrowych dystrybuowanych on-line, PME 2015, Nr 2, s. 12

⁴⁶ Zob. art. 385¹ § 1 KC.

⁴⁷ Zob. wyrok SN z 17.9.2014 r., I CSK 555/13, OSG 2015, Nr 3, poz. 15.

⁴⁸ C-191/15, ECLI:EU:C:2016:612.

⁴⁹ Zob. wyrok Sądu Krajowego w Berlinie z 17.12.2016 r., 20 O 172/15, file:///C:/Users/User/Downloads/20-o-172-15_urteil-vom-17-12-2015.pdf (dostęp z 30.3.2018 r.).

⁵⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 1215/2012 z 12.12.2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych, OJ L 351, p. 1.

⁵¹ Zob. art. 19 *ibidem*.

⁵² Regulamin z 31.1.2018 r., <https://www.facebook.com/legal/terms> (dostęp z 30.3.2018 r.).

⁵³ Regulamin z 19.4.2018 r., <https://www.facebook.com/legal/terms> (dostęp: 30.3.2018 r.).

⁵⁴ Zob. Regulamin z 19.4.2018 r., <https://www.facebook.com/legal/terms> (dostęp: 30.3.2018 r.).

⁵⁵ P. Księżak, Prawo..., s. 146.

⁵⁶ Zob. art. 941, 943, 944, 958 KC.

wynika, że jest on jednostronną i osobistą czynnością prawną *mortis causa*, wymagającą zachowania szczególnej formy, która stanowi podstawę powołania do spadku, będącą aktem woli, który nie jest skierowany do określonego adresata i może w każdej chwili być odwołalny. Warunkiem istnienia skutecznego testamentu jest minimum jedno rozrządzenie⁵⁷. Mając na względzie wcześniejsze rozważania, najprostszym sposobem wydawałoby się zamieszczenie danych logowania do konta w testamencie, dzięki czemu wskazana osoba mogłaby w dowolny sposób rozporządzić treściami cyfrowymi z nim powiązanymi. Jednak taki zapis stwarzałby konieczność aktualizowania danych w przypadku zmiany hasła dostępu, co z kolei mogłoby spowodować dodatkowe koszty (np. w przypadku testamentu notarialnego)⁵⁸, a ponadto tworzyłby zagrożenie uzyskania dostępu do treści powiązanych z kontem spadkodawcy przez wszystkich spadkobierców, a nawet osoby trzecie. Mimo bowiem że nie zawiadamia się osób zainteresowanych o terminie otwarcia i ogłoszenia testamentu, to mają oni prawo być obecni przy tej czynności w sądzie bądź u notariusza⁵⁹. Celem zabezpieczenia danych przed niechcianym dostępem można chociażby zaszyfrować treść aktu ostatniej woli, jednak mogłoby to spowodować jego nieważność. Już bowiem pismo nieczytelne wyklucza jego ważność⁶⁰, a tym bardziej użycie szyfru, który może uniemożliwić zbadanie, czy testator sporządził testament własnoręcznie (jeśli użyjemy znaków elementarnych) oraz utrudnić poznanie jego rzeczywistej woli⁶¹.

Warte uwagi jest też rozrządzenie na wypadek śmierci w formie zapisu windykacyjnego zamieszczonego w testamencie (w formie aktu notarialnego)⁶², na podstawie którego oznaczona osoba (nie musi być spadkobiercą) nabywa z mocy prawa, z chwilą otwarcia spadku, konkretny składnik majątku spadkodawcy (sukcesja syngularna)⁶³. W ustawie został wprowadzony zamknięty katalog przedmiotów podlegających dziedziczeniu w ten sposób, tj.:

- 1) rzeczy oznaczone co do tożsamości;
- 2) zbywalne prawa majątkowe;
- 3) przedsiębiorstwo lub gospodarstwo rolne;
- 4) ustanowienie na rzecz zapisobiorcy użytkowania lub służebności⁶⁴.

Co oczywiste, analizy wymagają tylko dwa pierwsze przypadki. Rzecz można uznać za oznaczoną co do tożsamości, jeśli jej opis pozwoli na jej zindywidualizowanie, tak by bez dalszych czynności faktycznych stała się, z chwilą otwarcia spadku, własnością zapisobiorcy⁶⁵. Wydaje się więc, że treści cyfrowe zgromadzone przez użytkownika w ramach konkretnego konta na Facebooku można by uznać za oznaczone co do tożsamości, jednak problem pojawia się przy słowie „rzecz”, którą mogą być tylko przedmioty materialne (art. 45 KC)⁶⁶. Z kolei druga kategoria przedmiotów jest dość obszerna i obejmuje m.in. prawa autorskie, prawa z umowy time-share, wierzytelności. Prawami zbywalnymi są takie prawa

podmiotowe, które można przenieść na drugą osobę w drodze czynności prawnej. W przypadku Facebooka sam usługodawca odniósł się do przesłanki zbywalności. I tak zgodnie z Regulaminem portalu niedozwolone jest przekazywanie jakichkolwiek praw wynikających z tego Regulaminu, jak też przenoszenie konta na inne osoby, bez zgody Facebooka⁶⁷. W świetle tych postanowień ustanowienie treści cyfrowych przedmiotem zapisu windykacyjnego budzi wątpliwości. Ponadto spory dotyczące majątkowego charakteru treści cyfrowych sprawiają, iż rozsądniejsze wydaje się niekorzystanie z tej instytucji w obecnym stanie prawnym, choć ciekawym rozwiązaniem zaproponowanym w literaturze byłoby przekazanie, w drodze zapisu, złożonych w skrytce bankowej⁶⁸ danych dostępowych.

Przedstawione wyżej rozwiązania nie wydają się wystarczające i należałoby się przyjrzeć, czy istnieje możliwość pozasпадkowej sukcesji syngularnej treści cyfrowych, w której spadkodawca wskazuje beneficjenta poprzez czynność jednostronną bądź klauzulę umowną. Dyspozycje jednostronne *mortis causa* zbliżone są do zapisów windykacyjnych i można je odnaleźć m.in. w ustawie z 29.8.1997 r. – Prawo bankowe⁶⁹, ustawie z 5.7.2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych⁷⁰ czy w ustawie z 20.4.2004 r. o pracowniczych programach emerytalnych⁷¹. Z uwagi na brak szczególnego przepisu mówiącego o treściach cyfrowych celowe wydaje się więc przyjrzenie się tej drugiej grupie – umowom dotyczącym spadku po osobie żyjącej, a dokładniej instytucji darowizny *mortis causa*, której skutki mają nastąpić dopiero z chwilą śmierci darczyńcy. W literaturze pojawia się wątpliwość co do rodzaju skutku takiej darowizny – jedni twierdzą, iż z chwilą śmierci darczyńcy wywoła ona jedynie skutek obligacyjny i po stronie obdarowanego powstanie roszczenie wobec spadkobierców o wykonanie darowizny (czyli właściwie działałaby ona jak zapis zwykły), drudzy stoją na stanowisku, że darowizna ta przypomina zapis windykacyjny i z chwilą

⁵⁷ Zob. E. Niezbecka, A. Kidyba (red.), Kodeks Cywilny. Komentarz, Tom IV. Spadki, wyd. 4, Warszawa 2015, s. 103.

⁵⁸ M. Mądel, *Następstwo prawne...*, s. 212.

⁵⁹ Zob. art. 646–654 KPC oraz art. 95d ustawy z 14.2.1991 r. – Prawo o notariacie (t.j. Dz. U. z 2017 r. poz. 2291 ze zm.).

⁶⁰ A. Dub-Brych, *Jak napisać testament własnoręczny*, 2015, <http://legetartis-kancelaria.pl/warto-wiedziec/41-jak-sporzadzic-wazny-wlasnoreczny-testament> (dostęp z 5.4.2018 r.).

⁶¹ M. Mądel, *Następstwo prawne...*, s. 203.

⁶² Zob. art. 981¹–981⁶ KC.

⁶³ S. Babiarz, *Spadek i darowizna w prawie cywilnym i podatkowym*, wyd. 4, Warszawa 2012, s. 119.

⁶⁴ Zob. art. 981¹ KC.

⁶⁵ Zob. M. Mądel, *Następstwo prawne...*, s. 208; P. Książak, *Zapis windykacyjny*, wyd. 1, Warszawa 2012, s. 100.

⁶⁶ M. Mądel, *Następstwo prawne...*, s. 210.

⁶⁷ Zob. Regulamin pkt 4.5.4 i 3.1, <https://www.facebook.com/legal/terms> (dostęp z 30.3.2018 r.).

⁶⁸ Zob. P. Książak, *Zapis...*, s. 99; M. Mądel, *Następstwo prawne...*, s. 211.

⁶⁹ T.j. Dz. U. z 2018 r. poz. 2187 ze zm.; dalej jako: PrBankU.

⁷⁰ T.j. Dz. U. z 2017 r. poz. 2065 ze zm.

⁷¹ T.j. Dz. U. z 2016 r. poz. 1449 ze zm.

śmierci wywoła skutek rzeczowy, a więc przedmiot przejdzie na obdarowanego⁷². Instytucja darowizny na wypadek śmierci nie została uregulowana w Kodeksie cywilnym, pozostając na etapie projektów ustawodawczych. W piśmiennictwie reprezentowane są różne stanowiska, z przewagą dopuszczalności takiej darowizny⁷³, przy czym przeciwnicy traktują ją jako naruszenie zakazu zawierania umów o spadek po osobie żyjącej (art. 1047 KC), jak też wyłączności testamentowej dla rozrządzeń (art. 941 KC), z czym jednak nie zgadza się SN w swojej uchwale z 13.12.2013 r., podkreślając, że darowiznę taką można by uznać za umowę o spadek po osobie żyjącej, tylko jeśli strony uczyniły jej przedmiotem cały spadek albo część ułamkową⁷⁴. Sąd Najwyższy potwierdził zatem dopuszczalność zawarcia takiej umowy darowizny, jeśli jej przedmiotem są konkretne rzeczy lub prawa, a sama umowa nie jest sprzeczna z zasadami współżycia społecznego. Wskazał ponadto, że niektóre przepisy szczególne w istocie zawierają instytucje będące postacią takiej darowizny, jak np. art. 56 PrBankU. Jeśli by zgodzić się z SN, że taka umowa jest dopuszczalna, to należałoby raczej stwierdzić, iż można ustanowić konkretne treści cyfrowe połączone z konkretnym kontem na Facebooku jej przedmiotem, lecz ze względu zarówno na odmienne poglądy w literaturze, jak i brak prawnego uregulowania tej instytucji, trzeba to raczej traktować jako opcję *contra legem*, którą można by wprowadzić w przyszłości.

Jak widać, każde z przedstawionych rozwiązań z polskiej regulacji nie jest do końca przystosowane do dziedziczenia treści cyfrowych, przy czym pozostaje jeszcze kwestia fizycznego przekazania danych do logowania za życia innej osobie, która po śmierci użytkownika mogłaby zarządzać treściami cyfrowymi w jego imieniu. Jednak najprostsze rozwiązanie, wydaje się nieskuteczne, ponieważ narusza zasady zaakceptowane przez użytkowników Facebooka w formie regulaminu⁷⁵, co może skutkować nawet usunięciem konta, a przynajmniej zablokowaniem dostępu do niego. Ponadto w kwestii udostępnienia swoich danych do logowania na portalu społecznościowym wypowiedział się SO w Siedlcach w wyroku z 4.5.2016 r.⁷⁶, który stwierdził, iż znajomość hasła do konta nie uprawnia do korzystania z niego i uzyskiwania informacji nieprzeznaczonych dla tej osoby bez wiedzy i zgody uprawnionego. Co więcej, użycie cudzego hasła, nawet przekazanego przez właściciela konta, powodujące nieuprawniony dostęp do serwisu, może doprowadzić do postawienia zarzutu popełnienia przestępstwa polegającego na ominięciu szczególnego zabezpieczenia⁷⁷, jakim jest hasło na Facebooku⁷⁸.

