t. LXXIII • nr 10/2020 (868) • DOI 10.33226/0137-5490.2020.10.5

Mgr Piotr Marciniak

Polska Akademia Nauk
ORCID: 0000-0002-4201-9311
e-mail: p.marciniak@doktorant.inp.pan.pl

Problem odpowiedzialności za błędy w oprogramowaniu IoT

The problem of liability for IoT software vulnerabilities

Streszczenie

Za poprawne działanie urządzeń IoT odpowiada zainstalowane w nich oprogramowanie. Może ono nie tylko zawierać luki, ale i ukryte przed nabywcą elementy lub może nie obejmować jakichkolwiek mechanizmów zapewniających cyberbezpieczeństwo. To sytuacja skrajnie niebezpieczna dla każdego użytkownika, również profesjonalnego. W artykule zaprezentowano obowiązujące regulacje w zakresie odpowiedzialności producentów za braki i błędy w oprogramowaniu, przybliżając istotne luki w zakresie ochrony nabywców z sektorów B2B i B2A. W konkluzjach, wskazując na celowość rozszerzenia obowiązujących na rynku konsumenckim regulacji dotyczących produktów niebezpiecznych, zawarto postulaty *de lege ferenda*.

Słowa kluczowe: IoT, oprogramowanie, prawo autorskie, produkt niebezpieczny, odpowiedzialność producenta

JEL: K240

Abstract

The firmware installed on IoT devices is responsible for their proper operation. It may have not only bugs, but also elements hidden from the buyer or the lack of any cybersecurity mechanisms. This is an extremely dangerous situation for any user, including professionals. The study introduces the applicable regulations in the field of producer responsibility for software deficiencies and errors, presenting significant lack of the protection of buyers from B2B and B2A sectors. The conclusions, pointing to the advisability of extending the regulations on defective products applicable to the consumer market, include *de lege ferenda* postulates.

Keywords: IoT, software, copyright, defective product, producer liability

Wstęp

Jednym z najważniejszych wyzwań legislacyjnych w nadchodzących latach, warunkującym najszerzej rozumiane bezpieczeństwo[1] wobec powszechnie wdrażanych rozwiązań informatycznych, jest uregulowanie kwestii odpowiedzialności producentów i dystrybutorów za wady oprogramowania urządzeń i systemów Internetu rzeczy (*Internet of Things* — IoT). Kategoria ta obejmuje zarówno sprzęt (*hardware*), jak i oprogramowanie (*software*), wsparte często centralnymi systemami przetwarzania i zarządzania gromadzonymi danymi.

Obowiązujące obecnie przepisy umożliwiają uniknięcie odpowiedzialności nie tylko za przypadkowe błędy w oprogramowaniu, ale również za wady kwalifikowane wskazane w treści niniejszego artykułu. Tymczasem trudno wyobrazić sobie dalszy rozwój technologii i wykorzystywanie jej na szeroką skalę, gdy jej dostawcy nie są skutecznie motywowani przepisami prawa do stosowania zabezpieczeń sprzętowych i programowych. W skrajnych przypadkach może to bowiem prowadzić m.in. do:

- ryzyka przejęcia kontroli nad urządzeniami medycznymi, takimi jak rozruszniki serca;
- zdalnego uruchomienia poduszek powietrznych lub hamulców w pojazdach;
- uwięzienia mieszkańców inteligentnego domu;
- katastrofy w ruchu lądowym, morskim lub lotniczym;
- sparaliżowania inteligentnego miasta, np. poprzez przejęcie kontroli nad sygnalizacją świetlną;
- ograniczania dostaw energii;
- zagrożenia dla bezpieczeństwa państwa poprzez ingerencję w funkcjonowanie systemów zarządzania kryzysowego opartych na rozwiązaniach IoT.

Artykuł ten ma charakter sygnalizacyjny. Skoncentrowa-

no się w nim na analizie polskiego porządku prawnego, a także na odniesieniach do konstrukcji produktu niebezpiecznego w regulacjach UE oraz orzecznictwie SN i TSUE. Sformułowano również wnioski *de lege ferenda*. Ramy artykułu uniemożliwiają podjęcie szerszych rozważań o ewentualnych rozwiązaniach problemu stosowanych w innych państwach. Odpowiedzialność za wady oprogramowania jest jednak kwestią kluczową, dlatego powinna być przedmiotem poszerzonej dyskusji akademickiej i skutecznej ochrony prawnej.

Raport Grupy Roboczej IoT z 31.07.2019 r.

Raport Grupy Roboczej do spraw Internetu Rzeczy (dalej GR IoT[2]) „IoT w polskiej gospodarce”[3] wskazuje jednoznacznie na konieczność wypracowania kompetencji i regulacji prawnych dotyczących IoT[4]. Adnotacja do rozdziału 8 „Bezpieczeństwo i certyfikacja” mówi wprost: „IoT bez cyberbezpieczeństwa stanowi większe zagrożenie dla państwa niż rezygnacja z użycia IoT”[5]. W rozdziale tym wskazuje się m.in. sześć kategorii, w jakich należy rozważać bezpieczeństwo systemów IoT. W niniejszych rozważaniach kluczowe są trzy następujące:

- cyberbezpieczeństwo produktu, rozumiane jako odpowiedni poziom wykonania produktu oraz wyposażenia go w narzędzia i mechanizmy przeciwdziałające zagrożeniom teleinformatycznym;
- bezpieczeństwo danych przetwarzanych przez produkt lub ekosystem informacji dotyczących otoczenia, zarówno osobowych, jak i technicznych (np. telemetrycznych, nieosobowych);
- bezpieczeństwo fizyczne dotyczące wpływu technologii IoT i jej zastosowania na świat fizyczny (oddziaływanie bezpośrednie i wpływ świata IoT na codzienne życie obywateli, np. funkcje blokady drzwi, ruch pojazdu autonomicznego, kontrola sieci energetycznych czy prawidłowe działanie urządzenia telemedycznego, takiego jak stymulator serca)[6].

Dodatkowo poruszana jest sygnalizacyjnie kategoria „bezpieczeństwo narodowe i militarne”[7] w kontekście przepisów kodeksu karnego.

Analiza Raportu i dorobku GR IoT wskazuje, iż w toku prac większość ekspertów koncentruje się przede wszystkim na szczegółowych problemach i propozycjach rozwiązań. To bezsprzecznie efektywne podejście, pozwalające wypracować szereg potrzebnych rozwiązań szczegółowych. Jednak wspólnym i krytycznym zagadnieniem dla wszystkich wdrożeń IoT jest kwestia odpowiedzialności producentów i dystrybutorów za jakość i bezpieczeństwo urządzeń IoT oraz powiązanych z nimi systemów. Bez przedmiotowych regulacji w świetle analizowanych poniżej przepisów odpowiedzialność producentów nawet za ewidentne wady lub braki sprzedawanych urządzeń jest symboliczna[8] lub żadna[9]. W efekcie producenci nie mają motywacji do dbania o bezpieczeństwo oprogramowania swoich urządzeń IoT[10], a użytkownicy nie mają zapewnionej niezbędnej ochrony prawnej.

