



Marek Świerczyński^{a)}

 <https://orcid.org/0000-0002-4079-0487>

Prawo właściwe dla zobowiązań deliktowych wynikających z naruszenia zasad ochrony danych osobowych przyjętych w RODO

Abstract: Disputes arising from international data breaches can be complex. Despite the introduction of new, unified EU regulation on the protection of personal data (GDPR), the European Union failed to amend the Rome II Regulation on the applicable law to non-contractual liability and to extend its scope to the infringements of privacy. GDPR only contains provisions on international civil procedure. However, there are no supplementing conflict-of-law rules. In order to determine the applicable law national courts have to apply divergent and dispersed national codifications of private international law. The aim of this study is to propose an optimal conflict-of-law model for determining the applicable law in case of infringement of the GDPR's privacy regime.

Keywords: GDPR, Rome II Regulation, privacy breach, conflict-of-law rules, torts, delictual liability

1. Wprowadzenie

Spory dotyczące naruszeń danych osobowych w skali międzynarodowej są złożone¹. Pomimo obowiązywania nowych, ujednoczonych regu-

^{a)} Dr hab., Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie.

¹ Przykładem jest wyrok TSUE w sprawie Evy Glawischmig-Piesczek p. Facebook Ireland Limited (C-18/18) z dnia 3 października 2019 r. Trybunał przyjął, że sądy mogą

lacji unijnych o ochronie danych osobowych (RODO²), Unia Europejska nie wypełniła istniejącej w rozporządzeniu Rzym II³ luki, która dotyczy ochrony prywatności (art. 1 ust. 2 lit. g). RODO zawiera jedynie przepisy z zakresu międzynarodowego postępowania cywilnego (art. 79 i n.). Brak jest natomiast komplementarnej regulacji kolizyjnoprawnej dotyczącej odpowiedzialności z tytułu naruszenia zasad ochrony danych osobowych. W celu ustalenia prawa właściwego (statutu pomocniczego względem RODO) sądy muszą więc stosować krajowe przepisy prawa prywatnego międzynarodowego⁴. Celem niniejszego opracowania jest zaproponowanie optymalnego modelu ustalania prawa właściwego.

Opracowanie nie obejmuje problematyki naruszeń prywatności wykraczających poza zakres zastosowania RODO. Należy bowiem pamiętać, że RODO ma ograniczony zakres zastosowania, tj. tylko do przetwarzania danych w sprawach regulowanych prawem unijnym (art. 2 ust. 2).

2. Trudności występujące przy ustalaniu statutu ochronnego

Określenie prawa właściwego dla poszczególnych zagadnień związanych z ochroną danych osobowych nie jest zadaniem łatwym⁵. Utrudnienia wynikają z następujących powodów: 1) eksterytorialnego zakresu

nakazać dostawcy usług hostingowych usuwanie nielegalnych treści w skali całego świata. Dopuszczał nakazanie kasowania pojawiających się wpisów identycznych i równoznacznych z tymi, które sąd uzna za bezprawne (np. zniesławiające).

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych). Dz.Urz. UE L nr 119, s. 1 ze zm.

³ Rozporządzenie nr 864/2007/WE Parlamentu Europejskiego i Rady dotyczące prawa właściwego dla zobowiązań pozaumownych („Rzym II”). Na temat znaczenia rozporządzenia w zakresie odpowiedzialności deliktowej zob. J. Pazdan: *Rozporządzenie Rzym II — nowe wspólnotowe unormowanie właściwości prawa dla zobowiązań pozaumownych*. W: „Problemy Prawa Prywatnego Międzynarodowego”. T. 4. Red. M. Pazdan. Katowice 2009, s. 23; A. Nowicka: *Prawo właściwe dla zobowiązań wynikających z czynów niedozwolonych w świetle przepisów rozporządzenia nr 864/2007*. W: „Prace Instytutu Prawa Własności Intelektualnej UJ”. Z. 100: *Prawo własności intelektualnej wczoraj, dziś i jutro*. Red. J. Barta, A. Matlak. Kraków 2007, s. 312 i n.

⁴ M. Brkan: *Data Protection and Conflict-of-Laws: A Challenging Relationship*. „European Data Protection Law Review” 2016, vol. 2 (3), s. 337.

⁵ J. Chen: *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation*. „International Data Privacy Law” 2016, vol. 6 (4), s. 310 i n.

zastosowania RODO (art. 3 RODO), przy czym wątpliwości wywołuje zarówno ustalenie zasięgu tej eksterytorialności, jak i jej wpływu na proces ustalania prawa właściwego⁶; 2) mieszanego, publiczno-prywatnoprawnego charakteru przepisów RODO; 3) posłużenia się przez RODOowymi kryteriami (jednostka organizacyjna, nakierowanie działalności, monitorowanie zachowania osób) na potrzeby ustalania zakresu jego zastosowania, co skutkuje powstaniem pytania o zbieżność tych kryteriów z łącznikami (np. siedzibą naruszcyciela, miejscem naruszenia) stosowanymi w normach kolizyjnych dotyczących odpowiedzialności pozaumownej; 4) wprowadzenia w RODO przepisów z zakresu międzynarodowego postępowania cywilnego, w szczególności jurysdykcji krajowej, korzystnych dla osób dochodzących roszczeń względem administratorów danych oraz podmiotów przetwarzających dane na zlecenie administratorów danych, co w połączeniu z brakiem jednoznacznej regulacji kolizyjnoprawnej zwiększa ryzyko *forum shopping* (manipulacji prawem właściwym) przez osobę, której dane dotyczą (poszkodowanego); 5) wspomnianego braku ujednoczonych norm kolizyjnych dla zobowiązań z naruszeń prywatności, przy czym jeśli chodzi o państwa członkowskie UE, to zobowiązania dotyczące ochrony prywatności zostały wyraźnie wyłączone spod zakresu zastosowania rozporządzenia Rzym II; oznacza to, że zależnie od organu rozpatrującego sprawę zastosowanie może znaleźć odmienne prawo właściwe (w zakresie kwestii nieuregulowanych wprost w RODO, np. wysokości odszkodowania za naruszenie prywatności)⁷; 6) potrzeby dokonania oceny, które z przepisów RODO mają charakter przepisów wymuszających swoje zastosowanie.

Nie ulega wątpliwości, że problematyka prawa prywatnego międzynarodowego została bardzo zaniedbana w trakcie prac nad RODO⁸. Nacisk położono na doprecyzowanie eksterytorialnego zastosowania RODO (art. 3). Jedną z najbardziej charakterystycznych cech RODO jest daleko posunięta ekstraterytorialność regulacji⁹. Rozwiązanie to jest uzasad-

⁶ P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Red. P. Litwiński. Warszawa 2018, s. 159–160; M. Górski, w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Red. M. Sankowska-Baryła. Warszawa 2018, s. 62–64.

⁷ C. Nagy: *The Word Is a Dangerous Weapon: Jurisdiction, Applicable Law and Personality Rights in EU Law — Missed and New Opportunities*. „Journal of Private International Law” 2012, vol. 2, s. 251–296.

⁸ M. Czepelak: *Would We Like to Have a European Code of Private International Law?* „European Review of Private Law” 2010, s. 705 i n.