W tym miejscu należy się przyjrzeć, w kontekście prawa krajowego, rozwiązaniom zaproponowanym przez Facebooka. Na wstępie warto przypomnieć poczyniony wyżej wniosek, że nie można jednoznacznie wykluczyć, iż treści cyfrowe mogą wchodzić w skład spadku, przy czym zaliczenie do niego samego konta budzi wiele wątpliwości na podsta-

wie art. 922 KC, czego nie można powiedzieć już o danych z kontem powiązanych, do których spadkobiercy zazwyczaj uzyskają prawo.

Pierwszym z rozwiązań, z których można skorzystać na wypadek śmierci użytkownika konta na Facebooku, jest jego usunięcie. Praktyka ta wydaje się jednak wysoce niezasadna i naruszająca polskie normy prawne, w tym prawo autorskie, przy możliwości zakwalifikowania w niektórych sytuacjach zamieszczonych treści na koncie jako utworu, np. opublikowanych fotografii. Nie ma wątpliwości, że prawa majątkowe do utworu podlegają dziedziczeniu, a więc skasowanie konta byłoby jednoznaczne ze zniszczeniem utworu⁷⁹. W kontekście facebookowej regulacji zastanawiające jest, czy osoby ze wskazanego katalogu, które mogą wystąpić z żądaniem usunięcia konta, można uznać za faktycznie do tego uprawnione. Zasadne wydaje się tu przywołanie art. 268a KK, który zawiera sankcję w postaci kary pozbawienia wolności, w przypadku zniszczenia, uszkodzenia, usunięcia, zmienienia lub utrudnienia dostępu do danych informatycznych, nie będąc osobą uprawnioną.

Druga z metod postępowania polega na zawieszeniu konta, a więc zmianie statusu konta na *In memoriam*. Rozwiązanie to pozwala zapobiec wielu problemom, jakie mogłyby powstać w konsekwencji istnienia aktywnego konta osoby zmarłej. Eliminując nieograniczony dostęp do konta, w szczególności przez brak możliwości logowania, konto jest jedynie odbiornikiem treści⁸⁰. Dodatkowym atutem jest możliwość ustanowienia tzw. pełnomocnika do spraw dorobku. Jednakże w literaturze rozwiązanie to jawi się jako tymczasowe, choć zasadne, ale mimo wszystko niewyłączające całkowicie możliwości naruszenia dóbr osobistych zmarłego (jeśli by uznać, że takowe istnieją), jak też dobra osobistego bliskich zmarłego, jakim jest poszanowanie pamięci o osobie zmarłej, przez dostęp do tego konta osób trzecich („znajomych” użytkownika)⁸¹. W kontekście dobra kultywowania pamięci osoby zmarłej, przynającemu w świecie fizycznym bliskim zmarłego szereg uprawnień, zasadne wydawałoby się przekazanie

⁷² P. Książak, Prawo..., s. 308.

⁷³ Zob. S. Babiarz, Spadek..., s. 246; tak m.in. J. Kosik, [w:] J.S. Piątkowski (red.), System prawa cywilnego, t. IV, Prawo spadkowe, Wrocław 1986, s. 581; I. Górecki, Umowa darowizny na wypadek śmierci, Rejent 2006, Nr 2, s. 40.

⁷⁴ III CZP 79/13, OSNC 2014, Nr 10, poz. 98.

⁷⁵ Zob. Regulamin pkt 3.1, <https://www.facebook.com/legal/terms> (dostęp: 30.3.2018 r.).

⁷⁶ II Ka 39/16 (Portal Orzeczeń Sądu Okręgowego w Siedlcach).

⁷⁷ Zob. art. 267 § 1 KK.

⁷⁸ Zob. wyrok SR w Białymstoku z 22.4.2015 r., VII K 922/14 (Portal Orzeczeń Sądu Rejonowego w Białymstoku).

⁷⁹ L. Goździaszek, Likwidacja tożsamości na portalu społecznościowym, [w:] J. Gołaczyński (red.), *Non omnis moriar*: osobiste i majątkowe aspekty prawne śmierci człowieka: zagadnienia wybrane, Wrocław 2015, s. 305. Zob. M. Mądel, Następstwo prawne..., s. 266.

⁸⁰ Zob. L. Goździaszek, Likwidacja tożsamości..., s. 306.

⁸¹ Zob. M. Mądel, Następstwo prawne..., s. 268.

całego konta w ręce spadkobierców, a dokładniej możliwości wglądu do niego, w celu monitorowania go i zapobiegania ewentualnym naruszeniom. Nowy Regulamin Facebooka przewiduje szerszy krąg osób mogących uzyskać dostęp do treści z konta zmarłego użytkownika – są to obecnie również osoby wprost wskazane przez użytkownika w ważnym testamencie bądź innym podobnym dokumencie, zawierającym wyraźną wolę udostępnienia danej osobie konkretnych treści. Warunkiem jest posiadanie przez konto statusu *In memoriam*. Z pewnością stawia to spadkobierców w lepszej sytuacji niż dotychczas, jednak świadomość możliwości dziedziczenia treści cyfrowych w naszym społeczeństwie jest na tyle niska, że większość osób z tego zapisu może po prostu nie skorzystać, a nawet nie mieć świadomości, że istnieje taka możliwość, przez co sytuacja spadkobierców w próbie polubownego uzyskania dostępu do konta zmarłego w zasadzie nie różni się od tej sprzed aktualizacji. Można więc stwierdzić, iż praktyka zawieszania konta jest zasadna, choć wymagałaby dopracowania, aby umożliwić bliskim pielęgnowanie pamięci o zmarłym użytkowniku, a także prostszy dostęp do treści, które podlegałyby dziedziczeniu⁸².

Podsumowanie

Chociaż polskie prawo spadkowe nie odnosi się do treści cyfrowych po śmierci ich właściciela, to jednak nie można wykluczyć możliwości dziedziczenia treści powiązanych z kontem na Facebooku. Zważywszy na ciągły rozwój cyber-

przestrzeni, w tym w szczególności portali społecznościowych, zagadnieniem tym powinien zająć się ustawodawca. Wydaje się, że zawieszenie konta poprzez ustanowienie statusu *In memoriam* nie odpowiada w pełni polskiej regulacji. Mimo to jest to obecnie najlepsza opcja, gdyż pozostałe mogą rodzić o wiele większe problemy. W niektórych sytuacjach, np. przy samobójczej śmierci dziecka, właściwsze wydawałoby się jednak udostępnienie całości konta do samodzielnego rozporządzania nim przez rodziców, przy czym należałoby to uregulować wprost w przepisach. Do tego momentu, aby uzyskać taki dostęp od Facebooka (jeśli w testamencie wyrażnie nie wyrażono zgody na ujawnienie konkretnych treści na profilu konkretnemu spadkobiercy), jedyną drogą jest droga sądowa. Z drugiej strony wkracza tutaj problematyka ochrony dóbr pozostałych użytkowników portalu, w szczególności ich prywatności czy tajemnicy korespondencji. Patrząc na ilość treści cyfrowych, nawet wyłącznie tych powiązanych z kontem na Facebooku, nikogo raczej nie powinny dziwić narastające problemy po śmierci użytkowników w przypadku braku konkretnych uregulowań. Technologia w końcu wymusi uwspółcześnienie prawa spadkowego, którego podstawowe konstrukcje mają swoje źródło jeszcze w rozwiązaniach starożytnych. Do tego czasu, jeśli prezentowane przez Facebooka opcje nie są zadowalające, zawsze, w przypadku sporu, spadkobiercy mogą wystąpić przeciwko serwisowi do sądu z konkretnymi żądaniami.

⁸² *Ibidem*, s. 269–270.

Słowa kluczowe: treści cyfrowe, Facebook, serwis społecznościowy, profil, dziedziczenie, testament, zapis windykacyjny, darowizna *mortis causa*, śmierć użytkownika, status *In memoriam*, opiekun konta, usunięcie konta, prawo właściwe, *click-wrap*.

Regulations in regard to inheriting profile which are included on Facebook in the context of Polish law

Based on increasing popularity of social networking services, the author of the present article points out the revealing need of regulating the situation of digital content after the death of its owner. In her paper, while defining digital content, the author points to a possibility of inheriting content connected with an account on Facebook, and also discusses the matter of the law applicable to issues between the users and the service provider.

The author's objective is mainly analysis of solutions proposed by Facebook in case of death of a user, in the context of Polish regulations of succession law.

Keywords: digital content, Facebook, social network, profile, inheriting, last will, specific bequest, donation *mortis causa*, death of user, memorialized account, legacy contact, deleting account, applicable law, *click-wrap*.

Prawnie uzasadnione interesy jako podstawa przetwarzania danych *online*

Michał Czerniawski¹

Nie budzi wątpliwości, że przesłanką legalizującą przetwarzanie danych osobowych, która jest najbezpieczniejsza z perspektywy administratora danych działającego *online* i która jednocześnie przyznaje podmiotowi danych najpełniejszą kontrolę nad tym, co dzieje się z jego danymi, jest zgoda osoby, której dane dotyczą. Wraz z postępem technologicznym i rozwojem zautomatyzowanych metod przetwarzania danych osobowych, a także wzrostem ich złożoności, zwłaszcza w Internecie, uzyskanie zgody spełniającej przewidziane w przepisach prawa wymogi staje się zadaniem coraz trudniejszym i mniej praktycznym z punktu widzenia administratora. Stąd też, m.in. w kontekście przetwarzania danych osobowych w celach marketingowych *online*, w przypadku danych niebędących danymi wrażliwymi, coraz częściej preferuje się przesłankę prawnie uzasadnionych interesów. W niniejszym opracowaniu autor analizuje przyczyny niewielkiej popularności prawnie usprawiedliwionych celów realizowanych przez administratorów jako podstawy przetwarzania danych osobowych, z którą mieliśmy do czynienia w Polsce przed 25.5.2018 r., a także stawia tezę, że po rozpoczęciu stosowania RODO powołanie się na prawnie uzasadnione interesy jako taką podstawę stało się znacznie łatwiejsze.

Uwagi wstępne

Jednym z powodów uchwalenia ogólnego rozporządzenia Parlamentu Europejskiego UE 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych², które zastąpiło dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych³, był szybki rozwój techniki, w szczególności Internetu⁴ i coraz większe niedostosowanie obowiązujących uprzednio przepisów prawa do realiów technologicznych. Wpływ technologii doprowadził przede wszystkim do wprowadzenia nowych (m.in. prawo do przenoszenia danych⁵) i rozszerzenia dotychczasowych (m.in. w zakresie obowiązku informacyjnego) uprawnień osób, których dane dotyczą. Choć RODO nie wprowadza diametralnych zmian w stosunku do podstaw przetwarzania danych ustanowionych już w dyrektywie 95/46/WE, to będąc aktem prawa bezpośrednio stosowanym w państwach członkowskich, w przypadku Polski eliminuje istniejącą dotychczas niezgodność pomiędzy ustawą z 29.8.1997 r. o ochronie danych osobowych⁶ a ww. dyrektywą w zakresie prawnie uzasadnionych interesów jako podstawy przetwarzania danych osobowych. W mojej ocenie od 25.5.2018 r. administratorzy danych mogą ją stosować w znacznie szerszym zakresie, niż było to możliwe pod rządami ustawy o ochronie danych osobowych z 1997 r.

Płynność przetwarzania danych osobowych w środowisku *online*

Funkcjonowanie w społeczeństwie informacyjnym wiąże się nieodzownie z przetwarzaniem danych osobowych.

