PME
3/2020

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

C·H·BECK

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

Contents

C·H·BECK

Szanowni Państwo,

z przyjemnością przedstawiam trzeci w 2020 r. numer kwartalnika naukowego Prawo Mediów Elektronicznych. Podobnie jak poprzednie numery, również ten został poświęcony zagadnieniem prawnym mającym związek z nowymi technologiami. Niezmiennie proponujemy współpracę i publikację artykułów, glos czy recenzji wszystkim tym autorom, którzy podejmują tematykę wpływu nowych technologii na prawo prywatne lub publiczne. Czasopismo ma charakter interdyscyplinarny i nie ogranicza się do jednej gałęzi prawa.

W bieżącym numerze znajdziecie Państwo opracowania poświęcone informatyzacji sektora opieki zdrowotnej. Zagadnienia te są niezwykle aktualne, a w Nr 3 szczegółowo zostały omówione kwestie dotyczące prawnych aspektów wykorzystania technologii *cloud computing* w sektorze opieki zdrowotnej, a także etycznych problemów wdrażania medycznego Internetu rzeczy. W dalszym ciągu niezwykle interesujące z zarówno praktycznego, jak i teoretycznego punktu widzenia pozostają zagadnienia dotyczące zasad ochrony danych osobowych. Z tego też względu proponujemy Państwu lekturę opracowania poświęconego umowom zawieranym w przedmiocie współadministrowania danymi osobowymi.

Z uwagi na to, że kwartalnik Prawo Mediów Elektronicznych cieszy się popularnością także wśród zagranicznych autorów, również w tym numerze znajdziemy publikację międzynarodową poświęconą najczęstszym podstawom prawnym przetwarzania danych osobowych w kontekście działań lokalnych władz publicznych.

Zapraszamy do publikacji na łamach Prawa Mediów Elektronicznych, a także do kontaktu z nami pod adresem: pme@beck.pl

Z poważaniem,
prof. dr hab. *Jacek Gołaczyński*

Etyczne problemy wdrażania medycznego Internetu rzeczy

dr Jarosław Greser[1]

W niniejszym opracowaniu autor porusza problematykę związaną z wdrażaniem medycznego Internetu rzeczy, przy czym z etycznego punktu widzenia. W literaturze podkreśla się, że problemy etyczne związane z korzystaniem z urządzeń H-IoT cieszą się zainteresowaniem badaczy od początków rozwoju tej technologii i są analizowane z różnych perspektyw, z których każda naświetla inne obawy[2]. Przedstawione zatem zostały wybrane problemy etyczne z perspektywy producentów urządzeń mających swoją siedzibę na terenie UE. Artykuł podzielono na cztery części, z których pierwsza jest wprowadzeniem do zagadnień związanych z etyką biznesu – swoistego zespołu norm, którego adresatem są przedsiębiorcy. Następnie przeanalizowano prywatność w wymiarze związanym ze stygmatyzacją związaną z korzystaniem z urządzeń H-IoT oraz problemy dotyczące własności danych zbieranych przez te urządzenia, a także zapewnienia cyberbezpieczeństwa ich użytkownikom.

Uwagi wstępne

Rozwój Internetu rzeczy stworzył nowe sposoby świadczenia usług medycznych. Technologia ta, którą w literaturze określa się jako *Health – Related Internet of Things* (H-IoT)[3] obejmuje bardzo szerokie spektrum urządzeń: od złożonych systemów podtrzymywania życia czy prowadzenia badań klinicznych do nieskomplikowanych konstrukcji monitorujących jeden parametr życiowy, na przykład temperaturę lub ciśnienie krwi. Równie szeroki jest zakres zastosowania takich urządzeń, który obejmuje monitorowanie pacjentów nie tylko w przypadkach nagłych, lecz również tych cierpiących na choroby przewlekłe czy też rejestrację zachowań mających wpływ na zdrowie takich jak sen lub nawyki żywieniowe. Badania wskazują, że wdrożenie rozwiązań H-IoT zmniejsza koszt opieki zdrowotnej[4], wskaźnik hospitalizacji[5] oraz poprawia standard opieki nad osobami przewlekle chorymi[6]. Dlatego ich wdrożenie jest priorytetem zarówno podmiotów prywatnych, które chcą zwiększyć w ten sposób swoją przewagę konkurencyjną[7], jak i celem stawianym w krajowych i unijnych politykach rozwoju[8]. Prowadzi to do coraz szerszego wykorzystania tych urządzeń w procedurach medycznych, a trend ten ma tendencję dynamicznie wzrostową.

Jednocześnie funkcjonowanie urządzeń medycznego Internetu rzeczy nie zostało w sposób kompleksowy uregulowane w żadnym akcie prawnym. Jedną z przyczyn jest zróżnicowanie tych urządzeń. Należy zauważyć, że do kategorii H-IoT są zaliczane zarówno wyroby medyczne, których wprowadzanie na rynek i użytkowanie jest regulowane odpowiednimi przepisami prawa[9], jak i rozwiązania, które mogą zmienić dowolne urządzenie w H-IoT na przykład aplikacje do monitorowania aktywności fizycznej instalowane na smartfonach, które nie posiadają dedykowanej regulacji. Ponadto, ze względu na specyfikę ich działania, do urządzeń tych mogą być stosowane przepisy dotyczące ochrony danych osobowych, cyberbezpieczeństwa, odpowiedzialności za produkt niebezpieczny, praw konsumenta czy regulujące problematykę własności intelektualnej.

Brak wprowadzenia regulacji prawnych dotyczących problematyki medycznego Internetu rzeczy może stanowić ponadto wynik świadomej decyzji prawodawcy czy też przejaw niemożności jego szybkiej reakcji na postępujące zmiany technologiczne. Obszary pozostające poza regulacją prawną mogą być jednak normowane środkami pozaprawnymi, wśród których pierwszoplanowe znaczenie mają normy

[1] Uniwersytet im. Adama Mickiewicza w Poznaniu.

[2] *B. Mittelstadt*, Ethics of the health-related internet of things: a narrative review, Ethics and Information Technology 2017, Nr 19(3), s. 157–175.

[3] *B. Mittelstadt*, Ethics of the health-related internet of things…, s. 157–175.

[4] *C. Henderson*, *M. Knapp*, *J.-L. Fernandez*, *J. Beecham*, *S.P. Hirani*, *M. Cartwright*, et al, Cost effectiveness of telehealth for patients with long term conditions (whole systems demonstrator telehealth questionnaire study): Nested economic evaluation in a pragmatic, cluster randomised controlled trial, British Medical Journal 2013, Nr 346, s. 1–19.

[5] *C. Lomas*, Telehealth system slashes hospital admissions in COPD patients, Nursing Times 2009, Nr 105(9), http://www.nursingtimes.net/nursing-practice/clinical-zones/copd/telehealth-system-slashes-hospital--admis-sions-in-copd-patients/5005885.article (dostęp z 24.7.2020 r.).

[6] *D. Su*, *J. Zhou*, *M.S. Kelley*, *T.L. Michuad*, *M. Siahpush*, *J. Kim*, *F. Wilson*, *J.P. Stimpson*, *J.A. Pagánde*, Does telemedicine improve treatment outcomes for diabetes? A meta-analysis of results from 55 randomized controlled trials, Diabetes Research and Clinical Practice 2016, Nr 116.

[7] *L. Sobieski*, Koncepcja e-zdrowia w świetle regulacji publicznoprawnych, [w:] *K. Kokocińska* (red.), Innowacyjne technologie w ochronie zdrowia. Aspekty prawne, Warszawa 2020, s. 35.

[8] *K. Kokocińska*, Działania władzy publicznej na rzecz rozwoju innowacyjnych technologii w sektorze zdrowia (polityka unijna i krajowa), [w:] *K. Kokocińska* (red.), Innowacyjne technologie w ochronie zdrowia. Aspekty prawne, Warszawa 2020, s. 16–32.

[9] Od maja 2021 r. kwestie związane z wyrobami medycznymi będzie regulować rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z 5.4.2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) Nr 178/2002 i rozporządzenia (WE) Nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG, Dz.Urz. UE L Nr 117, s. 1; dalej jako: rozporządzenie 2017/745. Akt ten nie odnosi się w szczególny sposób do urządzeń IoT. Zob. *J. Greser*, Cyberbezpieczeństwo wyrobów medycznych w świetle rozporządzenia 2017/745, iKAR 2020, Nr 2, *passim*.

etyczne oraz normy typu *soft-law*, w szczególności działalność samoregulacyjna uczestników rynku w postaci kodeksów postępowań lub zaleceń branżowych i wytyczne organów władzy publicznej.

Etyka biznesu jako źródło obowiązków przedsiębiorstw

Kwestia przypisania odpowiedzialności etycznej przedsiębiorstwu jest przedmiotem sporu wśród etyków[10]. Zwolennicy jej istnienia twierdzą, że podmiot ten jako jednostka czyniąca dobro i zło nie może całkowicie uciec od ponoszenia odpowiedzialności moralnej za swe czyny. Przeciwnicy wskazują, że osobowość prawna zwalnia z posiadania zobowiązań moralnych, gdyż osoba prawna nie jest podmiotem moralnym, ponieważ nie ma sumienia.

Oczywiste jest, że przedsiębiorstwo nie może posiadać intencji ani motywów analogicznych do zachowań człowieka. Natomiast gdy potraktujemy je jako korelat jednostek, możemy jej przypisać cechy intencjonalne. Przyjmując, że jest to wysoko zorganizowana struktura, w której działania jednostek ukierunkowane są na osiągnięcie celu organizacji, można przyjąć, że istnieje pewien nadrzędny poziom intencji przedsiębiorstwa. Jest on jednak czymś więcej niż sumą intencji pojedynczych jednostek, ponieważ kształtują go również nieformalne relacje pomiędzy pracownikami oraz wartości, normy i przekonania, które są w przedsiębiorstwie akceptowane i przestrzegane[11]. Łącznie składają się one na kulturę organizacyjną, która jest podstawą przypisania odpowiedzialności etycznej przedsiębiorstwu.

Zespół norm regulujący kwestie etyczne związane z prowadzeniem działalności gospodarczej nazywany jest etyką biznesu. Definiowana jest ona jako działania, które są zgodne z prawem i oczekiwaniami społecznymi[12]. O ile zakres pierwszej z tych przesłanek jest względnie łatwy do ustalenia, o tyle w przypadku drugiej może rodzić to problemy. Punktem wyjścia do ustalenia zakresu etycznej odpowiedzialności przedsiębiorstw jest założenie, że działają one na podstawie tak zwanej społecznej licencji na funkcjonowanie (*social license to operate*). Wyznacza ona obszar aktywności ludzkiej, w którym operują podmioty gospodarcze, i zasady, w jakich powinno się to odbywać. Działanie zgodnie z nią wymaga zarówno przestrzegania norm narzuconych, jak np. normy prawne, czy dobrowolnie przyjętych, jak np. normy społecznej odpowiedzialności biznesu[13], jak i takich, które zgodnie ze społecznym oczekiwaniem powinny być przestrzegane[14]. Należy jednak zauważyć, że interpretacja norm etyki biznesu nie ma charakteru uniwersalnego, ponieważ są one formułowane przez pryzmat historii lub kultury danego kraju. Tym samym ma ona charakter krajowy lub wręcz regionalny[15]. Pojawia się zatem możliwość relatywizacji pojęć poprzez nadawanie im autonomicznego znaczenia w etyce biznesu. Tym samym przypisanie odpowiedzialności za naruszenie norm etycznych może być niemożliwe ze względu na trudności z jednoznacznym ustaleniem treści tych norm lub sprzeczność ich treści w różnych miejscach. Jako przykład przywołać można wdrożony w Chinach system do oceny zachowań obywateli (*social credit system*). Jeśli założymy, że takie rozwiązanie jest zgodne z prawem krajowym, to dostarczanie urządzeń do realizacji tego celu nie rodzi konfliktu etycznego z perspektywy przedsiębiorstw chińskich, ale w przypadku przedsiębiorstw europejskich możemy mówić o jego istnieniu ze względu na inne rozumienie koncepcji prywatności.

W przypadku H-IoT sytuację dodatkowo komplikuje fakt globalnego charakteru powiązań związanych z ich tworzeniem i wykorzystywaniem. Jak zauważyła *M. Ossowska*, do osiągnięcia skuteczności sankcji za naruszenie norm etycznych konieczne jest, aby skład grupy społecznej dokonującej oceny postępowania naruszyciela był względnie stały[16]. Zależności w obrębie współczesnego systemu gospodarczego utrudniają, a niejednokrotnie uniemożliwiają ustalenie podmiotu, który dokonał naruszenia norm. Tym samym można przyjąć, że etyka nie jest źródłem norm, na podstawie którego można dochodzić skutecznie jego odpowiedzialności. Nie oznacza to jednak, że istnienie norm etycznych lub powoływanie się na nie jest bezprzedmiotowe. Ich rolą jest zwracanie uwagi na problemy, które pozostają poza sferą regulacji prawnych wraz z przedstawianiem propozycji ich rozwiązań. W tym znaczeniu są one niezwykle przydatne dla ustalenia reguł tworzenia i korzystania z H-IoT, ze względu na możliwość wypełnienia treścią normatywną elementów niedoprecyzowanych przez prawo. Przywoływane w dalszej części artykułu problemy etyczne będę analizował przez ten pryzmat.

[10] Por. *J. Filek*, Wprowadzenie do etyki biznesu, Kraków 2001, s. 110; *G.D. Chryssides*, *J.H. Kaler*, Wprowadzenie do etyki biznesu, Warszawa 1999, s. 248.

[11] *M. Kapusta*, *M. Sukiennik*, *P. Bąk*, Wybrane determinanty kształtujące kulturę korporacyjną, Finanse, Rynki Finansowe, Ubezpieczenia 2017(89), Nr 5, cz. 2, s. 486.

[12] *W. Gasparski*, Wykłady z etyki biznesu. Nowa edycja uzupełniona, Warszawa 2007, s. 95 oraz 108.

[13] *J. Filek*, Wprowadzenie do…, s. 111; *C. Dierksmeier*, *P. Seele*, Cryptocurrencies and Business Ethics, J Bus Ethics 2018, Nr 152, s. 1–14.

[14] *J. Ruggie*, Protect, Respect and Remedy: a Framework for Business and Human Rights, Report of the Special Representative of the United Nations Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 2008, https://www.mitpressjournals.org/doi/pdf/10.1162/itgg.2008.3.2.189 (dostęp z 24.7.2020 r.).

[15] *W. Gasparski*, Wykłady z etyki…, s. 196.

[16] *M. Ossowska*, Socjologia moralności: zarys zagadnień, Warszawa 1969, s. 109–112.

Problematyka prywatności pacjentów korzystających z H-IoT

Prawo do prywatności jest ugruntowanym pojęciem na poziomie prawnym. Ma status prawa człowieka chronionego umowami międzynarodowymi, jak również umocowanie w konstytucjach wielu państw, w tym Polski[17]. W kontekście H-IoT konkretyzacją tego prawa są przepisy chroniące autonomię informacyjną pacjenta zawarte w przepisach o ochronie danych osobowych i regulujących tajemnicę lekarską[18]. Wyznaczają one zakres zachowań poszczególnych podmiotów, który ma gwarantować zachowanie odpowiedniego poziomu prywatności jednostek. Z perspektywy etycznej prywatność ujmowana jest szerzej niż w normach prawnych. W literaturze oprócz zagadnień związanych z prawem do posiadania i ochrony przestrzeni osobistej i bycia pozostawionym w spokoju wskazuje się również, że to pojęcie ma swój materialny wymiar[19]. Inaczej mówiąc, będzie odnosić się do fizycznej obecności urządzeń, których działanie wkracza w sferę prywatności jednostki. Na tym tle rodzą się problemy z wykorzystaniem urządzeń H-IoT, które są na stałe zamontowane w określonych miejscach. W literaturze wskazuje się, że takie rozwiązania mogą prowadzić do stopniowej utraty prywatności i wywoływać uciążliwe poczucie bycia obserwowanym[20]. Jednocześnie instalacja urządzeń w taki sposób, że są one niewidoczne dla osób monitorowanych, tak jak przykładowo czujników w domach opieki, również wywołuje pewne problemy etyczne. Wskazuje się, że w takich przypadkach informacja o działaniu urządzeń oraz ewentualne zgody na ich wykorzystywanie powinny być ponawiane[21]. Należy zauważyć, że takie ponawiane uzyskiwanie zgody wykracza poza obowiązki nałożone normami prawnymi. Przykładowo art. 7 ust. 3 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/WE[22] zakłada jednorazowe udzielenie zgody, która uprawnia administratora do przetwarzania danych dopóty, dopóki zgoda taka nie zostanie wycofana. W przypadku obowiązków informacyjnych zarówno art. 13 ust. 4, jak i art. 14 ust. 5 lit. a RODO wskazują, że jeżeli osoba już dysponuje informacjami wymaganymi przez przepisy, to nie ma potrzeby ponownego ich przekazywania. Będzie to miało szczególne znaczenie w przypadku przetwarzania danych osobowych przez urządzenia H-IoT, gdyż podstawą prawną tego działania zasadniczo nie będzie zgoda – administrator raczej powoła się na konieczność zapewnienia opieki zdrowotnej lub leczenia (art. 9 ust. 1 lit. h RODO) lub ochrony żywotnych interesów (art. 9 ust. 1 lit. c RODO) w przypadku danych wrażliwych, a w przypadku danych zwykłych wykonanie umowy (art. 6 ust. 1 lit. b RODO), obowiązek prawny (art. 6 ust. 1 lit. c RODO) lub uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO). Może to więc prowadzić do sytuacji, w której wykonanie obowiązku informacyjnego jest jedynym momentem przekazywania informacji o wykorzystywaniu urządzeń H-IoT.

Inny problem etyczny jest związany z wykorzystaniem urządzeń H-IoT, których używanie wymaga zamontowania urządzenia na ciele pacjenta. Będzie to dotyczyło zarówno urządzeń zintegrowanych na stałe, np. rozruszniki serca, jak i takich, które można łatwo usnąć, np. pompy insulinowe czy opaski ułatwiające znalezienie osób cierpiących na zaburzenia pamięci. W literaturze wskazuje się, że widoczność urządzeń może prowadzić do stygmatyzacji ich użytkowników, podobnie jak alarmy i raportowanie przez nie o sytuacjach zagrożenia[23]. Obniża to chęć korzystania z tych urządzeń w długim okresie, tym samym może prowadzić do pogorszenia stanu opieki nad pacjentem zamiast jej polepszenia[24]. Należy zauważyć, że problem ten dotyczy w szczególności urządzeń do zastosowań klinicznych. Badania wskazują, że jeżeli jako H-IoT jest wykorzystywane urządzenie mające w odbiorze społecznym inny cel, np. smartfon, to chęć pacjentów do wykorzystania rozwiązań jest dużo wyższa[25]. Prowadzi to do wniosku, że kluczowym aspektem jest sposób zaprojektowania urządzenia, w trakcie którego koniecznie jest branie pod uwagę wartości i doświadczeń pacjentów, ponieważ od nich będzie zależał poziom akceptacji urządzenia[26]. Należy zauważyć, że rozporządzenie 2017/745 odnosi się do ergonomii wyrobu medycznego w zakresie dotyczącym eliminowania

[17] *M. Wujczyk*, Prawo pracownika do ochrony prywatności, Warszawa 2012, s. 28; *P. Sarnecki*, Komentarz do art. 47, [w:] *L. Garlicki* (red.), *K. Działocha*, *P. Sarnecki*, *W. Sokolewicz*, *J. Trzciński*, Konstytucja Rzeczypospolitej Polskiej. Komentarz. T. III, Warszawa 2001, s. 1.

[18] *J. Greser*, Ochrona danych dotyczących zdrowia a nowoczesne technologie medyczne, [w:] *K. Kokocińska*, Innowacyjne technologie w ochronie zdrowia. Aspekty prawne, Warszawa 2020, s. 137–158.

[19] *A. Essén*, The two facets of electronic care surveillance: An exploration of the views of older people who live with monitoring devices, Social Science & Medicine 2008, Nr 67, s. 128–136; *A. Bowes*, *A. Dawson*, *A. Bell*, Ethical implications of lifestyle monitoring data in ageing research, Information, Communication & Society 2012, Nr 15(1), s. 5–22.

[20] *R. Steele*, *A. Lo*, *C. Secombe*, *Y. Wong*, Elderly per-sons' perception and acceptance of using wireless sensor net-works to assist healthcare, International Journal of Medical Informatics 2009, Nr 78, s. 788–801; *A.M. Dorsten*, *S.K. Sifford*, *A. Bharucha*, *L.P. Mecca*, *H. Wactlar*, Ethical perspectives on emerging assistive technologies: insights from focus groups with stakeholders in long-term care facilities, Journal of Empirical Research on Human Research Ethics 2009, Nr 4, s. 25–36.