Pojęcie Internetu rzeczy (IoT)

W polskim prawie brakuje definicji legalnej pojęcia Internetu rzeczy. Jednak definicje IoT zawiera wiele opracowań krajowych i międzynarodowych[11]. Raport GR IoT przybliża kilka możliwych, opisowych perspektyw spojrzenia na Internet rzeczy[12]. Co istotne, w kontekście niniejszych rozważań dokument ten koncentruje się na perspektywie makro obejmującej kilka możliwych spojrzeń na cały ekosystem IoT. Tymczasem analiza i projektowanie zasad odpowiedzialności za wady oprogramowania konkretnego urządzenia lub modelu urządzeń wymaga również spojrzenia w skali mikro, koncentrującego się na pojedynczym urządzeniu lub systemie zależności (np. czujnik–sieć–kontroler).

Na potrzeby niniejszego artykułu za Internet rzeczy (IoT) w ujęciu mikro uznaje się urządzenie lub zespół urządzeń wyposażonych w oprogramowanie i podłączonych do sieci telekomunikacyjnej, z wykorzystaniem której przesyłane są dane, polecenia oraz aktualizacje do i z urządzeń. Transfer danych w ramach sieci IoT odbywa się zarówno pomiędzy urządzeniami (M2M), jak i do centrów ich przetwarzania. Stąd nie zawsze można rozważać IoT w oderwaniu od *Big Data* i ujęcia makro, czyli również baz danych i mechanizmów gromadzenia oraz przetwarzania danych[13]. Należy również wyraźnie podkreślić, że urządzenia bez oprogramowania lub dostępu do sieci nie należą do grupy IoT.

Jak widać z powyższych rozważań, tym co wyróżnia IoT spośród wszystkich innych urządzeń, jest zdolność gromadzenia i przekazywania danych z wykorzystaniem sieci telekomunikacyjnej. Niektóre z urządzeń posiadają ponadto możliwość ich analizy i podejmowania działań[14]. Stąd urządzenia IoT często potocznie i marketingowo określane są jako „inteligentne” (*smart*).

Przykładem prostego urządzenia IoT jest „inteligentny” termometr. Mierzy on temperaturę (jako czujnik) i udostępnia tę informację, wykorzystując swoje oprogramowanie i sieć telekomunikacyjną, odbiorcom, którymi mogą być zarówno inne urządzenia (np. monitorujące warunki środowiskowe czy procesy technologiczne), jak i aplikacje wykorzystywane przez człowieka.

Bardziej złożonym przykładem IoT jest pojazd autonomiczny, który w zależności od wyposażenia, uczestnicząc w ruchu drogowym, może równocześnie:

- gromadzić dane dotyczące otoczenia i innych użytkowników ruchu;
- komunikować się z czujnikami i urządzeniami umieszczonymi w pasie ruchu celem uzyskania dodatkowych informacji o otoczeniu, zdarzeniach, zagrożeniach;
- wymieniać informacje z centrami sterowania ruchem lub innymi pojazdami, które również mogą być źródłem informacji związanych z monitoringiem ruchu drogowego, wykroczeniami, analizami środowiskowymi itd.;
- wspierając kierującego, przetwarzać dane[15], które w przypadku pojazdów w pełni autonomicznych będą decydowały o zachowaniu się pojazdu na drodze[16].

W każdym przypadku elementem odróżniającym choćby zwykły termometr cyfrowy od inteligentnego termometru jest nie tyle samo oprogramowanie, ale dostęp urządzenia do sieci telekomunikacyjnej.

Podatności IoT na cyberzagrożenia

Urządzenia podłączone do sieci muszą być badane w kontekście cyberbezpieczeństwa (a nie tylko ich fizycznego bezpieczeństwa), a zatem:

- ich odporności lub podatności (Hoffmann, Stanik, Napiórkowski, 2017)[17] na dostęp osób nieuprawnionych — przede wszystkim pod kątem istnienia skutecznych zapór sieciowych (*firewall*), bezpiecznych protokołów komunikacji i braku sztywno zdefiniowanych kont administracyjnych i serwisowych, dla których nie można zmienić hasła;
- ukrytych w oprogramowaniu urządzenia funkcjonalności i kont umożliwiających dostęp do urządzenia przez osoby trzecie;
- możliwości i warunków uruchomienia dodatkowego kodu lub funkcjonalności;
- nadzorowania bezpieczeństwa aktualizacji oprogramowania.

Należy wyraźnie odróżnić przypadkową lukę w oprogramowaniu od świadomie umieszczonych w nim podatności na ataki lub braku jakichkolwiek zabezpieczeń. Wiedzę tę, przynajmniej na podstawowym poziomie, muszą posiadać zarówno prawnicy zajmujący się odpowiedzialnością za wady oprogramowania, jak i składy orzekające w tego typu sprawach.

Liczba urządzeń IoT szacowana jest obecnie na 10–50 mld szt.[18] i będzie rosła. Nie istnieje jednak ich rejestr, a i same urządzenia pełnią różne funkcje. To właśnie wzrost liczby urządzeń IoT i prognozowanej ilości przesyłanych przez nie danych jest głównym powodem wdrażania sieci 5G na świecie. A blisko połowę z nich przetwarzają obecnie systemy rozproszone — czasem są to same urządzenia IoT[19]. Fakt ten dodatkowo wzmacnia tezę o konieczności budowy spójnej regulacji w zakresie bezpieczeństwa oprogramowania i odpowiedzialności za efekty jego działania — zarówno w zakresie urządzeń IoT, jak i powiązanych z nimi systemów sztucznej inteligencji (*artificial intelligence* — AI)[20] oraz *Big Data*.

Tymczasem cyberbezpieczeństwo dla większości osób jest pojęciem abstrakcyjnym, filmowym, ewentualnie ograniczonym do wąskich sfer, takich jak poczta elektroniczna czy dostęp do konta bankowego. Pojawia się ono czasem w kontekście wycieku prywatnych zdjęć celebrytów czy artykułów o możliwych manipulacjach wyborczych. Jednak dynamicznie rosnąca liczba inteligentnych urządzeń poszerza horyzont potencjalnych naruszeń, a także umożliwia wpływanie na obywateli, przedsiębiorstwa i państwa lub wręcz ich kontrolowanie. Jest to możliwe dzięki gromadzonym oraz przetwarzanym danym i kontroli działania różnorodnych systemów. Trzeba przy tym pamiętać, iż w sieci nie ma urządzeń, których nie można wykorzystać do innych celów niż ich formalne przeznaczenie. Obok lub zamiast oryginalnego oprogramowania może bowiem znajdować się inne, realizujące dodatkowe zadania.