Jednocześnie wraz z rozwojem techniki i nowych sposobów przetwarzania, coraz bardziej złożonych oraz w znacznej mierze opartych na rozwiązaniach niezależnych od ludzkiej decyzji (przede wszystkim algorytmach) bądź na decyzjach podejmowanych w czasie rzeczywistym przez użytkowników sieci (a więc wymagających szybkiej reakcji i coraz częściej zautomatyzowanych), wzrasta dążenie administratorów danych do dysponowania podstawą do przetwarzania danych o odpowiednim poziomie elastyczności. Specjaliści od marketingu badają m.in., ile czasu użytkownik sieci potrzebuje na podjęcie decyzji czy też co może go zniechęcić do zrobienia zakupów na konkretnej witrynie internetowej (np. liczba niezbędnych kliknięć, ilość potrzebnych zgód, czas trwania całego procesu itd.). Naturalnym kierunkiem działania administratorów danych, zwłaszcza w środowisku *online*, jest jak najdalsze usprawnianie procesów przetwarzania danych oso-

¹ Autor jest prawnikiem w Stałym Przedstawicielstwie RP w Brukseli, gdzie zajmuje się m.in. ochroną danych osobowych i cyberbezpieczeństwem. Był jednym z negocjatorów ogólnego rozporządzenia o ochronie danych.

² Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

³ Dz.Urz. UE L Nr 281, s. 31; dalej jako: dyrektywa 95/46/WE.

⁴ Motyw 6 RODO wprost stanowi, iż „szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności”.

⁵ Szerzej na ten temat prawa do przenoszenia danych M. Czerniawski, Obowiązki administratora danych wynikające z prawa do przenoszenia danych, [w:] G. Sibiga (red.), Wdrażanie ogólnego rozporządzenia o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych, Warszawa 2017, s. 28–34; W.R. Wiewiórowski, Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych, EPS 2017, Nr 5, s. 23–30.

⁶ Ustawa z 29.8.1997 r. o ochronie danych osobowych, t.j. Dz.U. z 2016 r. poz. 922 ze zm. – częściowo uchylona; dalej jako: OchronaDanychU97 lub ustawa z 1997 r.

bowych. Operacje przetwarzania danych osobowych coraz częściej zachodzą automatycznie, bez ingerencji administratora danych, często są przeprowadzane przez różne podmioty, w wielu celach, z wykorzystaniem zróżnicowanych środków. Żyjemy także w czasach, w których coraz rzadziej zdarza się, aby pojedynczy podmiot miał pełną kontrolę nad całym procesem przetwarzania danych osobowych. Standardem stało się, że w procesy przetwarzania danych zaangażowanych jest wiele podmiotów, a każdy z nich wykonuje tylko część operacji. W społeczeństwie informacyjnym bez dysponowania podstawą przetwarzania danych osobowych o odpowiedniej elastyczności coraz trudniejsze staje się nie tylko świadczenie złożonych usług, ale także wykorzystanie w pełni potencjału Internetu rzeczy czy też rozwiązań opartych na sztucznej inteligencji (AI)⁷. Podsumowując, nie powinno dziwić dążenie administratorów danych do ograniczania liczby zgód zbieranych od użytkowników w środowisku *online* i skorelowana z nim rosnąca popularność prawnie uzasadnionych interesów jako podstawy przetwarzania danych osobowych w Internecie (do której jednak polscy administratorzy danych wciąż podchodzą z pewną ostrożnością).

Regulujący tę podstawę prawną art. 6 ust. 1 lit. f) RODO wskazuje, że zgodne z prawem jest przetwarzanie niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Podstawa ta, co istotne w środowisku *online*, nie wymaga więc aktywnego działania po stronie użytkownika, w szczególności składania przez niego jakiegokolwiek oświadczenia woli. Jednocześnie sam art. 6 ust. 1 lit. f) RODO nie pozwala na swobodne przetwarzanie danych na podstawie ww. interesów – nakazuje bowiem wyważenie interesów administratora lub strony trzeciej z interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą. Nie budzi wątpliwości, że przetwarzanie oparte na art. 6 ust. 1 lit. f) RODO powinno odbywać się z pełnym poszanowaniem praw osoby, której dane dotyczą, a wprowadzenie dodatkowego obostrzenia w postaci „testu nadrzędności” pozwalającego na przetwarzanie danych, tylko w sytuacji gdy interesy administratora lub strony trzeciej przeważają nad interesami, prawami lub wolnościami podmiotu danych, było słusznym zabiegiem unijnego prawodawcy. Nie wolno zapominać, iż podstawa ta stanowi odejście od zasady samostanowienia przez osobę, której dane dotyczą, o tym, co dzieje się z jej danymi, a przez to potencjalnie wiąże się z większym ryzykiem naruszenia jej praw czy wolności. Tytułem przykładu słusznie zauważa się w doktrynie, że wykluczone jest powołanie się na przesłankę z art. 6 ust. 1 lit. f) RODO w przypadku za-

miaru przetwarzania danych w celach marketingowych, gdy osoba, której dane dotyczą, uprzednio wyraźnie odmówiła udzielenia zgody na przetwarzanie danych w tych celach⁸. Takie działanie stanowiłoby bowiem naruszenie jej praw. W doktrynie obecny jest pogląd, że w ogóle nie można powoływać się na art. 6 ust. 1 lit. f) rozporządzenia 2016/679, przetwarzając dane osobowe dziecka⁹. Stanowisko to wydaje się zbyt daleko idące, wciąż bowiem trzeba przeprowadzić „test nadrzędności” i decyzję oprzeć na jego rezultacie. Należy jednak zgodzić się z twierdzeniem, że co do zasady prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią nie będą mieć nadrzędnego charakteru wobec interesów bądź podstawowych praw i wolności dziecka, a ewentualne przetwarzanie takich danych na podstawie tej przesłanki będzie wymagać podjęcia przez administratora danych szczególnych środków ochrony. Ponadto art. 6 ust. 1 lit. f) znajduje ograniczone zastosowanie względem organów publicznych, ponieważ RODO wprost zakazuje powoływania się na tę podstawę, w przypadku gdy przetwarzania dokonują organy publiczne w ramach realizacji swoich zadań¹⁰. Warto jednak pamiętać, że dane osobowe są przetwarzane przez organy publiczne także poza wykonywaniem takich zadań, w ramach codziennej działalności, ale niejako w ich sferze „prywatnej” np. w celu dochodzenia roszczeń. Dobrym przykładem obrazującym przetwarzanie danych *online* przez sektor publiczny poza realizacją jego zadań, jest stan faktyczny w sprawie C-582/14 *Breyer*, w której ustalono, że zbieranie przez niemiecką administrację federalną adresów IP użytkowników Internetu odwiedzających jej strony podlega przepisom dyrektywy 95/46/WE, gdyż świadcząc usługi medialne *online* i odpowiadając za przetwarzanie dynamicznych adresów IP, działa ona, mimo przysługującego jej statusu władz publicznych, w charakterze podmiotu prywatnego¹¹. Stąd też, w niektórych sytuacjach, organy publiczne mogą

⁷ Wymaga to jednak istnienia odpowiednich gwarancji praw osób, których dane dotyczą. Przestrożką powinny być tu chociażby rozwiązania oparte na AI wprowadzane na szeroką skalę w Chińskiej Republice Ludowej, gdzie z jednej strony spółki takie jak Alibaba czy Tencent inwestują olbrzymie środki w rozwój tej technologii i jest ona też intensywnie wspierana przez chiński rząd, z drugiej strony jest ona wykorzystywana przez rząd w sposób budzący zastrzeżenia z perspektywy praw osób, których dane dotyczą. Zob. G. Williams, *Why China will win the global race for complete AI dominance*, Wired, <https://www.wired.co.uk/article/why-china-will-win-the-global-battle-for-ai-dominance> (dostęp z 29.8.2018 r.); P. Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, The New York Times, <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> (dostęp z 29.8.2018 r.).

⁸ Za: P. Litwiński, P. Barta, M. Kawecki, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych*. Komentarz, Legalis/el. 2017, komentarz do art. 6.

⁹ *Ibidem*.

¹⁰ Szerzej na temat uzasadnionych interesów administratora w sektorze publicznym M. Gumularz, *Uzasadniony interes w sektorze publicznym – na przykładzie monitoringu*, ABI Expert, 2018, Nr 2, s. 16–18.

¹¹ Zob. wyrok TS z 19.10.2016 r., C-582/14 *Patrick Breyer* przeciwko Bundesrepublik Deutschland, pkt 53.

wykorzystywać art. 6 ust. 1 lit. f) RODO jako podstawę przetwarzania danych osobowych.

Podstawa ta dobrze wpisuje się w przyjętą w RODO zasadę podejścia opartego na ryzyku, pozwalając administratorowi na większą swobodę przetwarzania danych, bez konieczności angażowania osoby, której dane dotyczą (nie wymagając wyrażenia przez nią zgody, podpisania umowy itd.), ale także narażając go na odpowiedzialność za naruszenie przepisów, w przypadku gdy jego działania okażą się niezgodne z przepisami RODO. Powołanie się na nią związane jest z koniecznością przeprowadzenia wspomnianego powyżej „testu nadrzędności”, a motyw 69 RODO jednoznacznie wskazuje, że za wykazanie, iż ważne prawnie uzasadnione interesy administratora mają nadrzędny charakter wobec interesów lub podstawowych praw i wolności osoby, której dane dotyczą, powinien odpowiadać administrator. Stąd też w przypadku powoływania się na art. 6 ust. 1 lit. f) RODO warto dobrze udokumentować podstawy swojej decyzji. Nie wolno także zapominać, że po stronie administratora danych wymaga on wykonania obowiązku informacyjnego.

Prawnie uzasadnione interesy a pewność prawa

Wbrew pierwotnym intencjom Komisji Europejskiej¹² w ostatecznej wersji tekstu RODO nie znalazła się delegacja dla Komisji do wydania wytycznych doprecyzowujących i harmonizujących rozumienie art. 6 ust. 1 lit. f) RODO. Brak takiego aktu prawnego z jednej strony uniemożliwił Komisji Europejskiej jakąkolwiek regulację tej kwestii, pozostawiając ją w gestii organów nadzorczych i sądów, za drugiej – potencjalnie prowadzi do powstania niepewności prawnej. W ostatecznym rozrachunku, mając na względzie charakter tego przepisu, a stanowi on klauzulę generalną, brak takiej delegacji należy ocenić pozytywnie, gdyż powinien on pozostać dostatecznie ogólny i elastyczny, aby można go było stosować, uwzględniając zachodzące zmiany tak technologiczne, jak i związane ze sposobami przetwarzania danych osobowych.

W przypadku chęci powołania się na prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią konieczna jest indywidualna ocena każdego stanu faktycznego. Interesy, aby można było się na nie powoływać, muszą być dostatecznie skonkretyzowane, nie mogą być czymś potencjalnym i niepewnym. Przykładowo przy przetwarzaniu danych w celach marketingowych będziemy co do zasady mówić o interesie ekonomicznym – dopasowanie reklam czy dotarcie do potencjalnych klientów z towarami lub usługami służy *de facto* lepszemu sprzedaniu tychże towarów bądź usług. Uzasadniony interes może obejmować interesy gospodarcze, faktyczne lub prawne, a gdy podmiot nie prowadzi działalności gospodarczej – interesy oparte na celach statutowych¹³.

Należy zgodzić się ze stanowiskiem, że prawnie uzasadnione interesy to nie interesy wynikające z przepisów prawa (choć muszą być one z nimi zgodne). Mogą one wprawdzie wynikać z aktów wewnętrznych jednostki administratora, ale częściej będą znajdować swoją podstawę w określonym stanie faktycznym¹⁴, np. relacji sprzedawca – klient. Uzasadnione interesy administratora danych będącego osobą fizyczną, co potwierdził TS, obejmują także ochronę własności, zdrowia i życia tego administratora, a także jego rodziny¹⁵. Wreszcie modelowy przykład uzasadnionych interesów realizowanych przez stronę trzecią stanowi interes publiczny (a więc działanie dla dobra ogółu, np. pomoc ofiarom klęsk żywiołowych czy walka z terroryzmem).

