Jarosław Greser*

Cyberbezpieczeństwo wyrobów medycznych w świetle rozporządzenia 2017/745

Spis treści

Streszczenie

Specyfika wyrobów medycznych wymaga, aby ich producenci kładli szczególny nacisk na kwestie związane z bezpieczeństwem ich stosowania. Jednocześnie rozwój technologii informatycznych, a szczególnie Internetu rzeczy, spowodował że w medycynie powszechnie zaczęto wykorzystywać wyroby komunikujące się za pośrednictwem sieci, także takie, które są na stałe do niej podłączone. Budzi to uzasadnione pytanie w zakresie ich zabezpieczenia z perspektywy cyberbezpieczeństwa. Niniejszy artykuł jest próbą analizy tego zagadnienia z perspektywy przepisów rozporządzenia 2017/745, które wchodzi w życie w maju 2020 roku. W jego ramach zostanie zarysowana problematyka związana z korzystaniem z wyrobów medycznych w perspektywie zagrożeń, których źródłem jest Internet oraz obecny stan prawny dotyczący badania wyrobów medycznych pod kątem cyberbezpieczeństwa. Ponadto zostaną przeanalizowane przepisy dotyczące definicji wyrobu medycznego, w szczególności przesłanek uznających oprogramowanie za samodzielny wyrób, zasady klasyfikacji wyrobów medycznych oraz zasady ich wprowadzania do obrotu a następnie nadzorowania urządzeń będących w obrocie. Osią wspólną analiz jest pytanie o zasady stwierdzenia bezpieczeństwa z perspektywy zagrożeń płynących z sieci.

Słowa kluczowe: cyberbezpieczeństwo; wyroby medyczne; rozporządzenie 2017/746; IoT.

JEL: K24, K32

* Adiunkt w Szkole Nauk Ścisłych Uniwersytetu im. Adama Mickiewicza w Poznaniu; e-mail: greser@amu.edu.pl; https://orcid.org/0000-0002-1021-6142.

I. Zagadnienia wprowadzające

Rozwój technologii informacyjnych doprowadził do rewolucji w sposobie diagnostyki i leczenia pacjentów. Szczególną rolę w tym zakresie odgrywa technologia Internetu rzeczy (dalej: IoT) definiowana jako infrastruktura społeczeństwa informacyjnego pozwalającą na zaawansowane usługi poprzez łączenie fizycznych rzeczy i ich wirtualnych odpowiedników w oparciu o istniejące technologie informacyjne i komunikacyjne (ITU-T 2015). Wykorzystanie tych urządzeń pozwala na zbieranie szerokiego zakresu danych o stanie zdrowia w czasie rzeczywistym zarówno od pacjentów monitorowanych w warunkach szpitalnych, jak i od osób przebywających w domu. Urządzenia te znajdują coraz szersze zastosowanie w leczeniu i działaniach mających na celu poprawę jakości życia osób cierpiących na choroby przewlekłe (Jara, Hopp i Weaver, 2018, s. 587–593), osób starszych (Jurczak, 2020) oraz wspomagają leczenie najnowszymi metodami terapeutycznymi, takimi jak medycyna precyzyjna (Kosowska, Sowa i Świerczyński, 2019, s. 152).

Priorytetem działania urządzeń medycznych jest bezpieczeństwo ich użytkowania dla pacjentów. Należy podkreślić, że przepisy wyraźnie rozgraniczają urządzenia będące wyrobami medycznymi i takie, które pomimo swoich funkcji nie posiadają tego statusu. Przykładem tych ostatnich są urządzenia typu *werables*, takie jak opaski dostarczające dane o aktywności fizycznej lub informujące o konieczności pomocy użytkownikowi (Gomułka, 2019). Należy zauważyć, że pozyskiwane dane za pomocą takich właśnie urządzeń nie mają wartości danych klinicznych i nie mogą być wykorzystywane w procesie leczenia.

W przypadku wyrobów medycznych będących jednocześnie urządzeniami IoT zasadniczą kwestią w zakresie bezpieczeństwa ich używania jest problematyka zabezpieczenia tych urządzeń przed zagrożeniami mającymi swoje źródło w cyberprzestrzeni. Należy zwrócić uwagę, że Internet rzeczy uznawany jest za szczególnie wrażliwy w tym zakresie (ENISA, 2017, s. 22–23). Wskazuje się, że jedną z najważniejszych przyczyn tego zjawiska jest liczba i różnorodność typów urządzeń, które prowadzą do stosowania autorskich rozwiązań w zakresie oprogramowania, które następnie nie są aktualizowane po zakończeniu projektu (OWASP, 2018). Jednocześnie, ze względu na warunki licencji użytkownicy nie mają możliwości samodzielnej zmiany oprogramowania (ENISA, 2017, s. 44). Prowadzi to do powstania luk bezpieczeństwa, które mogą być wykorzystane w atakach, których celem są urządzenia medyczne. Skutkiem tego może być naruszenie bezpieczeństwa informacji rozumianego jako zapewnienie poufności, integralności i kompletności danych (Chmielewski i Waćkowski, 2018, s. 79). W przypadku urządzeń medycznych może to skutkować czasowym lub trwałym pogorszeniem stanu zdrowia pacjenta lub poważnym zagrożeniem zdrowia publicznego. Powstaje zatem pytanie czy bezpieczeństwo wyrobów medycznych obejmuje również kwestie związane z odpowiednim poziomem bezpieczeństwa oprogramowania niezbędnego do korzystania z takich urządzeń. Celem niniejszego artykułu jest rozważenie tego zagadnienia w kontekście zmiany przepisów dotyczących wyrobów medycznych.

II. Obecne regulacje

Aktualnie obowiązujące regulacje dotyczące certyfikacji urządzeń medycznych opierają się na dyrektywach, uchwalonych w latach 1990[1] i 1993[2], a następnie nowelizowanych w latach 2000[3] i 2007[4]. Akty te stały się podstawą polskich unormowań wprowadzonych ustawą z 20 maja 2010 r. o wyrobach medycznych[5]. Przepisy te opierają się na założeniu, że tylko wyroby medyczne mogą być wykorzystywane w trakcie realizacji procedur medycznych. Związany z tym jest nakaz zawarty w art. 17 ust. 1 pkt 2 i art. 18 ust. 1 pkt 3 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[6] posługiwania się przez podmioty i praktyki lekarskie wyłącznie produktami i wyrobami medycznymi w rozumieniu ustawy o wyrobach medycznych oraz liczne obowiązki nałożone na producentów i importerów wyrobów medycznych, których spełnienie konieczne jest przed wprowadzeniem produktu do obrotu. Ma to gwarantować uzyskanie możliwie najwyższego poziomu bezpieczeństwa dla pacjentów.