Przedmiot i przyczyny odpowiedzialności producenta. Wady kwalifikowane

Rewolucja cyfrowa obejmująca wszystkie dziedziny życia (m.in. edukację, zdrowie, przemysł, rolnictwo, transport, cyfrową tożsamość, bezpieczeństwo państwa) wymaga przedefiniowania problematyki odpowiedzialności producenta[21] za oprogramowanie. Istnieją formalnie dwa sposoby pociągnięcia do odpowiedzialności producenta lub dystrybutora za wady IoT:

1. Odpowiedzialność z tytułu sprzedaży rzeczy[22].
2. Odpowiedzialność z tytułu wad oprogramowania[23].

Gdy elementy rozwiązań IoT są sprzedawane jako rzecz, zastosowanie ma rękojmia i bardzo często — gwarancja. Egzekucja odpowiedzialności w tym zakresie nie wymaga rozwinięcia w niniejszym opracowaniu (szerzej o tym: Falkowska, 2010, s. 271–272; Kwasiński, Łanowy, 2018)[24]. Jeśli jednak oprogramowanie (*software* lub *firmware*[25]) podlega odrębnej regulacji kontraktowej lub licencyjnej (Barta (red.), 2017, s. 752–765; Barta, Markiewicz, 2019)[26] od sprzedaży samych urządzeń (*hardware*), pojawia się problem zdefiniowania prawnych granic odpowiedzialności producenta za oprogramowanie. Nasuwa suwa się też pytanie, czy i jakie klauzule wyłączeniowe mogą być zawarte zarówno w kontraktach, jak i licencjach adresowanych do różnych odbiorców (B2C/B2B). W kontekście powyższych rozważań należy wskazać na dwie sytuacje, które wymagają analizy pod względem odpowiedzialności cywilnej i karnej producentów IoT:

1. Odpowiedzialność za wady oprogramowania prostych urządzeń, które nie analizują pozyskiwanych danych, ale mogą stanowić bramę do naruszeń bezpieczeństwa sieci telekomunikacyjnych w przypadku, gdy ich oprogramowanie nie posiada zabezpieczeń uniemożliwiających nieautoryzowany dostęp i ich wykorzystanie w celu wyrządzenia szkody przez osoby trzecie. W tym przypadku chodzi zarówno o pozyskanie danych (np. z systemu monitoringu) do popełnienia przestępstwa lub wyrządzenia szkody, jak i sytuacje, w których istnieje możliwość uruchomienia w urządzeniu dodatkowych funkcji (nieujętych w specyfikacji) lub instalacji dodatkowego oprogramowania, które służy lub może służyć do wyrządzenia szkody lub popełnienia przestępstwa z wykorzystaniem danego urządzenia.

2. Odpowiedzialność za efekty działania urządzeń wyposażonych w zdolność analizowania danych (np. pojazdu autonomicznego) lub zarządzania innymi urządzeniami (np. systemów sterowania oświetleniem miejskim), a więc posiadających algorytmy decyzyjne wsparte rozwiązaniami określanymi jako sztuczna inteligencja. W takim przypadku odpowiedzialność powinna dotyczyć nie tylko mechanizmów wskazanych w pkt. 1, ale również zaimplementowanych algorytmów i odpowiedzialności za błędne ich działanie (np. doprowadzenie do wypadku drogowego w wyniku włączenia na skrzyżowaniu wszystkim uczestnikom ruchu zielonego światła).

W krótkim czasie życia handlowego produktów *smart* dało się zauważyć, że niezwykle często ich **oprogramowanie w warstwie komunikacyjnej nie zawiera żadnych mechanizmów cyberbezpieczeństwa lub zastosowane rozwiązania są niewystarczające**[27]. Dlatego należy zaprojektować i wprowadzić do systemu prawa regulacje statuujące jednoznaczną **odpowiedzialność producentów za braki i błędy w oprogramowaniu**. Równocześnie i ze szczegól-

nym naciskiem należy **wprowadzić nielimitowaną co do wartości szkody** (a już na pewno nie ograniczaną do ceny programu lub urządzenia *smart*) **odpowiedzialność za wady kwalifikowane, czyli umieszczanie w sprzedawanych urządzeniach i oprogramowaniu złośliwego kodu i furtek typu *backdoor***[28].

Rozważania na temat odpowiedzialności za oprogramowanie wymagają prześledzenia obowiązujących regulacji z zakresu prawa cywilnego, począwszy od prawa autorskiego.

Odpowiedzialność cywilna — prawo autorskie

Podstawę ochrony praw autorskich i odpowiedzialności za oprogramowanie w prawie polskim stanowi art. 55 ustawy o prawie autorskim i prawach pokrewnych (dalej zwanej u.o.p.a.) (Podrecki (red.), 2004, s. 430 i n.)[29]. Przepis ten stworzony został przede wszystkim w celu ochrony praw autora indywidualnie stworzonego dzieła. Wskazane przepisy nie zostały opracowane dla programów komputerowych, są jednak odpowiednio wykorzystywane, gdyż program komputerowy jest traktowany w prawie polskim jak utwór literacki[30]. Rozwiązanie to — jakkolwiek stosowane powszechne na świecie — tworzy swoistą fikcję prawną i jest nieadekwatne w zakresie odpowiedzialności za wady programów i urządzeń IoT przeznaczonych dla masowego odbiorcy (por. KBZ Żuradzka & Wspólnicy, 2001, s. 1). W praktyce obrotu bowiem nie jest on zamawiającym dzieło informatyczne, a kupującym produkt seryjny lub częściej — licencjonującym oprogramowanie. Mimo wszystko warto prześledzić ramy odpowiedzialności twórcy za wady oprogramowania przewidziane w prawie autorskim, gdyż producent urządzeń IoT może dowodzić, że jego ewentualna odpowiedzialność w sprawie wynika z błędu w oprogramowaniu urządzenia.

Art. 55 u.o.p.a. wprowadza odpowiedzialność za wady prawne i inne niż prawne (nazywane niezbyt adekwatnie dla oprogramowania fizycznymi), co odpowiada podziałowi obowiązującemu na gruncie prawa cywilnego. Wątpliwości budzi przede wszystkim regulacja odpowiedzialności za wady fizyczne[31], do których można zaliczyć m.in.:

- nieistnienie w programie wszystkich uzgodnionych modułów,
- niewykonywanie lub nienależyte wykonywanie przez program wszystkich lub niektórych określonych w dokumentacji funkcji,
- brak zasadniczej bezbłędności wykonywania przez program jego podstawowych funkcji,
- nieergonomiczność pracy programu,
- niezdolność programu do pracy w określonym przez twórcę systemie operacyjnym i przy określonych wymaganiach sprzętowych,
- niespełnianie przez program określonej funkcji, jaką ma on spełniać u nabywcy[32].

W przypadku oprogramowania (które w zakresie cyberbezpieczeństwa jest źródłem dyskutowanych tu podatności) art. 55 u.o.p.a. stanowi samodzielną podstawę odpowiedzialności autora za oprogramowanie i jako taki wyłącza bezpośrednie stosowanie przepisów o rękojmi[33]. Stąd dla IoT regulacja zakresu odpowiedzialności za szkodę wynikłą z wady fizycznej oprogramowania, która najczęściej oddziałuje nie tyle na samo urządzenie, ile na otoczenie, w którym podatne urządzenie pracuje[34], w świetle brzmienia art. 55 ust. 1 u.o.p.a. (ograniczenie do części otrzymanego wynagrodzenia) jest zdecydowanie niewystarczająca. Szkody mogą wielokrotnie przekraczać wartość zakupionego urządzenia IoT, a i samo urządzenie może być celowo wyposażone w kod (wada kwalifikowana oprogramowania) umożliwiający uzyskanie przez osobę nieupoważnioną dostępu do danych, urządzeń lub sieci, w której zostanie ono zainstalowane. Stąd odpowiedzialność za wady oprogramowania powinna być tożsama z regulacją przewidzianą w art. 55 ust. 2 u.o.p.a.