⁹ Por. P. De Hert, V. Papakonstantinou: *The Council of Europe Data Protection Convention reform. Analysis of the new text and critical comment on its global ambition*. „Computer Law & Security Review” 2014, vol. 30, s. 637 i n.

nione, gdyby bowiem UE nie rozszerzyła ochrony danych na działalność podmiotów zagranicznych (w szczególności z USA, ale także z Chin czy Rosji), nie zapewniłaby skutecznej ochrony swoich obywateli. Eksterytorialne stosowanie RODO (do czego zmierzają państwa trzecie w swoich analogicznych regulacjach¹⁰) utrudnia działalność działających globalnie przedsiębiorców¹¹ i ogranicza prowadzenie handlu międzynarodowego¹². Pojawia się więc pytanie, czy rozwiązania te pozostają w zgodzie z neutralnym charakterem norm kolizyjnych prawa prywatnego międzynarodowego, których zasadniczym celem nie jest uprzywilejowanie żadnej ze stron stosunku prawnego.

Powstaje jednak pytanie, czy eksterytorialność RODO jest fenomenem z omawianej perspektywy prawa prywatnego międzynarodowego. Prawo publiczne danego państwa niejednokrotnie obejmuje swym zakresem zastosowania działania na danym terytorium podejmowane przez podmioty zagraniczne. Przykładem są obowiązki podatkowe. W kolejnym punkcie postaram się uzasadnić tezę, że rozwiązania przyjęte w RODO mają szczególny charakter i wywierają wpływ na stosowanie przepisów prawa prywatnego międzynarodowego.

3. Eksterytorialność RODO a prawo prywatne międzynarodowe

Eksterytorialne stosowanie RODO nie skutkuje wyłączeniem stosowania dotychczasowych przepisów prawa prywatnego międzynarodowego. Okoliczność, że ustawodawca unijny starał się jak najbardziej precyzyjnie (wręcz kazuistycznie) określić zakres zastosowania RODO nie oznacza, że regulacja ta stanowi kompletny system prawny. Nie jest to regulacja pełna (wyczerpująca) i zastępująca krajowe systemy prawne w zakresie konsekwencji cywilnoprawnych naruszenia zasad ochrony

¹⁰ Przykładami są nowe przepisy przyjęte w Singapurze, Afryce Południowej, Filipinach i Malezji. Prowadzi to do odejścia od neutralności sieci.

¹¹ J. Hörnle: *The Jurisdictional Challenge of the Internet*. In *Law and the Internet*. Eds. L. Edwards, Ch. Waelde. Oxford 2008, s. 121 i n.

¹² Tak trafnie D. Svantesson w rozdziale E. 3 *Electronic Commerce*, in: *Encyclopedia of Private International Law*. Eds. J. Basedow, G. Rühl, F. Ferrari, P. de Miguel Asensio. Elgar 2017, s. 593—599; por. A. Themelis: *The Internet, Jurisdiction and EU Competition Law: The Concept of „Over-territoriality” in Addressing Jurisdictional Implications in the Online World*. „World Competition” 2012, vol. 2, s. 325—354.

danych osobowych. Dla rozstrzygnięcia danej kwestii konieczne będzie ustalenie statutu pomocniczego (prawa krajowego). Przykładem są zasady przyznania odszkodowania (zadośćuczynienia) osobie, której prawa i wolności zostały naruszone w związku z niedozwolonym przetwarzaniem jej danych osobowych. Jednak stosowanie norm kolizyjnych w odezwaniu od kryteriów zastosowania przyjętych w RODO będzie podważać międzynarodową skuteczność i ochronny charakter tej regulacji. Brak należytego wyjaśnienia relacji tych przepisów względem siebie będzie prowadzić do rozbieżności w orzecznictwie. Na przykład sądy jednego państwa będą stosować własne prawo, uzasadniając to przepisami RODO, a sądy innego państwa będą stosować własne prawo, uzasadniając to przepisami prawa prywatnego międzynarodowego.

Nie powinno ulegać wątpliwości, że podstawą ustalenia prawa właściwego nie są przepisy art. 82 ust. 6 RODO. Wskazano w nim, że postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym **na mocy prawa krajowego państwa członkowskiego**, o którym mowa w art. 79 ust. 2 RODO [podkr. M.Ś.]. Pomimo niejednoznacznego brzmienia, przepis ten nie stanowi normy kolizyjnej określającej prawo właściwe dla odszkodowania z tytułu sprzecznego z prawem przetwarzania danych osobowych, a jedynie rozszerza zakres norm jurysdykcyjnych z art. 79 ust. 2 (dotyczących środków prawnych) na powództwa dotyczące odszkodowania.

Regulacja RODO w zakresie cywilnoprawnych aspektów ochrony prywatności jest szcążkowa (przykładem jest art. 82 RODO, stanowiący bezpośrednią podstawę dochodzenia roszczeń deliktowych¹³). Oceniając sprawę z perspektywy polskich przepisów kolizyjnoprawnych, trzeba przyjąć, że przepisy RODO mają dominujący publicznoprawny charakter. Ich podstawowym celem jest nałożenie określonych obowiązków publicznoprawnych na administratora danych oraz podmiot przetwarzający dane na jego zlecenie (procesora). To właśnie dla skutecznej realizacji tego celu prawodawca unijny starał się jednoznacznie określić zasięg obowiązywania RODO¹⁴. Większość danych osobowych osób przebywających w UE jest przetwarzana poza UE, przy czym przepisy państw trzecich nie zapewniają ochrony zgodnej z RODO¹⁵.

¹³ Zob. szerzej P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie...*, s. 822–826.

¹⁴ P. Voigt, A. von dem Bussche: *The EU General Data Protection Regulation (GDPR). A Practical Guide*. Cham 2017, s. 22.

¹⁵ G. Haas: *La réglementation sur la protection des données personnelles*. St. Herblain 2018, s. 20.

4. Kryteria stosowania RODO a łączniki norm kolizyjnych

Z art. 3 RODO wynika, że w celu ustalenia zakresu obowiązywania RODO stosuje się trzy główne łączniki (kryteria)¹⁶: 1) istnienie na terenie UE jednostki organizacyjnej, 2) oferowanie towarów i usług na terenie UE osobom przebywającym na tym terenie, 3) monitorowanie ich zachowania. Kryteria te służą także określeniu zakresu obowiązywania przepisów prawa krajowego uzupełniających RODO¹⁷, w tym polskiej ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. Dla prawidłowej wykładni powyższych kryteriów przydatne jest dotychczasowe orzecznictwo TSUE dotyczące ochrony osób fizycznych, których dane są przetwarzane¹⁸.

Nie bez przyczyny pierwszym wymienionym w RODO kryterium jest elastyczne¹⁹ kryterium miejsca położenia jednostki organizacyjnej podmiotu przetwarzającego dane osobowe²⁰. Należy je rozumieć szerzej niż dotychczasowe kryterium siedziby²¹. W istocie RODO nawiązuje tym nowym (w polskiej wersji językowej) pojęciem do elastycznej wykładni siedziby przyjmowanej w prawie prywatnym międzynarodowym. Jego interpretacja sprawia jednak duże problemy²². Wątpliwości wzbudza samo posłużenie się pojęciem „jednostka organizacyjna”. RODO nie zawiera jego definicji. W motywie 22 preambuły wskazano jedynie, że przetwarzanie danych osobowych w kontekście działalności prowadzonej przez jednostkę

¹⁶ Por. P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie...*, s. 153—154, 159—160; M. Gömann: *The new territorial scope of EU data protection law: deconstructing a revolutionary achievement*. „Common Market Law Review” 2017, vol. 54 (2), s. 567—690.

¹⁷ Por. P. Schantz: *Beck'scher Online-Kommentar Datenschutzrecht*. Hrsg. H. Wolff, S. Brink. Munich 2017, art. 3.

¹⁸ M. Czerniawski: *Zakres terytorialny a pojęcie „jednostki organizacyjnej” w przepisach ogólnego rozporządzenia o ochronie danych — zarys problemu: Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*. Red. G. Sibiga. Warszawa 2016, s. 22—23.