Należy zauważyć, że definicja zawarta w art. 2 ust. 1 pkt 38 o wyrobach medycznych za wyrób medyczny uznaje zarówno samo oprogramowanie, jak i narzędzia, przyrządy, urządzenia, materiał lub inny artykuł stosowany w połączeniu z oprogramowaniem. Jednocześnie procedury certyfikacyjne nie odnoszą się bezpośrednio do problematyki cyberbezpieczeństwa. Nakaz uwzględniania tego zagadnienia można wyinterpretować z art. 6 ustawy, który zakazuje wprowadzania do obrotu, wprowadzania do używania, przekazywania do oceny działania, dystrybuowania, dostarczania, udostępniania, instalowania, uruchamiania i używania wyrobów, które stwarzają zagrożenie dla bezpieczeństwa, życia lub zdrowia pacjentów, użytkowników lub innych osób, przekraczające akceptowalne granice ryzyka, określone na podstawie aktualnego stanu wiedzy, kiedy są prawidłowo dostarczone, zainstalowane, utrzymywane oraz używane zgodnie z ich przewidzianym zastosowaniem. Przesłanka aktualnego stanu wiedzy będzie w przypadku oprogramowania dotyczyła odporności urządzenia na znane podatności i wektory cyberataku. Interpretacja ta jest wsparta unormowaniami rozporządzenia Ministra Zdrowia w sprawie wymagań zasadniczych oraz procedur oceny zgodności wyrobów medycznych[7], które nakłada obowiązek walidacji oprogramowania zgodnie z aktualnym stanem wiedzy i z uwzględnieniem zasad cyklu rozwoju oraz zarządzania ryzykiem.

Natomiast w zakresie możliwości reagowania na nieznane wcześniej zagrożenia ustawa nie nakłada na wytwórcę, importera i dystrybutora wprowadzającego wyrób medyczny do obrotu bezpośredniego obowiązku dostarczania aktualizacji. Przepisy wymagają jedynie, aby użytkownik używał produktu zgodnie z przewidzianym zastosowaniem i w oparciu o zalecenia zawarte w instrukcji używania. Jednocześnie art. 90 ust. 4 ustawy nakazuje wskazać podmioty upoważnione

[1] Dyrektywa Rady nr 90/385/EWG z dnia 20 czerwca 1990 r. w sprawie zbliżenia ustawodawstw państw członkowskich odnoszących się do wyrobów medycznych aktywnego osadzania (Dz.Urz. WE 1990 L 189/17).

[2] Dyrektywa Rady 93/42/EWG z dnia 14 czerwca 1993 r. dotycząca wyrobów medycznych (Dz.Urz. WE 1993 L 169/1).

[3] Dyrektywa 2000/70/WE Parlamentu Europejskiego i Rady z dnia 16 listopada 2000 r. zmieniająca dyrektywę 93/42/EWG w odniesieniu do wyrobów medycznych zawierających trwałe pochodne krwi ludzkiej lub osocza ludzkiego (Dz.Urz. WE L 313 z 13.12.2000 r., s. 22).

[4] Dyrektywa 2007/47/WE Parlamentu Europejskiego i Rady z dnia 5września 2007 r. zmieniająca dyrektywę Rady 90/385/EWG w sprawie zbliżenia ustawodawstw państw członkowskich odnoszących się do wyrobów medycznych aktywnego osadzania, dyrektywę Rady 93/42/EWG dotyczącą wyrobów medycznych oraz dyrektywę 98/8/WE dotyczącą wprowadzania do obrotu produktów biobójczych (Dz.Urz. UE L 247 z 21.09.2007 r., s. 21).

[5] Ustawa z dnia 20 maja 2010 r. o wyrobach medycznych (t.j. DzU 2019, poz. 175 z późn. zm.).

[6] Ustawa z dnia 11 kwietnia 2011 r. o działalności leczniczej (t.j. DzU 2018, poz. 2190 z późn. zm.).

[7] Rozporządzenie Ministra Zdrowia z 17 lutego 2016 w sprawie wymagań zasadniczych oraz procedur oceny zgodności wyrobów medycznych (DzU 2016, poz. 211).

przez wytwórcę lub autoryzowanego przedstawiciela do dokonywania aktualizacji, o ile zgodnie z instrukcją użytkownik nie może jej przeprowadzić samodzielnie. Należy zwrócić uwagę, że obowiązki nałożone na użytkowników w zakresie utrzymywania i użytkowania rzeczy nie powinny przekraczać zwyczajowych działań przyjętych w danych stosunkach. W związku z tym to po stronie producenta, a nie użytkownika, leży analizowanie pojawiających się podatności na ataki i przygotowanie aktualizacji oprogramowania zmniejszających ryzyko jego skutecznego przeprowadzenia. Obowiązkiem użytkownika jest natomiast instalacja aktualizacji zgodnie z wytycznymi producenta.

III. Regulacje wprowadzane rozporządzeniem 2017/745

1. Uwagi wprowadzające

Zasadnicze prace nad dyrektywami 90/385/EWG i 93/42/EWG prowadzone były w latach 80. XX wieku. Mimo późniejszych nowelizacji, akty te nie sprostały wyzwaniom związanych z postępem technologii i zmianą uwarunkowań rynkowych. Zjawiska te skłoniły prawodawcę unijnego do przeprowadzenia przeglądu tych aktów prawnych. Rezultatem tego było uchwalenie 5 kwietnia 2017 r. rozporządzenia 2017/745[8] uchylającego wskazywane dyrektywy i kompleksowo normującego problematykę wprowadzania na rynek, obrotu i nadzoru nad rynkiem wyrobów medycznych oraz zasad prowadzenia na terenie Unii badań klinicznych dotyczących takich wyrobów.