Odpowiedzialność cywilna — kodeks cywilny

Na gruncie kodeksu cywilnego należy postawić następujące pytania:

1. Kiedy kwalifikacja odpowiedzialności za błędy w komponencie programowym urządzenia IoT jest ustalana na podstawie przepisów kodeksu cywilnego dotyczących sprzedaży rzeczy? A kiedy możliwe jest rozdzielenie zasad odpowiedzialności za wady oprogramowania (*firmware*) i sprzętu (*hardware*) IoT[35]?
2. Czy można wyegzekwować zapewnienie przez producenta minimum bezpieczeństwa i staranności w oprogramowaniu IoT? W kontekście dalszych rozważań o produktach niebezpiecznych pytanie to należy postawić w dwóch kontekstach formalno-prawnych: B2B oraz B2C.

Jeśli na sprzedaż urządzeń IoT spojrzymy jak na cywilnoprawną umowę sprzedaży rzeczy, problem odpowiedzialności producenta za wady urządzenia i wyrządzone szkody mogą regulować przepisy art. 556 i następnych kodeksu cywilnego — rękojmia za wady (Zoll, 2018). Zgodnie z ich treścią sprzedawca odpowiada wobec nabywcy za wady fizyczne i prawne sprzedanej rzeczy bez względu na to, czy została ona nabyta w lokalu, czy poza lokalem przedsiębiorstwa. Rękojmia co do zasady dotyczy również transakcji B2B, ale sprzedawca może swoją odpowiedzialność umownie ograniczyć lub wyłączyć, co jest powszechną praktyką. Podobnie jak w przypadku licencji, przy zakupie rozwiązań IoT obowiązują jednostronnie narzucane wzorce umowne, których negocjowanie przez nabywcę jest w zasadzie niemożliwe.

Jednak w praktyce obrotu producenci i dostawcy oprogramowania niemal zawsze stosują licencjonowanie (a nie sprzedaż) oprogramowania (również na rynku B2C), co skutkuje brakiem możliwości zastosowania przepisów dotyczących sprzedaży rzeczy (w tym rękojmi). Program nie jest rzeczą, licencja zaś nie przenosi praw do programu (zob. KBZ Żuradzka & Wspólnicy, 2001, s. 5). **A sednem urządzeń inteligentnych jest oprogramowanie** (Krupanek, Bogacz, 2018, s. 1)[36]. Należy też pamiętać, że niekiedy dane

z urządzeń IoT przekazywane są do odrębnych, osobno nabywanych i licencjonowanych systemów[37]. Podobnie jak przy rękojmi, w przypadku licencji B2B również obowiązuje domniemanie swobody umów, które opiera się na założeniu, iż umowy między podmiotami gospodarczymi lub instytucjami są negocjowane i zawierane dobrowolnie[38].

Obrona praw nabywcy urządzenia IoT i ewentualnie odrębnej licencji na *firmware* może również opierać się na przepisach art. 354 i 471 k.c. Zgodnie z wyrokiem Sądu Najwyższego z 5.01.2011 r., III CSK 119/10, wykonanie zobowiązania powinno nastąpić przede wszystkim zgodnie z jego treścią[39]. Zakup urządzenia lub systemu IoT ma na celu wykorzystanie funkcji objętych specyfikacją. Należy więc przyjąć, iż producent urządzeń IoT powinien ponosić odpowiedzialność kontraktową zarówno za braki lub wadliwe działanie produktu, jak i za szkody spowodowane wadami oraz ukrytymi (a przynajmniej nieujętymi w dostarczonej specyfikacji) funkcjami urządzeń IoT.

Przesłankami odpowiedzialności na gruncie art. 471 k.c. są: szkoda (wyłącznie majątkowa), zdarzenie ją powodujące i związek przyczynowo-skutkowy między nimi, a także istnienie zobowiązania (w rozważanym przypadku IoT — umowy sprzedaży lub licencji). Szkoda musi być więc efektem wadliwego działania oprogramowania lub urządzenia (np. fizycznego błędu konstrukcji czujnika, podającego oprogramowaniu błędne dane, w wyniku czego np. błędnie działa proces technologiczny). Ciężar dowodowy leży po stronie dłużnika[40], który musi udowodnić, iż szkoda nie jest efektem przyczyn leżących po jego stronie. W efekcie dłużnik ponosi również odpowiedzialność za niezachowanie należytej staranności, czyli np. za wady będące efektem braku lub niewłaściwego audytu oprogramowania pozyskanego od podmiotów trzecich, a zainstalowanego w produkowanych przez siebie urządzeniach lub systemach IoT[41].

Roszczenia podnoszone na podstawie art. 471 k.c. są niezależne od roszczeń, których można dochodzić na podstawie rękojmi. Wierzyciel[42], który nie odstąpił od umowy, może dochodzić naprawienia szkody na zasadach ogólnych bez ograniczeń związanych z wysokością ewentualnego zadatku[43]. Przy realizacji roszczenia na gruncie wyżej wymienionych przepisów należy pamiętać, iż w przypadku istnienia umowy licencyjnej jej treść (a więc i umowny zakres odpowiedzialności) najczęściej narzuca dostawca oprogramowania (tzw. *shrink wrap licence* lub licencje celofanowe). Rzadziej jest ona wynikiem negocjacji między stronami (licencja właściwa). Choć przepisy umów licencyjnych standardowo zawierają część dotyczącą gwarancji, to wprowadzają one liczne ograniczenia (np. wyłącznie do obowiązku dostarczenia poprawionej lub nowej wersji programu). Można również spotkać (będące wręcz przedmiotem anegdot branżowych) zapisy mówiące o braku gwarancji na prawidłowe działanie programu. Powszechną praktyką jest maksymalne ograniczanie ewentualnej odpowiedzialności licencjodawcy (por. KBZ Żuradzka & Wspólnicy, 2001, s. 10–11). Należy jednak wątpić, aby producent mógł umownie wyłączyć odpowiedzialność za wady i funkcje nieobjęte specyfikacją, w szczególności podatności ukryte, takie jak *backdoor*.

Odpowiedzialność cywilna — art. 415 i produkt niebezpieczny

Odpowiedzialność deliktowa przewidziana jest w art. 415 i n. kodeksu cywilnego. Opiera się ona na trzech przesłankach analogicznych, jak w przypadku omawianego wyżej art. 471 k.c. Nie jest jednak powiązana z kontraktem, ale z winą umyślną bądź nieumyślną sprawcy. Ciężar dowodowy wykazania winy, precyzyjnego określenia sprawcy oraz związku przyczynowo-skutkowego między szkodą a działaniem sprawcy spoczywa na skarżącym, co zdecydowanie utrudnia efektywne dochodzenie praw przez pokrzywdzonego, szczególnie wobec globalnych dostawców urządzeń IoT z ich rozbudowaną siecią powiązań[44].

W kontekście opisanych wyżej problemów z realizacją skutecznej odpowiedzialności za wady oprogramowania na gruncie art. 415 k.c., efektywne ustalenie odpowiedzialności producenta urządzeń IoT za braki w zakresie cyberbezpieczeństwa powinno się oprzeć na przepisach dotyczących szkód analogicznych do zagrożeń zdefiniowanych w przepisach, które wprowadziły do kodeksu cywilnego odpowiedzialność za produkt niebezpieczny (Zoll, 2018)[45].