¹⁹ P. Voigt, A. von dem Bussche: *The EU...*, s. 22.

²⁰ Co podkreślano od początku na etapie projektowania rozporządzenia — P. De Hert, V. Papakonstantinou: *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*. „Computer Law & Security Review” 2012, vol. 28, s. 130—142.

²¹ D. Svantesson: *Article 4(1)(A) ‘Establishment of the Controller’ in EU Data Privacy Law — Time to Rein in this Expanding Concept?* „International Data Privacy Law” 2016, vol. 6 (3), s. 210.

²² P. De Hert, M. Czerniawski: *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*. „International Data Protection Law” 2016, vol. 6 (3), s. 230.

organizacyjną administratora lub podmiotu przetwarzającego w UE powinno odbywać się zgodnie z RODO, niezależnie od tego, czy samo przetwarzanie danych ma miejsce w UE. Dodatkowo stwierdzono, że pojęcie „jednostka organizacyjna” zakłada skuteczne i faktyczne prowadzenie działalności przez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział, czy spółkę zależną posiadającą osobowość prawną, nie jest w tym względzie czynnikiem decydującym²³.

Przy interpretacji pojęcia jednostki organizacyjnej pomocne jest orzecznictwo TSUE, w szczególności wyroki w sprawach C-131/12, Google Spain²⁴ i C-230/14, Weltimmo, które mimo że wydane zostały na podstawie przepisów dyrektywy 95/46/WE, nadal zachowują aktualność²⁵. Dotyczą one zakresu terytorialnego stosowania przepisów dyrektywy 95/46/WE oraz implementujących ją przepisów krajowych państw członkowskich UE. W pierwszej sprawie Trybunał uznał, że art. 4 ust. 1 lit. a dyrektywy 95/46/WE należy interpretować w ten sposób, że przetwarzanie danych osobowych ma miejsce w ramach działalności gospodarczej prowadzonej przez administratora danych, odpowiedzialnego za to przetwarzanie na terytorium danego państwa członkowskiego w rozumieniu tego przepisu, jeśli operator wyszukiwarki internetowej ustanawia w danym państwie członkowskim oddział lub spółkę zależną, których celem jest promocja i sprzedaż powierzchni reklamowych oferowanych za pośrednictwem tej wyszukiwarki, a działalność tego oddziału lub spółki zależnej jest skierowana do osób zamieszkujących to państwo. Powyższa działalność powinna być uznana za spełniającą kryterium prowadzenia jednostki organizacyjnej na potrzeby art. 3 RODO. Jak widać, przyjęta interpretacja tego pojęcia jest zbieżna z rozumieniem pojęcia siedziby w znaczeniu funkcjonalnym, jakie stosujemy na potrzeby prawa prywatnego międzynarodowego.

Z kolei w sprawie C-230/14 Weltimmo spółka prawa słowackiego twierdziła, że prowadzi działalność gospodarczą wyłącznie na terenie Słowacji, tj. w państwie członkowskim, w którym posiada siedzibę rejestrową.

²³ Por. P. Voigt, A. von dem Bussche: *The EU...*, s. 23.

²⁴ B. Van Alsenoy, M. Koekoek: *Internet and Jurisdiction after Google Spain: the extraterritorial reach of the „right to be delisted”*. „International Data Protection Law” 2015, vol. 5 (2), s. 105—120; zob. także dokumenty grupy roboczej art. 29 dyrektywy, tj. Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on „Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12’ (WP 225); Article 29 Working Party, ‘Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain’ (WP 179 update).

²⁵ D. Svantesson: *The CJEU’S Weltimmo Data Privacy Ruling — Lost in the Data Privacy Turmoil, Yet So Very Important*. „Maastricht Journal of European and Comparative Law” 2016, vol. 23 (2), s. 332.

Węgierski organ nadzorczy na podstawie art. 4 ust. 1 lit. a dyrektywy 95/46/WE uznał swoją właściwość względem tej spółki, argumentując, że działalność Weltimmo, operatora strony internetowej z ogłoszeniami, koncentrowała się na terytorium Węgier. TSUE wyjaśnił, że z przepisów dyrektywy 95/46/WE wyłania się: „elastyczna koncepcja pojęcia prowadzenia działalności gospodarczej, odbiegająca od podejścia formalistycznego, zgodnie z którym przedsiębiorstwo prowadzi działalność gospodarczą wyłącznie w miejscu, w którym jest zarejestrowane. Tym samym w celu ustalenia, czy dana spółka będąca administratorem danych prowadzi działalność gospodarczą w rozumieniu dyrektywy 95/46/WE w innym państwie członkowskim niż państwo członkowskie lub trzecie, w którym jest zarejestrowana, należy ocenić stopień stabilności rozwiązania organizacyjnego, jak również faktyczny charakter prowadzenia działalności w tym drugim państwie członkowskim, z uwzględnieniem szczególnego charakteru rozpatrywanej działalności gospodarczej oraz świadczenia rozpatrywanych usług. Dotyczy to w szczególności przedsiębiorstw, które zajmują się oferowaniem usług wyłącznie za pośrednictwem internetu”. TSUE przyjął szerokie rozumienie pojęcia „prowadzenie działalności gospodarczej”, zakładając, że: „obecność pojedynczego przedstawiciela może w pewnych okolicznościach wystarczyć, aby istniało stabilne rozwiązanie organizacyjne, jeżeli działa on z wystarczającym stopniem stabilności, przy pomocy niezbędnych środków do świadczenia konkretnych rozpatrywanych usług, w danym państwie członkowskim”.

Z orzecznictwa TSUE wynika zatem, że prowadzeniem działalności w sposób efektywny i rzeczywisty przez stabilne struktury jest nawet posiadanie przedstawicielstwa w postaci kilku osób reprezentujących spółkę na terenie danego państwa, które kontaktuje się z klientami na obszarze tego państwa w sprawie usług, które świadczone są przez spółkę już z terytorium innego państwa.

Nawet jeśli podmiot przetwarzający dane nie ma w UE jednostki organizacyjnej (w tak szerokim rozumieniu, jak przedstawione powyżej), to będzie musiał stosować przepisy RODO, o ile oferuje towary i usługi na terenie UE osobom znajdującym się w UE²⁶. Kwestii tej dotyczy drugie z kryteriów przewidziane w art. 3 RODO.

Zgodnie z art. 3 ust. 2 lit a oraz motywem 23 preambuły RODO, aby osoby fizyczne nie zostały pozbawione ochrony przysługującej im na mocy tego rozporządzenia, przetwarzanie danych osobowych osób, których dane dotyczą, znajdujących się w UE, przez administratora lub podmiot przetwarzający, którzy nie posiadają jednostki organizacyjnej

²⁶ Por. C. Raul: *The Privacy, Data Protection and Cybersecurity Law Review*. Eds. A. Raul. London 2015, s. 12.

w Unii, powinno podlegać RODO, jeżeli czynności przetwarzania wiążą się z oferowaniem takim osobom towarów lub usług, niezależnie od tego, czy pociąga to za sobą płatność.

Aby stwierdzić, czy administrator lub podmiot przetwarzający oferują towary lub usługi znajdującym się w Unii osobom, których dane dotyczą, należy ustalić, czy jest oczywiste, że administrator lub podmiot przetwarzający planują oferować usługi osobom, których dane dotyczą, w co najmniej jednym państwie członkowskim UE²⁷. Do ustalenia takiego zamiaru nie wystarczy sama dostępność w UE strony internetowej administratora, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub innych danych kontaktowych ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym jednostkę organizacyjną ma administrator²⁸. Jednak znaczenie mają czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach, lub użytkownikach znajdujących się w Unii²⁹.