Rozbieżności między ustawą z 1997 r. a dyrektywą 95/46/WE

Nie sposób analizować kwestii prawnie uzasadnionych interesów w oderwaniu od przepisów obowiązujących w Polsce przez ponad 20 lat ustawy z 1997 r. Należy odnotować, że ustawa ta była jednym z najbardziej restrykcyjnych aktów prawnych tego typu w Europie. Dotyczyło to także przesłanki prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, jako podstawy przetwarzania danych. Zgodnie z art. 23 ust. 1 pkt 5 OchronaDanychU97 przetwarzanie danych było dopuszczalne tylko wtedy, gdy było to niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie naruszało praw i wolności osoby, której dane dotyczą. Z kolei zgodnie z art. 23 ust. 4 OchronaDanychU97, za prawnie usprawiedliwiony cel uważano w szczególności marketing bezpośredni własnych produktów lub usług administratora danych oraz dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

W tym samym czasie znacznie szerszą podstawę przetwarzania danych przewidywała dyrektywa 95/46/WE. Zgodnie z brzmieniem jej art. 7 lit. f) dane osobowe mogły być przetwarzane, gdy przetwarzanie danych było konieczne na potrzeby wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej lub osób, którym dane są

¹² Art. 6 ust. 5 projektu RODO przedłożonego przez Komisję Europejską stanowił, iż „Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania warunków, o których mowa w ust. 1 lit. f, dla różnych sektorów i sytuacji, w których przetwarza się dane, w tym jeśli chodzi o przetwarzanie danych osobowych dotyczących dziecka”.

¹³ W. Chomiczewski, [w:] E. Bielak-Jomaa, D. Lubasz, RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2017, s. 392.

¹⁴ M. Sakowska-Baryła, A. Nerka, [w:] M. Sakowska-Baryła (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz do art. 6, Legalis.

¹⁵ Zob. wyrok TS z 11.12.2014 r. w sprawie C-212/13, www.eur-lex.europa.eu; por. także M. Czerniawski, Glosa do wyroku TS z 11.12.2014 r., C-212/13, Lex/el. 2014.

ujawniane, z wyjątkiem sytuacji, kiedy interesy takie były podporządkowane interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą. Dyrektywa 95/46/WE, inaczej niż ustawa z 1997 r., nie zabraniała więc przetwarzania danych osobowych, w sytuacji gdy dochodziło do naruszenia praw i wolności osoby, której dane dotyczą, a jedynie nakazywała wyważenie tych praw z interesami administratora danych¹⁶. Należy odnotować, że polski ustawodawca w ustawie z 1997 r., odmiennie niż było to w dyrektywie 95/46/WE, odniósł się do „celów”, a nie „interesów”. Natomiast warto podkreślić, że na poziomie unijnym, zarówno w dyrektywie 95/46/WE, jak i w RODO w źródłowej, angielskiej wersji językowej tekstu, używa się określenia *legitimate interests* i w odniesieniu do tego pojęcia pomiędzy dyrektywą a rozporządzeniem nie zaszła żadna zmiana.

Wydaje się, że wbrew prezentowanemu w doktrynie pogładowi¹⁷ pojęcia „prawnie usprawiedliwionych celów” z ustawy z 1997 r. oraz „prawnie uzasadnionych interesów” z RODO nie można uznać za równoważne. Można się natomiast zgodzić ze stanowiskiem, że co do zasady wszelkie cele zidentyfikowane jako prawnie usprawiedliwione pod ustawą z 1997 r., w szczególności te wskazane w art. 23 ust. 4 OchronaDanychU97, będą stanowić prawnie uzasadnione interesy w rozumieniu RODO. Teza o równoważności tych pojęć byłaby bardziej uzasadniona, w sytuacji gdyby w polskim porządku prawnym poprawnie implementowano dyrektywę 95/46/WE, a przede wszystkim gdyby nie istniał w nim wspomniany powyżej art. 23 ust. 4 OchronaDanychU97 i odniesienie do marketingu bezpośredniego jedynie własnych produktów lub usług. Ponad wszelką wątpliwość, inaczej niż to było to pod ustawą z 1997 r., art. 6 ust. 1 lit. f) RODO obejmuje marketing bezpośredni nie tylko własnych, ale także produktów i usług osób trzecich¹⁸. W tym kontekście pojęcie prawnie usprawiedliwionych celów z ustawy z 1997 r. było więc pojęciem węższym.

Prawnie uzasadnione interesy a marketing

Temat prawnie uzasadnionych interesów administratora w pierwszej kolejności pojawia się w kontekście działalności marketingowej. Jak wcześniej wspomniano, już ustawa z 1997 r. wskazywała, że za prawnie usprawiedliwiony cel uważa się w szczególności marketing bezpośredni własnych produktów lub usług administratora danych. Stan prawny pod rządami ustawy z 1997 r. dobrze obrazuje sprawa dotycząca dealera samochodowego, którą rozpatrywał NSA¹⁹. W sprawie tej spółka W. przetwarzała w celach marketingowych dane osób, które wyraziły chęć odbycia jazdy próbnej samochodami marki Mercedes-Benz. Spółka nie zbierała przy tym od tych osób zgód, argumentując, że sprzedaje własne,

tj. zakupione przez siebie u producenta pojazdy samochodowe, oraz świadczy usługi w ramach prowadzonej działalności (np. prezentacja pojazdu, jazda próbna). Po przeprowadzeniu kontroli Generalny Inspektor Ochrony Danych Osobowych (GIODO) nakazał spółce W. zaprzestanie przetwarzania danych (a więc *de facto* usunięcia całego zbioru danych osobowych przetwarzanych w celach marketingowych). Od tej decyzji podmiot ten się odwołał. Sąd administracyjny zajął się odpowiedzią na pytanie, czy dealer samochodowy może powołać się na swoje prawnie usprawiedliwione cele, przetwarzając dane osób zainteresowanych zakupem samochodu. W opisanym stanie faktycznym NSA wskazał, że „w ramach własnej działalności może być rozpowszechniany »towa« lub ewentualnie »produkt«, ale przez to ten towar lub produkt nie staje się »produktem własnym« w rozumieniu pkt 1 ust. 4 art. 23. Odmienna interpretacja przeczyłaby racjonalności ustawodawcy, w ogóle bowiem zbędne byłoby precyzowanie, że marketing bezpośredni dotyczy własnych produktów lub usług”²⁰. To i podobne rozstrzygnięcia doprowadziły do sytuacji, w której art. 23 ust. 1 pkt 5 OchronaDanychU97, nadmiernie ograniczając postanowienia dyrektywy 95/46/WE, był wykorzystywany jako podstawa przetwarzania danych osobowych niezwykle rzadko, a katalog usprawiedliwionych celów ukształtował się w szczególności poprzez decyzje GIODO i orzecznictwo sądów.

¹⁶ Niezgodność tę starały się eliminować sądy administracyjne, tytułem przykładu, NSA w Warszawie w wyroku z 13.2.2014 r., I OSK 1641/12, Legalis, wbrew brzmieniu ustawy z 1997 r. dopuścił wyważanie interesów: „ocena ta sprowadza się do wyważania racji i interesów »właściciela« danych, objętego ochroną prawną, a z drugiej administratora danych, również chronionego przez prawo w zakresie, w jakim może realizować prawnie usprawiedliwione cele i uprawnienia (...). Tak też rozumiane są postanowienia dyrektywy 95/46 WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Przepis art. 7 lit. f dyrektywy dopuszcza przetwarzanie danych osobowych przez administratora, gdy jest to konieczne z punktu widzenia potrzeb wynikających z uzasadnionych interesów administratora lub osoby trzeciej, chyba że interesy te są podporządkowane interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą. Oznacza to, że dyrektywa nakazuje ważyć interesy obu stron w konkretnym przypadku i – co do zasady – dopuszcza przetwarzanie danych, które jest konieczne do realizacji prawnie usprawiedliwionych celów administratora”.

¹⁷ Tak P. Fajgielski, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, s. 174.

¹⁸ Tak słusznie P. Litwiński, P. Barta, M. Kawecki, [w:] P. Litwiński (red.), Rozporządzenie UE w sprawie ochrony... Komentarz do art. 6. Warto także zauważyć, że analizowana podstawa przetwarzania danych osobowych w kształcie wprowadzonym w RODO była wcześniej znana innym europejskim systemom prawnym, w których implementowano dyrektywę 95/46/WE, jak choćby prawu niemieckiemu. Szerzej na temat rozwiązań niemieckich zob. K. Reszczyk-Król, Prawne granice przetwarzania danych osobowych do celów marketingu bezpośredniego bez zgody podmiotu danych – perspektywa prawa polskiego i niemieckiego w świetle ogólnego rozporządzenia o ochronie danych, MoP 2017, Nr 19, s. 1022–1030.

¹⁹ Zob. wyrok NSA w Warszawie z 5.1.2010 r., I OSK 399/09, Legalis.

²⁰ *Ibidem*.

Podsumowanie

Po okresie ponad 20 lat, w czasie których podstawa przetwarzania danych osobowych, jakim są prawnie usprawiedliwione cele, była sformułowana w prawie polskim bardziej restrykcyjnie, niż wynikałoby to z przepisów unijnych, i tak też interpretowana przez polski organ nadzorczy oraz sądy administracyjne, rozpoczęcie stosowania RODO należy ocenić jako istotną zmianę. Rozporządzenie unijne pozwala bowiem administratorom częściej niż dotychczas polegać na prawnie uzasadnionych interesach, zarówno swoich, jak i strony trzeciej, jako podstawie przetwarzania danych osobowych, w tym w kontekście marketingu. Umożliwia ona administratorowi przetwarzanie danych osobowych bez konieczności angażowania osoby, której dane dotyczą, wpisując się jednocześnie w przyjętą w RODO zasadę podejścia opartego na ryzyku. Związana z tym elastyczność jest szczególnie istotna w środowisku *online*. Jednocześnie, ponieważ podstawa ta wiąże się dla administratora danych z większym ryzykiem niż np. uzyskanie zgody czy wykonanie umowy, polscy administratorzy danych wciąż podchodzą do niej z ostrożnością, co wynika też po części z podejścia wykształconego jeszcze pod rządami przepisów OchronaDanychU97. Należy zgodzić się z tym, że w odniesieniu do art. 6 ust. 1 lit. f) RODO wciąż potrzebna jest większa pewność prawa, zwłaszcza w kontekście praktyki jego stosowania, to na administratorze spoczywa bowiem obowiązek przeprowadzenia „testu nadrzędności” i wykazania nadrzędnego charakteru interesów, na które się powołuje. Przy stosowaniu art. 6 ust. 1 lit. f) RODO konieczne

jest także zapewnienie odpowiednich gwarancji praw osób, których dane dotyczą. Wreszcie warto pamiętać, że podstawa ta nie znajdzie zastosowania wobec tak zwanych danych wrażliwych, o których mowa w art. 9 RODO. Ponieważ do tej kategorii zalicza się np. wiele metadanych, które coraz chętniej przetwarza się w celach marketingowych, jest to także czynnik, który trzeba brać pod uwagę. Powyższe utrudnienia nie zmieniają jednak faktu, że powszechność stosowania tej przesłanki legalizującej przetwarzanie danych osobowych powinna się zwiększać.

Osobnym pytaniem o dużej doniosłości praktycznej pozostaje to, jak zareagują na nowe realia prawne polskie sądy administracyjne. W zakresie uzasadnionych interesów istnieje bogate orzecznictwo krajowe²¹, od którego sądom może być trudno odciąć się przy ocenie art. 6 ust. 1 lit. f) RODO. Zdaniem autora dotychczasowy dorobek orzeczniczy choćby w zakresie wyważania interesów może zachować aktualność, bardziej złożona jest natomiast kwestia „prawnie usprawiedliwionych celów”. Wydaje się, że w odniesieniu do nich dotychczasowe orzecznictwo krajowe może być brane pod uwagę tylko wtedy, gdy nie stoi w sprzeczności z przyjętym w RODO rozumieniem prawnie uzasadnionych interesów, a w szczególności zagadnienia marketingu bezpośredniego.