Konstrukcję produktu niebezpiecznego wprowadziła dyrektywa 85/374/EWG w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe[46]. **Jej implementację w prawie krajowym stanowią art. 449^1–449^{11} kodeksu cywilnego** umieszczone w Tytule VI^1 — Odpowiedzialność za szkodę wyrządzoną przez produkt niebezpieczny.

Powyższe przepisy wychodzą naprzeciw potrzebom i koncepcjom rozwijanym przez judykaturę i doktrynę, w których poszukiwano rozwiązań mogących chronić interesy indywidualnych konsumentów jako osób poszkodowanych. Zgodnie z polską doktryną odpowiedzialność producenta w stosunku do konsumenta powinna mieć charakter absolutny i uniezależniony od winy. Wskazane wyżej przepisy definiują „nowy rodzaj reżimu bezumownej odpowiedzialności odszkodowawczej konstruowanej w oparciu o zasadę ryzyka, która występuje zarówno w reżimie odpowiedzialności deliktowej, jak i kontraktowej". Regulacja ma jednak charakter niezupełny i powinna być stosowana odpowiednio z przepisami art. 415 k.c.[47]

Art. 449^1 § 1 k.c. stanowi, iż kto wytwarza w zakresie swojej działalności gospodarczej produkt niebezpieczny, odpowiada za szkodę wyrządzoną komukolwiek przez ten produkt. Przepisy omawianego tytułu zakreślają jednak szeroki krąg osób odpowiedzialnych solidarnie za wprowadzenie produktu do obrotu, obejmujący obok producenta także importera i w określonych okolicznościach — dostawców producenta[48].

Sąd Najwyższy w wyroku z 12.07.2002 r., V CKN 1112/00, stwierdził, że wprowadzenie do obrotu towaru niebezpiecznego powodującego szkodę stanowi czyn niedozwolony. Ustalenie odpowiedzialności można oprzeć na domniemaniu faktycznym wynikającym z doświadczenia[49]. Na konieczność obiektywizacji kryterium winy producenta wskazuje również wyrok Sądu Najwyższego z 8.11.2006 r., III CSK

174/06, który dodatkowo podnosi, że wystarczające jest wskazanie przez poszkodowanego zaniedbań typu organizacyjnego u przedsiębiorcy, któremu można przypisać winę organizacyjną, również za wady wynikające z przyjętej technologii i braki w nadzorze procesu produkcji. Sąd Najwyższy konstatuje, iż omawiane przepisy dotyczące produktów niebezpiecznych stanowią odejście od klasycznego ujęcia winy, postrzeganej jako ujemna ocena psychiczna działania sprawcy szkody[50].

W kontekście rozważań na temat odpowiedzialności za wady IoT należy zauważyć, iż **zastosowanie wyżej wymienionych przepisów napotyka potencjalnie istotne ograniczenie. Art. 449[2] k.c. stanowi bowiem, że producent odpowiada za szkodę na mieniu tylko wówczas, gdy rzecz zniszczona lub uszkodzona należy do rzeczy zwykle przeznaczanych do osobistego użytku i w taki przede wszystkim sposób korzystał z niej poszkodowany**. Z przepisu tego wywodzi się przede wszystkim ochronę konsumenta (rynek B2C).

W świetle obowiązujących przepisów do wprowadzenia pełnej ochrony za wady IoT konieczne wydaje się potwierdzenie, iż ochrona ta powinna obowiązywać bez względu na to, czy nabywcą jest osoba fizyczna, czy jakikolwiek inny podmiot. Jakkolwiek bowiem preambuła dyrektywy 85/374/EWG odwołuje się do ochrony konsumenta, to dyrektywa ta co do zasady wskazuje na konieczność ustanowienia niezależnej od winy odpowiedzialności ze strony producenta. Jak już wskazano, faktyczna pozycja kupującego jest zazwyczaj tożsama bez względu na to, czy nabywcą jest osoba fizyczna, przedsiębiorca czy instytucja. Ponadto wady oprogramowania powodujące, że dane urządzenie IoT jest produktem niebezpiecznym, są nimi niezależnie od tego, kto jest ich nabywcą. W szczególności umyślna luka w oprogramowaniu urządzenia IoT nie tylko nie zmienia swojego charakteru ze względu na nabywcę, ale w przypadku odbiorców instytucjonalnych oraz przedsiębiorstw może przynieść dalece bardziej dotkliwe straty.

W analizie legislacyjnej należy też uwzględnić wyrok TSUE z 4.06.2009 r. w sprawie C-285/08. Trybunał uznał w nim, że wykładnia dyrektywy powinna być dokonywana tak, aby nie ograniczać poszkodowanemu żądania naprawienia szkody rzeczy przeznaczonej do profesjonalnego użytku na podstawie regulacji krajowych dotyczących odpowiedzialności za produkt niebezpieczny. Prawo krajowe może regulować takie sytuacje, gdyż znajdują się one poza zakresem regulacji zawartej w dyrektywie. W świetle wskazanego wyroku TSUE nic więc nie stoi na przeszkodzie, by przyjąć odpowiedzialność za produkt niebezpieczny również w sytuacji profesjonalnego wykorzystywania przedmiotu (rynek B2B/B2A).

Prawo karne

Kodeks karny w rozdziale XXXIII definiuje szereg przestępstw przeciwko ochronie informacji (Radoniewicz, 2016, s. 271 i n.). Żaden z tych przepisów nie obejmuje jednak odpowiedzialności karnej za wprowadzenie na rynek wadliwego oprogramowania, wyposażonego m.in. w *backdoor*, lub za brak jakichkolwiek zabezpieczeń przed dostępem osób nieupoważnionych. Wskazany rozdział odnosi się w istocie do odpowiedzialności za aktywne naruszenie bezpieczeństwa i integralności systemów informatycznych. Gdy omawiane podatności dotyczą systemów krytycznych dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji publicznej, możemy przywołać art. 269 k.k., w którym definiuje się odpowiedzialność za sabotaż informatyczny określany jako „zakłócanie lub uniemożliwianie przetwarzania, gromadzenia lub przekazywania (…) danych". W części przypadków pozwoli to powiązać odpowiedzialności producenta za wady oprogramowania z określeniem „uniemożliwia". Podstawa ta nie będzie jednak miała zastosowania w przypadkach B2B oraz B2C.

Na gruncie pozostałych przepisów ewentualna odpowiedzialność producenta będzie wymagać udowodnienia np. pomocnictwa, co przynajmniej w części przypadków związanych z niedbalstwem w zakresie walidacji bezpieczeństwa wprowadzanych na rynek urządzeń może być niezmiernie trudne do przeprowadzenia.