Jak się wydaje, art. 3 ust. 2 lit. a RODO odwołuje się do kryterium prostego pobytu osób, którym oferowane są towary lub usługi (zatem nie jest wymagane posiadanie polskiego obywatelstwa czy też miejsca zamieszkania w Polsce). Miejsce pobytu prostego (lub po prostu pobytu) oznacza miejsce każdego, nawet przemijającego, chwilowego przebywania (wypoczynek, wizyta itp.). W przypadku pobytu prostego osoba fizyczna nie ma zamiaru stałego przebywania w danym miejscu. Dla prostego pobytu charakterystyczny jest fakt mniejszej trwałości przebywania w danym miejscu — wystarczająca jest nawet krótka obecność. Nie ma znaczenia ani stały charakter faktycznego przebywania w danym miejscu, ani zamiar pobytu.

Przetwarzanie danych osobowych osób znajdujących się w UE przez administratora lub podmiot przetwarzający, którzy nie mają jednostki organizacyjnej w Unii, podlega RODO także w przypadkach, gdy wiąże się z monitorowaniem zachowania takich osób, o ile zachowanie to ma miejsce na terytorium Unii. Jest to trzecie kryterium z art. 3 RODO. Aby stwierdzić, czy czynność przetwarzania można uznać za „monitorowanie zachowania” osób, należy ustalić, czy aktywności osób fizycznych są obserwowane w jakikolwiek sposób (np. aktywność w Internecie śledzona za pomocą plików cookies lub informacji przekazywanych przez wyszukiwarki internetowe, fizyczne ruchy śledzone za pomocą danych

²⁷ F. Lecomte: *Nouvelle donne pour les données. Le RGDP*. Paris 2018, s. 24–25.

²⁸ G. Haas: *La réglementation...*, s. 18–20.

²⁹ Por. P. Voigt, A. von dem Bussche: *The EU...*, s. 26.

przekazywanych przez telefony komórkowe)³⁰. Należy podkreślić, że kryterium to będzie spełnione niezależnie od tego, czy w odniesieniu do tak zebranych danych później stosowane będą techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania, lub prognozowania jej osobistych preferencji, zachowań i postaw³¹.

Ze względu na trudności interpretacyjne pod koniec 2019 r. Europejska Rada Ochrony Danych (EROD) opublikowała wytyczne w sprawie terytorialnego zakresu stosowania RODO³². Nie ma tu miejsca na szczegółowe omówienie wytycznych, warto jednak zwrócić uwagę na kilka spostrzeżeń, mogących mieć znaczenie również w przypadku stosowania norm kolizyjnych prawa prywatnego międzynarodowego.

Po pierwsze, w ocenie EROD posiadanie strony internetowej dostępnej w UE samo w sobie nie wystarcza do stwierdzenia istnienia „jednostki organizacyjnej” na terenie UE.

Po drugie, aby określić, czy kryterium „ukierunkowania” działalności, o którym mowa w RODO, jest spełnione, w wytycznych przedstawiono różne czynniki, które zostały przyjęte na podstawie europejskiego prawa ochrony konsumentów, i które w połączeniu z sobą mogą oznaczać ukierunkowanie na podmioty danych w UE. Obejmują one m.in.: a) zapłatę dysponentowi wyszukiwarki w celu zapewnienia usługi odsyłania dla ułatwienia konsumentom w UE dostępu do strony internetowej lub uruchomienie kampanii marketingowych i reklamowych skierowanych do danego kraju UE; b) międzynarodowy charakter działalności; c) używanie języka/waluty innego niż powszechnie stosowany w kraju przedsiębiorcy, zwłaszcza języka/waluty jednego lub kilku państw członkowskich UE, a także d) oferowanie dostawy towarów w państwach członkowskich UE.

Po trzecie, w ocenie EROD oferta usług obejmuje również oferowanie „usług społeczeństwa informacyjnego”, które są zdefiniowane jako „wszelkie usługi społeczeństwa informacyjnego, to znaczy wszelkie usługi normalnie świadczone za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług”. Obejmują one m.in. strony internetowe, aplikacje i inne usługi online.

³⁰ Por. D. Svantesson: *Extraterritoriality in Data Privacy Law*. Kopenhaga 2013, s. 226; P. Cadot, T. Livenais: *Photographie du champ territorial du règlement données personnelles: de nouveaux opérateurs concernés?* In: Le RGDP. Eds. S. Prévost, E. Royer. Paris 2018, s. 33–35.

³¹ P. Voigt, A. von dem Bussche: *The EU...*, s. 27.

³² https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en [Dostęp: 26.03.2020 r.].

Po czwarte, w wytycznych stwierdza się, że chociaż w motywach do RODO wspomina się o monitorowaniu w odniesieniu do śledzenia zachowań w Internecie, śledzenie za pomocą innych technologii lub sieci związanych z przetwarzaniem danych osobowych powinno być również brane pod uwagę przy podejmowaniu decyzji, czy przetwarzanie jest równoznaczne z „monitorowaniem zachowań”, i wymienia się przykłady, takie jak urządzenia noszone i inteligentne. Z tych też względów w wytycznych podano kilka przykładów działań, które stanowią „monitoring” dla tych celów, w tym: a) reklamę behawioralną; b) geolokalizację, w szczególności dla celów marketingowych; c) śledzenie online z wykorzystaniem plików cookies lub innych technik śledzenia (np. pobierania odcisków palców); d) spersonalizowane usługi w zakresie analizy diety i zdrowia online; e) telewizję przemysłową; f) badania rynku i inne badania behawioralne oparte na indywidualnych profilach, a także g) monitorowanie lub regularne składanie sprawozdań na temat statusu poszczególnych profili oraz zdrowie jednostki.

Jak widać, wraz z postępem technologicznym pogłębieniu ulega interpretacja kryteriów służących do ustalenia, w jakich międzynarodowych sytuacjach RODO znajduje zastosowanie, co faktycznie musi wpływać na proces ustalenia prawa właściwego w przypadku naruszenia reżimu ochronnego RODO. Mam tu na myśli nie tylko lokalizację samego naruszciciela (ustalenie siedziby czy jego jednostki organizacyjnej), lecz także „lokalizację” jego działalności skutkującej naruszeniem RODO i pociągającej za sobą odpowiedzialność deliktową sprawcy naruszenia. Istnieje potrzeba jednolitego wykorzystania powyższych wskazówek, zarówno na potrzeby ustalenia zakresu zastosowania RODO, jak i cywilnoprawnych konsekwencji naruszenia przyjętych w nim zasad ochrony danych. Wymienione okoliczności dodatkowo uzasadniają sięgnięcie do ujednoliconych przepisów kolizyjnych rozporządzenia Rzym II i przyjmowania wykładni stosowanych w nim łączników w duchu kryteriów przyjętych w art. 3 RODO.

5. Prawo właściwe dla zobowiązań deliktowych z naruszenia zasad ochrony danych przyjętych w RODO

Wiarygodne ustalenie prawa właściwego dla odpowiedzialności pozaumownej z tytułu naruszenia zasad ochrony danych, w szczególności w przypadku komunikacji elektronicznej, staje się zadaniem karkołom-

nym³³. Sądom krajowym zbyt łatwo jest przyjąć właściwość własnego prawa (obowiązującego w ich siedzibie) na podstawie zasadniczo dowolnych kryteriów. Podstawowy problem polega na wyłączeniu z zakresu rozporządzenia Rzym II określającego prawo właściwe dla zobowiązań pozaumownych „zobowiązań pozaumownych wynikających z naruszenia prawa do prywatności i innych dóbr osobistych, w tym zniesławienia” (art. 1 ust. 2 pkt g). Skutkuje to powstaniem istotnej luki w międzynarodowym systemie ochronnym RODO³⁴. Sądy krajowe powinny sięgać do odmiennie regulujących kwestie ochrony prywatności krajowych regulacji prawa prywatnego międzynarodowego.