Celem tej regulacji jest zapewnienie wysokiego poziomu ochrony zdrowia poprzez sprawne funkcjonowanie rynku wewnętrznego w obszarze wyrobów medycznych oraz ustanowienie wysokich norm jakości i bezpieczeństwa tych wyrobów. Prawodawca w motywie 2 rozporządzenia wskazuje, że oba te cele są równie istotne i współzależne, a do ich osiągnięcia należy dążyć jednocześnie. Podkreśleniem tego założenia jest wskazanie w motywie 88 wartości, które należy uwzględniać przy interpretacji, który wprost odnosi się do uwzględniania w jej trakcie praw podstawowych, szczególnie chronionych w Karcie Praw Podstawowych[9], takich jak godność człowieka, jego integralność, ochrona danych osobowych[10], wolności sztuki i nauki, wolności prowadzenia działalności gospodarczej i prawa własności. Takie założenie wpisuje się we wskazywany w literaturze ścisły związek cyberbezpieczeństwa z prawami człowieka (Cavelty i Kavanagh, 2019, s. 73–75) W szczególności należy zgodzić się z poglądem, że zagadnienie to wykracza poza zakres związany z autonomią informacyjną jednostki, prawa do życia oraz prawa do najwyższego osiągalnego poziomu zdrowia. Tym samym rozporządzenie 2017/745 można uznać za wpisujące się w zakres realizacji obowiązków państw członkowskich wynikających z praw człowieka (Nowak, 2003, s. 51–54), co rzutuje na jego wykładnię systemową (Eide i Eide, 2006).

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 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 2017 L 117/1).

[9] Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE 2012 C 326/391).

[10] Problematyka ochrony danych osobowych przez urządzenia medyczne była szeroko uwzględniania w trakcie tworzenia Rozporządzenia 2017/745 włącznie z opinią Europejskiego Inspektora Ochrony Danych wydaną 8.02.2013 (Dz.Urz. UE 2013 C 358/7). Niemniej jednak problematyka ta pozostaje na marginesie regulacji tego aktu prawnego, dlatego pomijam ją w dalszych rozważaniach.

2. Definicja wyrobu medycznego

Rozporządzenie w art. 2 pkt 1 zawiera definicję legalną wyrobu medycznego. Zgodnie z nią do kategorii tej są zaliczane produkty spełniające łącznie dwa rodzaje przesłanek. Pierwszą z nich jest forma oddziaływania na pacjenta. W tym zakresie wyrobem medycznym prawodawca przewidział katalog otwarty, wskazując, że można do niego zaliczyć narzędzia, aparaty, urządzenia, implanty, odczynniki, materiały oraz oprogramowanie. Jednocześnie wyrobem medycznym nie będzie wytwór, który nie osiąga swojego zasadniczego przewidzianego działania środkami farmakologicznymi, immunologicznymi lub metabolicznymi w ludzkim ciele lub na nim, ale którego działanie może być wspomagane takimi środkami.

Należy zauważyć, że za wyrób może być uznany również sam program funkcjonujący niezależnie. Tym samym problematyka cyberbezpieczeństwa będzie obejmowała wyroby będące rzeczami, o ile do ich funkcjonowania niezbędne są programy komputerowe, jak również same programy występujące wyłącznie w postaci cyfrowej.

Drugą grupą przesłanek jest cel stosowania wyrobu założony przez producenta. Po pierwsze, musi być on przeznaczony dla ludzi. Po drugie, ma być wykorzystywany do szczególnych zastosowań medycznych, które obejmują diagnozowanie, profilaktykę, monitorowanie, przewidywanie, prognozowanie, leczenie lub łagodzenie choroby, urazu lub niepełnosprawności oraz dostarczanie informacji poprzez badanie *in vitro* próbek pobranych z organizmu ludzkiego. Do kategorii wyrobów medycznych zalicza się również wyroby do celów kontroli poczęć lub wspomagania poczęcia oraz produkty specjalnie przeznaczone do czyszczenia, dezynfekcji lub sterylizacji wyrobów medycznych. Jednocześnie, na podstawie art. 1 ust. 6 rozporządzenia, z zakresu wyrobów medycznych wyłączono między innymi produkty lecznicze w rozumieniu art. 1 pkt 2 dyrektywy 2001/83/WE[11] oraz produkty lecznicze terapii zaawansowanych[12] i wyroby medyczne do diagnostyki *in vitro* objęte rozporządzeniem (UE) 2017/746[13].

Ustawodawca przewidział regulację produktów, które mogą być stosowane do celów tak medycznych, jak i niemedycznych. Zgodnie z art. 1 ust. 3 rozporządzenia w takiej sytuacji konieczne jest łączne spełnienie wymogów dla wyrobów medycznych oraz dla wyrobów niemających przewidzianego takiego zastosowania. Należy zwrócić uwagę, że z perspektywy cyberbezpieczeństwa źródłem takich wymagań mogą być zobowiązania publicznoprawne, prywatnoprawne i standardy własne (Rojszczak, 2018, s. 306–309). Tym samym miernik spełnienia wymagań dla wyrobu medycznego może znajdować się poza normami prawa powszechnie obowiązującego. Należy zauważyć, że jest to korzystna sytuacja w kontekście zapewnienia bezpieczeństwa pacjentom, przy jednoczesnej dynamice zagrożeń w cyberprzestrzeni, która sprawia, że normy prawne nie zawsze zapewniają optymalne formy przeciwdziałania im. Normy branżowe zapewniają większą elastyczność w tym zakresie przez co skuteczniej przyczyniają się do tworzenia bezpiecznych urządzeń i oprogramowania z perspektywy cyberzagrożeń.

[11] Dyrektywa 2001/83/WE Parlamentu Europejskiego i Rady z dnia 6 listopada 2001 r. w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi (Dz.Urz. WE 2001 L 311/21).

[12] Rozporządzenie (WE) nr 1394/2007 z 13.11.2007 r. Parlamentu Europejskiego i Rady w sprawie produktów leczniczych terapii zaawansowanej i zmieniające dyrektywę 2001/83/WE oraz rozporządzenie (WE) nr 726/2004 (Dz.Urz. UE 2007 L 324/121).

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5.04.2017 r. w sprawie wyrobów medycznych do diagnostyki *in vitro* oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz.Urz. UE 2017 L 117/176).