Należy więc rozważyć uzupełnienie kodeksu karnego o przepisy definiujące odpowiedzialność karną wobec osoby, która umieszcza w oprogramowaniu ukryte lub niemożliwe do usunięcia konta, jak również inne funkcjonalności pozwalające na wykorzystanie lub dostęp do urządzeń i systemów informatycznych osób nieuprawnionych, oraz wobec osób, które wprowadzają na rynek urządzenia zawierające wymienione wyżej podatności — przede wszystkim producentów. W sytuacjach krytycznych lub szczególnych należy rozważyć również odpowiedzialność programistów, podwykonawców i dystrybutorów — może to być kluczowe zarówno w przypadku systemów złożonych z różnych części składowych, jak i rozwiązań wykorzystywanych w systemach kluczowych dla gospodarki i bezpieczeństwa państwa[51].

Wskazane jest rozważenie wprowadzenia niższego wymiaru kary dla osoby, która wprowadzając na rynek urządzenie zawierające oprogramowanie umożliwiające jego podłączenie do Internetu, nie wyposaży go w rozwiązania uniemożliwiające ograniczenie dostępu osób nieupoważnionych — *firewall*. Podobnej karze powinny podlegać osoby, które wiedząc o (kwalifikowanej?) podatności wprowadzonych na rynek urządzeń, nie umożliwiają ich użytkownikom instalacji dostępnych aktualizacji oprogramowania.

Zdanie ostatnie wymaga rozwinięcia w ewentualnych szerszych rozważaniach, gdyż odnosi się do wielu różnych sytuacji dotyczących możliwości usunięcia kwalifikowanych wad oprogramowania (por. wyżej w części dotyczącej odpowiedzialności na gruncie prawa cywilnego[52]), z których w tym miejscu wskazać należy dwie:

- Producent posiada aktualizację wolną od omawianych tu wad, ale odmawia jej udostępnienia użytkownikom, którzy nie mają zawartych kontraktów serwisowych lub nie wykupią prawa do aktualizacji albo nie zdecydują się na

zakup nowej wersji oprogramowania wolnej od omawianych wyżej wad.

● Producent ma możliwość przygotowania aktualizacji oprogramowania wolnej od omawianych wad, ale odmawia jej wykonania, tłumacząc to zakończeniem produkcji lub zakończeniem wsparcia obciążonych wadą urządzeń IoT.

Wątek odpowiedzialności karnej na obecnym etapie rozważań ma charakter jedynie sygnalizacyjny.

Propozycje *de lege ferenda*

Poruszone w niniejszym artykule ramowe zagadnienia są krytyczne dla większości rozważań dotyczących cyberbezpieczeństwa rozpatrywanego z dwóch perspektyw:

● możliwości wywierania skutecznej, finansowej presji na producentów i dystrybutorów urządzeń oraz oprogramowania w kwestii dbałości o zachowanie podstawowych standardów bezpieczeństwa wprowadzanych na rynek produktów;

● zapewnienia efektywnej możliwości dochodzenia odszkodowania od producentów przez wszystkich nabywców co najmniej za wady kwalifikowane oprogramowania, czyli zgodnie z niniejszym opracowaniem — wady polegające przede wszystkim na:

– braku jakichkolwiek mechanizmów kontroli dostępu;

– umieszczeniu w oprogramowaniu mechanizmów typu *backdoor* umożliwiających nieautoryzowany, a w szczególności niemożliwy do zablokowania przez użytkownika dostęp[53].

Celem ustawodawcy powinno być nakreślenie jasnych zasad **odpowiedzialności producenta za bezpieczeństwo oprogramowania wprowadzanych na rynek produktów, co może zostać zrealizowane poprzez dokonanie nowelizacji art. 449[2] k.c.** na jeden z poniższych sposobów:

● Wykreślenie art. 449[2] — stosunkowo najmniej właściwe rozwiązanie.

● Skreślenie w art. 449[2] słowa „tylko" i dodanie do niego punktu 2 o treści: „Producent odpowiada za szkodę na mieniu również wtedy, gdy rzecz zniszczona lub uszkodzona należy do rzeczy przeznaczanych do użytku zawodowego i zarobkowego" — w nawiązaniu do art. 22 (1) k.c.

● Skreślenie w art. 449[2] słowa „tylko" i dodanie art. 449[11] o treści: „Przepisy art. 449[1]–449[10] stosuje się odpowiednio wobec odpowiedzialności producenta za szkodę na mieniu w sytuacji, gdy rzecz zniszczona lub uszkodzona należy do rzeczy przeznaczanych do użytku profesjonalnego". Mając na uwadze przedmiot niniejszej rekomendacji, a więc odpowiedzialność za wady *firmware*, ewentualnie szerzej — oprogramowania, można rozważyć dodatkowo uzupełnienie przepisu doprecyzowaniem: „a szkoda jest efektem wad oprogramowania (urządzeń), w szczególności braku należytej ochrony przed nieuprawnionym dostępem".

Wnioski

Zarówno w legislacji, jak i w orzecznictwie, należy konsekwentnie wiązać obiektywną odpowiedzialność producenta za produkt niebezpieczny z brakiem możliwości kontraktowego wyłączenia odpowiedzialności z tego tytułu. Z uwagi na charakter oprogramowania i rodzaje omawianych zagrożeń należy również wprowadzić obowiązek udostępniania aktualizacji urządzeń IoT dla wykrytych podatności kwalifikowanych[54]. Warto zaznaczyć, że konstrukcja produktu niebezpiecznego nie wyłącza odpowiedzialności producenta z tytułu odpowiedzialności kontraktowej, pozakontraktowej lub wynikającej z innych przepisów szczególnych[55].

Postulowane zmiany *de lege ferenda* muszą zapewniać bezpieczeństwo wszystkim nabywcom i użytkownikom produktów wyposażonych w oprogramowanie, a więc również B2B i B2A. Jedynym gwarantem spełnienia minimalnych wymagań w tym zakresie może i musi być producent składowych części ekosystemu IoT, odpowiadający ewentualnie solidarnie z dystrybutorem (z uwagi na praktyczną trudność w egzekwowaniu odpowiedzialności wobec dostawców zagranicznych, w szczególności spoza obszaru Unii Europejskiej). Bez jasno zdefiniowanej odpowiedzialności producentów za oprogramowanie nie da się wymusić dbałości o bezpieczeństwo produkowanych i instalowanych masowo urządzeń IoT. Tylko w ten sposób upowszechnianie rozwiązań cyfrowych będzie bezpieczniejsze na każdym poziomie — od bezpieczeństwa użytkownika domowego po bezpieczeństwo państwa.

Przypisy/Notes

[1] Rozbudowa systemów IoT oddziałuje w coraz większym stopniu na osoby fizyczne, prawne i instytucje, a także różnorodne systemy i urządzenia zarówno hierarchiczne M2M (machine-to-machine), jak i autonomiczne. Należy bez żadnej przesady przyjąć, iż bezpieczne środowisko IoT w każdym jego przejawie z każdym nadchodzącym rokiem będzie coraz bardziej odpowiedzialne za bezpieczeństwo świata, w którym żyjemy.

[2] Powołanej 24.08.2018 r. w Ministerstwie Cyfryzacji — https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-internetu-rzeczy-internet-of-things-iot.

[3] https://www.gov.pl/attachment/82ad18f8-2ac1-4433-a1ea-f887b522e46b.