Niezależnie od powyższego, trudności zwiększa możliwość powołania się przez podmioty przetwarzające dane w ramach świadczenia usług drogą elektroniczną na unijne przepisy o handlu elektronicznym³⁵. Dotyczy to m.in. zasady państwa pochodzenia wynikającej z art. 3 dyrektywy o handlu elektronicznym³⁶. W wyroku z dnia 25 października 2010 r. w sprawach połączonych C-509/09 i C-161/10 eDate Advertising GmbH przeciwko X, Olivier Martinez, Robert Martinez przeciwko MGN Limited (2011), dotyczącym naruszenia prywatności, TSUE orzekł, że w świetle art. 3 dyrektywy o handlu elektronicznym państwa członkowskie UE muszą zapewnić, że „dostawca usługi handlu elektronicznego nie podlega bardziej rygorystycznym wymogom niż wymogi przewidziane w prawie materialnym mającym zastosowanie w państwie członkowskim, w którym usługodawca ma siedzibę”³⁷. Powstaje zatem pytanie, czy zasada państwa pochodzenia może stanowić przeszkodę dla zastosowania bardziej restrykcyjnej interpretacji RODO (np. przyjmowanej przez francuskie organy) wobec usługodawcy internetowego mającego siedzibę (jednostkę organizacyjną) w państwie, które, dla przyjęcia odpowiedzialności podmiotu przetwarzającego dane osobowe, przewiduje

³³ P. Litwiński, P. Barta, M. Kawecki, w: *Rozporządzenie...*, s. 811.

³⁴ Por. A. Całus: *Znaczenie rozporządzenia Rzym II dla unifikacji prawa właściwego dla czynów niedozwolonych w państwach członkowskich Unii Europejskiej*. W: *Czyny niedozwolone w prawie polskim i w prawie porównawczym*. Red. M. Nesterowicz. Warszawa 2012.

³⁵ S. Francq: *Responsabilité du fournisseur d'information sur Internet: affaires eDate Advertising et Martinez*. „La Semaine Juridique — édition generale” 2012, n° 1—2, s. 35—38.

³⁶ Dyrektywa 2000/31 z dnia 8 czerwca 2000 r. o niektórych aspektach prawnych usług społeczeństwa informacyjnego, a w szczególności handlu elektronicznego. Dz.Urz. UE L 178, 17.07.2000.

³⁷ O znaczeniu wyroku zob. S. Bollée, B. Haftel: *Les nouveaux (dés)équilibres de la compétence internationale en matière de cyberdélits après l'arrêt eDate Advertising et Martinez*. „Recueil Dalloz” 2012, s. 1285 i n.; M. Bogdan: *Defamation on the Internet, Forum Delicti and the E-Commerce Directive: Some Comments on the ECJ Judgment in the eDate Case*. „Yearbook of Private International Law” 2011, vol. 13, s. 483—491.

znacznie wyższe wymogi. Uważam, że prawo właściwe wyznaczone przez odpowiednią normę kolizyjną powinno w tym przypadku ustąpić zasadzie państwa pochodzenia. Oznacza to, że stosowanie prawa właściwego musi zostać skorygowane lub tak dostosowane, aby zapobiec utrudnieniom swobody świadczenia usług elektronicznych w Unii Europejskiej. Wątku tego w tym miejscu jednak nie poszerzam, ponieważ dotyczy etapu rozstrzygnięcia sporu już po ustaleniu prawa właściwego.

Uprowadzając dalsze rozważania, uważam za kluczowe, aby organ orzekający w sprawie — niezależnie od tego, którego państwa członkowskiego jest to organ — stosował to samo prawo do oceny roszczeń osoby podmiotu danych³⁸. Przyjęty mechanizm kolizyjny chroniący prywatność powinien zapewniać równowagę stron. Należy unikać rozwiązań, które chronią nadmiernie tylko jedną z nich³⁹. Przykładem wadliwego, moim zdaniem, rozwiązania będzie przyjęcie właściwości prawa państwa, w którym znajduje się miejsce zwykłego pobytu poszkodowanego. Choć jest to rozwiązanie proste do zastosowania, jednak nasuwa zastrzeżenia co do jego neutralności oraz racjonalności w przypadku naruszenia reżimu ochronnego danych osobowych.

Według art. 16 ust. 1 polskiej ustawy o prawie prywatnym międzynarodowym z 2011 r., dobra osobiste osoby fizycznej podlegają jej prawu ojczystemu. Prawo to wyznacza katalog dóbr osobistych i towarzyszących im praw podmiotowych, decyduje o ich powstaniu, treści, zasięgu i ustaniu. Prawo właściwe dla ochrony dóbr osobistych należy natomiast odszukać, stosując przepisy art. 16 ust. 2 i 3. Zgodnie z art. 16 ust. 2, osoba fizyczna, której dobro osobiste jest zagrożone naruszeniem lub zostało naruszone, może żądać ochrony na podstawie prawa państwa, na którego terytorium nastąpiło zdarzenie powodujące to zagrożenie naruszenia lub naruszenie, albo prawa państwa, na którego terytorium wystąpiły skutki tego naruszenia. Mamy więc do czynienia ze wskazaniem opcyjnym⁴⁰. Jeżeli zakwalifikujemy naruszenie zasad RODO do kategorii naruszeń dóbr osobistych (prywatności), osoba, której dane dotyczą, może dokonać takiego wskazania, co zwiększa ryzyko manipulacji prawem właściwym.

³⁸ Por. wyroki Trybunału Sprawiedliwości Unii Europejskiej: z dnia 30 listopada 1976 r. w sprawie 21/76, *Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA*, z dnia 7 marca 1995 r. w sprawie C-68/93, *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA*, oraz z dnia 25 listopada 2011 r. w sprawach połączonych C509/09 *eDate Advertising GmbH v X i C161/10 Olivier Martinez, Robert Martinez v MGN Limited*.

³⁹ O. Feraci: *La legge applicabile alla tutela dei diritti della personalità nella prospettiva comunitaria*. „Rivista di diritto internazionale” 2009, n° 4, s. 1020—1085.

⁴⁰ Por. J. Balcarczyk: *Wybrane problemy związane z projektem ustawy — Prawo prywatne międzynarodowe*. „Rejent” 2009, nr 7—8, s. 140.

Nie jest jednak oczywiste, czy powyższe przepisy znajdują — bądź też czy powinny znaleźć — zastosowanie w przypadku naruszeń reżimu ochronnego RODO. Zanim zastosujemy omawiane przepisy, należy dokonać kwalifikacji kolizyjnoprawnej naruszeń RODO. Jak wiadomo, RODO ma charakter odrębny w stosunku do przepisów chroniących dobra osobiste⁴¹. Podkreśla to fakt utworzenia oddzielnych podstaw dochodzenia roszczeń przez osoby, których dane są przetwarzane, zarówno w treści RODO, jak i w ramach nowej polskiej ustawy o ochronie danych osobowych z 2018 r.⁴² Powstaje więc pytanie, czy w celu odszukania prawa właściwego możemy sięgnąć do modelu kolizyjnoprawnego przyjętego w rozporządzeniu Rzym II⁴³, niejako ignorując przewidziane w nim wyłączenie dotyczące ochrony prywatności (wprowadzone na długo przed przyjęciem RODO). Zdaję sobie sprawę, że stanowisko przewidujące, zgodnie z którym, wyłączenie zawarte w rozporządzeniu Rzym II nie dotyczy naruszeń nowego reżimu ochrony danych osobowych stworzonego przez RODO, może zostać uznane za kontrowersyjne. Ma jednak istot-

⁴¹ Por. J. Braciak: *Prawo do prywatności*. Warszawa 2004, s. 92.