Prawodawca przewidział specjalną procedurę dla produktów niemających przewidzianego zastosowania medycznego, ale jednocześnie w odniesieniu do ich właściwości oraz związanego z nimi ryzyka mających uzasadnione podobieństwo do wyrobu medycznego. Wykaz takich produktów znajduje się w załączniku XVI do rozporządzenia 2017/745 i obejmuje między innymi sprzęt emitujący promieniowanie elektromagnetyczne o wysokim natężeniu oraz sprzęt przeznaczony do stymulacji mózgu za pomocą prądów elektrycznych lub pól magnetycznych lub elektromagnetycznych, które przenikają przez czaszkę, aby zmienić czynność neuronów w mózgu. W tym zakresie przewidziane jest stosowanie stosowania wspólnych specyfikacji, które będą bazować na istniejących normach zharmonizowanych dla analogicznych wyrobów o zastosowaniu medycznym opartych na podobnej technologii. Artykuł 1 ust. 2 rozporządzenia przewiduje, że akty te zostaną przyjęte do 26 maja 2020 r., co powoduje, że wejdą w życie równocześnie z rozporządzeniem. Wydaje się, że taka regulacja powinna zabezpieczać osoby, które w przeciwnym wypadku zdane byłyby na przepisy prawa konsumenckiego zapewniającego niższy standard ochrony.

3. Oprogramowanie odrębne jako wyrób medyczny

Jak wskazano powyżej, oprogramowanie odrębne to takie, które jest niezależne od urządzenia i może być uznane za wyrób medyczny. Należy zauważyć, że kategoria „oprogramowań odrębnych" jest bardzo zróżnicowana zarówno pod kątem skomplikowania, jak i sposobów tworzenia i dystrybucji. Do tej grupy mogą zaliczać się proste aplikacje wspierające udzielanie usług medycznych na odległość, czy darmowe aplikacje na telefony komórkowe zawierające ćwiczenia dla osób ze schorzeniami narządów ruchu. Równocześnie w obrocie funkcjonują złożone systemy, takie jak IBM Watson for Oncology[14], który analizuje dokumentację medyczną pacjenta przez pryzmat wytycznych dotyczących leczenia i publikacji naukowych i proponuje potencjalne metody terapii uszeregowane według skuteczności czy też GastroView[15] automatycznie klasyfikujący anomalie w układzie pokarmowym na podstawie obrazu z badania endoskopowego.

Zakwalifikowanie danego typu oprogramowania jako wyrobu medycznego jest zależne od celu, w jakim zostało ono stworzone. Zgodnie z motywem 19 rozporządzenia, jeżeli producent przewidział zastosowanie danej aplikacji do co najmniej jednego z zastosowań medycznych wyszczególnionych w definicji wyrobu medycznego, wówczas oprogramowanie to będzie stanowić taki wyrób. Natomiast w sytuacji, w której dany program ma zastosowania ogólne, mimo że jest używany w ochronie zdrowia, nie będzie miał charakteru wyrobu medycznego, podobnie jak aplikacje związane ze stylem życia lub samopoczuciem.

Ma to szczególnie istotne znaczenie wobec regulacji dyrektywy 2019/770[16], która normuje stosunki pomiędzy przedsiębiorcami a konsumentami w zakresie umów o dostarczanie treści cyfrowych lub usługi cyfrowej. Zgodnie z art. 8 ust. 1 lit. a tego aktu prawnego obowiązkiem dostarczającego jest zagwarantowanie bezpieczeństwa, jakie jest typowe dla tego samego rodzaju treści cyfrowych lub usług cyfrowych i którego konsument może zasadnie oczekiwać, biorąc pod uwagę charakter treści cyfrowych lub usług cyfrowych oraz oświadczenia publiczne złożone przez przedsiębiorcę. Jednocześnie motyw 29 tej dyrektywy wskazuje, że nie ma ona zastosowania

[14] https://www.ibm.com/pl-pl/marketplace/clinical-decision-support-oncology (dostęp: 15.01.2020).

[15] http://cta.ai/pl/projekty/gastro-view (dostęp: 15.01.2020).

[16] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.Urz. UE 2019 L 136/1).

do wyrobów medycznych przepisywanych lub dostarczanych przez pracownika służby zdrowia. Natomiast w przypadku wyrobów, które konsument może otrzymać bez ich przepisania lub dostarczenia przez pracownika służby zdrowia, takich jak aplikacje zdrowotne, przepisy dyrektywy powinny znajdować zastosowanie.

W przypadku oprogramowania o charakterze ogólnym, do którego zaliczają się przykładowo systemy zarządzania ruchem pacjentów czy dokumentacją medyczną, należy pozytywnie ocenić zamysł prawodawcy. Natomiast w przypadku aplikacji związanych ze stylem życia trzeba wskazać na jego niekonsekwencję. Brakuje bowiem procedury powielającej rozwiązania dla produktów mających uzasadnione podobieństwo do wyrobu medycznego. Wydaje się, że z perspektywy bezpieczeństwa odbiorcy kryterium kwalifikacji do zbioru wyrobów medycznych powinna być spełniana funkcja, a nie decyzja producenta o jego zastosowaniu.

4. Klasyfikacja oprogramowania jako wyrobu medycznego

Dotychczasowe przepisy oraz międzynarodowa praktyka dotycząca wyrobów medycznych wprowadzały ich podział na cztery klasy: I, IIa, IIb oraz III. Art. 51 ust. 1 rozporządzenia 2017/745 utrzymuje ten podział. Zgodnie z tym przepisem kryterium przypisania do poszczególnych kategorii jest poziom ryzyka związanego narażeniem życia i zdrowia człowieka. Jednocześnie motyw 58 rozporządzenia wskazuje, że powinno się również uwzględniać sposób produkcji wyrobów i ich projekt techniczny. Ostatnia z przesłanek jest podstawą do zbadania czy zostały uwzględnione zasady cyberbezpieczeństwa na etapie jego projektowania. Należy zwrócić uwagę, że koncepcja *secure by design* odnosząca się w szczególności do oprogramowania i urządzeń Internetu rzeczy jest standardem branżowym (OWASP, 2019) i zalecanym sposobem postępowania przez brytyjskie ministerstwo do spraw cyfryzacji i przemysłów kreatywnych (DCMS, 2018a, s. 19–23).

Klasyfikację wyrobów medycznych przeprowadza się zgodnie z załącznikiem VIII do rozporządzenia. W przypadku oprogramowania zależy ona od tego czy steruje ono wyrobem lub wpływa na jego używanie, czy też jest to oprogramowanie odrębne. W pierwszej sytuacji program klasyfikuje się w tej samej klasie, co dany wyrób. Natomiast w drugiej proces kwalifikacji jest niezależny.