²¹ Wybrane orzecznictwo w odniesieniu do art. 23 ust. 1 pkt 5 OchronaDanychU97 wyroki NSA w Warszawie: z 5.11.2015 r., I OSK 193/14, Legalis; z 5.11.2015 r., I OSK 407/14, Legalis; z 13.2.2014 r., I OSK 1641/12, Legalis; z 10.11.2015 r., I OSK 1210/14, Legalis; z 13.2.2014 r., I OSK 2436/12, Legalis; z 25.2.2013 r., II SA/Wa 2267/12, Legalis.

Słowa kluczowe: RODO, uodo, podstawy przetwarzania danych, zgoda, prawnie uzasadnione interesy, marketing.

Legitimate interests as a basis for online data processing

There is no doubt that from the point of view of an administrator of data and giving a subject of data full control over their data, the most dangerous premise legalizing processing of personal data is the consent of a person whose data is in question. Along with technological progress and development of automated processing of personal data, and an increase of their complexity, especially online, acquiring consent, which meets the rules stipulated in legal regulations, becomes a more and more difficult task and less practical from the point of view of an administrator of data. Therefore, i.a. in the context of processing of personal data for online marketing purposes, for non-sensitive personal data, it is more and more preferred to use a legally justified premise of an administrator of data as a legal basis for their processing.

In the present article the author analyses reasons of low popularity of legally justified goals realized by administrators as a basis for processing of personal data, which we had to deal with in Poland before 25.5.2018, he also comes up with a thesis that legitimate interests, as a basis of processing of personal data, will quickly become more relevant.

Keywords: GDPR, basis of processing data, consent, legitimate interests, marketing, PDPA.

Adjusting to change: how communication in mediation is moving into digital environment in e-MEDIATION

Raya Tsvetkova¹

Sofia Nenova²

Mediation is an important tool of dispute resolution being brought into the new century with some important changes. Digital environment is introducing interesting challenges to mediators, mostly related to correct ways to translate their communication techniques into online space. The following article delves into this issue, discussing the evolution of mediation and communication, communication skills' adaptation and presents the reader with recommendations on the process of online mediation. The article is supported by research done by the team of the e-MEDIATION project.

Introduction

Mediation, as a dispute resolution tool, is picking up traction faster than ever in the business area as a means with which to protect both the business interests of companies and their fruitful relationships with important partners. With more and more of humanity's time being spent online, however, changes are imminent in all areas of life, including dispute resolution. Online mediation (also electronic mediation or just e-mediation) is not a new phenomenon, it has been practiced for more than 20 years in different parts around the world, and has opened the doors for many high-tech solutions, which save time and other resources by transferring the process of mediation to the online environment.

One effort to support the penetration of digital mediation in everyday live of business is the project e-MEDIATION: promoting ICT tools to cross-border disputes resolution, which has been financed by the JUSTICE program of the European Commission and is being implemented by three Bulgarian organizations: Law and Internet Foundation, the Bulgarian Chamber of Commerce and Industry, and Dextro Research. The goals of the project include building a platform for easy, affordable and efficient online mediation, as well as raising awareness for the opportunity of using mediation as a dispute resolution mechanism and improving mediation culture.

In the following text, some of the findings of the e-MEDIATION project will be discussed, namely how communications can and should be adapted for the online environment, as well as what additional steps mediators should undertake when taking on mediation cases online. The article includes suggestions and recommendations on communication techniques after a thorough analysis of the historical background and the implications, introduced by the digital environment.

Communication in mediation throughout history

The roots of mediation trace back to antiquity. Historians identify early cases of mediation in ancient India and Phoenicia. Disputes were solved with the support of a third independent person in ancient Greece and later in the Roman Empire (the Roman law has implemented mediation through the Corpus Juris Civilis).

In the last two decades, mediation has become a preferable dispute resolution method not only in the United States – it has paved its way into the European legal system.

In the twentieth century mediation became institutionalized in the secular arena. The Conciliation Act relating to the conduct of industrial relations was enacted in the United Kingdom as early as 1896. In the United States alternative dispute resolution (ADR) processes were being formalized as an alternative to litigation early on with the U.S. Department of Labor (established in 1913) appointing a panel called "the commissioners of conciliation" to deal with labor/management disputes. Later that entity became the Federal Mediation and Conciliation Service.

The adoption of mediation as a mechanism for dispute resolution in countries of the European Union dates back only a few decades ago. There are also countries that started

¹ Author is Certified mediator, registered with the Ministry of Justice in Bulgaria. She is the Head of Trainings and Education Department of Law and Internet Foundation, and has completed her education in Bulgaria and Greece with a bachelor's degree in Business Studies and a master's degree in Business Analysis and ERP Systems. Affiliation: Law and Internet Foundation.

² Author holds a BA degree in International Relations from the University of Essex, UK, and a MA degree in European Union Law from both Sofia University and the University of Lorraine. She is the Head of Human Rights Department of Law and Internet Foundation and currently a PhD candidate with her research focused on the management of information and communication processes in the European Union. Affiliation: Law and Internet Foundation.

implementing it some years ago, which can lead to the conclusion that mediation is still under development in some ways and will prove to be much more polished and improved in the years to come. Some EU countries have applied mediation earlier and faster – for example Great Britain and the Netherlands, while other countries with shorter mediation history have done extensive researches and have a good legal base – like Austria and Germany.

There is evolution in the legal framework in regard to mediation on EU level; a strong impetus was definitely given by the EU Directive on Mediation. A lot of countries have since regulated not only cross-border mediation but have developed the legal framework covering mediation on national level as well.

A key element in the mediation process is communication between the parties and the mediator. The most open definition of communicative action given by Habermas³ is that it is an action in which: „the actors seek to reach an understanding about the situation and their plans in order to coordinate their actions by way of agreement... A type of interaction that is coordinated through speech acts and does not coincide with them”. Although the theory of communicative action is abstract, dealing with the grounds of how people get along, it still demonstrates how people actually do seek to relate to each other. Mediators can take advantage of this to remain centered and proactive through the conflict resolution process. By weaving together this theory with mediation practice, both theory and practice are enriched and enlivened.

From ancient times and looking forward, mediation is a form of communication – a form of overcoming differences with the goal of aligning interests, supporting relationships and finding the best possible solutions. However, those communication processes have usually always existed in the face-to-face context; now, as mentioned before, with the fast penetration of technology into the world, communication in mediation should also adapt appropriately, as discussed further below.

Changes of digital environment

On the international level, mediation is used in a number of areas: family matters – pre-marriage agreements, financial misunderstanding, separation, divorce, child and elder people care, family business relationships, property disputes; in the working place – working conditions, discrimination, termination of labor contracts, compensations, peer disputes; in commerce – tenant/landlord relations, contractual relations, medical services, business partnerships; society matters – environment, disputes in education institutions, non-governmental organizations, victim/criminal relations, etc.

As the ICT is penetrating faster and faster in the everyday life influencing almost every person on the planet, logically the next step in the mediation process is to transform itself into an online process or simply – e-mediation.

Electronic mediation is a part of alternative dispute resolution methods and can be used in practice for all cases where mediation is applicable. Most often it is used to resolve consumer disputes, including online commerce, where both parties are distant from each other. As a result of the increasingly active use of information and communication technologies in trade, in fact, online dispute resolution (ODR) was initiated. Other factors that have influenced the emergence of ODR are: rapid development and penetration of digital technologies; new communication tools; mobility of citizens; globalization. It is important to notice that ODR includes more than online mediation.

The implementation of online dispute resolution includes the following stages: input of initial information, launch of the procedure/thanks to the initiative of at least one party and the work of technologies/, gathering of information, evidence, etc., hearing if needed, conducting online discussions – audio and video, developing an agreement.

A key element in ODR is the use of technology/computer, mobile device, telephone, etc./and software. In e-mediation, the mediator and the parties are supported in the following actions: organizing information, sending automatic messages, drafting a written communication, blocking rough language, video and audio conferencing, drafting agreements, etc. The software can monitor meetings – start, duration, clarification of interests and priorities, etc. activities, depending on the development parameters. To some extent, ICT can even reduce the role of the mediator.

With ICT development, online dispute resolution is also developing – efficiency increases due to more functionality and cost savings. The project e-MEDIATION was created with a goal to develop an online platform to facilitate all mentioned processes.

The platform is developed in two languages, to accommodate for transnational disputes, and it is focused exclusively on commercial issues. The user profiles are easy to make and are not publicly available in the platform, so as to keep the anonymity of users; registered mediators, on the other hand, can manage visibility of their profile and can be active or inactive, depending on their work availability. The e-MEDIATION platform gives the parties in a dispute the options to have online conversations, video conferences with the mediator, to have more than one mediator for a procedure, to safely and securely exchange documents between each other and between themselves and the mediator.

³ J. Habermas, *Theory of Communicative Action, Volume One: Reason and the Rationalization of Society* (Book), Boston 1981.

All of these options show both the new environment in which all of us function, and the possibility to seamlessly move the process of mediation into the digital space. In the following sections, some suggestions, ideas and tips will be provided for a better adjustment of mediators to the new area of communication, in which we are gifted with some new options, while deprived of other innate abilities, such as reading body language in person.

Communication techniques for mediation in the digital environment and in the platform e-MEDIATION

A significant number of techniques, utilized by mediators, demand a type of personal contact, skills in managing the mood of a room, clearly reading intentions and body language, etc. One of the great challenges of translating the process of mediation into the online environment is the loss of many of those opportunities of finding solutions, potential interests, as well as a general feel of the tone and the direction of negotiations. This barrier is most easily overcome in platforms through transforming this apparent weakness into a strength for the mediator. This can be seen through the lens that online communication (in written form) usually means a slower response time, as well as a slower exchanging of information between different sessions. This gives the opportunity for a calmer pace of work for the mediator, as well as sufficient time for creating and adapting a strategy for dealing with the issues at hand. Moreover, experts notice a tendency for well-thought and calmer communication between the parties, when they can see their behavior „from the outside” – something rare in direct communication, when the parties are usually strongly affected⁴.

Deriving from this, it is important for mediators to take advantage of these tendencies by giving sufficient time for response for both parties, writing well-thought out responses to questions and feelings, as well as sometimes even intentionally slowing down communication in order to give parties „air” in the virtual space.

Something else crucial, when taking into account the change of environment to the digital, is that not all participants will be equally tech-savvy in most cases. This is why mediators, who have been put in this environment before, agree that there should be special attention paid to an introduction of the participants to the process of mediation, the functionalities of the platform used, as well as the options and rules that all participants should abide to. This thorough introduction (which can include a tour, written notes, screenshots of the environment, guidelines or a „practice” session for the participants, which they learn by doing) is key to a flawless and easy process of e-mediation afterwards⁵.

Another important note to hit on from the process of mediation and part of techniques, which should be adapted, is building trust with parties – an element of the process, which can decide the outcome of the whole mediation. A 2014 research⁶ discusses the use of video conferences as a tool for trust-building and notes that it can be used to overcome the barriers, connected to non-verbal communication and its interpretation, discussed above as a part of traditional mediation techniques. The authors also indicate that using video calls is pointed at by many experts as the solve-all tool for all problems, originating by text-based communication. However, video conference calls often create completely new challenges for trust-building between the mediator and the parties. There is a period of adjustment for all parties, as one article phrases it, to adapt from „face-to-face” to „screen-to-screen” communication⁷. It is recommended that trust-building should be established through the use of at least one video conference with all parties, which will introduce them to the mediator, give them a feeling of the mediator as a person, and put them at ease when considering what and when to say.

While not a panacea, it is still important to remember that a truly large part of the issues, connected to developing trust between the mediators and the parties, is indeed solved through the introduction of a video – and even more importantly, conference calls – which include all parties (and potentially their legal representatives) and the mediator at the same time.

On the topic of guaranteeing privacy in the online environment, a 2015 publication⁸ shows that as people grow closer to technologies, their trust in digital means of communication increases together with their desire to solve as many problems as possible through online and digital means. This does not exclude privacy in procedures, such as mediation, where the authors specifically note that it is enough to have in place processes of erasure and lack of collection of data for parties. This fact should also be clearly conveyed to parties in order to ensure their strong trust towards technology, the platform and the process of mediation.