⁴² Dz.U. 2018, poz. 1000, t.j. Dz.U. 2019, poz. 1781.

⁴³ Rozporządzeniu Rzym II poświęcono obszerną literaturę. Przeważa w niej krytyczna ocena dotycząca wyłączenia z jego zakresu deliktów dotyczących prywatności. Zob. w szczególności A. Dickinson: *The Rome II Regulation*. Oxford 2009; R. Plender, M. Wilderspin: *European Private International Law of Obligation*. London 2009; J. Ahern, W. Binchy: *Rome II Regulation on Law Applicable to Non-Contractual Obligations*, 2009; J. Fawcett, J.M. Carruthers, G. Cheshire, P. North: *Private International Law*. Oxford 2008; *Rome Regulations: Commentary on the European Rules of the Conflict of law. Part Two*. Ed. G. Calliess. Wolters Kluwer 2011, s. 358—654; *Rome II Regulation*. Hrsg. P. Huber. Munich 2011; A. Rushworth, A. Scott: *Rome II: Choice of law for non-contractual obligations*. „Lloyd’s Maritime and Commercial Law Quarterly” 2008, s. 274—306; T. Hartley: *Choice of Law for Non-Contractual Liability: Selected Problems under the Rome II Regulation*. „International & Comparative Law Quarterly” 2008, vol. 57, s. 899—908; C. Briere: *Le reglement (CE) no 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II)*. „Journal de droit international” 2008, vol. 135, s. 31; S. Leible, M. Lechmann: *Die neue EG-Verordnung über aufervertragliche Schuldverhältnisse anzuwendende Recht (Rom II)*. „Recht der Internationalen Wirtschaft” 2007, vol. 53, s. 721; T. Graziano: *Das auf aufervertragliche Schuldverhältnisse anzuwendende Recht nach Inkrafttreten der Rom II — Verordnung*. „Rebels Zeitschrift für ausländisches und internationales Privatrecht” 2009, Nr. 73, s. 1—177; T. Dornis: *When in Rome, do as the Romans do? — a defense of the lex domicilii communis: in the Rome II Regulation*. „European Legal Forum” 2007, vol. 4, s. 152—159; S. Symeonides: *Rome II and Tort Conflicts: A Missed Opportunity*. „American Journal of Comparative Law” 2008, vol. 56, s. 173—222; P. Kozyris: *Rome II: Tort Conflicts on the Right Track! A Postscript to Symeon Symeonides’ Missed Opportunity*. „American Journal of Comparative Law” 2008, vol. 56, s. 471—497; M. Carruthers, E. Crawford: *Variations on a theme of Rome II. Reflections on proposed choice of law rules for non-contractual obligations: Part I*. „Edinburgh Law Review” 2005, vol. 9, s. 65—97; *Part II*. „Edinburgh Law Review” 2005, vol. 9, s. 238—266.

ne zalety, co wynika z przyjętej w rozporządzeniu Rzym II nowoczesnej, zbalansowanej oraz elastycznej regulacji ustalania prawa właściwego. Kluczowym argumentem jest możliwość zbieżnej interpretacji kryteriów przyjętych dla zastosowania RODO (art. 3) oraz ogólnych łączników norm kolizyjnych rozporządzenia Rzym II, co ma zasadnicze znaczenie w przypadku naruszeń dokonywanych przy wykorzystaniu nowych technologii przetwarzania danych.

6. Rekomendacja i wnioski

Podstawową regułą kolizyjną, według rozporządzenia Rzym II, jest zasada właściwości prawa państwa, w którym szkodę poniesiono, niezależnie od tego, w jakim państwie miało miejsce zdarzenie wyrządzające szkodę, ani w jakim państwie lub państwach wystąpiły pośrednie skutki tego zdarzenia (art. 4 ust. 1). Zastosowanie tej reguły w odniesieniu do naruszeń RODO nie powinno budzić większych wątpliwości. Ponadto, rozporządzenie Rzym II zawiera reguły dodatkowe oraz uzupełniające. Warto zatem przypomnieć, jak na podstawie rozporządzenia Rzym II powinien wyglądać proces wyboru właściwej normy kolizyjnej.

W pierwszej kolejności sąd powinien sprawdzić, czy strony dokonały ważnego, tj. spełniającego przesłanki art. 14 Rzym II, wyboru prawa właściwego. Również to rozwiązanie ma zalety w przypadku zobowiązania z naruszenia zasad ochrony danych osobowych. Uwzględnia autonomię woli stron. W braku ważnego wyboru prawa należy sprawdzić, czy istnieją przesłanki do zastosowania reguł dotyczących ujętych odrębnie typów czynów niedozwolonych (art. 5–9 Rzym II). Jeśli odpowiedź jest negatywna, a tak jest w przypadku naruszenia zasad ochrony danych osobowych, zasadne staje się sięgnięcie do norm ogólnych z art. 4 Rzym II, począwszy od normy z ust. 2 (właściwość wspólnego prawa personalnego stron, co *notabene* będzie rozwiązaniem spójnym z przepisami jurysdykcyjnymi wynikającymi z art. 79 i n. RODO). Dopiero gdy brak jest wspólnego prawa personalnego, należy skorzystać z podstawowej normy z art. 4 ust. 1, przewidującej właściwość prawa państwa, w którym powstała bezpośrednia szkoda. W obu powyższych sytuacjach celowe jest ustalenie przez sąd, czy istnieje możliwość korekty wskazania prawa na podstawie art. 4 ust. 3 Rzym II. Widzimy tu spójny model ustalania prawa właściwego i brak zasadniczych przeszkód, aby znalazł zastosowanie w przypadku naruszenia przepisów RODO.

Uważam ponadto, że zasady ustalania prawa właściwego przewidziane w rozporządzeniu Rzym II można, w miarę możliwości, interpretować z uwzględnieniem wykładni dokonanej na potrzeby przepisów RODO (art. 3, ale także art. 79 i n.). Wykładnia powinna bowiem być do pewnego stopnia zbieżna, ponieważ wszystkie te instrumenty prawne mają za zadanie zapewnienie przewidywalności rozstrzygnięć sądowych. Powyższe nie oznacza jednak możliwości dokonywania interpretacji pojęcia miejsca szkody wynikającej z naruszenia zasad ochrony danych osobowych przyjętych w RODO w sposób rozszerzający, tak aby obejmowało wszystkie miejsca, w których mogą być doznawane ujemne skutki zdarzenia, które już spowodowało szkodę rzeczywiście powstałą w innym miejscu⁴⁴.

Warto mieć na uwadze, że wprowadzenie do art. 4 ust. 1 Rzym II łącznika miejsca szkody, zamiast bardziej ogólnie sformułowanego łącznika miejsca deliktu, uwzględnia przypadek wielomiejscowości stanu faktycznego naruszenia⁴⁵. W rozporządzeniu Rzym II przyjęto, że decydujące znaczenie ma lokalizacja szkody rozumianej jako miejsce bezpośredniego naruszenia dobra prawnego poszkodowanego, ponieważ to w nim realizuje się zdarzenie decydujące o powstaniu odpowiedzialności. Bez znaczenia jest natomiast miejsce, w którym poszkodowany poniósł szkodę następczą, wynikającą ze szkody pierwotnej, powstałej w innym państwie. W motywie 17 preambuły rozporządzenia Rzym II przedstawiono ogólną wskazówkę co do sposobu rozumienia wyrażenia „szkoda bezpośrednia”. Wskazano tam, że: „państwem, w którym powstaje szkoda, powinno być państwo, w którym [...] została poniesiona szkoda na osobie lub szkoda na mieniu”.