[21] *K. Ebersold*, *R. Glass*, The internet of things: A cause for ethical concern, Issues in Information Systems 2016, Nr 17, s. 145–151, http://www.iacis.org/iis/2016/4_iis_2016_145-151.pdf (dostęp z 24.7.2020 r.).

[22] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

[23] *K.L. Courtney*, *G. Demiris*, *M. Rantz*, *M. Skubic*, Needing smart home technologies: The perspectives of older adults in continuing care retirement communities, Informatics in Primary Care 2008, Nr 16, s. 195–201.

[24] *G. Demiris*, *B.K. Hensel*, „Smart homes" for patients at the end of life, Journal of Housing for the Elderly 2009, Nr 23, s. 106–115.

[25] *B.K. Hensel*, *G. Demiris*, *K.L. Courtney*, Defining obtrusiveness in home telehealth technologies: A conceptual framework, Journal of the American Medical Informatics Association 2006, Nr 13, s. 428–431.

[26] *B. Mittelstadt*, Ethics of the health-related internet of things: a narrative review, Ethics and Information Technology 2017, Nr 19(3), s. 162.

ryzyka związanego z błędem użytkowym (załącznik 1 pkt 5 lit. a oraz pkt 14 ust. 2), wskazując, że wystąpienie takiego błędu trzeba zaliczyć do kategorii incydentu (art. 2 pkt 64). W konsekwencji należy stwierdzić, że inne wartości niż bezpośrednio związane z bezpieczeństwem użytkowania nie są brane przez prawodawcę pod uwagę. Tym samym działania mające na celu zapewnienie komfortu psychicznego użytkowników wykraczają poza obowiązki prawne, ale jednocześnie, ze względu na swój wpływ na jednostkę, można je zaliczyć do zobowiązań o charakterze etycznym.

Własność i dzielenie się danymi generowanymi przez urządzenia H-IoT

Ocenia się, że w 2019 r. ilość danych generowanych przez IoT wyniosła 500 zettabajtów i będzie w kolejnych latach rosła wykładniczo[27]. Jednocześnie wskazuje się na urządzenia H-IoT jako jedno z głównych źródeł tych danych[28]. Wśród problemów etycznych wskazywanych w literaturze, które są związane z gromadzeniem danych na pierwszy plan wysuwają się zagadnienia minimalizacji zbieranych danych oraz dostęp do zgromadzonych informacji przez pacjenta.

Odnosząc się do pierwszej kwestii, należy zauważyć, że H-IoT zbierają i generują zarówno dane osobowe, jak i nieosobowe. W odniesieniu do tych drugich rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w UE[29], wprost wskazuje w motywie 3, że swoboda przedsiębiorczości i swoboda świadczenia usług mają zastosowanie do usług przetwarzania danych. Tym samym nie można nakładać ograniczeń ani w zakresie ilości danych, które są gromadzone przez określony podmiot, ani w zakresie działań, które są na nich prowadzone, np. agregacji, analizy, obrotu czy dystrybucji.

W przypadku danych osobowych zagadnienie minimalizacji jest uregulowane prawnie. Artykuł 5 ust. 1 lit. c RODO wskazuje, że można przetwarzać tylko te dane, które są adekwatne, stosowne oraz ograniczone do tego co niezbędne do celów, w których są przetwarzane. Przepis ten ma status zasady przetwarzania, co oznacza, że ma nadrzędną moc wobec pozostałych przepisów, a jednocześnie stanowi dla nich dyrektywę interpretacyjną[30]. Na tej podstawie można przyjąć, że zakres zbieranych danych powinien być wyznaczany potrzebami terapeutycznymi określonego użytkownika. Jednocześnie zbieranie dodatkowych informacji może mieć wpływ na zwiększenie skuteczności terapii albo zmniejszenie częstotliwości występowania skutków ubocznych. Należy przez to rozumieć inne dane niż te, których przetwarzanie nie wynika z obowiązku prawnego lub uzasadnionego interesu administratora, jakim jest bezpieczeństwo urządzenia. Będą to np. metadane, które są źródłem do wyszukiwania ukrytych korelacji za pomocą algorytmów sztucznej inteligencji. Intuicyjnym rozwiązaniem do zastosowania w tym przypadku jest wyrażenie zgody przez użytkownika. Zasadą jest, że w licencjach końcowych producenci urządzenia zastrzegają sobie prawo do agregacji zebranych i udostępniania ich innym podmiotom zarówno dla celów naukowych, jak i komercyjnych. Zasadniczo zgoda jest udzielana na jednorazowe badanie. Jednocześnie etycy wskazują, że w przypadku HIoT bardzo trudno jest doprowadzić do sytuacji, w której zgoda jest świadoma[31]. Wynika to z braku odpowiedniej wiedzy i aparatu poznawczego pacjenta wymaganego, aby zrozumieć poziom szczegółowości zbieranych danych i konsekwencje przeprowadzonych analiz, które, jak się wskazuje, mogą prowadzić do wykluczenia ze świadczenia określonego rodzaju usług[32]. Podobny problem pojawia się przy uzyskaniu zgody na pozyskiwanie danych dotyczących stosowania H-IoT ze źródeł nieformalnych, jak opisy samopoczucia w mediach społecznościowych czy analizy zapytań do wyszukiwarek[33].

Alternatywą jest anonimizacja informacji, co pozbawia je statusu danych osobowych (motyw 26 RODO). Należy jednak pamiętać, że przeprowadzenie takiego procesu jest bardzo trudne, jeśli w ogóle możliwe. Przeprowadzone w 2013 r. testy potwierdziły, że odpowiednio gęste ułożenie anten BTS pozwala na jednoznaczną identyfikację 95% osób, które korzystały z telefonów komórkowych[34]. W przypadku urządzeń H-IoT, których konstrukcja wymaga stałego kontaktu z Internetem, można założyć, że wynik ten byłby porównywalny.

Drugim wskazywanym problemem jest dostęp pacjentów do zgromadzonych danych zbieranych przez urządzenia H-IoT. W typowej sytuacji można wyróżnić trzy grupy podmiotów. Pierwszą jest producent urządzenia, który dysponuje wszystkimi zebranymi informacjami, zarówno przetworzonymi, jak i nieprzetworzonymi, które są generowane przez urządzenie. Drugą grupę stanowią podmioty wykonujące działalność leczniczą. Zakres przekazywanych

[27] Cisco, Cisco Annual Internet Report (2018-2023) White Paper, 2020 https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html (dostęp z 24.7.2020 r.).

[28] *J. Lima*, 10 of the biggest IoT data generators, Computer Business Review, 2015, https://www.cbronline.com/internet-of-things/10-of-the-biggest-iot-data-generators-4586937/ (dostęp z 24.7.2020 r.).

[29] Dz.Urz. UE L Nr 303, s. 59; dalej jako: rozporządzenie 2018/1807.

[30] *P. Drobek*, Komentarz do artykułu 5, [w:] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, s. 323–324.

[31] *M.J. Bietz*, *C.S. Bloss*, *S. Calvert*, *J.G. Godino*, *J. Gregory*, *M.P. Claffey*, et al, Opportunities and challenges in the use of personal health data for health research, Journal of the American Medical Informatics Association 2016, Nr 23(e1), s. 42–48; *K. Denecke*, *P. Bamidis*, *C. Bond*, *E. Gabarron*, *M. Househ, A.Y.S. Lau*, et al, Ethical issues of social media usage in healthcare, IMIA Yearbook of Medical Informatics 2015, Nr 10(1), s. 137–47.

[32] *B. Mittelstadt*, Ethics of the health-related internet…, s. 165.

[33] *Ibidem*, s. 165.

[34] *Y.A. de Montjoye*, *A.C. Hidalgo*, *M. Verleysena* i *V.D. Blondela*, Unique in the Crowd: The privacy bounds of human mobility, Nature 2013, s. 1376.

danych zależy od umów dotyczących korzystania z H-IoT. Najczęściej przybierają one formę licencji dla użytkownika końcowego i obejmują określony zestaw informacji dotyczący bezpośrednio stanu zdrowia pacjenta. Pomijane są więc metadane i inne informacje, które nie mają bezpośredniego związku z leczeniem. Trzecią grupą są pacjenci, którzy mogą otrzymywać uproszczony zestaw podstawowych informacji wraz z ich interpretacją lub otrzymywać zinterpretowane informacje wyłącznie od lekarza.

Na tym tle pojawia się kilka wątpliwości. Po pierwsze, zebrane dane mają wartość finansową, której beneficjentem jest producent urządzenia. Podmiot ten nie dzieli się przy tym zyskami z pacjentami. Podobnie jak w przypadku badań w przemyśle farmaceutycznym, podmioty badań mogą dysponować roszczeniem do udziału w zysku z produktów i usług powstałych dzięki przekazaniu danych. Źródła takiego roszczenia należy upatrywać w normach etycznych, a nie prawnych[35].

Po drugie, podmioty prywatne nie mają żadnego obowiązku dzielenia się uzyskanymi informacjami. Dysponowanie danymi w zakresie ich sprzedaży, licencjonowania czy tworzenia baz danych regulowane są przez prawo cywilne. Głównym podmiotem zainteresowanym dostępem do danych są naukowcy, dla których jest to otwarcie nowych możliwości w badaniach. Dotyczy to zarówno obszaru medycyny, jak i nauk społecznych czy humanistyki. Trzeba pamiętać, że w przypadku podmiotów publicznych istnieją normy kształtujące zasady ponownego wykorzystania danych. W UE wynikają one z dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 z 20.6.2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego[36]. Jednocześnie wskazuje się, że normy praw człowieka, w szczególności w zakresie prawa do najwyższego osiągalnego standardu zdrowia, jak też wolności akademickiej, mogą ograniczać prawa własności intelektualnej, jednakże w praktyce ma to znikome znaczenie[37].

Kolejnym problemem jest obawa, że nieograniczony dostęp do surowych danych może zaszkodzić pacjentowi ze względu na możliwe problemy z ich interpretacją wynikającą z braku odpowiedniej wiedzy i doświadczenia[38]. Jak się wskazuje, przyjęcie założenia, że takie osoby zdobędą odpowiednie zasoby do interpretacji, jest nieracjonalne[39]. Jednocześnie udostępnienie nieprzetworzonych informacji może mieć zasadnicze znaczenie dla postawienia alternatywnej diagnozy przez innego lekarza. Należy zauważyć, że art. 20 RODO zawiera prawo do przeniesienia danych zgromadzonych przez administratora. Należy jednak zauważyć, że dotyczy ono tylko danych osobowych, a więc poza zakresem normowania mogą być informacje niemające takiego charakteru, a cenne z perspektywy diagnostycznej, jak np. czas zażywania leku. Ponadto prawo to dotyczy wyłącznie danych przetwarzanych na podstawie zgody (art. 6 ust. 1 lit. a RODO lub art. 9 ust. 2 lit. a RODO) lub na podstawie umowy (art. 6 ust. 1 lit. b RODO). Wyłącza to zatem informacje o stanie zdrowia, które przetwarzane są na podstawie art. 9 ust. 1 lit. h RODO będącego podstawą najczęściej wykorzystywaną w trakcie świadczenia usług medycznych.

Czwartym problemem jest format danych. Pomimo że art. 20 ust. 1 RODO wprost wskazuje, że dane powinny być przekazane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, to brak interoperacyjności urządzeń IoT jest powszechnie występującym problemem w praktyce[40].

Ostatnim zagadnieniem związanym z ograniczonym dostępem do danych zbieranych przez H-IoT jest niemożność oceny prawidłowości działania urządzenia przez osoby trzecie. W przypadku wyrobów medycznych kwestia ta jest przedmiotem regulacji prawnych określających zasady klasyfikowania i certyfikowania urządzeń pod kątem bezpieczeństwa, do których należy wspomniane powyżej rozporządzenie 2017/745. Jednocześnie wskazuje się, że system ten może mieć wady, szczególnie w przypadku nowoczesnych technologii. Problem ten dotyczy różnych technologii medycznych[41], ale można go zilustrować amerykańskim przykładem urządzenia do leczenia bezdechu sennego. Urządzenie to było skonfigurowane w taki sposób, że jego działanie nie przynosiło korzyści terapeutycznych pacjentom odbiegającym od założonej przez producenta średniej[42]. Jednocześnie pacjent nie miał możliwości ani konfiguracji urządzenia pod kątem swoich potrzeb, ani dostępu do informacji, które urządzenie zbierało, co mogłoby potwierdzić brak zysków terapeutycznych z jego używania. Dowody dotyczące skuteczności terapii uzyskano, zmieniając oprogramowanie sterujące urządzeniem, co było naruszeniem warunków licencji i spotkało się z prawną reakcją producenta urządzenia, który zażądał zwrotu urządzeń

[35] *S. Chapman*, *E. Reeve*, *G. Rajaratnam*, *R. Neary*, Setting up an outcomes guarantee for pharmaceuticals: new approach to risk sharing in primary care, British Medical Journal 2003, Nr 326(7391), s. 707; *A. Petryna*, *A. Lakoff*, *A. Kleinman*, Global pharmaceuticals: Ethics, markets, practices, Durham 2006, s. 301.

[36] Dz.Urz. UE L Nr 172, s. 56; dalej jako: dyrektywa 2019/1024.

[37] *J. Greser*, Prawa autorskie a prawa człowieka, [w:] *J. Kępiński*, *K. Klafkowska-Wiśniowska*, *R. Sikorski* (red.), Granice prawa autorskiego, Warszawa 2010, s. s. 202–206.

[38] *D. Boyd*, *K. Crawford*, Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon, Information Communication & Society 2012, Nr 15(5), s. 662–679.

[39] *M. Andrejevic*, Big data, big questions, the big data divide, International Journal of Communication 2014, Nr 8(0), s. 17.

[40] Problem ten jest przedmiotem badań Komisji Europejskiej pod kątem naruszania reguł konkurencji. Zob. Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1326 (dostęp z 24.7.2020 r.).

[41] *S. Hanselman*, The Promising State of Diabetes Technology in 2016, https://www.hanselman.com/blog/ThePromisingStateOfDiabetesTechnologyIn2016.aspx (dostęp z 24.7.2020 r.).

[42] *A. Wesołowska*, Hakowanie warunkiem przeżycia – o łamaniu zabezpieczeń, które ratuje pacjentów, Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl/post/hakowanie-warunkiem-przezycia-o-lamaniu-zabezpieczen-ktore-ratuje-pacjentow/ (dostęp z 24.7.2020 r.).

i groził wszczęciem postępowań karnych. Trzeba zwrócić uwagę, że w tym przypadku pojawia się również zagadnienie udostępnienia danych osobom, które mogą mieć problem z ich właściwą interpretacją. Natomiast z perspektywy etycznej zachowanie przedsiębiorstwa nie może być uznane za zgodne z tymi normami.

Problemy etyczne a zapewnienie cyberbezpieczeństwa H-IoT

Cyberbezpieczeństwo nie jest rozważane jako osobna kwestia etyczna, ale wskazuje się na bardzo silny związek tego zagadnienia z prywatnością[43]. Należy podzielić ten pogląd, jednocześnie zwracając uwagę, że cele działań na rzecz bezpieczeństwa i prywatności są różne. W pierwszym przypadku będzie to zapewnienie „poufności, integralności i dostępności"[44] informacji, co pozwala osobie, której dane dotyczą, zachować prywatność w rozumieniu sprawowania kontroli nad tym, jak są one wykorzystywane[45]. Tym samym cele te są współzależne, a więc nie sposób zrealizować jednego bez realizacji drugiego.

Problematyka cyberbezpieczeństwa jest w pewnym zakresie regulowana przez normy prawne[46]. Poza tymi przepisami pozostaje część obszarów wykorzystania H-IoT, co wynika zarówno z celowych działań prawodawcy – jak w przypadku braku narzucania określonych standardów zabezpieczeń – jak i niewprowadzania takich regulacji z powodu opóźnień w reakcji organów państwa na zmiany technologiczne. W literaturze wskazuje się, że w takich przypadkach producent, tworząc standardy zabezpieczeń, powinien kierować się normami etyki biznesu[47].

Wśród zagadnień, które są przynajmniej częściowo regulowane normami etycznymi, można wskazać obowiązki producenta do dostarczania wsparcia dla urządzenia wycofanego ze sprzedaży. Należy zauważyć, że wyroby takie, nazywane *orphant devices*, stanowią istotne zagrożenie dla bezpieczeństwa osób z nich korzystających[48]. Problem ten został zauważony przez prawodawcę europejskiego i zaowocował wydaniem dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/770 z 20.5.2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych[49] oraz dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/771 z 20.5.2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniająca rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE i uchylająca dyrektywę 1999/44/WE[50], które częściowo regulują tę kwestię. Należy jednak zwrócić uwagę, że termin transpozycji przepisów został wskazany na 1.7.2021 r., a nie mogą one wejść w życie później niż 1.1.2022 r. Do tego czasu na producentach nie ciążą zobowiązania wynikające z przepisów prawa. Nie zmienia to jednak faktu istnienia obowiązku etycznego, który obciąża producenta. W tym zakresie można wyróżnić co najmniej trzy sytuacje. Pierwsza, gdy producent jasno deklaruje użytkownikowi, jaki jest cykl życia produktu i kiedy zakończy dla niego wsparcie oraz jakie konsekwencje są z tym związane. Druga, gdy nie ma takiego komunikatu, a wycofanie się ze wsparcia zależy od decyzji biznesowej. Trzecia obejmuje przypadki, gdy wycofanie się ze wsparcia produktu wynika z czynników zewnętrznych takich jak ogłoszenie niewypłacalności producenta.

Wspólny dla tych sytuacji jest wynikający z norm etycznych nakaz poinformowania użytkowników o zakończeniu wsparcia, związanych z tym konsekwencjach i potencjalnych ryzykach wynikających z dalszego korzystania z urządzenia. W przypadku H-IoT konieczne będzie również poinformowanie odpowiednich organów nadzorujących rynek wyrobów medycznych. Producent może również rozważyć uniemożliwienie korzystania z urządzenia poprzez jego programowe wyłączenie. Takie działanie musi być jednak poprzedzone staranną analizą, której wyniki wskażą, że ryzyko dalszego wykorzystania urządzenia znacznie przewyższa korzyści, które uzyskuje pacjent. Szczególnie należy wziąć pod uwagę możliwości wtórnego wykorzystania urządzenia przez pacjentów, którzy wcześniej nie mieli do niego dostępu ze względu na cenę.

Jednocześnie powinno się rozważyć udostępnienie plików źródłowych programów sterujących urządzeniem wraz z jego dokumentacją techniczną oraz objęcie ich wolną licencją. Taki zabieg pozwoli na rozwijanie oprogramowania przez grupy niezależnych programistów i dalsze utrzymywanie funkcjonalności urządzenia. Trzeba jednak zwrócić uwagę na liczne problemy, które mogą pojawić się w związku z takim działaniem zarówno w sferze prawnej, jak i praktycznej. W pierwszej z nich znaczącą rolę będą odgrywały regulacje

[43] *M. Chan*, *D. Estève*, *C. Escriba*, *E. Campo*, A review of smart homes: Present state and future challenges, Computer Methods and Programs in Biomedicine 2008, Nr 91, s. 55–81; *M. Mana*, *M. Feham*, *B.A. Bensaber*, Trust key management scheme for wireless body area networks, International Journal of Network Security 2011, Nr 12, s. 75–83; *H.F. Atlam*, *G.B. Wills*, IoT Security, Privacy, Safety and Ethics, [w:] *M. Farsi*, *A. Daneshkhah*, *A. Hosseinian-Far, H. Jahankhani* (red.), Digital Twin Technologies and Smart Cities, Internet of Things, Technology, Communications and Computing, Cham 2020, s. 140–141.

[44] *F. Giannotti*, *Y. Saygin*, Privacy and security in ubiquitous knowledge discovery, Lecture Notes in Computer Science, Berlin 2010, s. 75.

[45] *S.R. Peppet*, Regulating the internet of things: First steps toward managing discrimination, privacy, security and consent, Texas Law Review, 2014, 93, s. 85; *A. Greenfield*, Some guidelines for the ethical development of ubiquitous computing, Philosophical Transactions of the Royal Society A 2008, Nr 366(1881), s. 3823–3831.

[46] *C. Banasiński*, Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa, [w:] *C. Banasiński*, *M. Rojszczak* (red.), Cyberbezpieczeństwo, Warszawa 2020, s. 15.

[47] *M. Flyverbom*, *R. Deibert*, *D. Matten*, The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business, Business & Society 2019, Nr 58(1), s. 3–19.