⁴ P. Staff, Using E-Mediation and Online Mediation Techniques for Conflict Resolution, Harvard Law School Daily Blog 2018.

⁵ A. Hammond, How Do You Write 'Yes?': A Study on the Effectiveness of Online Dispute Resolution, Conflict Resolution Quarterly, Spring2003, Vol. 20, Issue 3, pp. 261–286.

⁶ N. Ebner, J. Thompson, @ Face Value? Nonverbal Communication & Trust Development in Online Video-Based Mediation, International Journal of Online Dispute Resolution 2014.

⁷ J. Hörnle, Online Dispute Resolution: The Emperor's New Clothes?, International Review of Law, Computers & Technology, Mar2003, Vol. 17, Issue 1, pp. 27–36.

⁸ C. Rule and I. Sen, Online Dispute Resolution and Ombuds: Bringing Technology to the Table, Journal of the International Ombudsman Association 2015.

⁹ J. Rifkin, Online Dispute Resolution: Theory and Practice of the Fourth Party, Conflict Resolution Quarterly, Fall2001, Vol. 19, Issue 1, pp. 117–124.

Communication changes when put into the digital environment, without argument⁹. However, mediators as agile supporters of the process of reconciliation, mutual understanding and cooperation, should be encouraging when taking on this means for the process. This includes not only advocating for the parties to take advantage of the options and functionalities of platforms they use, but also demonstrating their usefulness by example, and embracing new developments. The enthusiasm of the mediator, more than anything, can prove to be the key in acceptance of new means of technology, a powerful trust-builder for the process, and a driver of effective inter-personal communication for mediation.

Some additional communication techniques are outlined below as recommendations for mediators and sides in disputes.

Recommendations and conclusions

In order to help facilitate the process of transition into the online environment, the e-MEDIATION project team has created a Mediator's Code of Conduct, which highlights some of the most important elements of mediation online – some of which may be overlooked by mediators, who are just making the transition.

Based on that research, it is important to highlight some recommendations for the mediators in the online space:

- 1) The mediator should communicate with the parties about convenient times and find out the most suitable time for the first common meeting before inviting them. A good idea might be to set up a short questionnaire with possible dates and times through a Meeting Scheduler tool, for example Calendly, Doodle or TimeBridge.
- 2) The mediator should ensure a good environment for the first common meeting and meetings that follow. This includes setting up online etiquette rules, explaining functionalities and options the platform offers, giving the parties time and opportunity to clear up their use of the platform. The

online etiquette could include rules such as when to mute a microphone, how and when to use emoticons, how to go about asking for a separate meeting, etc.

- 3) Other things to be noted when having a conference call between parties and mediator/s are:
 - Test hardware and Internet connection before the time of the meeting;
 - Make sure to be in a well-lit space; the camera should cover the face and hand movements of the mediator/s;
 - Demonstrate to the parties that the mediator/s are alone in their space;
 - Wear headphones to improve the quality of the call, as well as to improve security;
 - Foresee potential distractions such as phone ringing, arrival of people in the room, etc. and eliminate them as much as possible;
 - Encourage the parties to turn on their cameras at least during the first, but also following conference calls;
 - Make eye-contact with the camera, instead of the screen, in order to create trust with the parties;
- 4) Confidentiality should be underlined specifically in the online setting – the parties should be reassured in the mediator's opening statement that the environment does not change confidentiality of the procedure; on the other hand, the mediator should not attempt to record conference calls, save chats or documents and should destroy their notes as soon as the procedure is over.

Mediators are faced with a new challenge in times of digital progress and integration of new technologies in the everyday life of people – managing and mediating communication in a new way. However, this is something which should not be seen as a hurdle to overcome, but a process of development and growth, which includes those mediators.

Processes are made easier, faster and cheaper through the introduction of new technologies to the world, and it is important to take advantage of their benefits and evolve them with technology.

Key words: mediation, dispute resolution, communication, communication techniques, e-MEDIATION project.



beck.pl
Wydawnictwo C.H. BECK



www.beck.pl

Recenzja monografii: *Filip Radoniewicz, Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warszawa 2016*

dr Piotr Siemkowicz¹

Monografia autorstwa F. Radoniewicza, pt. *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, jest ciekawym opracowaniem, w którym autor starał się w sposób możliwie pełny przedstawić najistotniejsze zagadnienia związane z pojęciem hackingu oraz innych przestępstw skierowanych przeciwko bezpieczeństwu danych komputerowych i systemów informatycznych w ujęciu praktycznym i karnoprawnym.

Już pierwszy rozdział pt. *Hacking – zagadnienia ogólne*, stanowi pogłębione spojrzenie na rozwój technologii komputerowej, poczynwszy od lat 40. ubiegłego wieku aż do czasów współczesnych. Autor sygnalizuje przy tym technologiczne uwarunkowania i przyczyny powstawania sieci komputerowych – zarówno lokalnych sieci LAN w standardzie Ethernet, jak i genezę powstania sieci Internet, wywodzącej swoje korzenie od sieci ARPANet. W rozdziale tym przedstawiono genezę pojęcia terminu „hacker” i „hacking”, przy czym autor wskazuje na ewolucję omawianych terminów, obecnie (odmiennie niż przed kilkoma dekadami) postrzeganych zazwyczaj w kontekście negatywnym.

Istotną zaletą rozdziału pierwszego jest niewątpliwie przedstawienie – niejako w „pigułce”, podstawowych pojęć informatycznych oraz technicznych, dotyczących budowy, struktury i funkcjonowania zarówno urządzeń komputerowych, jak i sieci komputerowych. Podkreślić przy tym należy, że w większości wypadków opracowania dotyczące cyberprzestępczości pomijają tego rodzaju wprowadzenie techniczne, co bez wątpienia uznać należy za błąd.

W omawianym rozdziale poddano także analizie techniczne aspekty działań hackerskich (zarówno na etapie przygotowawczym, ataku właściwego, jak i tzw. zacierania śladów po przeprowadzonym ataku) dokonywanych głównie w środowisku sieciowym, jak też omówiono najczęściej spotykane rodzaje ataków hackerów. Autor przedstawia na wstępie – w ślad za innymi cytowanymi w przypisach autorami, klasyfikację ataków hackerskich między innymi na podstawie: kryterium stopnia interakcji sprawcy z atakowanym systemem (ataki pasywne i aktywne), kryterium źródła ataku (ataki lokalne i zdalne) oraz z uwagi na kryterium liczby zaangażowanych komputerów (ataki bezpośrednie i rozproszone). Autor zamieścił także w swojej publikacji propozycję przyjęcia dla systematyzacji ataków hackerskich kryterium zamiaru sprawy – wyróżniając w tym zakresie ataki umyślne i nieumyślne. Ta ostatnia klasyfikacja może

jednak budzić pewne wątpliwości, a to z uwagi na uznanie, że atak hackerski może mieć *de facto* charakter nieumyślny. Warto zauważyć, że przestępstwa o charakterze hackerskim, w tym zwłaszcza z rozdziału XXXIII Kodeksu karnego, dla ich realizacji wymagają umyślności, a tym samym działania sprawcy w zamiarze bezpośrednim lub co najmniej ewentualnym. Tym samym wskazane przez autora na s. 76 niniejszej monografii opisy, iż: „wbrew pozorom wiele ataków ma taki właśnie charakter, jest dziełem przypadku lub wynika ze zwykłej ludzkiej nieostrożności”, a także dalej, iż „przykładowo, większość wirusów rozprzestrzenianych jest przez sieć przez nieświadomych tego użytkowników. Sieć może też zostać unieruchomiona przez użytkownika eksperymentującego z oprogramowaniem” – należałoby raczej zakwalifikować jako „incydenty sieciowe”, nie zaś ataki hackerskie *sensu stricto*. Reasumując, użycie sformułowania „atak” do zachowania nieumyślnego – które faktycznie, co do zasady, nie zrealizuje znamion przestępstwa zaliczanego do ogólnej grupy przestępstw hackerskich, wydaje się nieuprawnione.

Autor opisuje następnie w podrozdziale 1.3 najczęściej spotykane rodzaje ataków hackerskich takie jak: posłużenie się złośliwym oprogramowaniem w postaci m.in. koni trojańskich, exploitów, rootkitów czy też wirusów komputerowych, *sniffing*, *spoofing* i jego odmiany, *session hijacking*, *pharming* i *drive-by pharming*, *man-in-the-middle*, wykorzystanie luk i błędów w aplikacjach (przepełnienie buforów, SQL Injection oraz ataki XSS), łamanie haseł, *phishing*, ataki odmowy usługi – dostępu (DoS, DDoS i DRDoS), bomby e-mailowe oraz *bluejacking* i *bluehacking*. Autor jako jeden z rodzajów ataków hackerskich wymienia także stosowane przez hackerów socjotechniki (inżynierii społecznej), w tym tzw. odwrotną socjotechnikę. Pogląd ten może budzić pew-

¹ Autor wykonuje zawód adwokata. W ramach swoich zainteresowań naukowych autor zajmuje się prawem karnym, w tym w szczególności problematyką szeroko rozumianej przestępczości komputerowej i internetowej.

ne wątpliwości z uwagi na to, iż stosowane przez hackerów metody socjotechniczne, zmierzające do wykorzystania tzw. słabego ogniwa systemu (a więc naiwności czy też lekkomyślności pracownika – użytkownika systemu), najczęściej w celu zdobycia loginów, haseł dostępu i uzyskania istotnych dla przyszłego ataku informacji o systemie, zazwyczaj mają charakter czynności przygotowawczych. Tym samym pomimo że czynności te faktycznie często warunkują późniejszą skuteczność ataku hackerskiego, zazwyczaj samym atakiem sieciowym jeszcze nie są, chyba że mają charakter powiązany z inną metodą hackerską – w tym głównie *pharmingiem* lub *phishingiem* – i są dokonywane w celu skierowania użytkownika np. na fałszywą stronę WWW instytucji bankowej po to, aby wyłudzić wpisywane na niej hasła i loginy.

Niezależnie od wskazanych powyżej uwag, sposób zaprezentowania przez autora poszczególnych rodzajów działań hackerskich, w tym głównie o charakterze destrukcyjnym, uznać należy za pełny i przejrzysty.

W omawianym podrozdziale przedstawiono także wiele informacji praktycznych, poczynając od szczegółowego nazewnictwa i sposobu działania złośliwego oprogramowania, a także potencjalnych skutków użycia takich programów komputerowych przez hackera. Autor w szczególności poddał analizie kilka rodzajów wirusów komputerowych w kontekście sposobu ich działania, cech charakterystycznych oraz umiejscowienia. Szczegółowe rozważania dotyczą wykorzystania w inwazyjnych działaniach hackerskich koni trojańskich i innych odmian złośliwego oprogramowania, przy czym autor sposób działania tych programów komputerowych przedstawił na podstawie praktycznych przykładów.

Do złośliwego oprogramowania autor zalicza także nie bez racji pliki *cookies* i *tracking cookies* (ciasteczka śledzące), które co do zasady nie mają charakteru szkodliwego lub destrukcyjnego dla systemów i danych komputerowych, służą jednak do gromadzenia danych wrażliwych dotyczących użytkownika odwiedzającego daną stronę WWW, a w przypadku *tracking cookies* także do obserwowania działań podejmowanych przez użytkownika w sieci, co służy w efekcie dopasowaniu reklam do gustu i zainteresowań użytkownika. W rzeczywistości nie można jednak wykluczyć, że dane zdobyte we wskazany sposób mogą być także wykorzystane w celach przestępczych, w tym także do podszywania się pod cudzą tożsamość.