Stosowanie łącznika bezpośredniej szkody stanowi kompromis pomiędzy przyznaniem właściwości prawu państwa, w którym znajduje się miejsce czynu niedozwolonego, a upoważnieniem poszkodowanego do dokonania wyboru prawa państwa, w którym wystąpił czyn, albo prawa państwa, w którym wystąpiła szkoda⁴⁶. Przyjęte w rozporządzeniu Rzym II rozwiązanie skutkuje pewnym usztywnieniem wskazania prawa właściwego w porównaniu z ogólnym łącznikiem miejsca deliktu, który podlegał w praktyce elastycznej interpretacji, pozwalając na przyjęcie,

⁴⁴ Por. S. Marino: *Nuovi sviluppi in materia di illecito extracontrattuale on line*. „Rivista di diritto internazionale privato e processuale” 2012, n° 4, s. 879—896.

⁴⁵ O różnych wymiarach wielomiejscowości deliktu M. Sośniak: „*Lex loci delicti commissi*” w prawie międzynarodowym prywatnym. „Studia Cywilistyczne” [Kraków] 1963, T. 4, s. 148—149; Idem: *Zobowiązania nie wynikające z czynności prawnych w prawie prywatnym międzynarodowym*. Katowice 1971, s. 30—31; Idem: *Prawo prywatne międzynarodowe*. Katowice 1991, s. 143.

⁴⁶ Por. T. Pajor: *Nowe tendencje w części ogólnej prawa prywatnego międzynarodowego państw europejskich*. „Problemy Prawne Handlu Zagranicznego” 1995, T. 18, s. 68 i n.

zależnie od okoliczności danej sprawy, właściwości prawa miejsca czynu bądź prawa miejsca szkody (skutku czynu niedozwolonego)⁴⁷. Może to powodować trudności w przypadku naruszeń zasad ochronnych przyjętych w RODO. Dlatego warto mieć na uwadze, że usztywnienie to złączono ze względu na możliwość zastosowania reguły korekcyjnej z art. 4 ust. 3 rozporządzenia Rzym II, a więc sąd może na jej podstawie, w drodze wyjątku, zastosować prawo miejsca czynu (zdarzenia) sprawczego, np. działania administratora danych⁴⁸. Niestety, nadal przy poszukiwaniu i stosowaniu prawa właściwego dla zobowiązań pozaumownych sądy napotykały na trudności, stosując art. 4 ust. 3 rozporządzenia Rzym II. Problemy dotyczą konfrontacji dwóch kryteriów, które w przepisie tym się pojawiają: kryterium „znacznie silniejszego związku” czynu niedozwolonego z innym państwem niż państwo wskazane w art. 4 ust. 1 lub 2, użytego w art. 4 ust. 3 zd. 1, oraz kryterium „ściślego związku czynu niedozwolonego z wcześniejszą umową”, wskazanego w art. 4 ust. 3 zd. 2 rozporządzenia Rzym II. Trudności te mogą zostać ograniczone przy wykorzystaniu przyjętych w RODO rozwiązań dotyczących zarówno jego zakresu zastosowania (a więc mogących wpływać na interpretację kryterium „znacznie ściślejszego związku” z rozporządzenia Rzym II), jak i wcześniejszych umów dotyczących ochrony danych osobowych (por. np. art. 28 RODO dotyczący umów zawieranych pomiędzy administratorem a podmiotem przetwarzającym). Nietrafne będzie jednak powoływanie reguły korekcyjnej w celu zanegowania wyboru prawa dokonanego przez stronę bądź nieuzasadnione korygowanie wskazań reguł kolizyjnych ze względu na realizację danego celu materialnoprawnego (np. realizacji interesów państwa sądu). Niezbędne jest zachowanie powściągliwości w korzystaniu z korygującego działania reguły korekcyjnej.

Podsumowując, uważam za najbardziej racjonalne stosowanie przepisów kolizyjnoprawnych rozporządzenia Rzym II w celu ustalenia prawa właściwego dla odpowiedzialności deliktowej administratora danych

⁴⁷ Tendencją współczesnego prawa prywatnego międzynarodowego jest bowiem uelastycznienie i zróżnicowanie rozwiązań kolizyjnych. Por. T. Pajor: *Odpowiedzialność deliktowa w prawie prywatnym międzynarodowym*. Warszawa 1989, s. 5 i n.; M. Sośniak: *Zobowiązania...*, s. 49 i n.

⁴⁸ Zob. wyr. SN z dnia 5 lutego 2015 r., V CSK 164/14. Legalis. Na temat sposobów rozwiązywania problemu wielomiejscowości po stronie miejsca szkody — zob. szerzej M. Pazdan: *Prawo prywatne międzynarodowe*. Warszawa 2017, s. 247—274. Warto przypomnieć projekt normy kolizyjnej zaproponowanej przez M. Sośniaka: „W zakresie zobowiązań nie wynikających z czynności prawnych właściwe jest prawo państwa, gdzie zaistniał czynnik, który w przeważający sposób zadecydował o powstaniu zobowiązania, chyba że z okoliczności wynika powiązanie z prawem innego państwa”. M. Sośniak: *Uwagi do projektu polskiego prawa prywatnego międzynarodowego*. „Nowe Prawo” 1962, nr 7—8, s. 1019.

badź podmiotu przetwarzającego w przypadku naruszenia przez niego zasad ochrony danych osobowych przewidzianych w RODO. Powyższa teza jest dodatkowo uzasadniona rozwiązaniami przyjętymi w nowej polskiej ustawie o ochronie danych osobowych. Według ustawy, każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, będzie mogła żądać zaniechania tego działania, a także może żądać, aby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. W przepisach ustawy przesądzono, że dochodzenie omawianych roszczeń nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych. Ustawa, bez potrzeby definiowania dobra osobistego (danych osobowych), konstruuje bezpośrednią podstawę dochodzenia cywilnoprawnych roszczeń niemajątkowych w razie naruszenia praw przysługujących na podstawie przepisów o ochronie danych osobowych, co może mieć istotne znaczenie praktyczne dla prawidłowego przestrzegania zasad wprowadzanych przez RODO.

Bibliografia

- Ahern J., Binehy W.: *Rome II Regulation on Law Applicable to Non-Contractual Obligations*, 2009.
- Balcarczyk J.: *Wybrane problemy związane z projektem ustawy — Prawo prywatne międzynarodowe*. „Rejent” 2009, nr 7—8.
- Bogdan M.: *Defamation on the Internet, Forum Delicti and the E-Commerce Directive: Some Comments on the ECJ Judgment in the eDate Case*. „Yearbook of Private International Law” 2011, vol. 13.
- Bollée S., Haftel B.: *Les nouveaux (dés)équilibres de la compétence internationale en matière de cyberdélits après l'arrêt eDate Advertising et Martinez*. „Recueil Dalloz” 2012.
- Braciak J.: *Prawo do prywatności*. Warszawa 2004.
- Briere C.: *Le règlement (CE) no 864/2007 du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II)*. „Journal de droit international” 2008, vol. 135.
- Brkan M.: *Data Protection and Conflict-of-Laws: A Challenging Relationship*. „European Data Protection Law Review” 2016, vol. 2 (3).
- Cadio P., Livenais T.: *Photographie du champ territorial du règlement données personnelles: de nouveaux opérateurs concernées?* In: Le RGDP. Eds. S. Prévost, E. Royer. Paris 2018.
- Całus A.: *Znaczenie rozporządzenia Rzym II dla unifikacji prawa właściwego dla czynów niedozwolonych w państwach członkowskich Unii Europejskiej*.