Zgodnie z punktem 6.3 załącznika VIII do klasy IIa zalicza się programy dostarczające informacje wykorzystywane przy podejmowaniu decyzji do celów diagnostycznych lub terapeutycznych oraz oprogramowanie przeznaczone do monitorowania procesów fizjologicznych oraz zgodnie z punktem 7.4 wyroby przeznaczone specjalnie do rejestracji obrazów diagnostycznych uzyskiwanych za pomocą promieniowania rentgenowskiego. Klasa IIb jest przeznaczona dla programów dostarczających informacje do podejmowania decyzji w przypadku, gdy skutkiem takiej decyzji może być poważne pogorszenie stanu zdrowia danej osoby lub konieczność interwencji chirurgicznej oraz programy monitorujące procesy fizjologiczne w przypadku, gdy zmiana tych parametrów może powodować bezpośrednie zagrożenie dla pacjenta.

Do klasy III zalicza się oprogramowanie wykorzystywane przy podejmowaniu decyzji, jeżeli ich skutkiem może być zgon danej osoby albo nieodwracalne pogorszenie stanu jej zdrowia oraz zgodnie z punktem 7.9 aktywne wyroby terapeutyczne ze zintegrowaną lub wbudowaną funkcją diagnostyczną, która w istotnym stopniu wpływa na postępowanie z pacjentem za pośrednictwem wyrobu, takie jak systemy o obiegu zamkniętym lub automatyczne defibrylatory zewnętrzne. Pozostałe oprogramowanie zalicza się do klasy I.

Przypisanie do określonej kategorii wyrobów rodzi skutki związane z wyborem typu procedury oceny zgodności, a tym samym ma wpływ na koszty ich wprowadzenia na rynek. Jednocześnie w przypadku wyrobów klasy IIa, IIb i III w procesie klasyfikacji obowiązkowy jest udział jednostki notyfikowanej. W przypadku wyrobów klasy I klasyfikacja może być przeprowadzana na wyłączną odpowiedzialność producentów. Należy jednak zwrócić uwagę, że w procesie oceny powinny być brane pod uwagę kwestie związane z cyberbezpieczeństwem, a w szczególności skutki przejęcia kontroli nad programem, zakłócenie działania programu polegające na wskazywaniu błędnych decyzji, na przykład w wyniku ataku typu *poison pill* oraz brak dostępu do oprogramowania na przykład w wyniku ataku typu *ransomware* lub DDoS. Odmienne rozumienie skutków, a w szczególności stopnia ryzyka przeprowadzenia ataku może rodzić potencjalne pole sporu pomiędzy producentami i jednostkami notyfikowanymi. Prawodawca przewidział w art. 51 ust. 2 rozporządzenia 2017/745, że co do zasady będą one rozstrzygane przez właściwy organ w państwie członkowskim, w którym producent ma zarejestrowane miejsce prowadzenia działalności. W przypadku polskiego porządku prawnego, zgodnie z art. 37 ust. 1 ustawy o wyrobach medycznych nadzór nad autoryzowanymi przez ministra właściwego do spraw zdrowia jednostkami notyfikowanym sprawuje ten minister, we współpracy z Prezesem Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych. Wydaje się więc, że będą to właściwe organy do rozstrzygania takiego sporu. Jednocześnie w przypadku cyberbezpieczeństwa należy mieć na względzie, że naczelną regułą powinna być dyrektywa bezpieczeństwa pacjenta.

IV. Zasady wprowadzania do obrotu urządzeń medycznych

Artykuł 5 ust. 1 rozporządzenia 2017/745 wprowadza ogólną regułę stanowiącą, że wyrób medyczny może zostać wprowadzony do obrotu lub używania jedynie wtedy, gdy przy należytym dostarczeniu i prawidłowej instalacji, konserwacji i używaniu zgodnie z przewidzianym zastosowaniem jest on zgodny ze wszystkimi przepisami zawartymi w rozporządzeniu. W pierwszym rzędzie dotyczy to ogólnych wymogów dotyczących bezpieczeństwa określonych w załączniku I. Ponadto wymagane jest ustanowienie i utrzymywanie systemu zarządzania ryzykiem, prowadzenie oceny klinicznej produktu, w tym obserwacji klinicznych po wprowadzeniu do obrotu, sporządzanie i bieżące aktualizowanie dokumentacji technicznej, sporządzanie deklaracji zgodności UE i umieszczenie oznakowania zgodności CE.

W przypadku programów komputerowych załącznik I, oprócz ogólnej reguły nakazującej ich projektowanie i produkowanie w taki sposób, by w normalnych warunkach używania były odpowiednie do ich przewidzianego zastosowania, prawodawca przewidział specjalne regulacje dotyczące elektronicznych systemów programowalnych. W rozumieniu punktu 17 ust. 1 systemy te obejmują oprogramowania zarówno połączone z innym urządzeniem, jak i odrębne. W zakresie cyberbezpieczeństwa podstawowe znaczenie ma norma zawarta w punkcie 17 ust. 2, która wprost nakazuje wytwarzanie i rozwijanie oprogramowania zgodnie z aktualnym stanem wiedzy dotyczącym bezpieczeństwa informacji. Biorąc pod uwagę cel rozporządzenia, wydaje się, że właściwym miernikiem oceny zachowania producenta będzie najwyższa staranność. Z tego można wyinterpretować obowiązek spełnienia zaostrzonych norm bezpieczeństwa w chwili produkcji urządzenia, ale również monitorowania i reagowania na pojawiające się podatności zagrażające bezpieczeństwu korzystania z oprogramowania zgodnie z jego cyklem życia. Ma to szczególne

znaczenie z perspektywy bezpieczeństwa pacjenta, zwłaszcza w kontekście wskazywanej w literaturze tendencji pomijania kwestii bezpieczeństwa na etapie modernizacji oprogramowania (Nowak, 2018, s. 193).

Kolejnym wymogiem bezpieczeństwa, wynikającym z punktu 17 ust. 4 załącznika I, jest określenie przez producenta minimalnych wymagań dotyczących sprzętu, właściwości sieci informatycznej oraz środków bezpieczeństwa informatycznego, niezbędnych do zgodnego z przeznaczeniem działania oprogramowania. O ile dwie pierwsze przesłanki można potraktować jako określenie minimalnych wymagań sprzętowych, o tyle trzecia może mieć kluczowe znaczenie z perspektywy przenoszenia odpowiedzialności za cyberbezpieczeństwo urządzenia na nabywcę. Taka sytuacja będzie miała miejsce, jeśli producent wskaże bez koniecznego uzasadnienia rygorystyczne środki bezpieczeństwa, na przykład polegające na analizie oprogramowania pod kątem ujawnianych podatności. Należy jednak w tym względzie mieć na uwadze wskazanie przez prawodawcę określenia „minimalne wymagania". Wykładnia językowa tego zwrotu przesądza o przyjęciu perspektywy równoważącej ryzyko związane z korzystaniem ze sprzętu z obowiązkami użytkownika. Wydaje się, że nie powinny wychodzić one poza katalog dobrych praktyk, takich jak regularne aktualizacje, stosowanie oprogramowania antywirusowego czy *firewall*. Natomiast kwestia monitorowania zagrożeń i podatności powinna być zawsze po stronie producenta.