[4] Por. m.in.: „Znaczącą barierą jest również brak kompetencji związanych z kwestiami powiązanymi z IoT, takimi jak aspekty prawne (np. ochrona prywatności). Wciąż jest niewielu specjalistów na rynku, mogących świadczyć profesjonalne usługi w tym zakresie. (…) W polskim systemie prawnym brak jest odrębnych i szczegółowych regulacji dla technologii IoT. Rozproszone po wielu aktach prawnych (m.in. RODO, prawo telekomunikacyjne i tajemnice sektorowe, NIS) regulacje". (Raport GR IoT „IoT w polskiej gospodarce", s. 14).

[5] Tamże, s. 20.

[6] Tamże, s. 21.

[7] Tamże.

[8] Zob. dalsze omówienie art. 55 ustawy z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24 poz. 83 z późn. zm.).

[9] M.in. (choć nie tylko) z uwagi na wyłączenia licencyjne omówione w dalszej części niniejszego opracowania.

[10] W zasadzie każde opracowanie poświęcone cyberbezpieczeństwu wskazuje, że zabezpieczenie urządzeń IoT jest znacznie trudniejsze niż komputerów lub telefonów. Większość elementów IoT ma bowiem nieaktualizowane, stare oprogramowanie, zdefiniowane na sztywno zasady dostępu lub jest projektowana wręcz bez wdrażania jakichkolwiek zabezpieczeń. Charakter tych urządzeń powoduje, iż bezpieczeństwo ich użytkowników jest niemal zawsze zależne od procedur producentów. Por. The First Steps in Effective IoT Device Security, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-first-steps-in-effective-iot-device--security?utm_source=trendmicroresearch&utm_medium=socal.

[11] Zob. Rekomendacja ITU-T Y. 2060 (06/2012) w pkt. 3.2.2: „Globalna infrastruktura społeczeństwa informacyjnego, umożliwiająca zaawansowane usługi, poprzez łączenie (fizycznych i wirtualnych) rzeczy, w oparciu o istniejące i rozwijające się interoperacyjne technologie informacyjne i komunikacyjne". Doprecyzowuje równocześnie w pkt. 3.2.3 pojęcie rzeczy w kontekście IoT, jako „obiekt fizyczny lub wirtualny, który można zidentyfikować i zintegrować w sieciach komunikacyjnych". https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items.

[12] Podtytuł rozdziału brzmi wprost: „Definicje IoT z różnych perspektyw" (Raport GR IoT, s. 5).

[13] Aktualny przykład problemu braku zabezpieczenia danych gromadzonych na serwerach producenta przez urządzenia z kategorii *wearables* opisuje artykuł o dziecięcych zegarkach inteligentnych. Brak zabezpieczeń umożliwia „nieuwierzytelniony dostęp do lokalizacji, zdjęć, imion, adresów, wiadomości głosowych". Unaocznia on dobitnie, że przypisanie odpowiedzialności za wady lub braki w zakresie bezpieczeństwa IoT (lub precyzyjniej w tym przypadku — gromadzonych przez nie danych) nie może być ograniczane do podatności jedynie urządzeń IoT. https://sekurak.pl/dzieciece-smartwatche-tej-firmy-daja-nieuwierzytelniony-dostep-do-lokalizacji-zdjec-imion-adresow-wiadomosci-glosowych-chyba-najwiecej-dotknietych-w-polsce/.

[14] Np. systemy regulacji ruchu, oświetlenia, ogrzewania czy kontroli dostępu.

[15] Np. nawigacja, e-myto, asystent pasa ruchu, aktywny tempomat, automatyczne powiadomienie o kolizji.

[16] Decyzje podejmowane przez pojazd realizowane są z wykorzystaniem oprogramowania określanego najczęściej mianem sztucznej inteligencji (AI — *artificial intelligence*). Pojęcie to jest wielowymiarowe i podobnie jak w przypadku pojęcia *Big Data*, AI musi być brane pod uwagę w rozważaniach o IoT.

[17] Pojęcie podatności lub luki w oprogramowaniu jest różnie definiowane w literaturze. To najczęściej wynik błędów powstałych na etapie specyfikacji, projektowania, implementowania lub konfiguracji oprogramowania, w wyniku których można przejąć nad nim kontrolę lub wykorzystać je niezgodnie z wolą właściciela lub użytkownika. (tak: Hoffmann, Stanik, Napiórkowski, 2017). W praktyce cyberbezpieczeństwa odróżnia się jednak (1) błędy lub braki nieintencjonalne, (2) błędy konfiguracyjne i (3) intencjonalne nadużycia funkcji oprogramowania. Te ostatnie (np. *backdoor*) nie pojawiają się w oprogramowaniu przypadkiem, są zawsze efektem świadomego działania. Dlatego odpowiedzialność producenta w przypadku ich stwierdzenia, nie powinna podlegać żadnym ograniczeniom (zob. https://developer.mozilla.org/pl/docs/Web/Bezpiecze%C5%84stwo/Podstawy_bezpieczenstwa_informacji/Podatnosci).

[18] Urządzenia IoT mają różny charakter. Najczęściej powoływany jest w źródłach raport Gartnera. Przyjmuje on, że do 2020 r. na świecie będzie nawet 20 mld urządzeń Internetu rzeczy. Z kolei Ericsson ocenia, że w 2021 r. na 28 mld urządzeń podłączonych do Internetu ponad połowę, czyli 16 mld, będą stanowiły urządzenia IoT. Dla porównania liczba inteligentnych przedmiotów podłączonych do sieci w 2013 r. sięgała 3 mld, a w 2015 r. 5 mld (zob. https: //innowacje. newseria.pl/news/internet-rzeczy-z-liczba,1306006251 i https://www.computerworld.pl/news/Internet-rzeczy-zaczyna-rzadzic-swiatem, 414760.html).

[19] W raporcie IDC „FutureScape Worldwide IoT 2017 Predictions" szacowano, że w 2019 r. nawet 40% danych generowanych przez urządzenia IoT będzie przetwarzanych w systemach rozproszonych (tamże).

[20] AI to oprogramowanie umożliwiające komputerom wykonywanie określonych zadań poprzez przetwarzanie i rozpoznawanie wzorców w dostępnych danych (zob. https://www.sas.com/pl_pl/insights/analytics/what-is-artificial-intelligence. html).

[21] Mnogość rozwiązań informatycznych, powszechne wykorzystywanie kodu pochodzącego z różnych źródeł, utrudniają, a często wręcz uniemożliwiają wskazanie autora oprogramowania urządzeń. Dobrym przykładem jest oprogramowanie smartfonów. To producent urządzeń decyduje o tym, co umieszcza na swoim urządzeniu i to on dysponuje kodami źródłowymi oraz odpowiada za realizację audytów bezpieczeństwa. Na globalnym rynku za wprowadzony do lokalnego obrotu produkt (np. na terenie UE) odpowiada jego dystrybutor (bliżej: w rozważaniach na temat produktów niebezpiecznych).

[22] Tutaj — urządzenia IoT w komplecie z oprogramowaniem.

[23] Jeśli oprogramowanie objęte jest odrębną umową (np. licencyjną) lub stanowi element odrębnego systemu (np. zarządzającego siecią urządzeń IoT).

[24] Stosunek odpowiedzialności z tytułu rękojmi i gwarancji (zob. Falkowska, 2010, s. 271–272; Kwasiński, Łanowy, 2018).