Także szczegółowa analiza poszczególnych rodzajów ataków hackerskich (s. 89–113) dokonana przez autora jawi się jako przedstawiona w sposób profesjonalny oraz przydatny z punktu widzenia celu, dla którego przedmiotowa monografia została przygotowana. Zastrzeżenia budzi jedynie kilkukrotne odwoływanie się w przypisach podrozdziału 1.3 do wpisów opublikowanych w Wikipedii. Z natury rzeczy trudno uznać Wikipedię za źródło o charakterze naukowym, a zarazem w pełni wiarygodne. Poszczególne hasła opracowywane

są bowiem w jej ramach przez często bliżej nieokreślonych autorów i pochodzą niekiedy z wątpliwych naukowo źródeł. Tym samym odwołania w przypisach: Nr 182 (w zakresie dotyczącym *bluejackingu*), Nr 186, 187, 189, 190 (w zakresie dotyczącym systemów wykrywania ataków) oraz Nr 194 i 195 (w zakresie dotyczącym programów wykorzystywanych w informatyce śledczej – EnCase i PTK_Forensics) bezpośrednio do polskiej i angielskiej edycji Wikipedii wydają się istotnym mankamentem publikacji o charakterze *stricte* naukowym.

Rozdział drugi poświęcony został natomiast wprowadzeniu w problematykę przestępczości komputerowej. Autor przedstawia w nim ogólne pojęcie przestępstwa komputerowego, sygnalizując zarazem, że dotychczas żaden ustawodawca nie zdecydował się na wprowadzenie do systemu prawnego definicji legalnej przestępstwa komputerowego, a spotykane dotychczas próby zdefiniowania tego pojęcia mają wyłącznie miejsce w ramach doktryny prawa karnego. Autor przedstawia także w tym zakresie własną „roboczą” definicję przestępstwa komputerowego (cyberprzestępstwa) jako każdego nielegalnego działania skierowanego przeciwko systemom komputerowym, sieciom komputerowym lub danym komputerowym, albo takiego, w którym system komputerowy lub sieć komputerowa są narzędziem służącym jego popełnieniu.

W dalszej części rozdziału drugiego autor, poza sygnalizacją zagrożeń oraz nowych wyzwań związanych z pojawieniem się przestępczości komputerowej oraz krótkim zarysem historii kryminalizacji tego zjawiska, poddaje również analizie podstawowe pojęcia istotne z punktu widzenia znamion czynów o charakterze hackingu, takie jak: „informacja”, „dane”, „program komputerowy”, a także „poufność”, „integralność” i „dostępność danych komputerowych”.

Rozdział trzeci poświęcony został natomiast inicjatywom międzynarodowym mającym na celu zwalczanie cyberprzestępczości. Autor poddał w przedmiotowym rozdziale analizie wiele działań i instytucji międzynarodowych bezpośrednio wiążących się z przeciwdziałaniem przestępczości komputerowej i internetowej. W rozdziale tym autor pogłębianej analizie poddaje w szczególności przepisy Konwencji o cyberprzestępczości – przyjętej przez Komitet Ministrów Rady Europy 8.11.2001 r., a otwartej do podpisu 23.11.2001 r. w trakcie Międzynarodowego Kongresu w sprawie cyberprzestępczości w Budapeszcie.

Rozdział czwarty recenzowanej monografii poświęcony został z kolei zagadnieniom cyberprzestępczości w ramach prawa Unii Europejskiej. Autor przedstawił w nim poszczególne akty prawa europejskiego – poczynając od decyzji Rady 92/242/WE z 31.3.1992 r. w dziedzinie bezpieczeństwa systemów informatycznych, skończywszy na komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów COM (2009) 149 z 30.3.2009 r. w sprawie ochrony krytycznej infrastruktury informatycznej „Ochrona Europy przed

zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności” wraz z załączonym do niego raportem na temat bezpieczeństwa sieciowego.

Ostatnia część tego rozdziału poświęcona została natomiast szczegółowej analizie decyzji ramowej Rady Unii Europejskiej Nr 2005/222 z 24.2.2005 r. w sprawie ataków na systemy informatyczne oraz późniejszej i analogicznej zakresowo dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z 12.8.2013 r. dotyczącej ataków na systemy informatyczne oraz uchylającej decyzję ramową Rady 2005/222/WSiSW. Przedmiotowa analiza, mająca częściowo charakter porównawczy w kontekście uprzednich aktów prawa międzynarodowego – w tym zwłaszcza Konwencji o cyberprzestępczości, przeprowadzona została przez autora w sposób pełny i niebudzący zastrzeżeń.

Rozdział piąty recenzowanej monografii pt. Przestępstwa przeciwko danym komputerowym i systemom informatycznym w polskim Kodeksie karnym, został poświęcony omówieniu poszczególnych typów przestępstw z rozdziału XXXIII oraz stanowi on tym samym formę komentarza autorskiego.

W „uwagach wstępnych” zamieszczonych przez Autora na początku rozdziału piątego zwrócono uwagę na kilka istotnych kwestii mających znaczenie dla dokonywania prawidłowej wykładni gramatycznej (językowej) przepisów rozdziału XXXIII Kodeksu karnego. W szczególności słusznie podnosi autor, iż w sytuacji gdy dane określenie odnoszące się do terminologii bezpośrednio związanej z katalogiem przestępstw z art. 267–269b KK jest nieostre lub wieloznaczne, a jego znaczenie nie jest powszechnie zrozumiałe, istnieje konieczność ustalenia właściwego (nowego) znaczenia tego pojęcia w ustawie lub w innym akcie prawnym. Niestety, zdarza się – jak słusznie podkreśla autor – że ustawodawca próbuje często znaleźć polski odpowiednik terminologiczny danego pojęcia zapożyczonego z aktów prawa międzynarodowego w trakcie procesu dostosowywania polskiego prawa do standardów światowych bądź europejskich, na co trafnie przywołany przez autora przykładem jest dosyć nieszczęśliwy przykład pojęcia *interface* zapożyczonego z dyrektywy Rady 1991/250/EWG z 14.5.1991 r. w sprawie ochrony prawnej programów komputerowych, gdzie w rozdziale 7 ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych przetłumaczono to pojęcie jako „łącze”.

Słuszne były także uwagi autora (poczynione na bazie poprzednio obowiązującej regulacji prawnej w tym zakresie), iż posługiwanie się uprzednio przez ustawodawcę w rozdziale XXXIII Kodeksu karnego dwoma odmiennymi pojęciami „system informatyczny” (w art. 267 § 2 KK) oraz „system komputerowy” (w art. 269a i 269b § 1 KK – w ich brzmieniu sprzed 27.4.2017 r.) wydawało się działaniem zamierzonym i faktycznie odnosiło się do zakresu stosowania ww. regulacji.

Jak bowiem celnie wskazano, zakres przedmiotowy pojęcia „system komputerowy” jest znacznie węższy niż zakres pojęcia „system informatyczny” – pierwszy obejmuje faktycznie pojedynczy host w rozumieniu komputera, telefonu komórkowego, smartfona, dekodera, drugi zaś oznacza z reguły połączone ze sobą co najmniej dwie jednostki (hosty) działające w sieci. W tym kontekście, zdaniem autora, nie jest możliwe zamienne stosowanie pojęć „systemu komputerowego” i „systemu informatycznego”.

Uwagi te obecnie, ze względu na nowelizację art. 269a oraz 269b § 1 KK dokonaną ustawą z 23.3.2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw², a także z uwagi na usunięcie z tych przepisów pojęcia „systemu komputerowego” i „sieci informatycznej” oraz zastąpienia ich nowymi pojęciami „systemu informatycznego”, „systemu teleinformatycznego” oraz „sieci teleinformatycznej”, utraciły swoją aktualność.

Ciekawymi jawią się rozważania autora poczynione na kanwie art. 267 § 2 KK, a dotyczące skutków uzyskania przez sprawcę dostępu do niezabezpieczonej sieci bezprzewodowej. Zwrócono w tym zakresie uwagę na zjawiska określane jako *wardriving* oraz *piggybacking*. Pierwsze z nich – polegające na poszukiwaniu za pomocą urządzenia (laptopa, notebooka) wyposażonego w kartę sieciową WLAN niezabezpieczonych sieci bezprzewodowych – jak słusznie zauważa autor, nie wyczerpuje znamion przestępstwa, jeśli nie wiąże się z próbą uzyskania dostępu do sieci. Czyn z art. 267 § 2 KK byłby w tej sytuacji zrealizowany dopiero wówczas, gdyby sprawca uzyskał dostęp do danych informatycznych przetwarzanych w tej sieci bezprzewodowej. Oczywiście jest przy tym, że dla bytu przestępstwa z art. 267 § 2 KK nie ma znaczenia, czy sprawca w celu uzyskania takiego dostępu przełamuje zabezpieczenia. W sytuacji jednak gdy sprawca w celu uzyskania dostępu do danych informatycznych takie zabezpieczenia złamie lub ominie (przy założeniu, że zabezpieczenia takie w ogóle zostały zastosowane), a następnie uzyska informację, do której nie jest uprawniony, to wówczas – jak celnie wskazuje autor – zrealizuje znamiona czynu z art. 267 § 1 KK.

W odniesieniu do zjawiska *piggybackingu* – związanego z uzyskaniem dostępu do systemu informatycznego w wyniku wykorzystania uprawnień innego użytkownika – autor trafnie zauważa, że zachowanie takie realizują także ataki typu *session hijacking* oraz *man-in-the-middle*, które powinny być kwalifikowane jako przestępstwa z art. 267 § 3 KK. W pełni należy zgodzić się przy tym z dalszymi rozważaniami poczynionymi w tym zakresie, iż w przypadku *piggybackingu* w ramach sieci Wi-Fi, polegającego na uzyskaniu nieuprawnionego dostępu do sieci bezprzewodowej (zwłaszcza w przypadku gdy nie była ona zabezpieczona)

² Dz.U. poz. 768.

– wyłącznie w celu korzystania z usług sieciowych na rachunek konkretnego hosta z takiej sieci, poza faktycznym efektem w postaci spadku wydajności sieci (co w przypadku istotnego zakłócenia jej funkcjonowania można byłoby ewentualnie kwalifikować jako czyn z art. 269a KK), trudno będzie przypisać sprawcy takiego działania realizację czynu o znamionach przestępstwa. Jak słusznie zwraca na to uwagę autor, w niektórych przypadkach może jednak dojść do określonych konsekwencji finansowych po stronie ofiary takiego działania, w szczególności gdy sprawca wykorzysta bezprawne uzyskanie dostępu do ww. sieci Wi-Fi do transferu lub pobierania znacznej ilości danych. Rodzić to może po stronie legalnego użytkownika określone konsekwencje finansowe w postaci zwiększonego rachunku za transfer, który został wykorzystany *de facto* przez sprawcę. Zauważyć przy tym należy, że do opisywanej sytuacji nie będzie mógł z oczywistych względów znaleźć zastosowania art. 285 § 1 KK – sankcjonujący tzw. kradzież impulsów telefonicznych, a to z uwagi na użycie przez ustawodawcę we wskazanym przepisie pojęcia „uruchomienia na cudzy rachunek impulsów telefonicznych”, co w żadnym zakresie nie może być utożsamiane z transferem danych informatycznych. Tym samym z uwagi na pominięcie przez ustawodawcę w treści art. 269a KK elementu „wyrządzenia szkody majątkowej”, w przypadku gdy łączy się ona z transmisją danych informatycznych dokonywanych bez uprawnienia przez sprawcę za pośrednictwem sieci Wi-Fi, faktycznie w większości wypadków opisywane powyżej działanie sprawcy nie będzie podlegało możliwości ścigania na gruncie ustawy karnej.

Za słuszne należy także uznać spostrzeżenie przedstawione w ramach omawianego rozdziału (s. 305), że art. 267 § 3 KK kryminalizuje jedynie przechwytywanie danych komputerowych w czasie ich przesyłania (w czasie rzeczywistym), co z oczywistych względów oznacza, że w przypadku uzyskania przez sprawcę danych przechowywanych np. na serwerze czy w prywatnym komputerze właściwa będzie kwalifikacja z art. 267 § 1 KK lub z art. 267 § 2 KK.