[48] (Marvin 2017).

[49] Dz.Urz. UE L Nr 136, s. 1; dalej jako: dyrektywa 2019/770.

[50] Dz.Urz. UE L Nr 136, s. 28; dalej jako: dyrektywa 2019/771.

związane z własnością intelektualną. Chodzi tu w szczególności o licencje do określonych komponentów programu, takich jak biblioteki programistyczne lub bazy danych, które zostały udzielone producentowi urządzenia. W standardowej sytuacji uniemożliwiają one ich wykorzystanie przez podmioty inne niż strony umowy. Zatem nie będzie możliwości prawnej do rozszerzenia kręgu licencjobiorców. W sferze praktycznej natomiast publikacja kodu źródłowego może pogorszyć poziom cyberbezpieczeństwa urządzenia, ponieważ wgląd do niego będą miały osoby chcące wykorzystać jego podatności. Udostępnienie kodu w formie otwartej znacznie ułatwia jego analizę, a tym samym wykrycie luk w bezpieczeństwie.

Rozważając sytuację, w której brak wsparcia wynika z niewypłacalności producenta, należy zauważyć, że dochodzi do naruszenia jego deklaracji dotyczących cyklu życia produktu, ale wynika ono z przyczyn od niego niezależnych. W tym przypadku zasadnicze znaczenie będzie miała forma upadłości. W sytuacji gdy prowadzi ona do likwidacji przedsiębiorstwa i nie ma podmiotu, który wchodzi w jego prawa i obowiązki, wydaje się, że konieczne jest przeprowadzenie procedury informacyjnej opisanej powyżej. Dobrą praktyką będzie też wskazanie producentów lub urządzeń komplementarnych, które mogą zastąpić produkowane rozwiązanie. Natomiast jeżeli prawa do urządzenia zostaną przejęte przez inny podmiot, to nabywa on również obowiązki etyczne związane z urządzeniem. Tym samym wsparcie dla użytkowników powinno być świadczone na zasadach ustalonych przez pierwotnego producenta.

Wśród innych problemów etycznych związanych z korzystaniem z H-IoT można wskazać zakres podejmowanych działań, w przypadku gdy luka w zabezpieczeniach urządzenia wynika z błędu podwykonawcy, oraz kwestie związane ze standaryzacją rozwiązań. Objętość niniejszego opracowania uniemożliwia ich rozwinięcie, jednak warto zasygnalizować, że w pierwszym przypadku konieczne będzie ustalenie, jakie są obowiązki producenta w zależności od tego, czy oprogramowanie było tworzone na zamówienie, czy jest częścią istniejącego programu. W drugim natomiast trzeba zwrócić uwagę na zagadnienie interoperacyjności urządzeń i protokołów, którą wskazuje się jako kluczową dla bezpieczeństwa[51], oraz zestawić je z polityką sprzedażową preferującą tworzenie odrębnych standardów, nad którymi tylko producent sprawuje kontrolę.

Podsumowanie

Korzyści wynikające z wdrażania rozwiązań H-IoT zarówno dla pacjentów, jak i podmiotów systemu ochrony zdrowia, prowadzą do coraz szerszego stosowania tej technologii. W przypadku UE normy prawne będą w różnym stopniu regulowały zasady korzystania w nich w zależności od tego, czy będziemy mieli do czynienia z wyrobem medycznym czy z produktem zbierającym informacje o stanie zdrowia. Jednocześnie do obu typów urządzeń mogą znaleźć zastosowanie przepisy dotyczące ochrony danych osobowych czy cyberbezpieczeństwa. Mimo tego, jak wskazywałem powyżej, brakuje norm prawnych regulujących niektóre, ważne aspekty związane z korzystaniem z tej technologii. W literaturze wskazuje się, że w przypadku urządzeń H-IoT oczekuje się wyjścia administratorów poza wyłącznie wymagania prawne[52]. Ten pogląd należy podzielić, zaznaczając jednak, że etyka biznesu będzie formułować wyłącznie metacele, które będą konkretyzowane na poziomie samoregulacji branżowych takich jak kodeksy postępowania. Takie działanie likwiduje mankament norm etycznych polegający na zróżnicowaniu ich treści, która prowadzi do możliwości arbitralnego ich rozumienia. Jednocześnie przedsiębiorstwo przystępujące do kodeksu nie będzie mogło twierdzić, że norma w nim zawarta nie obowiązuje go, co rozwiązuje problem ustalenia obowiązywania normy etycznej. Ponadto naruszanie postanowień kodeksu postępowania może prowadzić do odpowiedzialności prawnej. Artykuł 6 ust. 2 lit. b dyrektywy Parlamentu Europejskiego i Rady (UE) 2005/29/WE z 11.5.2005 r. dotyczącej nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniającej dyrektywę Rady (UE) 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE, 2002/65/WE Parlamentu Europejskiego i Rady (UE) oraz rozporządzenia (WE) Nr 2006/2004 Parlamentu Europejskiego i Rady (UE)[53] wskazuje, że takie działanie jest nieuczciwą praktyką rynkową, których stosowanie w zależności od wyboru państwa członkowskiego naraża na odpowiedzialność cywilną lub administracyjną.

Odnosząc się do szczegółowych problemów, należy podkreślić, że prywatność ma węższą definicję w prawie niż etyce. W pierwszym przypadku, mimo licznych dyskusji, koncentruje się wokół koncepcji *right to be alone* sformułowanej pod koniec XIX w. przez *S. Warrena* i *L. Brandeisa*, a więc skupia się na ochronie przed zewnętrzną ingerencją w prywatność. W drugim wymiarze obejmuje ono również aspekty wewnętrzne życia jednostki. Przywołany przykład urządzeń monitorujących znajdujących się w ciele pacjenta pokazuje, jak istotną rolę odgrywa zbadanie potrzeb pacjentów w kontekście projektu zewnętrznego urządzenia i jego funkcjonalności. O ile wymóg bezpieczeństwa ma źródło w przepisach prawa, o tyle dbałość o dobrostan użytkownika należy do zobowiązań etycznych.

[51] *S.R. Peppet*, Regulating the internet of things…, s. 85; *A. Greenfield*, Some guidelines for the ethical development…, s. 3823–3831.

[52] *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, Social Science Research Network 2017, s. 76–99, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 (dostęp z 24.7.2020 r.); *B. Mittelstadt*, Ethics of the health-related internet…, s. 166.

[53] Dz.Urz. UE L Nr 149, s. 22; dalej jako: dyrektywa 2005/29/WE.

Na prywatność rzutuje też kwestia monitorowania zachowań użytkowników H-IoT. Kwestia ta podlega regulacjom prawnym i, co do zasady, prowadzenie takiego monitoringu jest dopuszczalne. Rozważając tę kwestię z perspektywy RODO, trzeba zauważyć, że zachowanie standardu prawnego – to jest znalezienie podstawy przetwarzania i zrealizowanie obowiązku informacyjnego – może być niewystarczające z perspektywy oczekiwań użytkownika. W tym względzie należy postulować ponawianie wykonania tego obowiązku, szczególnie w sytuacji gdy monitoring prowadzony jest za pomocą urządzeń niewidocznych dla użytkownika. Wydaje się, że w celu wypełnienia zobowiązań etycznych taka informacja powinna być przekazana osobiście pacjentowi przez osobę, która ułatwi zrozumienie treści komunikatu i wyjaśni ewentualne wątpliwości pojawiające się w związku z jego treścią. Ma to szczególne znaczenie, w sytuacji gdy komunikat kierowany jest do osób o ograniczonych funkcjach poznawczych.

Problematyka etyczna dzielenia się danymi sprowadza się do dylematu, w jaki sposób wyważyć dobro prywatne, jakim jest prawo własności danych i czerpanie związanych z nim przychodów oraz dobro publiczne, jakim jest dostęp do nich dla celów naukowych. Wydaje się, że rozwiązaniem może być taka implementacja dyrektywy 2019/1024, która w zakresie ponownego wykorzystania danych będzie obejmowała również podmioty prywatne. Należy zauważyć, że motyw 39 tego aktu prawnego wskazuje, że państwa członkowskie mogą również postanowić o stosowaniu jej wymogów do przedsiębiorstw prywatnych, w szczególności tych, które świadczą usługi w interesie ogólnym. Istotne w tym przypadku byłoby stworzenie minimalnego standardu na poziomie europejskim w celu zachowania takich samych reguł konkurencji.

W przypadku dostępu pacjenta do danych zgromadzonych przez urządzenie wydaje się, że z perspektywy etycznej prawo do uzyskania diagnozy przez innego specjalistę przeważa nad własnościowymi uprawnieniami producenta urządzenia. Obejmuje to informacje, co do których obowiązek przekazania nie wynika z art. 20 RODO lub innych przepisów prawnych. Jednocześnie po udostępnieniu danych producent urządzenia nie jest obarczony odpowiedzialnością, etyczną lub prawną, za ich dalsze wykorzystanie.

W obszarze cyberbezpieczeństwa problematyka etyczna stosowania H-IoT obejmuje między innymi zapewnienie wsparcia dla użytkownika polegającego na dostarczaniu aktualizacji oprogramowania. Problem jest tym istotniejszy, że ewentualny atak może mieć skutki bezpośrednio w sferze życia i zdrowia pacjenta. W przypadku wyrobów medycznych można przyjąć, że brak takiego wsparcia jest przesłanką do usunięciu produktu z rynku, ze względu na niespełnienie kryterium bezpieczeństwa użytkowania. W stosunku do innych H-IoT sytuacja wydaje się dużo bardziej złożona, a spełnienie wymogów etycznych będzie uzależnione od przyczyny zaprzestania wsparcia.

Poruszone w niniejszym artykule problemy są jedynie przykładami dylematów etycznych, które powstają w związku z korzystaniem z H-IoT. W kontekście dyskusji na ten temat pojawiają się zagadnienia dyskryminacji ze względu na błędy w algorytmach obsługujących H-IoT, interoperacyjności urządzeń, tworzenia na podstawie zebranych danych profili konsumenckich i sprzedawanie ich przedsiębiorstwom ubezpieczeniowym lub marketingowym czy izolacji społecznej związanej z mniejszą koniecznością interakcji z człowiekiem. Kolejne wyzwania będą się pojawiać wraz z rozwojem tej technologii. Bez wątpienia prawo nie powinno być jedynym źródłem normowania w tym zakresie, ale ze względu na swoje mankamenty, a w szczególności opóźnienie ustawodawcy wobec zmian społecznych, kwestie etyczne powinny być również ważną częścią tworzenia regulacji. Szczególnie należy postulować wsparcie dla tworzenia samoregulacji branżowych, które wydają się najefektywniejszą formą instytucjonalizacji etyki biznesu.

Słowa kluczowe: Internet rzeczy, wyrób medyczny, prywatność, cyberbezpieczeństwo, RODO.

Ethical problems of implementing the Internet of Medical Things

In the present article, the author brings up the issue connected with the implementation of the Internet of Medical Things. The literature emphasizes that there are ethical dilemmas regarding the use of H-IoT devices which are popular among researchers since the beginning of this technology and they are being analyzed from different perspectives, all of which raise different doubts. The author presents chosen ethical problems from the perspective of manufacturers of these devices which are located in the EU. The article is divided into four parts. The first one is an introduction to issues connected with business ethics – a specific set of rules of which the recipients are entrepreneurs. Secondly, there is an analysis of privacy in the area connected with stigmatization regarding the use of H-IoT devices and problems regarding ownership of data collected by these devices, and ensuring cybersecurity of their users.

Keywords: Internet of Medical Things, medical device, privacy, cybersecurity, GDPR.

Prawne aspekty wykorzystania technologii *cloud computing* w sektorze opieki zdrowotnej

Katarzyna Biczysko-Pudełko[1]

Celem niniejszego opracowania jest próba poszukiwania odpowiedzi na pytanie o prawne implikacje wykorzystywania technologii *cloud computing* (chmury obliczeniowej) w sektorze opieki zdrowotnej, a ściślej możliwości przetwarzania danych dotyczących zdrowia w ramach elektronicznej dokumentacji medycznej funkcjonującej w takich systemach informatycznych jak chmura obliczeniowa. Stąd też głównym tłem rozważań będą przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 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/WE (ogólne rozporządzenie o ochronie danych)[2], a także – w mniejszym jednak zakresie – przepisy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[3], i przyjęte na jej podstawie przepisy prawa polskiego.

Uwagi wstępne

Chmura obliczeniowa (*cloud computing*), będąca właściwie synonimem przetwarzania danych, w praktyce sprowadza się do wszechobecnego, wygodnego i możliwego na żądanie dostępu za pośrednictwem sieci do dzielonych zasobów obliczeniowych (tj. sieć, serwery, pamięć masowa, aplikacje i usługi), które mogą być szybko zapewnione i uwolnione przy minimalnym zarządzaniu lub ingerencji dostawcy[4]. Przedmiotowa technologia, niegdyś określana mianem „technologii jutra", z roku na rok zyskuje coraz szersze grono użytkowników wykorzystujących jej możliwości w często zupełnie różnych od siebie celach, tj. od poczty elektronicznej wykorzystywanej *stricte* na potrzeby korespondencji prywatnej począwszy, poprzez portale społecznościowe, różnego rodzaju pakiety biurowe, a na zaawansowanych środowiskach programistycznych skończywszy. Powyższy trend nie ominął także sektora opieki zdrowotnej, w ramach funkcjonowania którego technologia ta zdaje się zyskiwać na znaczeniu i popularności. Każdego dnia w rzeczonym sektorze dochodzi do przetwarzania setek tysięcy danych, przy czym procesy te – w mojej ocenie – co do zasady odbywają się w dwóch obszarach, tj.:

- obszarze organizacyjnym, w ramach którego instaluje się system informatyczny, w praktyce pozwalający na zastąpienie dotychczasowych papierowych nośników danych o pacjencie nośnikami elektronicznymi i sprowadzający się m.in. do tworzenia elektronicznej dokumentacji medycznej;
- obszarze klinicznym – sprowadzającym się do wykorzystania usług chmury obliczeniowej do świadczenie usług opieki zdrowotnej (tj. diagnozowania, leczenia, profilaktyki chorób, a także urazów, jak również badań i ich oceny) w sytuacjach, w których pracownicy systemu opieki zdrowotnej i pacjenci znajdują się w różnych miejscach – tj. obszar telemedycyny.

Mając więc na uwadze powyższe, a także wzajemną implikację pomiędzy koniecznością zapewnienia pacjentom poufności i bezpieczeństwa ich danych – z jednej strony zwłaszcza z uwagi na potencjalne konsekwencje ich naruszenia[5], oraz z drugiej strony proces stale postępującej informatyzacji[6] sek-

[1] Uniwersytet Opolski.

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

[3] Dz.Urz. UE L Nr 194, s. 2; dalej jako: dyrektywa NIS.

[4] *P. Mell*, *T. Grance*, The NIST Definition of Cloud Computing: Recommendations of National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, MD September 2011, s. 2. Zob. także Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie wykorzystania potencjału chmury obliczeniowej w Europie, COM (2012) 529 final, s. 2; *J. Byrski*, *A. Wachowska*, Cloud computing w działalności instytucji płatniczej, Monitor Prawa Bankowego 2012, Nr 9, s. 59; *D. Szostek*, Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej, Warszawa 2012, s. 56–57.

[5] Odnosząc się do konsekwencji naruszenia danych osobowych przetwarzanych w sektorze ochrony zdrowia, wskazać należy, iż sektor ten słusznie oceniany jest jako krytyczny. Dowodzi tego fakt coraz częstszych ataków hakerskich, których to celami stają się m.in. szpitale czy placówki medyczne. Tytułem przykładu wskazać można chociażby na ataki, jakie nastąpiły w Wielkiej Brytanii, gdzie w 2017 r. nieznani hakerzy dokonali masowego ataku na szpitale należące do National Health Service, atakując m.in. komputery podmiotów leczniczych przez tzw. ransomware, czego konsekwencją była chociażby konieczność przeniesienia pacjentów do innych placówek i odwołanie części zabiegów. Co więcej, podnieść należy, iż np. w Stanach Zjednoczonych co dziesiąty podmiot leczniczy każdego dnia doświadcza próby włamania. Zob. więcej: *P. Najbuk*, *P. Kaźmierczak*, *W. Dziomdziora*, *P. Marczuk*, Cyberbezpieczeństwo w sektorze ochrony zdrowia, Warszawa 2017, s. 5, https://portal.dzp.pl/files/shares/Cyberbezpiecze%C5%84stwo%20w%20sektorze%20zdrowia% 20 raport% 20 DZP.pdf (dostęp z 20.12.2017 r.).

[6] Pojęcie informatyzacji jest pojęciem szerszym od określenia komputeryzacji i polega ono m.in. na racjonalnym wykorzystaniu uprzednio wprowadzonych już danych w postaci elektronicznej do systemów teleinformatycznych w możliwie największym dopuszczalnym zakresie, także przez systemy teleinformatyczne innych podmiotów, Zob. *S. Kotecka*, E-Government & E-Justice, [w:] *A. Burdziak*, *Ł. Cieślak*, *Ł. Goździaszek*, *S. Kotecka*, *P. Pęcherzewski*, *P. Rodziewicz*, *A. Zalesińska* (red.), Technologia informacyjna dla prawników (dokument elektroniczny), Wrocław 2011, s. 52. Na temat pojęcia informatyzacji i komputeryzacji. Szerzej zob. *J. Gołaczyński*, *S. Kostecka*, Klikając Temid@, Prawo Mediów Elektronicznych 2011/3, Warszawa 2011, s. 11–15.

tora opieki zdrowotnej, jako istotna, ale jednocześnie ciekawa, jawi się analiza dotycząca poszukiwania odpowiedzi na pytanie o prawne implikacje wykorzystywania interesującej nas technologii *cloud computing* właśnie w sektorze opieki zdrowotnej, przy czym zakres przedmiotowej analizy zostanie ograniczony tylko do wspomnianego wyżej obszaru organizacyjnego z jednoczesnym uwzględnieniem przepisów RODO. Powyższe znajduje swoje uzasadnienie chociażby w twierdzeniu, że o ile sam fakt stale rosnącej już przecież od co najmniej kilkunastu lat komputeryzacji[7] podmiotów świadczących usługi w systemie ochrony zdrowia zdawał się nie rodzić aż tak daleko idących konsekwencji dla ochrony danych osobowych, o tyle już zmiana podstawowego medycznego nośnika danych, tj. dokumentów w formie papierowej, na dane w postaci elektronicznej, a następnie ich przetwarzanie właśnie za pomocą chmury obliczeniowej z całą pewnością jest o wiele bardziej złożone i to nie tylko technologicznie, ale także prawnie, a to z następujących względów.

Przede wszystkim wymaga ono uwzględnienia kilku norm prawnych obowiązujących nie tylko w przestrzeni prawa ochrony danych osobowych, ale także tzw. regulacji sektorowych skupionych zarówno w wielu ustawach, jak i w aktach wykonawczych[8], które co do zasady – jak wskazują *A. Romaszewski* i *W. Trąbka*[9] – sklasyfikować można do następujących grup:

a) regulacje dotyczące kwestii elektronicznej dokumentacji medycznej, czego w szczególności[10] dotyczyć będzie ustawa z 28.4.2011 r. o systemie informacji w ochronie zdrowia[11];
b) regulacje dotyczące zasad postępowania z danymi o charakterze osobowym gromadzonymi przez podmioty udzielające świadczeń medycznych w procesie realizowania swoich zadań, które to dane mogą także zostać, w myśl art. 24 ust. 5 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta powierzone przez podmiot udzielający świadczeń zdrowotnych do dalszego przetwarzania na podstawie umowy o powierzenie przetwarzania danych osobowych, o której to mowa w art. 28 RODO;
c) regulacje dotyczące ochrony baz danych[12] ze szczególnym uwzględnieniem baz zawierających dane o stanie zdrowia, prowadzonych na zasadzie obowiązku przez wszystkie podmioty zobowiązane do tego ustawą o systemie informacji w ochronie zdrowia;
d) wiele przepisów zawartych w ustawie o systemie informacji w ochronie zdrowia oraz ustawie z 17.2.2005 r. o informatyzacji podmiotów publicznych realizujących zadania publiczne[13] wraz z rozporządzeniami wykonawczymi;
e) regulacje zapewniające odpowiedni poziom integralności sieci, usług oraz przekazu komunikatów przez operatorów (dostawców usług) świadczących usługi telekomunikacyjne[14].