Zgodnie z punktem 23 ust. 4 lit. ab informacje dotyczące minimalnych wymagań dotyczących sprzętu, właściwości sieci informatycznej oraz środków bezpieczeństwa informatycznego umieszcza się instrukcji obsługi wyrobu medycznego. Ponadto dokument ten zawiera specyfikacje niezbędne użytkownikowi do prawidłowego użycia produktu. W ich zakres będą wchodzić wyszczególnienie cech użytkowych programu oraz jego funkcji i zasad ich działania. Należy jednak zwrócić uwagę, że punkt 23 ust. 1 lit. d nie nakłada obowiązku dostarczania instrukcji dla wyrobów klasy I i IIa, o ile można z nich bezpiecznie korzystać bez takiego dokumentu. Wydaje się jednak, że tego wyjątku nie można zastosować do oprogramowania, chociażby ze względu na brak wiedzy dotyczący wymagań sprzętowych, który może uniemożliwić jego uruchomienie. W tym zakresie należy zatem postulować konieczność dostarczania instrukcji niezależnie od klasyfikacji do określonej klasy produktu medycznego.

Osobnym wymogiem w zakresie bezpieczeństwa jest interoperacyjność i kompatybilność wyrobów przeznaczonych do korzystania wraz z innymi wyrobami medycznymi. Zgodnie z definicją legalną zawartą w art. 2 pkt. 25 rozporządzenia 2017/745 kompatybilność oznacza zdolność wyrobu do łącznego stosowania go z najmniej jednym innym wyrobem bez utraty lub osłabienia zdolności do działania zgodnego z przeznaczeniem oraz bez konieczności modyfikacji lub dostosowania jakiejkolwiek części połączonych wyrobów. Natomiast definiowana w art. 2 pkt 26 rozporządzenia interoperacyjność oznacza możliwość współpracy i komunikowania się między sobą co najmniej dwóch różnych wyrobów oraz wymiany i stosowania informacji do prawidłowego wykonania konkretnej funkcji bez zmiany zawartości tych danych. Realizacja tych warunków wpływa w szczególności na dostępność informacji rozumianą jako wgląd w nią upoważnionej osoby (Dysarz, 2019, s. 9). W warunkach świadczenia usług medycznych ma to istotne znaczenie z perspektywy szybkości udzielenia pomocy oraz dysponowania pełnią danych przez osobę jej udzielającej, co może niejednokrotnie mieć rozstrzygające znaczenie w sytuacji zagrożenia życia. Jednocześnie zobowiązanie producentów do takiego działania przeciwdziała tendencji do

tworzenia własnych standardów wymiany danych, co wobec różnorodności urządzeń wykluczałoby w zasadzie wymianę danych.

Do obowiązków producenta związanych z wprowadzeniem produktu na rynek należy przygotowanie jego dokumentacji technicznej zgodnie z kryteriami zawartymi w załączniku II. W szczególności zawiera ona wyniki wszystkich testów lub badań weryfikacyjnych i walidacyjnych oraz ich krytyczną analizę, które zostały przeprowadzone w celu wykazania zgodności wyrobu z wymogami rozporządzenia 2017/745. W odniesieniu do oprogramowania pkt 6 ust. 1 lit. b wymaga zawarcia szczegółowych informacji dotyczących projektu badania, pełnych protokołów testów lub badania, metod analizy danych. Obejmuje to opis projektu oprogramowania, proces jego rozwoju oraz dowody potwierdzające walidację oprogramowania w postaci stosowanej w gotowym wyrobie, w tym opis testów w środowisku użytkownika. Ponadto konieczne jest uwzględnienie działania programu w różnych konfiguracjach sprzętowych. Należy zauważyć, że przepis nie wymaga wprost żadnych szczególnych badań w zakresie cyberbezpieczeństwa, takich jak testy penetracyjne. Należy jednak uznać, że bardzo szeroki zakres obowiązków producenta obejmuje również te kwestie, a brak szczegółowych wskazań wynika z chęci zachowania aktualności przepisów wobec szybko postępujących zmian w zakresie technologii.

Kluczowym zagadnieniem z perspektywy cyberbezpieczeństwa jest ustalenie wersji oprogramowania wykorzystywanego w określonym urządzeniu medycznym. Przepisy rozporządzenia nie narzucają w tej kwestii obowiązku umieszczania informacji na ten temat ani na etykiecie urządzenia, ani w instrukcji obsługi. Jednocześnie zgodnie z art. 10 ust. 7 rozporządzenia 2017/745 producent zobowiązany jest do oznaczenia wyrobu za pomocą kodu UDI. Według art. 2 pkt 5 tego aktu prawnego kod ten składa się z sekwencji znaków umożliwiających jednoznaczną identyfikację konkretnego wyrobu na rynku. Należy zauważyć, że umieszczenie kodu UDI jest niezależne od innych sposób oznakowania wyrobu i w żaden sposób ich nie zastępuje. Kod ten składa się z dwóch części: kodu UDI-DI i kodu UDI-PI. Pierwszy z nich wskazuje na model wyrobu, natomiast drugi identyfikuje jednostkę produkcji wyrobu.

Reguły nadawania kodu UDI w przypadku oprogramowania określone są w punkcie 6 załącznika VI do rozporządzenia. Zasadą jest nadawanie go na poziomie oprogramowania i umieszczanie go na opakowaniu, jeżeli program jest dostarczany na nośniku fizycznym lub na ekranie łatwo dostępnym dla użytkownika w łatwo czytelnym formacie zwykłego tekstu. Jeżeli program nie ma interfejsu użytkownika, wówczas kod powinien być przekazywany za pomocą API.