Za istotne uznać należy także spostrzeżenia przedstawione na s. 309 recenzowanej monografii, iż za niedopatrzenie ustawodawcy uznać należy brak w ramach regulacji art. 267 KK typu kwalifikowanego omawianego przestępstwa – a mianowicie czynu, który miałby polegać na posłużeniu się przez sprawcę w celu ujawnienia określonych informacji środkami masowego przekazu, na zasadach analogicznych do czynu z art. 212 § 2 KK. Oczywiście jest bowiem, że także dane uzyskane w ramach działań realizujących znamiona czynu z art. 267 § 1–3 KK mogą być następnie rozpowszechnione za pośrednictwem sieci Internet, w tym np. na stronie internetowej, w ramach portalu społecznościowego lub serwisu o zasięgu globalnym. Tym samym ściganie takich czynów jedynie w ramach art. 267 § 4 KK – sankcjonującego ujawnienie innej osobie informacji

uzyskanej w sposób określony w art. 267 § 1–3 KK, wydaje się daleko niewystarczające. Autor słusznie przytacza przy tym przykład działalności portalu Wikileaks.

W odniesieniu do czynu z art. 268 § 1 i 2 KK autor zauważa, że zniszczenie jednej z kopii zapisanej informacji (w sytuacji gdy użytkownik ma nadal dostęp do tych informacji w ramach innych kopii) nie wypełnia znamion omawianego przestępstwa. W tym zakresie podzielony został także pogląd A. Adamskiego, że znamion tego czynu nie wypełnia zachowanie sprawcy, który niszczy nośnik danych, w sytuacji gdy dysponent tych danych posiada kopię zapasową, oraz że zachowanie takie można kwalifikować jedynie jako usiłowanie czynu z art. 267 § 1 lub 2 KK.

W zakresie czynu z art. 268a § 1 lub 2 KK autor podejmuje m.in. polemikę z reprezentowanym w doktrynie poglądem, że wskazane przepisy dotyczą danych zgromadzonych w formie baz danych. Przecistawiając się temu pogładowi, autor wskazuje, że pojęcie bazy danych nie jest tożsame z pojęciem zbioru danych, przy czym zbiór danych w sensie informatycznym musi spełniać kilka dodatkowych kryteriów, aby można było uznać go za bazę danych. Pogląd ten, który w mojej ocenie należy podzielić, autor rozwija dodatkowo w przypisach Nr 772 i 773, systematyzując pojęcia baz danych oraz zbioru danych. Dodatkowo w przedmiotowym podrozdziale słusznie zwraca się uwagę na nieprecyzyjność art. 268a § 1 KK, a to w kontekście wątpliwości rodzących się na kanwie postawionego tam pytania o to, co faktycznie jest przedmiotem wykonawczym kryminalizowanych zachowań opisanych w tym przepisie. Przepis ten w swojej początkowej treści stanowi bowiem, że „kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych”, co z oczywistych względów rodzi pytanie, czy przedmiotem wykonawczym tego czynu jest „dostęp do danych informatycznych” czy też „dane informatyczne”. Autor przychylił się przy tym do stanowiska, że wskazanym przedmiotem wykonawczym są „dane informatyczne”. Stanowisko to należy uznać za przekonujące – a to z uwagi na wykładnię logiczną ww. przepisu. W sytuacji bowiem uznania (zgodnie z literalnym brzmieniem przepisu), iż przedmiotem wykonawczym czynu z art. 268a § 1 KK jest „dostęp do danych informatycznych”, należałoby uznać wszakże, że możliwe jest „niszczenie, uszkadzanie, usuwanie bądź zmienianie” takiego „dostępu” do przedmiotowych danych informatycznych, co z oczywistych względów jest niemożliwe. Niszczyć, uszkadzać, usuwać bądź zmieniać można bowiem wyłączenie dane informatyczne – po wcześniejszym uzyskaniu do nich dostępu.

W podrozdziale ósmym rozdziału piątego autor omawia czyn z art. 269 KK (sabotażu informatycznego), zauważając zarazem, że z uwagi na zdecydowanie wyższe znaczenie informacji chronionych przez art. 269 § 1 KK w porównaniu z informacjami podlegającymi ochronie na podstawie

art. 268 § 2 KK oraz podobieństwo pozostałych znamion czynów kryminalizowanych przez te przepisy, przy jednoczesnej różnicy w wysokości zagrożenia karą i środkami karnymi, przestępstwo z art. 269 § 1 KK uważa się za typ kwalifikowany w stosunku do przestępstw z art. 268 § 2 KK. Dodatkowo słusznie podkreśla się w ramach przedmiotowego omówienia, iż nie stanowi przestępstwa określonego w art. 269 § 2 KK takie zachowanie, które prowadzi do zniszczenia lub wymiany nośnika danych albo do zniszczenia lub uszkodzenia urządzenia służącego do przetwarzania, gromadzenia lub przekazywania danych, jeżeli jednocześnie sprawca nie zniszczył, nie uszkodził, nie usunął lub nie zmienił zapisu danych o szczególnym znaczeniu w rozumieniu tego przepisu bądź nie doprowadził do zakłócenia lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Autor trafnie zauważa jednak, że w przypadku gdy sprawca wiedział, jakie jest przeznaczenie urządzeń będących przedmiotem jego czynu – możliwe będzie zakwalifikowanie działania sprawcy jako usiłowania, przy czym w jego ocenie podobna sytuacja zajdzie wówczas, gdy czyn sprawcy skutkować będzie jedynie uszkodzeniem nośnika danych, a nie jego zniszczeniem.

W uwagach dotyczących art. 269a KK (zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej) autor wysuwa pogląd, iż wskazany przepis znajduje zastosowanie do wszystkich zamachów na bezpieczeństwo sieci o charakterze logicznym – a więc np. ataków odmowy usługi DoS, rozproszonej odmowy usługi DDoS lub polegających na manipulacji danymi wejściowymi, a tym samym ma on charakter szczególny w stosunku do art. 268a § 1 KK – istotnie ograniczając w związku z tym jego znaczenie i redukując jego zastosowanie do zamachów na dane informatyczne lub ewentualnie zamachów fizycznych na bezpieczeństwo sieci. W przypadku natomiast gdy sprawca wyrządzi znaczną szkodę, której możliwość przewidywał i na to się godził, odpowie za czyn z art. 268a § 2 KK.

W uwagach dotyczących czynu z art. 269b § 1 KK autor słusznie zwraca uwagę, iż przepis ten jest skonstruowany wadliwie, w tym poprzez brak wskazania w jego treści hackingu *sensu stricto* – a więc nieuprawnionego uzyskania informacji z art. 267 § 1 KK oraz nieuprawnionego dostępu do systemu informatycznego z art. 267 § 2 KK.

Dalsze uwagi autora co do oceny działań twórcy programu spełniającego faktycznie kilka funkcji, który może zostać następnie użyty przez inną osobę w celach przestępczych, z uwagi na nowelizację dokonaną ww. nowelizacją z 23.3.2017 r., utraciły, jak się wydaje, swoją aktualność. W szczególności bowiem z uwagi na wprowadzenie art. 269b § 1a KK stanowiącego, że nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymie-

nionego w tym przepisie albo opracowania metody takiego zabezpieczenia, brak jest obecnie możliwości pociągnięcia do odpowiedzialności karnej osoby, która wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy o cechach opisanych w art. 269b § 1 KK, jednakże czyni to jedynie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.

Podobny charakter ma również dodany tą samą ustawą art. 269c KK, który stanowi, iż nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a KK, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Dalsza część rozdziału piątego (podrozdział 5.11) poświęcona została omówieniu często poruszanej w doktrynie przedmiotu problematyki zbiegu przepisów i przestępstw w zakresie czynów rozdziału XXXIII – zarówno w relacji bezpośrednio pomiędzy tymi czynami, jak i w zbiegu z przestępstwami innych rozdziałów części szczególnej Kodeksu karnego. Autor, posiłkując się w tym zakresie poglądami innych autorów, jak też przedstawiając własne oceny poszczególnych możliwych zbiegów przepisów i przestępstw, analizuje zachodzące w tym zakresie sytuacje, w tym także wskazuje, który w jego ocenie przepis znajdzie w danym wypadku zastosowanie.

W rozdziale szóstym pt. Uwagi prawnoporównawcze autor dokonuje natomiast omówienia regulacji z zakresu prawa karnego materialnego, bezpośrednio związanych z szeroko rozumianą problematyką przestępstw hackerskich, w tym przestępstw skierowanych przeciwko bezpieczeństwu informacji, systemów komputerowych i sieci informatycznych, a obowiązujących w wybranych krajach europejskich. Należy przy tym z dużym szacunkiem odnieść się do znacznego nakładu pracy autora związanej z prześledzeniem poszczególnych, zagranicznych regulacji karnoprawnych, a także przedstawieniem ich w skondensowanej, ale zarazem przejrzystej i dostępnej formie.

Ostatni rozdział – siódmy, ma charakter opracowania kryminologicznego oraz obejmuje analizę badań opartych na metodzie statystycznej oraz badań empirycznych, a dotyczących skali i rozmiaru przestępczości komputerowej (w tym także zjawiska hackingu) w Polsce. Autor poddaje ocenie statystyki policyjne i zauważa, że większość przestępstw popełnianych głównie za pośrednictwem sieci Internet (ok. 80%) stanowią tzw. oszustwa internetowe, które co do zasady zazwyczaj realizują znamiona klasycznego

występków z art. 286 § 1 KK, oraz że można zaobserwować w Polsce zjawisko stałego wzrostu przestępstw stwierdzonych – popełnianych za pośrednictwem sieci Internet. Z uwagi także na zbiorczy sposób przedstawiania w statystykach policyjnych liczby wszczętych postępowań oraz przestępstw stwierdzonych, co przejawia się np. włączeniu w jedną grupę występów z art. 267 § 1, z art. 267 § 2, z art. 267 § 3 i z art. 267 § 4 KK, bez wyróżnienia, ile z nich dotyczy faktycznie przestępstw komputerowych, a ile przestępstw pospolitych (np. „przeciwko korespondencji” lub związanych z „tradycyjnym” podsłuchem telefonu), jak słusznie zauważa autor, statystyki te są mało przydatne dla zobrazowania rzeczywistej skali przestępczości komputerowej, w tym także *stricto* hackerskiej w Polsce.

Autor przedstawia także w rozdziale siódmym wyniki własnych badań empirycznych, w zakresie analizy akt prokuratorskich spraw dotyczących przestępstw z art. 267 § 2, z art. 268 § 2 i 3, z art. 268a § 1 i 2, z art. 269 § 1 i 2, z art. 269a oraz z art. 269b § 1 KK, zarejestrowanych w powszechnych jednostkach organizacyjnych prokuratur w latach 2009–2010, w łącznej liczbie 1163 spraw. Dodatkowo autor prezentuje w zanonimizowanej formie wybrane stany faktyczne, do-

tyczące niektórych spraw prowadzonych uprzednio przez prokuratury. Przedstawione przykłady omawianych stanów faktycznych – opartych na konkretnych sprawach karnych – pozwalają prześledzić pewien *modus operandi* sprawców najpopularniejszych w polskich warunkach czynów, realizowanych za pośrednictwem sieci Internet.

Reasumując, monografię F. Radoniewicza pt. Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym uznać można za bardzo istotną na polskim rynku prawniczym i wartą polecenia publikację. Z oczywistych względów wymaga ona aktualnie nieznacznej korekty (głównie w zakresie dotyczącym rozdziału piątego), z uwagi na zmiany ustawodawcze, które weszły w życie już po publikacji, a dotyczące nowelizacji treści art. 269a, art. 269b § 1 KK, oraz dodania do rozdziału XXXIII nowych przepisów, tj. art. 269b § 1a oraz art. 269c KK.

Nie ulega również wątpliwości, że publikacja ta w szerokim zakresie spełni oczekiwania praktyków, w tym także sędziów i prokuratorów, w zakresie umożliwiającym im uzyskanie niezbędnej wiedzy specjalistycznej z dziedziny tzw. przestępczości hackerskiej.



Teksty Ustaw Becka

Zamów:
tel. 22 31 12 222
www.ksiegarnia.beck.pl