Dodatkowo na złożoność problematyki przetwarzania danych dotyczących zdrowia wpływ ma także liczba podmiotów, które do przedmiotowego przetwarzania są uprawnione, tj.: pacjent, którego dane są przetwarzane, podmiot, który udziela świadczeń zdrowotnych, podmiot upoważniony na podstawie przepisów prawa i w zakresie określonym przepisami (np. NFZ[15]), czy też podmioty, które dostarczają zasoby, infrastrukturę lub inne usługi w chmurze, oraz podmioty odpowiedzialne za transmisje danych w sieciach teleinformatycznych[16]. Co znamienne, każda z wyżej wymienionych grup podlega innym regulacjom prawnym, to zaś prowadzi także do odmiennego kształtowania nie tylko ich praw i obowiązków, ale też ich odpowiedzialności[17].

[7] Pojęcie komputeryzacji należy rozumieć jako stosowanie komputerów w różnego rodzaju organizacjach i wprowadzanie metod przetwarzania danych przy ich użyciu. W ramach komputeryzacji zastępuje się np. własnoręcznie uzupełniane formularze – formularzami elektronicznymi wypełnianymi za pomocą edytorów tekstu, archiwa dokumentów sporządzonych na papierze – bazami dokumentów elektronicznych, wprowadza się pocztę elektroniczną lub komunikator internetowy jako prawnie relewantny środek komunikacji pomiędzy pracownikami danego podmiotu a klientami. Zmienia się jednak jedynie narzędzie pracy – z długopisu na klawiaturę i myszkę komputerową oraz monitor. Tworzone bazy dokumentów elektronicznych i danych zawartych w tych dokumentach nie są udostępniane nawet innym komórkom organizacyjnym danej jednostki, nie mówiąc o udostępnianiu tychże baz innym podmiotom. Pojęcie komputeryzacji jest pojęciem węższym w stosunku do określenia informatyzacji. Zob. *S. Kotecka*, E-Government & E-Justice..., s. 52.

[8] Np. rozporządzenie Prezesa Rady Ministrów z 14.9.2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz.U. z 2018 r. poz. 180); rozporządzenie Rady Ministrów z 12.4.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247 ze zm.); rozporządzenie Ministra Zdrowia z 25.3.2013 r. w sprawie klasyfikacji danych i systemu kodów w Systemie Informacji Medycznej (Dz.U. poz. 473 ze zm.); rozporządzenie Ministra Zdrowia z 6.4.2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. poz. 666), dalej jako: DokMedR.

[9] *A. Romaszewski*, *W. Trąbka*, Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych, Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie 2014, Nr 33, s. 37–38.

[10] Ponadto można wskazać jeszcze na następujące akty prawne: ustawę z 15.4.2011 r. o działalności leczniczej (t.j. Dz.U. z 2020 r. poz. 295 ze zm.; dalej jako: DziałLeczU), ustawę z 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2020 r. poz. 849 ze zm.; dalej jako: PrPacjentU); ustawę z 5.12.1996 r. o zawodach lekarza i lekarza dentysty (t.j. Dz.U. z 2020 r. poz. 514 ze zm.).

[11] T.j. Dz.U. z 2020 r. poz. 702 ze zm., dalej jako: SysInfZdrowU.

[12] Ustawa z 27.7.2001 r. o ochronie baz danych (Dz.U. Nr 128, poz. 1402 ze zm.).

[13] T.j. Dz.U. z 2017 r. poz. 570 ze zm.

[14] Ustawa z 16.7.2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2017 r. poz. 1907 ze zm.).

[15] Narodowy Fundusz Zdrowia jest państwową jednostką organizacyjną działającą na podstawie ustawy z 27.8.2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz.U. z 2020 r. poz. 1398 ze zm.; dalej jako: ŚwŚrodPubU) i w ramach polskiego systemu opieki zdrowotnej pełni funkcję płatnika.

[16] *A. Romaszewski*, *W. Trąbka*, Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych..., s. 38.

[17] *Ibidem*.

Kazus elektronicznej dokumentacji medycznej

Pomimo wskazanych wcześniej okoliczności obecnie podejmowane są realne działania mające na celu realizację w ramach systemu ochrony zdrowia bardzo dużych projektów właśnie na bazie technologii *cloud computing*[18], czego dobrym przykładem zdaje się być kazus elektronicznej dokumentacji medycznej. I jakkolwiek przepisy wprowadzające elektroniczną dokumentację medyczną jako standardową i powszechnie obowiązującą były już wielokrotnie nowelizowane[19], a ostateczny termin obowiązku posługiwania się tego typu dokumentacją zmieniany, niemniej jednak w praktyce systemu opieki zdrowotnej „papierowy" dokument przechodzi wolno do historii i zauważalne jest świadczenie przez wiele podmiotów usług medycznych przy wsparciu modelu elektronicznej dokumentacji medycznej, w tym także poza miejscem świadczenia usług zdrowotnych i przy wykorzystaniu technologii *cloud computing*[20].

Dostrzegając powyższe, nie sposób więc nie odnieść się do przedmiotowego zjawiska, co jednakże wcześniej warto poprzedzić kilkoma uwagami natury ogólnej.

W literaturze przedmiotu słusznie zauważa się, że w praktyce funkcjonowania rynku usług medycznych dane i informacje, które już są lub mają być w przyszłości przetwarzane w ramach chmury obliczeniowej, występują obecnie w różnych formach zarówno pod względem nazewnictwa, zawartości merytorycznej, jak i organizacyjnej[21].

Doskonale obrazują to chociażby przepisy ustawy o systemie informacji w ochronie zdrowia, w ramach której można, poza wspomnianą już elektroniczną dokumentacją medyczną, napotkać jeszcze kategorie takich pojęć jak: „dane"[22], „jednostkowe dane medyczne", „dokument elektroniczny"[23], „bazy danych"[24] czy „rejestr medyczny"[25]. Wspólnym mianownikiem dla wszystkich tych danych jest natomiast to, że funkcjonują w ramach tzw. systemu informacji w ochronie zdrowia, a więc systemu, w którym przetwarzane są dane niezbędne do prowadzenia polityki zdrowotnej państwa, podnoszenia jakości i dostępności świadczeń opieki zdrowotnej oraz finansowania zadań z zakresu ochrony zdrowia (art. 1 ust. 1 SysInfZdrowU) i który to obejmuje bazy danych tworzone przez podmioty obowiązane do ich prowadzenia, zawierające dane o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej, usługodawcach i pracownikach medycznych, usługobiorcach (art. 3 ust. 1 SysInfZdrowU) oraz które to bazy danych funkcjonują w ramach systemu informacji medycznej (SIM), dziedzinowych systemów teleinformatycznych, o których mowa w art. 5 ust. 1 pkt 2 SysInfZdrowU, oraz rejestrów medycznych (art. 5 ust. 1 SysInfZdrowU).

Z całego spektrum wskazanych powyżej danych to jednak elektroniczna dokumentacja medyczna będzie podstawowym nośnikiem danych i informacji o stanie zdrowia i to właśnie w ramach elektronicznej dokumentacji medycznej dochodzić będzie do przetwarzania zwłaszcza jednej ze szczególnych kategorii danych osobowych, o których mowa na gruncie art. 4 pkt 15 RODO, a więc do przetwarzania danych osobowych o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniających informacje o jej stanie zdrowia („dane dotyczące zdrowia").

Ustawodawca polski w ramach przepisów ustawy o systemie informacji w ochronie zdrowia zaproponował, by pod pojęciem elektronicznej dokumentacji medycznej rozumieć dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez ZUS:

a) recepty,
b) określone w przepisach wydanych na podstawie art. 13a,
c) skierowania określone w przepisach wydanych na podstawie art. 59aa ust. 2 ŚwŚrodPubU.

---

[18] *Ibidem*.

[19] Zgodnie z pierwotnym brzmieniem ustawy o systemie informacji w ochronie zdrowia, wszelka dokumentacja medyczna wytworzona po 31.7.2014 r. miała być prowadzona w wersji elektronicznej. Niemniej jednak na skutek nowelizacji dokonanej ustawą z 26.6.2014 r. o zmianie ustawy o systemie informacji w ochronie zdrowia (Dz.U. poz. 998) wprowadzono przepis, zgodnie z którym do 31.7.2017 r. dokumentacja medyczna może być prowadzona w wersji papierowej lub elektronicznej. Następnie mocą ustawy z 9.10.2015 r. termin wprowadzenia elektronicznej dokumentacji medycznej przesunięto do 31.12.2017 r. (Dz.U. poz. 1991). Wreszcie według stanu prawnego obowiązującego w momencie tworzenia niniejszego opracowania ostatecznie obowiązek prowadzenia jej w wersji elektronicznej istnieć będzie od 1.1.2019 r. (Dz.U. z 2017 r. poz. 1845), przy czym wskazać należy, iż ustawodawca dokonał rozróżnienia terminu dla elektronicznej dokumentacji medycznej, recept elektronicznych (tj. od 1.1.2020 r.) i skierowań w postaci elektronicznej (od 1.1.2021 r.).

[20] *A. Romaszewski*, *W. Trąbka*, *M. Kielar*, *K. Gajda*, Elektroniczna dokumentacja medyczna – przetwarzanie danych o stanie zdrowia poza miejscem świadczenia usług zdrowotnych, Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie 2017, Nr 44, s. 14.

[21] *A. Romaszewski*, *W. Trąbka*, Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych..., s. 42.

[22] Pod pojęciem tym, w świetle art. 2 pkt 4 SysInfZdrowU, rozumieć należy litery, wyrazy, cyfry, teksty, liczby, znaki, symbole, obrazy, kombinacje liter, cyfr, liczb, symboli i znaków, zebrane w zbiory o określonej strukturze, dostępne według określonych kryteriów, w tym dane osobowe.

[23] Przez sformułowanie dokument elektroniczny na gruncie ustawy o systemie informacji w ochronie zdrowia rozumieć należy dokument elektroniczny, o którym mowa w art. 3 pkt 2 ustawy z 17.2.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2020 r. poz. 346 ze zm.).

[24] Bazy danych, zgodnie z ustawą o systemie informacji w ochronie zdrowia, zawierają dane o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej; usługodawcach i pracownikach medycznych; usługobiorcach. Podmioty zobowiązane do ich prowadzenia wskazane zostały w art. 3 ust. 2 SysInfZdrowU.

[25] Zgodnie z art. 2 pkt 12 SysInfZdrowU rejestr medyczny to tworzony zgodnie z prawem rejestr, ewidencja, lista, spis albo inny uporządkowany zbiór danych osobowych, jednostkowych danych medycznych lub danych niebędących danymi osobowymi, służący do realizacji zadań publicznych, prowadzony przez podmiot funkcjonujący w systemie ochrony zdrowia.

Doprecyzowując powyższe, już na gruncie rozporządzenia w sprawie dokumentacji medycznej, ustawodawca wskazał, iż dokumentacja medyczna może być prowadzona w postaci papierowej, jeżeli przepis rozporządzenia tak stanowi lub warunki organizacyjno-techniczne uniemożliwiają prowadzenie dokumentacji w postaci elektronicznej (§ 1 DokMedR) i zasadniczo wyróżnić można dwa podstawowe jej rodzaje, tj. dokumentację indywidualną dotyczącą poszczególnych pacjentów korzystających ze świadczeń zdrowotnych oraz dokumentację zbiorczą odnoszącą się do ogółu pacjentów lub poszczególnych grup pacjentów korzystających ze świadczeń zdrowotnych (§ 2 DokMedR).

Co więcej, w ramach indywidualnej dokumentacji medycznej ustawodawca zdecydował się wyróżnić jeszcze tę przeznaczoną na potrzeby podmiotu udzielającego świadczeń zdrowotnych (tj. dokumentację indywidualną wewnętrzną) oraz tę przeznaczoną na potrzeby pacjenta korzystającego ze świadczeń zdrowotnych (tj. dokumentację indywidualną zewnętrzną). I to właśnie obie ze wskazanych powyżej kategorii dokumentacji indywidualnej będą z punktu widzenia przedmiotowej analizy mieć fundamentalne znaczenie. W zakresie pierwszej z nich mieścić będzie się w szczególności historia zdrowia i choroby, historia choroby, karta noworodka, karta indywidualnej opieki pielęgniarskiej, karta indywidualnej opieki prowadzonej przez położną, karta wizyty patronażowej itd. (§ 2 pkt 3 DokMedR). Z kolei indywidualna dokumentacja zewnętrzna dotyczyć będzie w szczególności skierowania do szpitala lub innego podmiotu na badania diagnostyczne, konsultacji lub leczenia, karty przebiegu ciąży, książeczki zdrowia dziecka, karty informacyjnej z leczenia szpitalnego czy też pisemnej informacji lekarza leczącego pacjenta w poradni specjalistycznej dla kierującego lekarza ubezpieczenia zdrowotnego lub felczera ubezpieczenia zdrowotnego oraz lekarza podstawowej opieki zdrowotnej o rozpoznaniu, sposobie leczenia, rokowaniu, ordynowanych lekach, środkach specjalnego przeznaczenia żywieniowego i wyrobach medycznych czy wreszcie też opinii lekarskiej (§ 2 pkt 4 DokMedR). Jednoznacznie więc – biorąc pod uwagę przytoczoną wcześniej definicję danych dotyczących zdrowia obowiązującą na gruncie RODO, wskazać należy, iż tego typu dane będą zawierać się właśnie w ramach indywidualnej dokumentacji medycznej i tym samym więc szerzej w ramach całej dokumentacji medycznej.

Powyższe prowadzi do wniosku, że elektroniczna dokumentacja medyczna będzie podstawowym nośnikiem danych i informacji o stanie zdrowia pacjenta[26], a warunkiem *sine quo non* do skorzystania z owej elektronicznej dokumentacji medycznej jest funkcjonowanie dedykowanego systemu teleinformatycznego[27].

W warunkach polskiej służby zdrowia, zgodnie z ustawą o systemie informacji w ochronie zdrowia, rolę owego dedykowanego systemu teleinformatycznego odgrywa tzw. SIM, tj. system informacji medycznej[28]. Zgodnie z art. 10 ust. 1 SysInfZdrowU, SIM jest systemem teleinformatycznym służącym przetwarzaniu danych dotyczących udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej udostępnianych przez systemy teleinformatyczne usługodawców[29]. W powiązaniu z danymi, o których mowa w ust. 1 art. 10 SysInfZdrowU, w SIM przetwarzane i udostępniane w postaci elektronicznej są m.in. dane osobowe i jednostkowe dane medyczne o usługobiorcach[30], dane o usługodawcach, dane o pracownikach medycznych, dane o płatnikach, o których mowa w art. 2 pkt 9 lit. a, oraz kilka innych danych wskazanych w art. 10 ust. 2 SysInfZdrowU. Ponadto, w myśl art. 11. ust. 3, usługodawca zamieszcza w SIM dane umożliwiające pobieranie danych zawartych w elektronicznej dokumentacji medycznej przez innego usługodawcę lub pobieranie dokumentów elektronicznych niezbędnych do prowadzenia diagnostyki, zapewnienia ciągłości leczenia. Szczegółowo katalog tychże danych określony został w art. 11 ust. 4 SysInfZdrowU i obejmuje on:

1) dane usługodawcy;
2) dane usługobiorcy;
3) dane identyfikujące świadczenie zdrowotne;
4) dane miejsca udzielenia świadczenia zdrowotnego;
5) dane pracownika medycznego udzielającego świadczenia zdrowotnego;
6) dane dotyczące dokumentacji medycznej wytworzonej w związku z udzielonym świadczeniem zdrowotnym;
7) inne dane pozwalające na identyfikację zdarzenia medycznego.

Jak wynika więc z powyższego, katalog danych, które usługodawca umieszcza w SIM, jest szeroki i z całą pewnością obejmuje on swoim zakresem również dane dotyczące zdrowia, stąd też konsekwencje naruszeń bezpieczeństwa tychże danych są potencjalnie znaczące i daleko idące.

Z tego względu nie może dziwić fakt nałożenia na podmioty udzielające świadczeń zdrowotnych wielu obowiązków i to nie tylko mocą przepisów z zakresu prawa ochrony danych, ale również regulacji sektorowych, jak np. normy rozporządzenia w sprawie dokumentacji medycznej. Te ostatnie zobowiązują podmioty udzielające świadczeń zdrowotnych do spełnienia wielu wymagań co do warunków prowadzenia

[26] *A. Romaszewski*, *W. Trąbka*, Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych..., s. 42.

[27] *A. Klich*, Wybrane zagadnienia prawne elektronicznej dokumentacji medycznej, Ekonomiczne Problemy Usług, 2017 (126), Nr 1, t. 2, Szczecin 2017, s. 355.

[28] Dalej jako: SIM.

[29] Zgodnie z art. 2 SysInfZdrowU pod pojęciem usługodawcy należy rozumieć świadczeniodawcę w rozumieniu art. 5 pkt 41 ŚwŚrodPubU, oraz aptekę ogólnodostępną i punkt apteczny.

[30] Usługobiorcą – w myśl art. 2 SysInfZdrowU – jest osoba fizyczna korzystająca lub uprawniona do korzystania ze świadczeń opieki zdrowotnej, w tym świadczeniobiorca w rozumieniu art. 2 ust. 1 ŚwŚrodPubU oraz osoba, o której mowa w art. 2 ust. 2 i art. 13 tej ustawy.

dokumentacji medycznej w postaci elektronicznej, warunków jej zabezpieczenia[31], a także warunków, jakie musi spełnić sam system teleinformatyczny, w ramach którego dochodzi do umieszczania elektronicznej dokumentacji medycznej[32].

Powyższy stan rzeczy sprawia, że znaczna część podmiotów udzielających świadczenia zdrowotne decyduje się na skorzystanie z możliwości, jaką daje art. 24 PrPacjentU, a mianowicie outsourcingu procesów przetwarzania danych medycznych na rzecz zewnętrznych podmiotów, w tym także w ramach usług *cloud computing*. Oczywiście w przedmiotowej sytuacji taki podmiot udzielający świadczeń zdrowotnych będzie zobligowany do spełnienia wielu innych obowiązków, które nakładają na niego, jako administratora tychże danych, przepisy RODO, tj. chociażby ustalenia, czy dany dostawca usług w chmurze obliczeniowej daje rękojmię zapewnienia odpowiedniego poziomu ochrony powierzonych mu danych osobowych, a sama realizacja tej umowy nie może powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej. Jednocześnie jednak podmiot, któremu powierzono przetwarzanie danych osobowych, obowiązany jest do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją tej umowy, a związanie przedmiotową tajemnicą nie ustaje nawet po śmierci pacjenta (art. 24 ust. 6 PrPacjetU), a także innych obowiązków, które wynikają już wprost z przepisów RODO, jak np. związanych z prawidłową realizacją umowy związanych m.in. ze wsparciem administratora w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane są przetwarzane, czy zapewnieniem odpowiednich środków technicznych i organizacyjnych ochrony powierzonych danych (art. 28 ust. 3 RODO). Ponadto, dostawca usług *cloud computing* powinien powstrzymać się od przekazywania danych do przetwarzania innym podmiotom bez uprzedniego uzyskania szczegółowej lub ogólnej pisemnej zgody administratora w tym zakresie (art. 28 ust. 2 RODO)[33]. W przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej podmiotowi, który powierzył przetwarzanie danych osobowych.

Technologia *cloud computing* w świetle przepisów dyrektywy NIS

Odnosząc się do tematu korzystania przez sektor opieki zdrowotnej z technologii *cloud computing*, nie można jednocześnie pominąć przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[34], i przyjętych na jej podstawie przepisów prawa polskiego.

W dużym uogólnieniu przepisy dyrektywy NIS nakładają na państwa członkowskie obowiązek zidentyfikowania do 9.11.2018 r. tzw. operatorów kluczowych (mających jednostkę organizacyjną na terytorium ich państwa – art. 5 ust. 1 dyrektywy NIS) oraz określenia obowiązków związanych z zapewnieniem bezpieczeństwa cybernetycznego, jakie owe podmioty muszą spełnić. Dyrektywa NIS jako operatorów usług kluczowych kwalifikuje podmiot publiczny lub prywatny należący do jednego z następujących sektorów, tj. energetyki, transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucję, infrastruktury cyfrowej, i który to podmiot świadczy usługę mającą kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, świadczenie tej usługi zależy od sieci i systemów informatycznych oraz incydent miałby istotny skutek zakłócający dla świadczenia tej usługi (art. 4 pkt 4 dyrektywy NIS). Innymi słowy, jak wynika z powyższego, dostawcy usług dla ochrony zdrowia, w tym ci obsługujący rozwiązania chmurowe, będą musieli być wskazani przez państwo[35].