Co do zasady wszelkie zmiany w oprogramowaniu wymagają zmiany kodu UDI. W szczególności jest to wymagane, gdy modyfikacja dotyczy pierwotnego działania, bezpieczeństwa lub przewidywanego użycia oprogramowania lub sposobu interpretacji danych. Zgodnie z punktem 6.5.3 załącznika VI niewielkie zmiany oprogramowania wymagają nowego kodu UDI-PI, ale nie nowego kodu UDI-DI. Decyzję w zakresie tego czy zmiana jest niewielka podejmuje producent wyrobu. Aby ułatwić podjęcie decyzji, prawodawca wskazał przykładowe czynności, które można zaliczyć do niewielkich zmian. Są nimi poprawki związane z usuwaniem błędów lub polepszaniem użyteczności, jeżeli nie służą podniesieniu bezpieczeństwa lub są poprawkami zabezpieczeń. Należy z tego wnioskować, że każda zmiana dotycząca cyberbezpieczeństwa wyrobu będzie wymagała nowego kodu UDI-PI. Jest to niewątpliwe korzystne z perspektywy bezpieczeństwa użytkownika zważywszy na to, że podatności w oprogramowaniu najczęściej dotyczą jego określonych wersji.

Tym samym producent nie tylko może ocenić ile wyrobów jest zagrożonych podatnością, lecz także dotrzeć do nabywców lub podmiotów wprowadzających wyrób na rynek i bezpośrednio zakomunikować im o konieczności przeprowadzenia aktualizacji.

V. Nadzór nad cyberbezpieczeństwem wyrobu wprowadzonego do obrotu

Zachowanie wysokiego poziomu cyberbezpieczeństwa jest procesem dynamicznym. Wynika to z funkcjonalnej definicji tego pojęcia, która wskazuje na zmienność jej poziomu w czasie i zależność od działań innych podmiotów (Banasiński, 2018, s. 29). Ma to szczególne znaczenie w przypadku wyrobów medycznych, co do których planowany jest wieloletni okres użytkowania. Jednocześnie w praktyce cykl życia produktu nie zawsze pokrywa się z cyklem życia oprogramowania, co prowadzi do powstania tzw. *orphant devices,* czyli urządzeń, których oprogramowanie nie jest aktualizowane. Tym samym są one potencjalnym źródłem zagrożeń zarówno dla użytkownika, jak i innych podmiotów użytkujących cyberprzestrzeń, służąc na przykład jako narzędzia do prowadzenia ataków DDoS (Marvin, 2017).

W przypadku wyrobów medycznych rozporządzenie 2017/745 przewiduje rozbudowany katalog obowiązków producenta związanych z bezpieczeństwem wyrobu, który został wprowadzony do obrotu. Obejmuje on również oprogramowanie odrębne oraz oprogramowanie będące częścią innego produktu. Podstawowym zadaniem wytwórcy jest ustanowienie systemu nadzoru każdego wyrobu, który został wprowadzony do obrotu. Artykuł 83 ust. 1 rozporządzenia stanowi, że ma być on proporcjonalny do klasy ryzyka i odpowiedni dla danego rodzaju wyrobu by pozwalać na systematyczne gromadzenie, zapisywanie i analizowanie odpowiednich danych dotyczących jakości, działania i bezpieczeństwa wyrobu w całym jego okresie używania. Podstawą tego systemu jest plan nadzoru, który jest również częścią dokumentacji technicznej wyrobu, chyba że został on wykonany na zamówienie.

Jednocześnie, niezależnie od spełnienia innych wymogów, rozporządzenie nakłada obowiązek sporządzania i aktualizowania dokumentacji technicznej dotyczącej nadzoru po wprowadzeniu do obrotu. Wymagania co do jej sporządzenia zawiera załącznik III. Nie zawiera on jednak wytycznych odnoszących się bezpośrednio do kwestii związanych z bezpieczeństwem cybernetycznym. Natomiast pośrednio kwestie te będą regulowane przez nakaz ustalenia odpowiednich wskaźników i wartości progowych, które są stosowane w stałej ocenie analizy stosunku korzyści do ryzyka oraz plan zarządzania ryzykiem, a także plan obserwacji klinicznych po wprowadzeniu do obrotu.

Częścią dokumentacji technicznej są również raport z nadzoru po wprowadzeniu do obrotu, o którym mowa w art. 85 oraz okresowy raport o bezpieczeństwie, o którym mowa w art. 86. Pierwszy z nich dotyczy wyrobów klasy I i jest podsumowaniem wyników i wniosków z analiz danych z nadzoru po wprowadzeniu do obrotu zebranych w wyniku realizacji planu nadzoru po wprowadzeniu do obrotu. Ponadto zawiera uzasadnienie i opis podjętych działań zapobiegawczych i korygujących. Producent aktualizuje raport tylko w razie zaistnienia takiej konieczności. Nie ma również obowiązku przesyłania go do organu nadzoru, chyba że organ ten wystąpi z takim żądaniem.

Sporządzanie okresowego raportu o bezpieczeństwie jest obowiązkiem producentów wyrobów przypisanych do innej klasy niż I. W jego treści oprócz dziedzin tożsamych z raportem nadzoru

po wprowadzeniu do obrotu muszą być uwzględnione wnioski wynikające z ustalenia stosunku korzyści do ryzyka, główne ustalenia wynikające z obserwacji klinicznych po wprowadzeniu do obrotu, wielkość sprzedaży danego wyrobu oraz oszacowana liczebność i inne właściwości populacji korzystającej z danego wyrobu. Artykuł 86 ust. 1 rozporządzenia wprowadza nakaz aktualizacji okresowego raportu o bezpieczeństwie nie rzadziej niż raz do roku w przypadku wyrobów klasy IIb i klasy III oraz nie rzadziej niż co dwa lata w przypadku wyrobów klasy IIa. W przypadku wyrobów klasy III producenci przedkładają okresowe raporty jednostce notyfikowanej uczestniczącej w ocenie zgodności, która zapoznaje się z raportem i dodaje swoją ocenę do systemu elektronicznego, a następnie przekazuje ją organowi nadzorczemu. Natomiast raporty dotyczące wyrobów klasy IIa i IIb są obligatoryjnie udostępnienie jednostce notyfikującej, a właściwym organom na ich żądanie.

Należy zauważyć, że co do zasady, programy komputerowe należeć będą do klasy IIa i IIb. W konsekwencji monitorowanie ich działania będzie obligatoryjne przez cały cykl życia produktu. Niemniej jednak wydaje się prawodawca powinien *explicite* uwzględnić kwestie związane z cyberbezpieczeństwem. Tym samym dużą rolę w sferze kształtowania się postępowania producentów będą odgrywały jednostki notyfikujące oraz organy nadzoru analizujące raporty i mogące wskazywać obszary do poprawy lub uwzględnienia. Należy w tym względzie postulować ich aktywność, biorąc pod uwagę, że kwestia ta przekłada się bezpośrednio na bezpieczeństwo pacjenta.