- W: *Czyny niedozwolone w prawie polskim i w prawie porównawczym*. Red. M. Nesterowicz. Warszawa 2012.
- Carruthers M., Crawford E.: *Variations on a theme of Rome II. Reflections on proposed choice of law rules for non-contractual obligations: Part I—II*. „Edinburgh Law Review” 2005, vol. 9.
- Chen J.: *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation*. „International Data Privacy Law” 2016, vol. 6 (4).
- Czepelak M.: *Would We Like to Have a European Code of Private International Law?* „European Review of Private Law” 2010.
- Czerniawski M.: *Zakres terytorialny a pojęcie „jednostki organizacyjnej” w przepisach ogólnego rozporządzenia o ochronie danych — zarys problemu: Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*. Red. G. Sibiga. Warszawa 2016.
- De Hert P., Czerniawski M.: *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*. „International Data Protection Law” 2016, vol. 6 (3).
- De Hert P., Papakonstantinou V.: *The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*. „Computer Law & Security Review” 2014, vol. 30.
- De Hert P., Papakonstantinou V.: *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*. „Computer Law & Security Review” 2012, vol. 28.
- Dickinson A.: *The Rome II Regulation*. Oxford 2009.
- Dornis T.: *When in Rome, do as the Romans do? — a defense of the lex domicilii communis: in the Rome II Regulation*. „European Legal Forum” 2007, vol. 4.
- Fawcett J., Carruthers J.M., Cheshire G., North P.: *Private International Law*. Oxford 2008.
- Feraci O.: *La legge applicabile alla tutela dei diritti della personalità nella prospettiva comunitaria*. „Rivista di diritto internazionale” 2009, n° 4.
- Franco S.: *Responsabilité du fournisseur d'information sur Internet: affaires eDate Advertising et Martinez*. „La Semaine Juridique — édition generale” 2012, n° 1—2.
- Gömann M.: *The new territorial scope of EU data protection law: deconstructing a revolutionary achievement*. „Common Market Law Review” 2017, vol. 54 (2).
- Górski M., w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Red. M. Sakowska-Baryła. Warszawa 2018.
- Graziano T.: *Das auf aufservertragliche Schuldverhältnisse anzuwendende Recht nach Inkrafttreten der Rom II — Verordnung*. „Rabels Zeitschrift für ausländisches und internationales Privatrecht” 2009, Nr. 73.
- Haas G.: *La réglementation sur la protection des données personnelles*. St. Herblain 2018.

- Hartley T.: *Choice of Law for Non-Contractual Liability: Selected Problems under the Rome II Regulation*. „International & Comparative Law Quarterly” 2008, vol. 57.
- Hörnle J.: *The Jurisdictional Challenge of the Internet*. In *Law and the Internet*. Eds. L. Edwards, Ch. Waelde. Oxford 2008.
- Kozyris P.: *Rome II: Tort Conflicts on the Right Track! A Postscript to Symeon Symeonides' Missed Opportunity*. „American Journal of Comparative Law” 2008, vol. 56.
- Lecomte F.: *Nouvelle donne pour les données. Le RGDP*. Paris 2018.
- Leible S., Lechmann M.: *Die neue EG-Verordnung über aufervertragliche Schuldverhältnisse anzuwendende Recht (Rom II)*. „Recht der Internationalen Wirtschaft” 2007, vol. 53.
- Litwiński P., Barta P., Kawecki M., w: *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Red. P. Litwiński. Warszawa 2018.
- Marino S.: *Nuovi sviluppi in materia di illecito extracontrattuale on line*. „Rivista di diritto internazionale privato e processuale” 2012, n° 4.
- Nagy C.: *The Word Is a Dangerous Weapon: Jurisdiction, Applicable Law and Personality Rights in EU Law — Missed and New Opportunities*. „Journal of Private International Law” 2012, vol. 2.
- Nowicka A.: *Prawo właściwe dla zobowiązań wynikających z czynów niedozwolonych w świetle przepisów rozporządzenia nr 864/2007*. W: „Prace Instytutu Prawa Własności Intelektualnej UJ”. Z. 100: *Prawo własności intelektualnej wczoraj, dziś i jutro*. Red. J. Barta, A. Matlak. Kraków 2007.
- Pajor T.: *Nowe tendencje w części ogólnej prawa prywatnego międzynarodowego państw europejskich*. „Problemy Prawne Handlu Zagranicznego” 1995, T. 18.
- Pajor T.: *Odpowiedzialność deliktowa w prawie prywatnym międzynarodowym*. Warszawa 1989.
- Pazdan J.: *Rozporządzenie Rzym II — nowe wspólnotowe unormowanie właściwości prawa dla zobowiązań pozaumownych*. W: „Problemy Prawa Prywatnego Międzynarodowego”. T. 4. Red. M. Pazdan. Katowice.
- Pazdan M.: *Prawo prywatne międzynarodowe*. Warszawa 2017.
- Plender R., Wilderspin M.: *European Private International Law of Obligation*. London 2009.
- Raul C.: *The Privacy, Data Protection and Cybersecurity Law Review*. Eds. A. Raul. London 2015.
- Rome Regulations: Commentary on the European Rules of the Conflict of law. Part Two*. Ed. G. Calliess. Wolters Kluwer 2011.
- Rome II Regulation*. Hrsg. P. Huber. Munich 2011.
- Rushworth A., Scott A.: *Rome II: Choice of law for non-contractual obligations*. „Lloyd's Maritime and Commercial Law Quarterly” 2008.
- Schantz P.: *Beck'scher Online-Kommentar Datenschutzrecht*. Hrsg. H. Wolff, S. Brink. Munich 2017.

- Sośniak M.: „*Lex loci delicti commissi*” w prawie międzynarodowym prywatnym. „*Studia Cywilistyczne*” [Kraków] 1963, T. 4.
- Sośniak M.: *Prawo prywatne międzynarodowe*. Katowice 1991.
- Sośniak M.: *Uwagi do projektu polskiego prawa prywatnego międzynarodowego*. „*Nowe Prawo*” 1962, nr 7—8.
- Sośniak M.: *Zobowiązania nie wynikające z czynności prawnych w prawie prywatnym międzynarodowym*. Katowice 1971.
- Svantesson D.: *Article 4(1)(A) ‘Establishment of the Controller’ in EU Data Privacy Law — Time to Rein in this Expanding Concept?* „*International Data Privacy Law*” 2016, vol. 6 (3).
- Svantesson D.: *Electronic Commerce*. In: *Encyclopedia of Private International Law*. Eds. J. Basedow, G. Rühl, F. Ferrari, P. de Miguel Asensio. Elgar 2017.
- Svantesson D.: *Extraterritoriality in Data Privacy Law*. Kopenhaga 2013.
- Svantesson D.: *The CJEU’S Weltimmo Data Privacy Ruling — Lost in the Data Privacy Turmoil, Yet So Very Important*. „*Maastricht Journal of European and Comparative Law*” 2016, vol. 23 (2).
- Symeonides S.: *Rome II and Tort Conflicts: A Missed Opportunity*. „*American Journal of Comparative Law*” 2008, vol. 56.
- Themelis A.: *The Internet, Jurisdiction and EU Competition Law: The Concept of „Over-territoriality” in Addressing Jurisdictional Implications in the Online World*. „*World Competition*” 2012, vol. 2.
- Van Alsenoy B., Koekkoek M.: *Internet and Jurisdiction after Google Spain: the extraterritorial reach of the „right to be delisted”*. „*International Data Protection Law*” 2015, vol. 5 (2).
- Voigt P., von dem Bussche A.: *The EU General Data Protection Regulation (GDPR). A Practical Guide*. Cham 2017.