Do polskiego systemu prawnego dyrektywa NIS została implementowana przepisami ustawy z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa[36], której to przepisy obowiązują od 28.8.2018 r., przy czym wskazać należy, iż zgodnie z samą dyrektywą NIS państwa członkowskie zobowiązane zostały do 9.5.2018 r. przyjąć i opublikować przepisy ustawo-

[31] Dokumentację prowadzoną w postaci elektronicznej – w myśl § 1 pkt 4 DokMedR uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki: 1) jest zapewniona jej dostępność wyłącznie dla osób uprawnionych, o których mowa w art. 24 ust. 2 i art. 26 PrPacjentU oraz innych przepisach prawa powszechnie obowiązującego; 2) są zastosowane metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

[32] Zgodnie z pkt 5 § 1 DokMedR zabezpieczenie dokumentacji wymaga w szczególności: 1) systematycznego szacowania ryzyka zagrożeń oraz zarządzania tym ryzykiem; 2) opracowania i stosowania udokumentowanych procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania; 3) stosowania środków bezpieczeństwa adekwatnych do zagrożeń, uwzględniających najnowszy stan wiedzy; 4) dbałości o aktualizację oprogramowania; 5) bieżącego kontrolowania funkcjonowania organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia, a także okresowego dokonywania oceny skuteczności tych sposobów; 6) przygotowania i realizacji planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

[33] Zob. więcej na temat obowiązków dostawcy usług *cloud computing* jako przetwarzającego dane: *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, Warszawa 2018, s. 441 i n.

[34] Dz.Urz. UE L Nr 194, s. 2; dalej jako: dyrektywa NIS.

[35] *A. Romaszewski*, *W. Trąbka*, *M. Kielar*, *K. Gajda*, Elektroniczna dokumentacja medyczna – przetwarzanie danych o stanie zdrowia poza miejscem świadczenia usług zdrowotnych..., s. 18.

[36] T.j. Dz.U. z 2020 r. poz. 1369 ze zm.; dalej jako: KrajSysCyberU.

we, wykonawcze i administracyjne[37] niezbędne do wykonania tejże dyrektywy (art. 25 ust. 1 dyrektywy NIS).

W przedmiotowej ustawie wskazano, iż będzie ona określać organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy, a także zakres oraz tryb stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. W tym kontekście wątpliwości nie może więc budzić fakt, że w przedmiotowej regulacji kluczowym pojęciem jest to dotyczące cyberbezpieczeństwa, przez które rozumieć należy – jak to ujęto w art. 2 pkt 4 KrajSysCyberU – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność, autentyczność i dostępność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Ponadto w art. 5 ust. 1 na wzór tego obowiązującego na gruncie dyrektywy NIS dookreślono pojęcie operatora usługi kluczowej jako podmiotu, o którym mowa w załączniku nr 1 do ustawy, posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do ustawy.

Usługę kluczową zdefiniowano natomiast jako usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych (art. 2 pkt 16 KrajSysCyberU).

Co istotne z punktu widzenia podjętej w niniejszym opracowania analizy, w załączniku nr 2 do KrajSysCyberU zdefiniowano także pojęcie usługi przetwarzania w chmurze, tj. jako usługi umożliwiającej dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników oraz – w art. 2 pkt 15 – usługi cyfrowej, tj. jako usługi świadczonej drogą elektroniczną w rozumieniu ustawy z 18.7.2002 r. o świadczeniu usług drogą elektroniczną[38] wymienioną w załączniku nr 2 KrajSysCyberU, a więc internetową platformą handlową, usługą przetwarzania w chmurze, wyszukiwarką internetową.

Odnosząc się jednak w pierwszej kolejności do podmiotów świadczących usługi w sektorze ochrony zdrowia, wskazać należy, iż w analizowanym tekście KrajSysCyberU jako operatorów usługi kluczowej należących do wspomnianego sektora wyodrębniono m.in.[39] podmiot leczniczy, o którym mowa w art. 4 ust. 1 DziałLeczU[40].

To więc na tych podmiotach leczniczych, wobec których właściwy organ wyda decyzję o uznaniu ich za operatów usług kluczowych, ciążyć będzie obowiązek spełnienia wielu wymogów określonych przepisami KrajSysCyberU, które sprowadzać będą się m.in. do:

1) prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem,
2) wdrożenia odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
   a) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
   b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
   c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
   d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,

[37] Ponadto funkcjonuje dokument w postaci Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, który to jest krajową strategią w zakresie bezpieczeństwa systemów teleinformatycznych w rozumieniu Dyrektywy NIS, zob. Ministerstwo Cyfryzacji, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, https://www.gov.pl/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022 (dostęp z 27.12.2017 r.).

[38] T.j. Dz. U. z 2017 r. poz. 1219 ze zm.

[39] Ponadto załącznik Nr 1 KrajSysCyberU obejmuje takie podmioty wchodzące w sektor ochrony zdrowia, jak: jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia; Narodowy Fundusz Zdrowia, podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z 6.9.2001 r. – Prawo farmaceutyczne (t.j. Dz.U. z 2017 r. poz. 2211 ze zm.); podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu prawa farmaceutycznego; przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu prawa farmaceutycznego; przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim UE lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego; importer produktu leczniczego/substancji czynnej w rozumieniu prawa farmaceutycznego; wytwórca produktu leczniczego/substancji czynnej w rozumieniu prawa farmaceutycznego; importer równoległy w rozumieniu prawa farmaceutycznego; dystrybutor substancji czynnej w rozumieniu prawa farmaceutycznego prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu prawa farmaceutycznego.

[40] Tj.: 1) przedsiębiorcy w rozumieniu przepisów ustawy z 6.3.2018 r. – Prawo przedsiębiorców (t.j. Dz.U. z 2019 r. poz. 1292 ze zm.) we wszelkich formach przewidzianych dla wykonywania działalności gospodarczej, jeżeli ustawa nie stanowi inaczej, 2) samodzielne publiczne zakłady opieki zdrowotnej, 3) jednostki budżetowe, w tym państwowe jednostki budżetowe tworzone i nadzorowane przez Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, Ministra Sprawiedliwości lub Szefa Agencji Bezpieczeństwa Wewnętrznego, posiadające w strukturze organizacyjnej ambulatorium, ambulatorium z izbą chorych lub lekarza podstawowej opieki zdrowotnej, 4) pielęgniarkę podstawowej opieki zdrowotnej lub położną podstawowej opieki zdrowotnej w rozumieniu przepisów ustawy z 27.10.2017 r. o podstawowej opiece zdrowotnej (t.j. Dz.U. z 2020 r. poz. 172 ze zm.), 5) instytuty badawcze, o których mowa w art. 3 ustawy z 30.4.2010 r. o instytutach badawczych (t.j. Dz.U. z 2020 r. poz. 1383), 5a) fundacje i stowarzyszenia, których celem statutowym jest wykonywanie zadań w zakresie ochrony zdrowia i których statut dopuszcza prowadzenie działalności leczniczej, posiadające osobowość prawną jednostki organizacyjne stowarzyszeń, o których mowa w pkt 5, 6) osoby prawne i jednostki organizacyjne działające na podstawie przepisów o stosunku Państwa do Kościoła Katolickiego w Rzeczypospolitej Polskiej, o stosunku Państwa do innych kościołów i związków wyznaniowych oraz o gwarancjach wolności sumienia i wyznania, 7) jednostki wojskowe – w zakresie w jakim wykonują działalność leczniczą (art. 4 ust. 1 DziałLeczU).

e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

3) zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
4) zarządzania incydentami;
5) stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
   a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
   b) dbałość o aktualizację oprogramowania,
   c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
   d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa (art. 8 KrajSysCyberU).

W odniesieniu do dostawców usług cyfrowych ustawa o krajowym systemie cyberbezpieczeństwa zakłada, że również i oni będą odpowiedzialni za zapewnienie cyberbezpieczeństwa świadczonych przez nich usług[41]. I choć z całą pewnością na podstawie regulacji przedmiotowej ustawy obowiązki dla dostawców usług cyfrowych będą objęte łagodniejszym reżimem[42], niemniej jednak wskazać jeszcze należy, że ich działalność objęta będzie regulacją rozporządzenia wykonawczego Komisji Europejskiej (UE) 2018/151 z 30.1.2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącym ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ[43], i które to rozporządzenie precyzuje, jakie środki techniczne i organizacyjne powinien podjąć dostawca usług cyfrowych, aby zapewnić bezpieczeństwo systemów teleinformatycznych służących do świadczenia usług cyfrowych.

Z punktu widzenia omawianego tematu zasadniczą kwestią pozostaje jednak ustalenie, że mocą przepisów dyrektywy NIS i będącej jej implementacją KrajSysCyberU nałożonych zostanie wiele obowiązków i to zarówno na podmioty lecznicze działające w sektorze ochrony zdrowia (w tym również na te przetwarzające dokumentację medyczną na bazie technologii *cloud computing*), jak i samych dostawców usług chmury obliczeniowej (także tych świadczących usługi w sektorze ochrony zdrowia).

Podsumowanie

Uwzględniając dotychczasowe ustalenia co do szerokiego zakresu obowiązków nałożonych na podmioty, które to przetwarzają dokumentację medyczną w postaci elektronicznej, zupełnie nie może dziwić fakt, iż znakomita większość świadczeniodawców, poradni podstawowej opieki zdrowotnej, gabinetów specjalistycznych, grupowych poradni lekarskich, pielęgniarskich czy rehabilitacyjnych, nie jest i nie będzie w stanie w najbliższej przyszłości sprostać tymże wymaganiom[44]. Stąd też dla części z nich remedium stanowić będzie bądź już obecnie stanowi właśnie technologia chmury obliczeniowej, niwelująca jednocześnie konieczność tworzenia i utrzymywania lokalnego ośrodka komputerowego, tworzenia specjalistycznych sieci transmisji danych czy zatrudniania wysoko wyspecjalizowanego personelu IT[45]. Z tego też względu wykorzystywanie usług podmiotów zewnętrznych, w szczególności dostawców usług *cloud computing*, przestało być w sektorze ochrony zdrowia nowością, a powoli staje się standardowym sposobem prowadzenia dokumentacji medycznej, czego doskonałym potwierdzeniem zdaje się być analiza rynku usług opieki zdrowotnej i możliwe do wskazania szerokie spektrum przykładów obejmujących współpracę zarówno na linii publicznej, jak i prywatnej opieki zdrowotnej z dostawcami usług medycznych.

W zakresie pierwszej z nich wskazać więc można zarówno na jednostkowe przykłady, tj. na współpracę, jaka

[41] W związku z tym zobowiązani będą oni m.in. podjąć właściwe i proporcjonalne środki techniczne i organizacyjne określone w rozporządzeniu wykonawczym 2018/151 w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te zapewniają cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniają: 1) bezpieczeństwo systemów informacyjnych i obiektów; 2) postępowanie w przypadku obsługi incydentu; 3) zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej; 4) monitorowanie, audyt i testowanie; 5) najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2018/151 (art. 17 ust. 2 KrajSysCyberU). Dostawca usługi cyfrowej podejmuje środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi (art. 17 ust. 3 KrajSysCyberU). Ponadto ustawodawca nałożył na dostawców usług cyfrowych m.in. obowiązki związane z identyfikowaniem incydentów oraz ich zgłaszaniem (art. 18 ust. 1 KrajSysCyberU) do CSIRT NASK i in.

[42] Szerzej o zakresie obowiązków dostawców usług cyfrowych na gruncie przepisów ustawy o krajowym systemie cyberbezpieczeństwa w rozdziale 4 KrajSysCyberU.

[43] Dz.Urz. UE L Nr 26, s. 48.

[44] *A. Romaszewski*, *W. Trąbka*, *M. Kielar*, *K. Gajda*, Elektroniczna dokumentacja medyczna – przetwarzanie danych o stanie zdrowia poza miejscem świadczenia usług zdrowotnych..., s. 16.

[45] Podkreślenia wymaga fakt, że implementacja elektronicznej dokumentacji medycznej, w tym także tej opartej na technologii *cloud computing*, przynosi nie tylko potencjalne zagrożenia i konieczność sprostania wielu wymaganiom, ale też niesie z sobą wiele korzyści, i to dla wielu uczestników ochrony zdrowia: tj. pacjentów, personelu medycznego, menadżerów placówek zdrowia, płatnika, a także całego systemu ochrony zdrowia. Zob. *D.M Szymczyk*, *A. Horoch*, Implementacja elektronicznej dokumentacji medycznej. Część 2 – korzyści dla uczestników systemu ochrony zdrowia, Medycyna Ogólna i Nauki o Zdrowiu, 2013, t. 19, Nr 3, s. 324–330.

nastąpiła do 2014 r. na linii między ePUAP[46] a Comarch, czy na współpracę na linii między Szpitalem Klinicznym Przemienienia Pańskiego Uniwersytetu Medycznego w Poznaniu a firmą Rightsoft Sp. z o.o.[47], jak też szerzej na przykłady dotyczące regionalnych projektów zrealizowanych w zakresie e-zdrowia w poszczególnych województwach[48].

Powszechnym zjawiskiem jest również korzystanie z podmiotów prywatnych oferujących opiekę zdrowotną z technologii chmury obliczeniowej udostępnianej chociażby przez takich dostawców, jak np. Microsoft[49].

[46] ePUAP, czyli Elektroniczna Platforma Usług Administracji Publicznej, to ogólnopolska platforma teleinformatyczna służąca do komunikacji obywateli z jednostkami administracji publicznej w ujednolicony, standardowy sposób. Umożliwia ona także komunikację między sobą podmiotom administracji publicznej. Po raz pierwszy ePUAP uruchomiony został 14.4.2008 r., natomiast 17.8.2015 r. został uruchomiony tzw. EPUAP2. Zarządzaniem platformą zajmuje się obecnie Centrum Projektów Informatycznych (CPI), https://www.gov.pl/cyfryzacja/serwis-epuap (dostęp z 17.12.2017 r.).

[47] Rightsoft Sp. z o.o. 28.9.2015 r. podpisała umowę ze Szpitalem Klinicznym Przemienienia Pańskiego UM w Poznaniu, na mocy której rozpoczęła wdrożenie Elektronicznej Dokumentacji Medycznej, https://www.systemeskulap.pl/wdrozenie-elektronicznej-dokumentacji-medycznej/ (dostęp z 19.12.2017 r.).

[48] Szerzej zob. *G. Fiuk*, Doświadczenia z realizacji regionalnych projektów e-zdrowie w Polsce – wyzwania, bariery, problemy, korzyści i rekomendacje, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), E-obywatel, E-sprawiedliwość, E-usługi, Warszawa 2017, s. 57–66.

[49] Zob. więcej Microsoft, Nowe możliwości w ochronie zdrowia, *www.houseofcloud.pl/wp-content/uploads/2017/.../Raport-Microsoft-dla-Zdrowia.pdf* (dostęp z 19.12.2017 r.).

Słowa kluczowe: *cloud computing*, dane osobowe, dane dotyczące zdrowia, elektroniczna dokumentacja medyczna, RODO, dyrektywa NIS.

Legal aspects of using cloud computing technology in the area of healthcare

The purpose of the present article is an attempt to answer the question regarding legal implications of using cloud computing technology in the area of healthcare, specifically the possibility to process data regarding health within electronic medical record which is present in such information systems as cloud computing. Therefore, the main background of deliberations are regulations of the European Parliament and the Council of 27 April 2016, on protection of natural persons in regard to processing of personal data and free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), and also – on a smaller scale – regulations of Directive of the European Parliament and the Council 2016/1148 of 6 July 2016, regarding resources for a high and common level of security of the Web and information systems within the EU, and regulations of Polish law amended on that basis.

Keywords: cloud computing, personal data, health data, electronic health record, GDPR, Network and Information Systems Directive.

Umowa w przedmiocie współadministrowania danymi osobowymi

r.pr. *Anna Popowicz-Pazdej*[1]

Współadministrowanie danymi osobowymi jest instytucją, która została pierwszy raz wyraźnie uregulowana w ramach rozporządzenia Parlamentu Europejskiego i Rady (UE) 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/WE (ogólne rozporządzenie o ochronie danych[2] zobowiązuje państwa członkowskie do podjęcia odpowiednich czynności w zakresie współadministrowania). Jeżeli dojdzie do zidentyfikowania takiej relacji współadministratorzy powinni m.in. uregulować wspólne uzgodnienia oraz udostępnić ich zasadniczą część. Przy czym RODO nie wskazuje ani formy, ani szczegółowych wytycznych w tym zakresie. Niniejszy artykuł ma zatem na celu zidentyfikowanie relacji współadministracji, a także analizę elementów określonych w ramach wspólnych uzgodnień dokonywanych pomiędzy współadministratorami. Poza elementami obligatoryjnymi w artykule znalazły się także propozycje elementów fakultatywnych wspomagających wywiązanie się współadministratorów z zasady rozliczalności.

Uwagi wstępne

W ramach RODO została po raz pierwszy uregulowana instytucja współadministrowania danymi osobowymi. Jak się okazało, w rzeczywistości zwykłe rozróżnienie pomiędzy administratorem danych osobowych a wykonawcą ujawniło się jako niewystarczające[3]. Nie obejmowało bowiem sytuacji, w których kilka podmiotów działa wspólnie w ramach przetwarzania danych osobowych[4].

Poprzednio obowiązująca unijna dyrektywa 95/46/WE nie zawierała pojęcia współadministrowania, niemniej jednak koncepcję tę można było wywnioskować z szerokiej interpretacji pojęcia administratora. Także poprzednio obowiązująca ustawa z 29.8.1997 r. o ochronie danych osobowych[5] nie zawierała definicji współadministracji. W praktyce można było jednak ją wyinterpretować także z rozszerzonej definicji administratora danych. Taka interpretacja była aprobowana także w doktrynie. Zgodnie z jej poglądami możliwa jest sytuacja, w której z jednego zbioru danych osobowych administratorzy korzystają na równych prawach. Każdy jednak przetwarza te dane do własnych celów, mając jednocześnie wpływ na cel i sposób przetwarzania danych osobowych, ich treść, możliwość uzupełniania zbioru oraz wykorzystywania zawartych w nim danych[6]. Koncepcja współadministrowania nie jest zatem całkowicie nowa.

Pojęcie współadministrowania danymi osobowymi w RODO

W ramach RODO instytucja współadministrowania została uregulowana w art. 26. Zgodnie z treścią tego przepisu do współadministrowania dochodzi w sytuacji, gdy co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania. Dodatkowo sama definicja administratora z art. 4 pkt 7 RODO uwzględnia także sytuacje współadministrowania[7]. To wyraźne uregulowanie kwestii współadministrowania ma na celu zapewnienie nie tylko ogólnej zgodności z przepisami rozporządzenia w zgodzie z zasadą rozliczalności, zgodności z zasadami przetwarzania (art. 5 RODO), ale przede wszystkim zapewnienia odpowiednich praw osobom, których dane dotyczą, w tym potrzeby pełnej kompensacji powstałej szkody w wyniku przetwarzania niezgodnego z prawem.

Aby to osiągnąć, w art. 26 zostały wskazane wytyczne co do zdefiniowania zakresu odpowiedzialności w ramach wspólnych uzgodnień. RODO nie wskazuje jednak konkretnych wytycznych co do kształtu czy też zakresu tych uzgodnień. Niezbędne jest zatem przeanalizowanie zarówno

[1] Studentka II roku Doktoranckich Studiów Stacjonarnych Prawa Na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

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

[3] Por. Opinia Europejskiego Inspektora Ochrony danych z 7.11.2019 r. dotycząca koncepcji administratora, procesora oraz współadministrowania danymi osobowymi, https://edps.europa.eu/sites/edp/files/publication/19-11. 07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf, s. 22–23 (dostęp z 30.8.2020 r.).

[4] Por. Opinia Grupy Roboczej art. 29 (WP29) 1/2010 z 16.2.2010 dotycząca koncepcji administratora oraz procesora, dostępna na stronie internetowej: https://archiwum.giodo.gov.pl/pl/1520057/3595, s. 18 (dostęp z 31.8.2020 r.).

[5] Ustawa z 29.8.1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883 ze zm.).

[6] Por. *A. Mednis*, Administrator danych i podmiot przetwarzający dane na zlecenie – status prawny, zakres praw i obowiązków, problemy definicyjne, [w:] *G. Szpor* (red), Ochrona danych osobowych, Warszawa 2009, s. 79. Por. podobnie *K. Witkowska-Nowakowska*, [w:] *D. Lubasz*, *E. Bielak-Jomaa* (red.), Komentarz do ogólnego rozporządzenia o ochronie danych, Warszawa 2018, s. 614.