VI. Podsumowanie

Rozporządzenie 2017/745 jest kompleksowym aktem regulującym całościowo kwestie związane z wyrobami medycznymi. Prawodawca uwzględnił fakt, że rozwój techniki doprowadził do powstania wyrobów medycznych ściśle powiązanych z oprogramowaniem oraz programów komputerowych działających niezależnie od urządzeń. Biorąc pod uwagę, że priorytetem konstrukcji wyrobów medycznych ma być bezpieczeństwo ich używania, w kontekście oprogramowania pierwszoplanową kwestią jest ich analiza pod kątem cyberbezpieczeństwa.

Należy zauważyć, że rozporządzenie nie posługuje się tym terminem. Można przyjąć, że prawodawca traktuje cyberbezpieczeństwo jako integralną część bezpieczeństwa produktu, nie poświęcając jednak temu zagadnieniu osobnego miejsca. Wydaje się, że wobec rozwoju technologii Internetu rzeczy, która jest szeroko wykorzystywana do celów medycznych, a także powszechnego wykorzystywania sieci i związanych z tym zagrożeń, problematyka ta powinna znaleźć szersze odbicie w rozporządzeniu, chociażby poprzez *explicite* wskazanie obowiązków w tym zakresie.

Jednocześnie należy pochwalić decyzję prawodawcy w zakresie kwalifikacji oprogramowania, które co do zasady będzie ujęte w klasie IIa. Przekłada się to zarówno na konieczność spełnienia większej liczby wymogów na etapie wprowadzania produktu na rynek, jak i obowiązku monitorowania działania urządzenia i aktualizowania dokumentacji technicznej po jego wprowadzeniu na rynek. Podkreślenia wymaga, że nie jest wprowadzony wprost obowiązek wydawania aktualizacji oprogramowania w przypadku stwierdzenia luk bezpieczeństwa, ale wykładnia przepisów nie pozostawia wątpliwości co do jego istnienia.

Podkreślić należy słuszną decyzję prawodawcy w zakresie konieczności oznaczania poszczególnych wersji oprogramowania, w których wprowadzono zmiany dotyczące bezpieczeństwa nowymi kodami UDI-PI. Pozwala to na weryfikację przez użytkownika czy wersja używana przez

niego jest aktualna, a także ocenę przez producenta ilościowej skali zagrożenia dotyczących niezaktualizowanych urządzeń.

Bardzo ważną częścią działań w zakresie cyberbezpieczeństwa będą praktyki jednostek notyfikowanych oraz organów nadzoru. Należy postulować, aby uwzględniały one ten aspekt zarówno w trakcie procedury wprowadzania produktu na rynek, jak i na etapie jego funkcjonowania na rynku, szczególnie w kontekście dynamiki procesu, jakim jest zapewnienie bezpieczeństwa wobec zagrożeń związanych z cyberprzestrzenią.

Bibliografia

Banasiński, C. (2018). Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni. W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

Cavelty, M.D., Camino Kavanagh, C. (2019). Cybersecurity and human rights. W: B. Wagner, M. Kettemann, K. Vieth (red.), *Research Handbook of Human Rights and Digital Technology.* Cheltenham: Edward Elgar. https://doi.org/10.4337/9781785367724.00012.

Chmielewski, J.M., Waćkowski, K. (2018). Technologie teleinformatyczne – podstawy, rozwój i bezpieczeństwo systemów teleinformatycznych. W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

DCMS. (2018). *Secure by Design: Improving the cyber security of consumer Internet of Things Report*. Department for Digital, Culture, Media and Sport. Pozyskano z: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf (15.01.2020).

Dysarz, J. (2019). Komentarz do artykułu 2. W: A. Beskierska (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz.* Warszawa: Wydawnictwo C.H. Beck.

Eide, A. i Eide, W.B. (2006). *A Commentary on the United Nations Convention on the Rights of the Child, Volume: 24*. Haga: Brill, Nijhoff.

ENISA. (2017). *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. Bruksela: European Union Agency For Network And Information Security. https://doi.org/10.2824/03228.

Gomułka, A. (2019). Tychy: seniorzy dostają z MOPS opaski monitorujące stan zdrowia, *Rynek Zdrowia*. Pozyskano z: http://www.rynekzdrowia.pl/Technologie-informacyjne/Tychy-seniorzy-dostaja-z-MOPS-opaski-monitorujace-stan-zdrowia,191338,7.html (15.01.2020).

Jara, S.M., Hopp, M.L. i Weaver, E.M. (2018). Association of Continuous Positive Airway Pressure Treatment With Sexual Quality of Life in Patients With Sleep Apnea – Follow-up Study of a Randomized Clinical Trial. *JAMA Otolaryngoly Head&Neck Surgery*, *7*(144). https://doi.org/10.1001/jamaoto.2018.0485.

Jurczak, T. (2020). *E-krzesło uratuje życie seniora*. Pozyskano z: https://www.sztucznainteligencja.org.pl/e-krzeslo-uratuje-zycie-seniora/ (15.01.2020).

Kosowska, A., Sowa, A. i Świerczyński, M. (2019). Medycyna precyzyjna w oparciu o dane z praktyki klinicznej. W: G. Szpor, K. Czaplicki (red.), *Internet. Analityka danych*. Warszawa: Wydawnictwo C.H. Beck.

Marvin, T. (2017). *Dziurawy Internet Rzeczy*. Pozyskano z: https://plblog.kaspersky.com/internet-of-vulnerabilities/8581/ (15.01.2020).

Nowak, M. (2003). *Introduction to the International Human Rights Regime*. Dordrecht: Brill, Nijhoff.

Nowak, W. (2019). Ochrona infrastruktury krytycznej w cyberprzestrzeni. W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

OWASP. (2018). *OWASP Internet of Things (IoT) Project*. Pozyskano z: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project (15.01.2020).

OWASP. (2019). *OWASP Security by Design Principles*. Pozyskano z: https://wiki.owasp.org/index.php/Security_by_Design_Principles (15.01.2020).

Rekomendacja ITU-T. (2013). *Overview of the Internet of things*. Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks. Next Generation Networks – Frameworks and functional architecture models. Recommendation ITU-T Y.2060. Geneva. Pozyskano z: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (15.01.2020).

Rojszczak, M. (2018). Cyberbezpieczeństwo z perspektywy przedsiębiorcy. W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.