[7] Zgodnie z treścią przepisu art. 4 pkt 7 RODO, administrator danych to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

elementów obligatoryjnych tych uzgodnień, jak i elementów fakultatywnych, które mogą wpłynąć na lepsze zabezpieczenie interesów administratorów w ramach wspólnej współpracy. W konsekwencji dojdzie także do wykazania spełnienia zasady rozliczalności[8]. Na początku konieczne jest jednak ustalenie, kiedy faktycznie mamy do czynienia ze współadministrowaniem danymi osobowymi.

Przesłanki występowania współadministrowania danymi osobowymi

Do współadministrowania danymi osobowymi dochodzi w przypadku choćby potencjalnej możliwości lub prawa decydowania o celach lub sposobach przetwarzania danych osobowych[9]. Stąd też, aby można było wskazywać na istnienie w konkretnym przypadku relacji współadministracji, konieczne jest kumulatywne spełnienie dwóch warunków: po pierwsze – w takiej relacji pozostawać musi co najmniej dwóch administratorów, po drugie – administratorzy ci muszą wspólnie ustalać cele i sposoby przetwarzania. Dla stwierdzenia współadministrowania oraz przyznania poszczególnym administratorom statusu „współadministratora" nie wystarcza zatem, by pozostawali oni w jakiejkolwiek relacji związanej z przetwarzaniem danych osobowych. Ich relacja bowiem nacechowana być musi współdziałaniem przy ustalaniu celów i sposobów przetwarzania[10].

Sytuację tę najlepiej obrazuje ostatnie orzeczenie TS z 5.6.2018 r. w sprawie Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH[11], dotyczące przetwarzania danych przez portal społecznościowy Facebook oraz właściciela fanpage'a utworzonego za pomocą narzędzi udostępnionych przez Facebooka. Oba podmioty w świetle powyższego zostały uznane za współadministratorów danych osobowych.

Nie ulega wątpliwości, że administratorem danych w tym przypadku jest Facebook, jako platforma przetwarzająca pliki cookies instalowane na komputerze użytkownika fanpage'a. Natomiast właściciel fanpage'a został uznany za administratora, ponieważ również może otrzymywać anonimowe statystyczne informacje dotyczące osób odwiedzających fanpage, które w powiązaniu z innymi danymi połączenia stanowią dane osobowe. W tym kontekście Trybunał podniósł, że utworzenie fanpage'a na Facebooku wiąże się z podjęciem przez jego administratora działań polegających na ustaleniu parametrów zależnych w szczególności od jego użytkowników docelowych, jak również od celów w zakresie zarządzania lub promocji jego działalności, co wpływa na przetwarzanie danych osobowych na potrzeby statystyk sporządzonych na podstawie liczby odwiedzających fanpage'a. Administrator ten może za pomocą filtrów udostępnionych przez Facebooka zdefiniować kryteria, na podstawie których statystyki te muszą być sporządzane, a nawet określić kategorie osób, których dane osobowe będą wykorzystywane przez Facebooka[12]. Fanpage natomiast jest stroną, która może być założona zarówno przez użytkowników indywidualnych, jak i biznesowych. W tym celu po zarejestrowaniu się na Facebooku właściciel fanpage'a może wykorzystywać go do zaprezentowania się użytkownikom tego portalu społecznościowego, jak również osobom odwiedzającym fanpage'a. Jest także uprawniony do zamieszczania informacji wszelkiego rodzaju na rynku mediów i poglądów. Wtedy jest także uprawniony automatycznie do otrzymania za pośrednictwem funkcji „Facebook Insights" anonimowych informacji statystycznych o użytkownikach fanpage'a. Dane te są gromadzone dzięki plikom cookies, z których każdy zawiera przypisany kod użytkownika. Są one aktywne przez dwa lata i zapisywane przez Facebooka na twardym dysku komputera lub na każdym innym nośniku osób odwiedzających fanpage'a. Kod użytkownika można następnie powiązać z danymi połączenia użytkowników zarejestrowanych na Facebooku. Zostaje on automatycznie pobrany i przetworzony w chwili otwarcia fanpage'ów[13]. W takiej sytuacji zatem możliwe jest zidentyfikowanie takiego użytkownika, a więc dochodzi do przetwarzania danych osobowych przez właściciela fanpage'a. Otrzymywanie tych informacji jest automatyczne w tym sensie, że nie jest możliwe wyłączenie ich otrzymywania. Chociaż decyzja odnośnie do sposobów przetwarzania należy do Facebooka, sama możliwość umieszczenia przez Facebooka plików cookies, do których dostęp ma właściciel fanpage'a, sprawia, że jest on w tym zakresie współodpowiedzialny za takie przetwarzanie[14].

[8] Por. art. 5 ust. 2 RODO.

[9] Por. Opinia Europejskiego Inspektora Ochrony Danych z 7.11.2019 r. dotycząca koncepcji administratora, procesora oraz współadministrowania danymi osobowymi, https://edps.europa.eu/sites/edp/files/publication/19-11 07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf, s. 23 (dostęp z 30.8.2020 r.). Jako przykłady współadministrowania wskazuje się współadministrowanie w grupach kapitałowych, gdy spółki wspólnie zarządzają talentami, w relacjach pomiędzy agencjami ubezpieczeń i ubezpieczycielami, a także przy bancassurance (sprzedaży ubezpieczeń przez banki), tak: *M. Gawroński*, RODO. Przewodnik ze wzorami, Warszawa 2018, s. 160.

[10] *M. Sakowska-Baryła*, Komentarz do art. 26 RODO, Legalis/el. 2018.

[11] Zob. wyrok TSUE z 5.6.2018 r., C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* przeciwko *Wirtschaftsakademie Schleswig-Holstein GmbH*, Legalis.

[12] *Ibidem*, pkt 36.

[13] Por. pkt 15 wyroku TSUE z 5.6.2018 r., C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* przeciwko *Wirtschaftsakademie Schleswig-Holstein GmbH*, Legalis.

[14] Podobne stanowisko zostało zaprezentowane w Opinii Grupy Roboczej Art. 29 (ang. *Article 29 Working Party's Opinion 5/2009 on online social networking*, przyjętej 12.6.2009 r., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf (dostęp z 30.8.2020 r.). Użytkownicy portali społecznościowych ściągający dane dotyczące osób trzecich mogą być uznani za administratorów, pod warunkiem że nie odbywa się to w zakresie wyjątku dotyczącego korzystania dla własnych celów (ang. *household exception*).

Z powyższego orzeczenia można wysnuć kilka wniosków. Po pierwsze, co od dawna nie jest kwestionowane, do współadministrowania może dojść niezależnie od faktycznego dostępu do danych osobowych przez obu (lub więcej) współadministratorów[15]. W tym zakresie wystarczający jest sam potencjalny dostęp do danych osobowych. Po drugie, samo prawo lub możliwość wpływania na cele i sposoby przetwarzania kwalifikuje dany podmiot jako administratora (lub współadministratora). Po trzecie, odpowiedzialność współadministratora, który nie jest właścicielem całego procesu przetwarzanie ogranicza się jedynie do zakresu, za który jest odpowiedzialny (ma wpływ)[16]. Oznacza to, że administrator może zwolnić się z tego zakresu odpowiedzialności, wobec którego jest w stanie wykazać, że w żaden sposób nie może być odpowiedzialny za tę szkodę[17]. Po czwarte, odpowiedzialność ta może być następnie limitowana w odniesieniu do konkretnego stanu faktycznego. Jest to zasada ogólna dotycząca odpowiedzialności ponoszonej na gruncie RODO. W tym zakresie jakiekolwiek wyłączenie z odpowiedzialności będzie wymagało wykazania przez danego współadministratora, że zastosował wszelkie możliwe środki, aby zapobiec szkodliwemu zdarzeniu. Z tego też względu nie będzie wystarczający dowód, że nie został naruszony jakikolwiek przepis prawa lub innych regulacji[18]. Oznacza to, że w pierwszej kolejności odpowiedzialność ta jest solidarna, przy czym nie jest wyłączona możliwość późniejszego dochodzenia zwrotnego odszkodowania w zależności od poziomu zawinienia. Po piąte, definicja współadminsitratora jest szeroka. Nie oznacza to jednak, zgodnie z opinią Rzecznika Generalnego *M. Bobka, ż*e instytucja współadministracji powinna być odnoszona do przetwarzania w ogólności. Powinno się ją bowiem interpretować w odniesieniu do czynności przetwarzania[19].

Powyższy wniosek jest bardzo istotny, ponieważ potwierdza, że również w stosunku do współadministratorów należy stosować zasady odpowiedzialności oparte na limitowaniu odpowiedzialności. Chociaż wobec osób, których dane dotyczą, taki współadministrator będzie odpowiadał za całość szkody, to jednak na zasadach roszczenia zwrotnego będzie on mógł domagać się zwrotu w części, w której nie ponosi odpowiedzialności w odniesieniu do konkretnej czynności przetwarzania. To zaś oznacza, że każdą sytuację faktyczną należy podzielić na konkretne czynności przetwarzania, jeśli to możliwe. Następnie w stosunku do każdej z nich ustalać, czy występuje stosunek współadministrowania. Stąd też np. jedynie wspólne korzystanie z oprogramowania nie będzie świadczyło o występowaniu współadministrowania.

Obowiązki ciążące na współadministratorach danych osobowych. Elementy obligatoryjne umowy o współadministrowaniu danymi osobowymi

Uznanie danych podmiotów za współadministratorów nakłada na nich obowiązek ustalenia wspólnych uzgodnień określających ramy współpracy w ramach wspólnego przetwarzania danych osobowych. W treści przepisu brak wytycznych co do formy zawarcia takich wspólnych uzgodnień. Nie ulega wątpliwości, iż wspólne uzgodnienia będą wywoływały skutki prawne umowy. Mogą zatem przybrać postać umowy[20]. Co do formy tej umowy pomiędzy współadministratorami brak jest wytycznych w treści art. 26 RODO. Z ust. 2 zd. 2 tego przepisu wynika jedynie, że zasadnicza część uzgodnień powinna mieć sformalizowaną formę, ponieważ powinna zostać udostępniona osobom, których dane dotyczą[21]. Zarówno zatem ta część zasadniczych uzgodnień, jak i całe porozumienie może być zawarte w dowolnej formie dla celów dowodowych. Dalsze szczegóły co do formy powinny być dokonane przez

[15] Por. wyroki TSUE: z 10.7.2018 r., C-25/17, *Tietosuojavaltuutettu* przy udziale Jahovan todistajat, Legalis oraz z 5.6.2018 r., C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* przeciwko *Wirtschaftsakademie Schleswig-Holstein GmbH,* Legalis, pkt 43.

[16] Niemiecka doktryna rozróżnia w tym zakresie dwie formy współadministrowania: pełne i częściowe współadministrowanie.

[17] Por. motyw 146 RODO, zgodnie z treścią którego: „Jeżeli administratorzy lub podmioty przetwarzające uczestniczą w tym samym przetwarzaniu, każdy administrator lub podmiot przetwarzający powinien odpowiadać prawnie za całość szkody. Jeżeli jednak zostaną włączeni do jednego postępowania sądowego zgodnie z prawem państwa członkowskiego, odszkodowaniem można obarczyć każdego z administratorów i każdy z podmiotów przetwarzających stosownie do ich winy za szkodę wynikłą z przetwarzania, o ile osobie, której dane dotyczą, zapewnione zostanie pełne i skuteczne odszkodowanie za poniesioną szkodę. Każdy administrator lub podmiot przetwarzający, który wypłacił pełne odszkodowanie, może następnie dochodzić roszczeń regresowych wobec innych administratorów lub podmiotów przetwarzających uczestniczących w tym samym przetwarzaniu" oraz wyrok TSUE z 29.7.2019 r., C-40/17, *Fashion ID GmbH & Co. KG* przeciwko *Verbraucherzentrale NRW eV*, Legalis.

[18] Por. *V. Colcelli*, Joint controller agreement under GDPR, Conference Paper, June 2019, s. 1041.

[19] Por. Opinia Rzecznika Generalnego *M. Bobka* do wyroku TSUE z 29.7.2019 r., C-40/17, Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW eV, Legalis – http://curia.europa.eu/juris/liste.jsf?num=C-40/17# (dostęp z 30.8.2019 r.).

[20] Załącznikiem do tej umowy mogą być Warunki Świadczenia Usług (ang. SLA – *Service Level Agreement*), zawierające specyfikacje techniczne takiego przetwarzania.

[21] W praktyce może zostać udostępniona na stronie internetowej w ramach tam umieszczonych klauzul informacyjnych lub polityki prywatności. Sugestię jednak co do umieszczenia tych informacji w ramach klauzuli informacyjnej wyraził Europejski Inspektor Ochrony Danych w treści Opinii z 7.11.2019 r. dotyczącej koncepcji administratora, procesora oraz współadministrowania danymi osobowymi, s. 29 oraz Angielski Urząd Ochrony Danych Osobowych, (ang. *Information Commissioners Office* – ICO) w informacji odnośnie do współadministracji – https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/ (dostęp z 31.8.2020 r.).

pryzmat innych przepisów RODO. Warto zatem zaczerpnąć rozwiązań, korzystając choćby z rozwiązań umowy powierzenia, a więc zastosować formę pisemną, w tym elektroniczną[22]. Forma pisemna do celów dowodowych tej umowy polega bowiem na możliwości udowodnienia przez danego współadministratora treści takiego porozumienia, zgodnie z zasadą rozliczalności z art. 5 ust. 2 RODO.

Z kolei w odniesieniu do wspomnianej wyżej „zasadniczej treści uzgodnień" w doktrynie niemieckiej wskazuje się, że sformułowanie „zasadnicze" obejmuje właśnie podział obowiązków łącznie ze wskazaniem ich realizacji w odniesieniu do osób, których dane dotyczą, obowiązki prawne, jak też wyznaczenie punktu kontaktowego[23]. Od zasadniczej treści uzgodnień należy odróżnić obligatoryjne elementy umowy wskazane w treści przepisu art. 26 RODO, które powinny zostać uregulowane pomiędzy stronami umowy o współadministrowaniu danymi osobowymi. Do obligatoryjnych elementów umowy art. 26 RODO zalicza znacznie szerszy katalog obejmujący: obowiązek ustalenia odpowiednich praw i obowiązków w zgodności z obowiązkami wynikającymi z RODO, odzwierciedlenie odpowiednich ról i odpowiedzialności w odniesieniu do osób, których dane dotyczą, zapewnienie ochrony praw i wolności osób, których dane dotyczą, wyznaczenia punktu kontaktowego, przejrzysty podział obowiązków pomiędzy administratorami oraz pomiędzy ich procesorami[24].

Koncepcja zastosowania konstrukcji klauzul z umowy powierzenia do umowy o współadministrowaniu danymi osobowymi. Elementy fakultatywne umowy o współadministrowaniu

Powyższe obowiązki współadministratorów są zbliżone do obowiązków zawartych w art. 28 RODO w odniesieniu do umowy powierzenia przetwarzania danych osobowych. Także cel umowy powierzenia oraz umowy o współadministracji jest zbliżony. Głównym celem obu instytucji jest takie uregulowanie relacji przetwarzania przez więcej niż jeden podmiot, aby odpowiednio zabezpieczyć prawa osób, których dane dotyczą. Obie instytucje w praktyce różnią się tym, w jaki sposób dochodzi do rozkładu kontroli nad ustaleniem celów i sposobów przetwarzania.

Nie sposób zatem nie zauważyć, że relacja współadministracji w swojej konstrukcji zakłada działanie dwóch odrębnych administratorów, którzy ze względu na wspólne działania są zobowiązani do uregulowania swojego stosunku prawnego w taki sposób, aby spełnić wymagania RODO wspólnie. Konsekwencją nieprawidłowego współdziałania jest ich odpowiedzialność za całość poniesionej szkody. Dlatego też powinni być zainteresowani w takim uregulowaniu swojego stosunku, by móc wykazać przestrzeganie zasady rozliczalności, tak jakby sami dokonywali danej czynności przetwarzania. Także z perspektywy osoby, której dane dotyczą, są traktowani jako jeden administrator zobowiązany do przestrzegania przepisów RODO. W razie naruszenia osoba, której dane dotyczą, może zwrócić się do któregokolwiek z administratorów, niezależnie od wskazania przez nich w ramach uzgodnień punktu kontaktowego. Natomiast koncepcja powierzenia przetwarzania danych osobowych zakłada, że podmiot powierzający działa w odniesieniu do danej czynności przetwarzania w imieniu administratora[25]. Musi on jednak wypełnić niektóre obowiązki lub zapewnić spełnienie pozostałych obowiązków związanych z przestrzeganiem RODO niejako „za niego". Podstawowa różnica zatem polega na tym, iż w stosunku powierzenia istnieją dwa podmioty, ale tylko jeden z nich pozostaje administratorem. Natomiast w stosunku współadministracji mamy do czynienia z dwoma osobnymi administratorami.

Kolejna różnica odnosi się do kwalifikacji prawnej umowy powierzenia oraz umowy o współadministracji na gruncie cywilnoprawnym. Ze względu na działanie przez podmiot powierzający jedynie w imieniu administratora w literaturze wykształconej na gruncie jeszcze poprzednio obowiązującej ustawy o ochronie danych osobowych[26] kwalifikowano umowę powierzenia jako postać umowy o świadczenie usług, do której odpowiednie zastosowanie znajdą przepisy Kodeksu cywilnego o zleceniu[27]. Z tej perspektywy podmiot powierzający traktowano jako dłużnika, natomiast administrator był w tej relacji wierzycielem. Natomiast w przypadku współadministracji należałoby uznać, że mamy analogicznie do czynienia albo z dwoma wierzycielami, ale zobowiązanymi do świadczenia pewnego rodzaju usług, albo z *quasi*-wspólnikami zobowiązanymi do działania w określonym celu. W związku z tym, w zależności od postanowień umowy można by kwalifikować ten stosunek jako bądź to dwustronną umowę zlecenia, bądź też stosunek *quasi-spółki*. Ta ostatnia kwalifikacja prawna byłaby o tyle właściwa, iż w ramach postanowień umowy spółki mamy realizację wspólnego celu, a odpowiedzialność wspólników za działania jest solidar-

[22] Por. art. 28 ust. 9 RODO.

[23] Por. *J. Hartung*, komentarz do art. 26, [w:] *J. Kühling*, *B. Buchner* (red.), Datenschutz – Grndverordnung/ BDSG, Warszawa 2017, pkt 26.

[24] Por. art. 26 RODO.

[25] Por. art. 28 RODO.

[26] Ustawa z 29.8.1997 r. o ochronie danych osobowych (Dz.U. z 1997 r., Nr 133, poz. 883).

[27] Tak: *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Komentarz do art. 28 ustawy o ochronie danych osobowych, Warszawa 2004, s. 619; podobnie *A. Drozd*, Komentarz do art. 28 ustawy o ochronie danych osobowych, Warszawa 2008, s. 197.

na[28]. Niemniej jednak odpowiednia kwalifikacja charakteru prawnego umowy o współadministracji wykracza znacznie poza ramy niniejszego opracowania. Co jest jednak ważne dla przedmiotowych rozważań, to zwrócenie uwagi na istotne różnice także pod względem charakteru prawnego pomiędzy umową powierzenia a umową o współadministracji.

Z tego względu instytucję powierzenia przetwarzania danych z art. 28 RODO należy stosować jedynie odpowiednio. Odpowiednie stosowanie przepisów prawa generalnie oznacza, że pewne przepisy ustanowione w swoim założeniu dla określonej grupy stosunków mogą być także stosowane w odniesieniu do innej grupy stosunków, przy czym – w zależności od rozmaitych uwarunkowań natury prawnej – mogą być one stosowane względem tej innej grupy stosunków bez żadnych zmian, z pewnymi zmianami albo też w ogóle nie mogą być stosowane[29].

W odniesieniu do art. 28 RODO, odnoszącego się do umowy powierzenia, nie będą na pewno stosowane postanowienia odnośnie do udokumentowanych poleceń administratora[30]. Nie ulega bowiem wątpliwości, że jest to obowiązek charakterystyczny dla stosunku powierzenia i działania przez podmiot powierzający w imieniu administratora. Kwestię wprowadzenia postanowień odnośnie do audytu także należy rozważyć w danym przypadku. Ponieważ jednak współadministratorzy są odrębnymi podmiotami zobowiązanymi samodzielnie do spełnienia obowiązków, z tego względu mogą zwyczajnie nie być skłonni do udostępnienia swoich pomieszczeń czy też dokumentacji[31]. Tym bardziej że przepisy prawa nie nakładają na nich wprost takiego obowiązku.

Z drugiej strony w ramach umowy o współadministracji mogą pojawić się postanowienia dodatkowe, które nie będą znajdowały się zwyczajowo w ramach umowy powierzenia. Do takich postanowień należy przykładowo kwestia przeprowadzania oceny skutków dla ochrony danych wywiedziona z art. 35 RODO. Zasadniczo ten obowiązek należy do administratora, podmiot przetwarzający może jedynie pomagać w jego wypełnieniu[32]. W stosunku współadministracji istnieje dwóch administratorów, którzy mogą być potencjalnie być zobowiązani do przeprowadzenia oceny skutków dla ochrony danych. W takich sytuacjach w ramach umowy o współadministracji należałoby uwzględnić rozkład obowiązków w tym zakresie pomiędzy współadministratorami.

W odniesieniu natomiast do pozostałych obowiązków wskazanych w art. 28 ust. 3 RODO – mogą one znaleźć zastosowanie wprost w tym znaczeniu, że mogą być pomocne w celu wykazania należytego przestrzegania RODO. A skoro prawodawca unijny w ramach umowy powierzenia uregulował tę relację bardziej szczegółowo, to w ramach umowy o współadministracji wskazane jest odpowiednie (z uwzględnieniem charakteru instytucji współadministracji) uregulowanie obowiązków do tych, które wynikają z umowy powierzenia.

Takie stanowisko zajmowane jest także w niemieckiej doktrynie[33]. Co istotne, dodatkowe elementy ponad te wskazane w art. 26 RODO będą fakultatywnymi elementami umowy o współadministracji, zabezpieczającymi jednak interes współadministratorów oraz osób, których dane dotyczą.

W związku z tym, w ramach wspólnych uzgodnień powinno dojść, po pierwsze, do dokładnego opisu całego procesu przetwarzania danych osobowych, w tym określenia celu, sposobów, okresu przetwarzania, kategorii danych objętych procesem[34]. Jest to o tyle istotne, że jak wyżej wskazano, w razie konieczności przypisania odpowiedzialności, istotne jest ustalenie, jaki jest rzeczywisty wpływ na przetwarzanie danych osobowych. Po drugie, w ramach takiej umowy powinno dojść do ogólnego opisu obowiązków każdego ze współadministratorów. Celem wyraźnego rozdziału obowiązków będzie możliwość potencjalnego zwrotnego dochodzenia odszkodowania w razie zaniedbania tych obowiązków. Pierwotna pozostaje odpowiedzialność wspólna współadminstratorów[35]. Jest to także warunek *sine qua non za*pewnienia należytej ochrony prawom i obowiązkom osób, których dane dotyczą[36]. Dodatkowo konieczne jest wskazanie, który ze współadministratorów i w jakim zakresie zapewnia odpowiednie udokumentowanie dla potrzeb wykazania zgodności przetwarzania z rozporządzeniem 2016/679.

W ramach takiej umowy powinno także dojść do wyraźnego uregulowania obowiązków w zakresie tzw. klauzul informacyjnych zgodnie z art. 13, 14 RODO oraz pozostałych obowiązków dotyczących udzielenia informacji podmiotom danych oraz realizacji praw osób, których dane dotyczą[37]. Co istotne, w odniesieniu do art. 13 RODO – informacje przekazywane przez współadministratorów powinny być przekazywane w trakcie przetwarzania danych osobowych. Natomiast w odniesieniu do klauzuli z art. 14 RODO – informacje te powinny być przekazywane najpóźniej w chwili ich otrzymania przez osoby, których dane dotyczą. W tym zakresie istotne jest też ustalenie odpowiedzialności za brak wypełnienia tych

[28] Chociaż w tym przypadku brak jest obowiązku wnoszenia jakichkolwiek wkładów.

[29] *J. Nowacki*, Odpowiednie stosowanie przepisów prawa, PiP 1964, z. 3, s. 367 i n.

[30] Por. art. 28 ust. 3 lit. a) RODO.

[31] Por. art. 28 ust. 3 lit. h) RODO.

[32] Por. art. 35 ust. 9 RODO.

[33] Por. podobnie *K. Witkowska-Nowakowska*, [w:] *D. Lubasz*, *E. Bielak-Jomaa* (red.), Komentarz do Ogólnego Rozporządzenia o Ochronie Danych, Warszawa 2018, s. 622.

[34] Por. art. 28 ust. 3 RODO.

[35] Por. *K. Witkowska-Nowakowska*, [w:] *D. Lubasz*, *E. Bielak-Jomaa* (red.), Komentarz…, s. 621.

[36] Por. motyw 79 RODO, zgodnie z treścią którego: „Ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna, administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach niniejszego rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora".

[37] W szczególności praw wynikających z art. 15 i 22 RODO.

obowiązków oraz powiązanych obowiązków z art. 24, 25, 32, 33, 34 i 35 RODO[38].

Ponadto w ramach umowy o współadministrowaniu danymi osobowymi powinny być zawarte informacje odnośnie do odpowiedzialności i zadań współadministratorów co do monitorowania oraz współpracy z organami nadzorczymi. Powyższa regulacja stanowi także wobec części doktryny podstawowy (obligatoryjny) element porozumienia. Celem jest odpowiednie zabezpieczenie praw osób, których dane dotyczą w razie wystąpienia naruszeń. Z tego też względu nie ma żadnego znaczenia, czy w relacji współadministratorów występują oni samodzielnie, czy też dochodzi do jakiegokolwiek powierzenia danych osobowych. Stąd też umowa w zakresie współadministrowania powinna także uwzględniać zasady postępowania wobec osób trzecich, w tym w zakresie powierzenia czynności przetwarzania czy też transferów danych do państw trzecich, z uwzględnieniem zasad wskazanych w RODO, zapewniających odpowiedni poziom ochrony[39].

Podsumowanie

Zidentyfikowanie relacji współadministrowania jest bardzo istotne dla spełnienia obowiązku rozliczalności, a RODO nakłada obowiązek kontroli takich relacji. Relacje te powstają niezależnie od faktycznego dostępu do danych osobowych – istotny pozostaje bowiem wpływ na sposoby i cele przetwarzania. Wpływ ten ponadto może być jedynie potencjalny. Nie musi zatem faktycznie być wykorzystywany przez danego współadministratora. Zidentyfikowanie relacji współadministracji nakłada na współadminsitratorów wiele obowiązków, których uregulowanie powinno nastąpić w formie umowy zawartej w formie pisemnej, w tym elektronicznej. Część tej umowy zwana „zasadniczą częścią uzgodnień" powinna być udostępniona podmiotom danych. Pozostałe obligatoryjne elementy umowy (wspólnych uzgodnień) zostały wskazane wprost w przepisie. Fakultatywne elementy można natomiast wywieźć z regulacji dotyczącej umowy powierzenia, stosowanej odpowiednio. Jest to bowiem w pewnym sensie analogiczna relacja, której sformalizowane elementy oraz forma zostały uregulowane wprost w przepisach RODO. Zastosowanie elementów fakultatywnych do umowy o współadministracji obok tych wprost wskazanych w przepisie może w przyszłości zapobiec nie tylko naruszeniu RODO, ale także może wzmocnić reputacje współadministratorów zobowiązanych do wydobycia na światło dzienne zasadniczej części swoich uzgodnień.

[38] Por. też *K. Witkowska-Nowakowska*, [w:] *D. Lubasz*, *E. Bielak-Jomaa* (red.), Komentarz…, s. 622.

[39] Por. art. 44 i n. RODO.

Słowa kluczowe: współadministrowanie, umowa o współadministrowaniu, dane osobowe, umowa powierzenia, RODO.

Agreement on coadministration of personal data

Coadministration of personal data is an institution which for the first time is clearly regulated within the regulation of the European Parliament and the Council of 27 April 2016, on protection of natural persons regarding processing of personal data and free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation makes member states oblige to take appropriate action regarding coadministration). If there is identification of such a relation, co-administrators should, i.a. regulate joint agreements and make them available. However, GDPR does not point to any forms nor specific guidelines in this regard. The present article aims to identify the relation of coadministration, and analyze the elements stipulated within joint agreements made among co-administrators. Apart from mandatory elements, in the article there are also proposals of facultative elements which support fulfillment of the accountability principle by co-administrators.

Keywords: coadministration, coadministration agreement, personal data, entrustment agreement, GDPR.

The nature of censorship and regulation of the darknet in the Digital Age

Petya Peteva[1]

Latest data from Freedom House shows that, up to date, over 3.8 billion people have access to the Internet[2]. With the advance of the Information Age and with the ever-growing number of Internet users worldwide, multiple heated debates continue taking place on whether cyberspace should be regulated and/or censored, and to what extent, so that it strikes the right balance between respecting fundamental human rights, such as freedom of expression on the one hand, and ensuring public security and safety on the other. While cyberspace censorship has turned to be a political hot potato, there are still corners of cyberspace that, in the meantime, are practically unregulatable due to their anonymity and intractability of their users. This so-called „darknet", while not without its benefits, has also infamously posed a considerable obstacle for law enforcement authorities in combating crime and has provided a safe haven for nefarious individuals and illegal activities to take place with impunity.

Introduction

„Cyber-space", understood as a concept, is a borderless and timeless, fully-digitalized dimension, which has even been considered as a „consensual hallucination"[3], where people can express thoughts and opinions and be connected through a global „network of networks"[4]. It is a revolutionary communication platform that has given rise to a "network society"[5].

The term became synonymous with the Internet and the World Wide Web in the 1990s[6], and when we refer to „cyberspace" in the context of whether it can be censored or not, we generally do not perceive it as an abstract idea on its own but rather conceive it to be the same as its content. Thus, when we debate the issue, we seem to prefer the use of the term „*Internet* censorship" instead.

The believes of „Net Utopians"[7] – that cyberspace/the Internet is nearly impossible to censor – have shifted in the last two decades and have not held up in the face of current and more restrictive practices, recent years being replete with examples, some of which we'll take heed of below.

The notion of cyberspace/Internet censorship itself has been contentious for years and can be regarded in the light of the libertarianism/paternalism debate surrounding it. For example, as Spinello[8] observes, the roots of cyberspace are clearly libertarian, defending the classical liberal approach adopted by Mill[9], thus endorsing a censorship-free Internet. On the other hand, censorship can be defended from a paternalistic point of view, in that it aims to prevent possible harms from occurring, which in turn justifies strengthening state interference and surveillance, and restricting free speech to an extent.

Regardless of the stance one can take on the matter, however, the reality remains that in purely practical terms, cyberspace/the Internet is not entirely „censorship-proof" and various censorship techniques exist that have been utilized in multiple contexts in order to support this view.

Censorship techniques

The so-called man-in-the-middle (MITM) attacks that disrupt the connection between web browsers and servers have been stated to be in the heart of all censorship methods utilized[10]. The OpenNet Initiative lists four different possibilities for censorship of cyberspace[11]: first, technical methods (blocking IP addresses, DNS and URLs, as well as dynamic content analysis and DOS attacks, transparent proxies); second, search result removals by ISPs after being required by the authorities or justified under the „right to be forgotten"

[1] Author is a Legal Projects' Expert at the Law and Internet Foundation in Sofia, Bulgaria.

[2] *A. Shahbaz*, *A. Funk*, The crisis of Social Media, Freedom on the Net 2019, Freedom House, https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf (accessed 15.9.2020).

[3] *W. Gibson*, Neuromancer (Ace Books 1984) 69.

[4] *R.J. Deibert*, Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace' (2003) 32 Millennium 501.

[5] *M. Castells*, The Rise of the Network Society: The Information Age: Economy, Society, and Culture Volume 1 (2nd ed., Wiley-Blackwell 2009).

[6] New World Encyclopedia contributors, Cyberspace, New World Encyclopedia (2014), http://www.newworldencyclopedia.org/entry/Cyberspace#cite_note-0 (accessed 2.11.2016).

[7] *Y. Jewkes, M. Yvonne*, Introduction: the Internet, cybercrime and the challenges of the twenty-first century, [in:] *Y. Jewkes*, *M. Yvonne* (ed), Handbook of Internet Crime, Willan Publishing 2010.

[8] *R.A Spinello*, Regulating Cyberspace: The Policies and Technologies of Control, Quorum Books 2002, p. 34.

[9] *J.S. Mill*, On Liberty, *J.W. Parker* and Son 1859.

[10] *A.A. Niaki* et al., ICLab: A Global, Longitudinal Internet Censorship Measurement Platform, 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 135–151, DOI: 10.1109/SP40000.2020.00014.

[11] OpenNet Initiative, About Filtering, https://opennet.net/about-filtering (accessed 2.11.2016).

granted by the CJEU[12]; third, taking down the problematic website or deregistering the domain; and fourth, induced self-censorship by netizens and journalists due to fear of being prosecuted or adversely affected in some other way.

DPI (Deep Packet Inspection) is another technical possibility and is an established practice by ISPs in China, it has also been attempted by a US company in the UK[13].

Justifications for censorship

Examples of censorship justification include national security arguments, especially in the post-9/11 world which marked the age of strengthened government surveillance all around the world[14]. The perceived looming threats to national security stemming from terrorist attacks, as well as external cyberattacks, have been perceived as valid reasons for states to strengthen encryption techniques and boost cybersecurity[15]. It is a rather onerous task to define the science itself behind cybersecurity due to its constantly evolving nature, however, the „access controls and authentication protocols", utilized within its context, have been likened to the physical barriers of fortress walls that protect users from existing cyber threats[16]. Also, cybersecurity is identified with the provision of dynamic defenses, such as predictive analytics[17], which operate on a proactive basis so that they would be able to detect and negate possible future security risks.

Public safety, and particularly that of minors, is another major factor – a harrowing case in point being the Elysium platform, which has resulted in four convictions[18]. Cyber-bullying is another prominent example – it led, for instance, to the proposal of the Megan Meier Act in the US[19]. There's an emerging concern about the supposedly increased rate of suicides and homicides attributed to the Internet, even with little to no empirical data to back it up[20].

The potential harm of online harassment and hate speech is taken into consideration, some of the claims being that it incites violence, especially with „hate sites" on the rise[21].

There are also arguments on the basis of a loss of reputation, especially by the commercial world as it has the most to lose, however, the CJEU did try to provide a balance, requiring „a sufficient level of seriousness", in order to impose censorship on free speech[22] and national legislation as well, such as the Defamation Act 2013[23] in the UK, for instance, which seems to adopt a similar approach.

The views on the necessary protection of moral standards are not homogenous either, however, the line clearly seems to be drawn at child pornography[24]. Furthermore, there is „a general consensus" that the right to freedom of speech should be restricted if such „invariably illegal content" is involved[25].

Censorship as oppression

While many democratic countries struggle with striking the right balance between freedom of expression on the one hand and its proportionate restriction on the other, non-democratic ones often blatantly use censorship in an oppressive manner, in the form of the so-called „digital authoritarianism"[26].

North Korea has been ranked the leading country in Internet censorship, where any disseminated information to the public is government controlled and heavily censored in its entirety[27]. China is ranked the second place, which has created an extremely effective method for censoring cyber-space materials through its so-called „Great Firewall" that blocks „undesirable content from its „netizens"[28] and, as Deibert states, „China… is a „hard case" for those who

[12] *J. Vincent*, Hidden From Google' website lists articles removed from search results, Independent (16 June 2014,) http://www.independent.co.uk/life-style/gadgets-and-tech/hidden-from-google-lists-articles-removed--from-googles-search-results-9608692.html (accessed 2.11.2016).

[13] *D. Geere*, How deep packet inspection works, Wired (27 April 2012), http://www.wired.co.uk/article/how-deep-packet-inspection-works (accessed 2.11.2016).

[14] Patriot Act 2001; Regulation of Investigatory Powers Act 2000; Anti--Terrorism, Crime and Security Act 2001; Terrorism Act 2006.

[15] Directorate-General for External Policies, Policy Department, Surveillance and censorship: The impact of technologies on human rights (European Parliament 2015), https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf (accessed 15.9.2020).

[16] American Association for the Advancement of Science, What is the Science of Cybersecurity?, AAAS (21.2.2014), https://www.aaas.org/news/what-science-cybersecurity (accessed 12.9.2020).

[17] *Ibidem*.

[18] *R. Fuchs*, German child porn network 'Elysium' founders sentenced to lengthy jail terms, DW (7.3.2019), https://www.dw.com/en/german--child-porn-network-elysium-founders-sentenced-to-lengthy-jail-terms/a-47794610 (accessed 17.9.2020).

[19] *S. Kotler*, Cyberbullying Bill Could Ensnare Free Speech Rights', FoxNews (14.5.2009), http://www.foxnews.com/politics/2009/05/14/cyberbullying-ensnare-free-speech-rights.html (accessed 2.11.2016).

[20] *M. Wykes*, 'Harm, suicide and homicide in cyberspace: assessing causality and control' in Y Jewkes and M Yvonne(ed), Handbook of Internet Crime (Willan Publishing 2010).

[21] *M. Yar*, Cybercrime and Society (London: SAGE 2006) chap. 6.

[22] Axel Springer AG v. Germany [2012] 55 EHRR 183, para. 83.

[23] Defamation Act 2013, p. 1.

[24] *Y. Akdeniz*, Governance of Pornography and Child Pornography on the Global Internet: A Multy-Layered Approach, in *L. Edwards, C. Waelde* (eds.), Law and the Internet: Regulating Cyberspace (Hart Publishing 1997) 223.

[25] *Ibidem*.

[26] *A. Shahbaz*, *A. Funk*, The crisis of Social Media, Freedom on the Net 2019, Freedom House, https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf (accessed 15.9.2020).

[27] *P. Bischoff*, Internet Censorship 2020: A Global Map of Internet Restrictions', Comparitech (15.1.2020), https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/> accessed 15 September 2020.

[28] *J. Lee*, *C. Liu*, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China (13, Minn. J.L. Sci. & Tech. 2012) 125.

argue that the Internet cannot be controlled"[29]. In its 2015 Report, Freedom House displays numerous topics that are being censored[30].

Other countries, such as Russia with its „blacklist law"[31] and Vietnam with its Decree 72 law that criminalizes government opposition[32], are other instances of increasing attempts at filtering content and oppressive censorship. A recent example is the turbulent political situation in Sudan, where authorities imposed severe restrictions on social media in order to prevent people from sharing and receiving information in regard to the now ousted President Omar al-Bashir[33]. Also, concerns are currently on the rise in regard to the new Hong Kong security law which significantly limits free speech and increases surveillance[34], as well as the newly passed legislation in Turkey which would expand government control over content on large social media platforms on its territory[35].

What is more, oppressive regimes have not only utilized a multiplicity of censorship techniques but they have also vastly manipulated information on social platforms, as well as frequently undertaken unregulated mass surveillance, therefore grossly infringing on both individuals' fundamental human rights and data protection rights.

We should bear in mind, however, that as vast as the regular Internet is, it doesn't constitute all of cyberspace. In fact, censorship is not limitless and there are still some parts of the Web where filtering practices don't work as they are hidden under the main surface. This „censorship-free" world frequented by anonymous users[36], referred to as the „darknet", is precisely what we turn to next.

What is the darknet and how does it work?

The darknet is a term used to separate it from the Clearnet, or the cyber-space with the websites we're using on a daily basis. Its so-called hidden services constitute a part of the deep web, which is simply content that is not indexed by mainstream search engines such as Google and Yahoo![37]. It can still be accessed through standard technologies (e.g. HTML, CSS) and web browsers (e.g. Chrome, Firefox), however, only with special rerouting software[38], which hides the IP addresses of their servers[39]. Thus, the darknet conceals its users' identities, provides them with anonymity and makes them virtually untraceable.

Its roots stem from the US Naval Research Laboratory, where a team of experts, using the work of *D. Chaum* as a guiding light[40], created the revolutionary onion routing and its most popular application – TOR (The Onion Router). Its initial purpose was „to protect overseas American operatives and dissidents"[41].

Just like the onion is multi-layered, the IP address of the end-user is hidden under layers of encryption. This means that all data traffic from an individual's computer passes through a multiple number of volunteering relaying computers called „nodes", changing their IP address with a different one on the TOR network. Each time data goes through another „relay", it loses one layer of encryption until it reaches the exit node[42].

TOR is arguably the most popular method of accessing the darknet, it is, however, not the only method, and others, such as the Invisible Internet Project (I2P)[43] and Freenet[44], are also used as alternatives.

Different uses of the darknet

As we can see from the research of what the darknet constitutes, the concept of *anonymity* is at its core.

The primary purpose of onion routing is still relevant today and a substantial part of the users are „military, gov-

[29] *R. J. Deibert*, Dark guests and great firewalls: the Internet and Chinese security. (58 (1), Journal of Social Issues 2002) 143.

[30] Freedom on the Net, Freedom House, 2015, https://freedomhouse.org/sites/default/files/resources/FOTN%202015_China%20%28new%29.pdf (accessed 2.11.2016).

[31] Russia internet blacklist law takes effect, BBC News (1.11.2012), http://www.bbc.co.uk/news/technology-20096274 (accessed 2.11.2016).

[32] *E.E Schmidt, J. Cohen*, The Future of Internet Freedom, The New York Times (11.3.2014) http://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html?_r=0 (accessed 2.11.2016).,

[33] Freedom on the Net, The Crisis of Social Media', Freedom House, 2019, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media (accessed 31.7.2020).

[34] *G. Tsoi*, *L.C. Wai*, Hong Kong security law: What is it and is it worrying?, (BBC News, 30.6.2020), https://www.bbc.com/news/world-asia-china-52765838 (accessed 31.7.2020).

[35] *M. Santora*, Turkey Passes Law Extending Sweeping Powers Over Social Media, The New York Times (July 29 2020), https://www.nytimes.com/2020/07/29/world/europe/turkey-social-media-control.html (accessed 31.7.2020).

[36] *J. Bartlett*, How the mysterious dark net is going mainstream' (TEDTalks 2015) https://www.youtube.com/watch?v=pzN4WGPC4kc (accessed 2.11.2016).

[37] *J. Pagliery*, The Deep Web you don't know about, CNN (10.3.2014), http://money.cnn.com/2014/03/10/technology/deep-web/index.html (accessed 2.11.2016).

[38] *R. Gehl*, Illuminating the Dark Web (Scientific American, 21.10.2018), https://www.scientificamerican.com/article/illuminating-the-dark-web/ (accessed 17.9.2020).

[39] *C. Fulton*, *C. McGuinness*, Digital Detectives: Solving Information Dilemmas in an Online World (Chandos Publishing 2016) 105.

[40] *D. Chaum*, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms (1981] 24 ACM 84.

[41] *T. McCormick*, The Darknet. Foreign Policy, FP (9.12.2013), http://foreignpolicy.com/2013/12/09/the-darknet-a-short-history/ (accessed 3.11.2016).

[42] Darknet Series: What is the Darknet?, OWL Cybersecurity (26 August 2016), https://www.owlcyber.com/blog/2016/8/26/the-darknet-series-what-is-the-darknet (accessed 2.11.2016).

[43] The Invisible Internet Project < https://geti2p.net/en/ (accessed 3.11.2016).

[44] Freenet, https://freenetproject.org/index.html (accessed 3.11.2016).

ernment and law enforcement organizations"[45] within which sensitive information is often discussed and it would certainly be dangerous if it fell into the wrong hands.

The darknet can be and *is* used for legitimate purposes – it is, for instance, utilized by whistleblowers, such as Edward Snowden who used TOR with a piece of technology called TAILS to inform the media and the public about the government surveillance[46]. The new WikiLeaks submission system is also exclusively accessible through TOR[47].

It also plays a major role in some more restrictive countries with oppressive governments, where anonymity is not an opportunity[48] but a necessity if one wants to have their voice heard. Jardine[49] supports the rhetoric that all points of view must be considered in order for democracy to flourish, views previously expressed by Mill[50] as well. In Russia and China, for instance[51], Internet censorship is nothing new. All Chinese ISPs are required „to register with the police and all Internet users must sign a declaration that they will not visit forbidden sites"[52]. China's „Great Firewall" project was also able to censor TOR, however, ways to circumvent that hurdle have been discovered[53].

TOR has been associated with the Arab Spring that took place in the Middle East in 2011 – David Appelbaum explains how it was used by the political dissidents and journalists as well as the general public to give birth to the revolution[54].

The shroud of anonymity that the darknet provides is also a desired alternative by young people, such as the Youth Liberation Front (YLF), members of the LGBTQ+ community, as well as other disenfranchised minorities, which use it as a sanctuary in which they can feel comfortable and secure without any of the pressures and constraints of the Clearnet[55].

Still, primary due to the factor of anonymity as it has been reported[56], the darknet is largely associated with nefarious and illegal practices. It provides for a large number of crypto markets for drugs (such as Silk Road[57]), child pornography, weaponry, and, allegedly, the services of professional hitmen[58], all the more easy to purchase as it operates with cryptocurrencies. This means that, even if censorship is applied as a safety measure and is justified on the Clearnet, this step is undermined by the crime that reigns freely on the darknet. This brings us to the inevitable question – how impenetrable is the darknet?

Conclusions

While currently it is rather difficult to see how the darknet can be regulated in the same manner as the Clearnet, due to its very nature, including through legislative provisions and government control, to say that it is a cyberspace that lies entirely outside the limits of the law would be incorrect. For instance, even though the darknet protects its users through providing them with anonymity in terms of their identities and geographical locations, any data that is provided by an individual is visible by anyone that has accessed the specific website as it can potentially be used to identify them[59].

The darknet also serves as an incitement for law enforcement to keep up with technological advancements in order to tackle the criminal activities reported to be taking place there. Examples of this are the FBI taking down a major child pornography website by using a new hacking method called NIT[60], Operation Shrouded Horizon[61] and Operation Hyperion[62]. More

[45] *D. Walsh*, A Beginner's Guide to Exploring the Darknet, TurboFuture (29.8.2016), https://turbofuture.com/internet/A-Beg inners-Guide-to--Exploring-the-Darknet (accessed 3.11.2016).

[46] *K. Finley*, 'Out in the open: Inside the operating system Edward Snowden used to evade the NSA, Wired (14.4.2014), https://www.wired.com/2014/04/tails/ (accessed 3.11.2016).

[47] *R. Brandom*, 'After four years of downtime, WikiLeaks is once again accepting leaks online, The Verge (1.5.2015), http://www.theverge.com/2015/5/1/8531049/wikileaks-tor-browser-submission-page (accessed 3.11.2016).

[48] *E. Jardine*, Tor, what is it good for? Political repression and the use of online anonymity-granting technologies (2016), New Media & Society (as cited in Fuzzy, Paper: Oppressive and free countries use Tor the most, DeepDotWeb (10.4.2016), https://www.deepdotweb.com/2016/04/10/paper-oppressive-free-countries-use-tor/ (accessed 3.11.2016).

[49] *Ibidem.*

[50] Mill (n 7).

[51] *K. Paul*, Russia wants to block Tor, but it probably can't, Motherboard (18 February 2015) <http://motherboard.vice.com/read/russia-wants-to--block-tor-but-it-probably-cant (accessed 3.11.2016).

[52] *Y. Jewkes*, Crime Online (Willan Publishing 2007) chap. 1, 1.

[53] *P. Winter*, *S. Lindskog*, How the Great Firewall of China is blocking Tor, USENIX (2012), https://www.usenix.org/system/files/conference/foci12/foci12-final2.pdf (accessed 3.11.2016).

[54] *I. Zahorsky*, Interview with Jacob Appelbaum 'Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum', UPEACE (August 1 2011) <http://www.monitor.upeace.org/innerpg.cfm?id_article=816 (accessed 3.11.2016).

[55] *R. Gehl* et al, Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P (The MIT Press 2018).

[56] FBI, A Primer on DarkNet Marketplaces: What They Are and What Law Enforcement is Doing to Combat Them" (1 November 2016), https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces (accessed 21.7.2020).

[57] *W. Lacson*, *B. Jones*, The 21st Century DarkNet Market: Lessons from the Fall of Silk Road, International Journal of Cyber Criminology 10.1 (2016) 40, http://www.cybercrimejournal.com/Lacson&Jonesvol10issue1IJCC2016.pdf (accessed 2.11.2016).

[58] Daily Mail Reporter, The Disturbing World of the Deep Web, where contract killers and drug dealers ply their trade on the Internet, Daily Mail (11.10.2013), http://www.dailymail.co.uk/news/article-2454735/The-disturbing-world-Deep-Web-contract-killers-drug-dealers-ply-trade-internet.html (accessed 3.11.2016).

[59] *A. Zaunseder*, The darknet is not a hellhole, it's an answer to internet privacy, The Conversation (16.8.2018), https://theconversation.com/the--darknet-is-not-a-hellhole-its-an-answer-to-internet-privacy-101420 (accessed 31.7.2020).

[60] *M. Russon*, FBI crack Tor and catch 1,500 visitors to biggest child pornography website on the dark web', International Business Times (6.1.2016) <http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest--child-pornography-website-dark-web-1536417 (accessed 3.11.2016).

[61] *D. Kushner*, The Darknet: Is the Government Destroying 'the Wild West' of the Internet?', Rolling Stone (22.10.2015), http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022 (accessed 3.11.2016).

[62] FBI, A Primer on DarkNet Marketplaces: What They Are and What Law Enforcement is Doing to Combat Them" (1 November 2016), https://www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces (accessed 21.7.2020).

recently, in 2017, two major darknet markets, Alphabay and Hansa, were shut down after a successful international police operation[63]. Authorities, apart from monitoring darknet websites, utilize the help of companies, such as BrightPlanet and HoldSecurity, and there are even vigilantes[64] and „hacktivists"[65] that take matters into their own hands.

Challenges, however, still remain as the illegal networks that are taken down are quickly replaced by new markets, which maintain the resilience of the overall structure[66] and thus, further national and international coordination between authorities is needed, as well as an increased understanding of the nature and *modus operandi* of the darknet itself in order to successfully tackle such criminal activities.

[63] European Monitoring Centre for Drugs and Drug Addiction and Europol (2017), Drugs and the darknet: Perspectives for enforcement, research and policy, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg.

[64] *T. Holman*, How cyber-vigilantes catch pedophiles and terrorists lurking in the dark web (International Business Times, 12.12.2014) http://www.ibtimes.co.uk/how-cyber-vigilantes-catch-paedophiles-terrorists-lurking-deep-web-1479291> accessed 3 November 2016.

[65] *C. Baraniuk*, Ten Hacktivists who shook the Web (Dazed 2013) http://www.dazeddigital.com/artsandculture/article/16368/1/ten-hacktivists-who-shook-the-web (accessed 3.11.2016).

[66] European Monitoring Centre for Drugs and Drug Addiction and Europol (2017), Drugs and the darknet: Perspectives for enforcement, research and policy, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg.

Key words: darknet, censorship, Internet regulation.

WYMOGI EDYTORSKIE:

- język publikacji: polski, angielski, niemiecki, rosyjski;
- edytor tekstu Word (format .doc lub .docx);
- styl czcionki: Times New Roman;
- wielkość czcionki: tekst główny – 12 pkt, przypis – 10 pkt;
- interlinia: 1,5 wiersza (w przypadku przypisów – 1 wiersz);
- objętość artykułu: do 30 000 tys. znaków ze spacjami;
- marginesy: standardowe – wszystkie 2,5 cm;
- przypisy dolne: odsyłaczami przypisów powinny być cyfry arabskie; odsyłacz należy umieścić bezpośrednio po fragmencie, do którego odnosi się przypis (przed kropką kończącą zdanie);
- należy dołączyć słowa kluczowe w języku polskim i angielskim;
- tytuł powinien być napisany czcionką Times New Roman 14 pkt (czcionka pogrubiona);
- tekst powinien składać się z następujących części: lid (streszczenie ok. 1500 znaków ze spacjami), uwagi wstępne, rozwinięcie (z podziałem na zatytułowane części), podsumowanie;
- do artykułu należy załączyć także lid (streszczenie) w języku angielskim (ok. 1500 znaków ze spacjami);
- śródtytuły nie powinny być numerowane, lecz pogrubione;
- należy dołączyć notę biograficzną (ok. 800 znaków ze spacjami);
- prosimy o wskazanie afiliacji.

Powoływane w przypisach pozycje bibliograficzne prosimy pisać według wzoru:

Inicjał. Nazwisko, Tytuł, ew. numer wydania, tom, część itp., miejsce i rok wydania, a następnie cytowane strony skrótem „s.", np.:
J. Kowalski, Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku kolejnego powołania się **bezpośrednio** na cytowaną pozycję:

Ibidem, s. 15–16.

Powołanie kolejny raz, gdy cytujemy tylko jedną pozycję danego autora:

J. Kowalski, *op. cit*., s. 29–20.

Kolejne powołanie, gdy cytuje się kilka pozycji danego autora, zawiera pierwsze wyrazy tytułu, np.:

J. Kowalski, Jak pisać..., s. 28–29.

W przypadku **prac pod redakcją**, jeśli powoływana publikacja stanowi część całości:

P. Igrek, Cytowanie, [w:] *J. Kowalski* (red.), Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku publikacji w czasopismach tytuł czasopisma zastępuje nazwę wydawnictwa, po nim następuje rok (rocznik), przecinek, następnie numer (nr) w ramach rocznika ewentualnie także numer od początku wydawania pisma i numer strony:

J. Kowalski, Jak pisać przypisy?, Wiadomości Tekściarskie 2006, Nr 28 (236), s. 7.

Kilka kwestii specjalistycznych:

1. Oczekiwane oznaczenie ustawy wygląda następująco: Dz.U. z 2006 r. Nr 28, poz. 456.
2. Publikator prosimy podawać jedynie przy pierwszym przywołaniu aktu prawnego. Wówczas nazwę aktu i datę (miesiąc słownie) podajemy w tekście głównym (np. ustawa z 13.4.2003 r. o zasadach pisania artykułów), w przypisie zaś publikator (np. t.j. Dz.U. z 2006 r. Nr 28, poz. 456).
3. Zapisując artykuł, ustęp, punkt aktu prawnego, skrótów nie oddzielamy przecinkami, tak więc: art. 28 ust. 59 pkt (bez kropki!) 36, a nie: art. 28, ust. 59, pkt. 36.
4. W przypadku orzeczeń sądowych prosimy o zastosowanie następujących oznaczeń: Wyrok SN z 11.5.2011 r., I CA 123/11, OSNCP 2011, Nr 8, poz. 34. Nazwę orzeczenia i jego datę prosimy podać w tekście głównym (np. wyrok SN z 11.5.2011 r.), natomiast w przypisie publikator (I CA 123/11, OSNCP 2011, Nr 8, poz. 34).

Harmonogram publikacji:

Nr 1 – teksty do końca stycznia, druk luty/marzec
Nr 2 – teksty do końca kwietnia, druk maj/czerwiec
Nr 3 – teksty do końca lipca, druk sierpień/wrzesień
Nr 4 – teksty do końca października, druk listopad/grudzień

Osoba do kontaktu: dr *Aleksandra Klich*, e-mail: pme@beck.pl

EDITORIAL REQUIREMENTS:

- language of publication: Polish, English, German, Russian;
- text editor MS Word (.doc or .docx);
- font style: Times New Roman;
- font size: main text – 12 pts, footnote – 10 pts;
- line spacing: 1.5 line (for footnotes – 1 row);
- volume of the article: up to 30,000 characters with spaces;
- margins: standard – all 2.5 cm;
- footnotes: cross-referenced footnotes should be Arabic numerals; reference should be placed immediately after the passage to which the footnote regards (before the full stop ending a sentence);
- article must be attached with key words in Polish and English;
- the title should be written in Times New Roman 14 pts (bold);
- text should consist of following parts: lead (summary, around 1500 characters with spaces), initial comments, amplification (with a division into parts with titles), summation;
- article should also be attached with a lead (summary) in English (around 1500 characters with spaces);
- intertitles should not be numbered, but bold;
- article must be attached with a biographical note (approx. 800 characters including spaces);
- please indicate affiliation.

The referenced sources should adhere to the following style:

Initial(s). Last name, Title, edition number if applicable, volume, part, etc., place and year of publication, followed by the page(s) referred to with the 'p. (pp.)' abbreviation, e.g.: *J. Kowalski*, How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For subsequent reference made **directly** to the cited item:

Ibidem, p. 15–16.

Further reference, when several positions by a given author are being cited, include the first words of the title, e.g.:

J. Kowalski, How to..., p. 28–29.

For edited volumes, when the publication referenced forms a part of the whole:

P. Igrek, Citing, [in:] *J. Kowalski* (ed.), How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For publications in periodicals, the title of the periodical replaces the name of the publisher, followed by the year, comma, then the number (No.) within the year, possibly the consecutive number and page numbers:

J. Kowalski, How to do references?, Editorial news 2006, No. 28 (236) p. 7.

A few technical issues:

a. Expected indication of a legal act goes as follows: Journal of Laws of 2006, No. 28, item 456. The publishing body should only be provided when referring to the act for the first time. Then the name and date of the act (month – in words) shall be given in the body of the text (e.g. The Act of 13 April on the rules of writing articles), and the publishing body shall be given in the footnote (e.g. Journal of Laws of 2006, No. 28, item 456).
b. When writing article, paragraph, point of a legal act, abbreviations should not be separated by commas, that is: art. 28 par. 59 point (no full stop!) 36, not: art. 28, par. 59, pt. 36).
c. For court judgements, please use the following indications: Judgement of the Supreme Court of 11.5.2011, I CA 123/11, OSNCP 2011, No. 8, item 34. Mind that the appelative of the judgement and its date should be indicated in the main text (e.g. Judgement of the Supreme Court of 11.5.2011), and the publishing body in the footnote (I CA 123/11, OSNCP 2011, No. 8, item 34).

Publication schedule (deadlines):

No. 1 – submitting manuscripts – end of January (print – February/March)
No. 2 – submitting manuscripts – end of April (print – May/June)
No. 3 – submitting manuscripts – end of July (print – August/September)
No. 4 – submitting manuscripts – end of October (print – November/December)

Contact Person: *Aleksandra Klich* PhD, e-mail: pme@beck.pl

beckakademia
konferencje • szkolenia • webinaria

SZKOLENIA ONLINE dla prawników

- **Postępowanie w sprawach gospodarczych, postępowanie uproszczone, postępowanie nakazowe, upominawcze i elektroniczne postępowanie upominawcze**
  Termin: 7 grudnia 2020 r., 14:00-17:00, cena 299 zł • Prelegent: SSO Grzegorz Karaś

- **Przygotowana likwidacja (pre-pack) w dobie epidemii COVID-19. Z uwzględnieniem nowelizacji prawa upadłościowego 2020**
  Termin: 8 grudnia 2020 r., 10:00-14:00, cena 449 zł • Prelegent: SSR Cezary Zalewski

- **Wellbeing w kancelarii. Jak stworzyć zadowolony, zgrany i skuteczny zespół?**
  Termin: 9 grudnia 2020 r., 11:00-14:00, cena 249 zł • Prelegent: Agata Pelc

- **PPK w sektorze publicznym. Etapy wdrożenia**
  Termin: 10 grudnia 2020 r., 12:00-14:00, cena 199 zł • Prelegent: Oskar Sobolewski

- **Ustawa o kształtowaniu ustroju rolnego, a obrót nieruchomościami o przeznaczeniu nierolniczym**
  Termin: 14 stycznia 2021 r., 11.00-15.00, cena: 399 zł • Prelegenci: r. pr. Wojciech Koczara

- **Sprzedaż nieruchomości zadłużonych. Jak skutecznie przenieść nieruchomość zadłużoną, ekspektatywę prawa do lokalu lub prawa i obowiązki z umowy deweloperskiej**
  Termin: 15 stycznia 2021 r., 12.00-13.30, cena: 249 zł • Prelegenci: r. pr. Katarzyna Niekrasz-Gierejko

- **Prawo restrukturyzacyjne 2021 w praktyce. Z uwzględnieniem uproszczonego postępowania restrukturyzacyjnego**
  Termin: 19 stycznia 2021 r., 11.00-15.00, cena: 549 zł • Prelegenci: SSR Cezary Zalewski

- **REFORMA KPC. Postępowanie w sprawach gospodarczych**
  Termin: 29 stycznia 2021 r., 10.00-15.00, cena: 549 zł • Prelegenci: SSR Artur Żuk

- **Kontrola Prezesa Urzędu Ochrony Danych Osobowych**
  Termin: 10 lutego 2021 r., 12.00-15.00, cena: 399 zł • Prelegenci: Paweł Mielniczek

- **Skarga pauliańska, czyli jak skutecznie bronić się przed ukrywaniem majątku przez dłużników w dobie COVID-19**
  Termin: 16 lutego 2021 r., 12.00-13.30, cena: 249 zł • Prelegenci: r. pr. Katarzyna Niekrasz-Gierejko

- **Upadłość konsumencka w praktyce 2021**
  Termin: 18 lutego 2021 r., 10.00-14.00, cena: 549 zł • Prelegenci: SSR Cezary Zalewski

- **Przewłaszczenie na zabezpieczenie, czyli jak skutecznie zabezpieczać długi**
  Termin: 9 marca 2021 r., 12.00-13.30, cena: 249 zł • Prelegenci: r. pr. Katarzyna Niekrasz-Gierejko

- **Świadczenia złożone w VAT 2021**
  Termin: 17 marca 2021 r., 10.00-16.00, cena: 699 zł • Prelegenci: dr Jacek Matarewicz

Nie czekaj i zapisz się już dziś!

szkoleniaonline.beck.pl lub pod nr. telefonu: **81 461 33 05**