[25] *Software* — szerokie określenie każdego typu oprogramowania, w tym systemów operacyjnych, aplikacji itp. *Firmware* — węższe określenie obejmujące oprogramowanie urządzeń, np. sterowników, routerów, kontrolerów, urządzeń transmisyjnych itp.

[26] Istnieje wiele postaci licencji. Są one analizowane omawiane w literaturze przede wszystkim w kontekście zabezpieczenia praw autora oprogramowania (zob. Barta (red.), 2017, s. 752–765; Barta, Markiewicz, 2019).

[27] Analizując te kwestie, można odnieść się do regulacji dotyczących produktów nieinformatycznych — np. pojazdów. Nie wystarczy wyprodukować pojazd. By został dopuszczony do sprzedaży, a tym bardziej ruchu, musi spełniać szereg różnorodnych wymagań mających zapewnić jego bezpieczne użytkowanie. W przypadku cyberbezpieczeństwa wydaje się, że brak jest nie tylko wystarczających, ale jakichkolwiek regulacji definiujących minimalne wymagania wobec IoT.

[28] Anglojęzyczne pojęcie *backdoor* wykorzystywane jest powszechnie do określenia ukrytych w oprogramowaniu rozwiązań, pozwalających na przejęcie kontroli nad urządzeniem bez wiedzy jego właściciela lub użytkownika. Najczęściej jest to ukryte konto z uprawnieniami administratora.

[29] Ustawa z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. nr 23, poz. 83 z późn. zm.) — dalej u.o.p.a. Art. 55 u.o.p.a. analizowany jest w piśmiennictwie przede wszystkim z perspektywy ochrony twórcy, a nie nabywcy programu (zob. szerzej Podrecki (red.), 2004, s. 430 i n.).

[30] Art. 1 ust. 2 pkt. 1 u.o.p.a. oparty na konstrukcji dyrektywy Rady w sprawie ochrony prawnej programów komputerowych 91/250/EWG z 14.05.1991 r. (zob. również Wojdył, 2005).

[31] Tamże, s. 3–4.

[32] Tamże.

[33] Tamże, s. 7.

[34] Najczęściej służąc za bramę do cyberataku lub środek do przejęcia, przekierowania lub zablokowania komunikacji.

[35] Odrębna regulacja odpowiedzialności za oprogramowanie kieruje nas zazwyczaj na grunt rozważań w ramach prawa autorskiego albo licencji.

[36] „Ogólna koncepcja Internetu rzeczy zakłada, że każdy obiekt ma swój własny identyfikator, np. adres IP, oraz jest podłączony do globalnego systemu, jakim jest Internet. Urządzenia mogą komunikować się ze sobą za pomocą dostępnej dla nich platformy programowej. Użytkownik systemu ma możliwość komunikacji bezpośrednio z każdym urządzeniem, może sprawdzić jego stan, a także nim zdalnie sterować używając platformy". (Krupanek, Bogacz, 2018, s. 1).

[37] Np. oprogramowanie zarządzające systemem monitoringu, inteligentnym domem, zakładem przemysłowym czy miastem.

[38] W swojej istocie wpływ na postanowienia załączonego kontraktu lub umowy licencyjnej przy zakupie urządzeń IoT (np. kamery IP) przez klientów instytucjonalnych jest analogiczny do wpływu konsumenta, czyli żaden. W wielu przypadkach też, m.in. ze względu na brak kompatybilności lub wymagania gwarancyjne dla innych elementów wykorzystywanych systemów, nabywca nie ma możliwości zakupienia rozwiązań alternatywnych, do których byłyby dołączone bardziej korzystne postanowienia umowy sprzedaży lub licencji. Stąd konstrukcja swobody kontraktów w praktyce służy kwestionowaniu odpowiedzialności producenta nawet za wady kwalifikowane sprzedanych rozwiązań.

[39] Art. 354 k.c.

[40] Wyrok Sądu Najwyższego z 5.12.2008 r., III CSK 211/08.

[41] Art. 472 k.c. w zw. z art. 355 § 2 k.c. (Por. http://www.openlaw.com.pl/wikka.php?wakka=RoszczenieOdszkodowawczeArt471KC).

[42] Wyrok Sądu Najwyższego z 30.08.2006 r., II CSK 89/2006.

[43] Wyrok Sądu Najwyższego z 25.06.2009 r., III CZP 39/09.

[44] W kontekście winy wyrok Sądu Najwyższego z 8.11.2006 r., III CSK 174/06 wskazuje jednak na konieczność jej obiektywizacji wobec producenta. Szerzej w dalszej części niniejszej sekcji.

[45] Zob. szerzej porównanie odpowiedzialności za produkt niebezpieczny i z tytułu rękojmi (Zoll, 2018).

[46] Dz.Urz. WE L 210 z 7.08.1985 r., s. 29; polskie wydanie specjalne: Dz.Urz. UE rozdział 15, t. 1, s. 257.

[47] W uzasadnieniu wyroku Sądu Okręgowego w Poznaniu z 30.05.2017 r., XVIII C 606/15 wskazano m.in.: „Poszukiwanie rozwiązań zarówno przez judykaturę, jak i przez doktrynę, które w największym stopniu mogły chronić interesy osób poszkodowanych, zaprowadziło do wyodrębnienia nowej zasady odpowiedzialności (...). Odpowiedzialność za szkody wyrządzone przez wadliwe przedmioty świadczenia, zanim komentowane rozwiązanie znalazło swoje miejsce w kodeksie cywilnym, została określona mianem odpowiedzialności absolutnej (…). Jest to odpowiedzialność za sam skutek nie tylko uniezależniona od winy podmiotu, na którym ciąży, lecz także niedopuszczająca w ogóle możliwości uwolnienia się od niej".

[48] Art. 4495. k.c. Zob. wyrok Sądu Najwyższego z 2.10.2015 r., II CSK 818/14.

[49] Wyrok Sądu Najwyższego z 12.07.2002 r., V CKN 1112/00.

[50] Wyrok Sądu Najwyższego z 8.11.2006 r. Sygn. akt III CSK 174/06.

[51] Poza rozwiązaniami IoT, problem dotyczy np. danych gromadzonych i przetwarzanych w systemach chmurowych.

[52] Dla przypomnienia — kwalifikowane wady oprogramowania to problemy takie jak obecność w systemie ukrytych kont czy świadomie umieszczonych podatności lub ukrytego kodu realizującego lub mogącego realizować dodatkowe operacje bez wiedzy posiadacza/użytkownika.

[53] Oczywiście każde urządzenie można odłączyć od sieci lub ograniczyć do niego dostęp. Jeśli jednak urządzenie IoT udostępnia dane wyłącznie przez serwis www działający na standardowym porcie 80, a luka w jego *firmware* pozwala na przejęcie nad nim kontroli właśnie przez port 80, to blokada tego portu celem ograniczenia możliwości przejęcia kontroli oznacza wykluczenie użyteczności zakupionego urządzenia.

[54] Kwalifikowanych w ujęciu omówionym w niniejszym opracowaniu.

[55] Art. 44910 k.c. oraz Artykuł 13 dyrektywy 85/374/EWG.

Bibliografia/References

Literatura/Literature

Barta, J. (2017). *System prawa prywatnego. Prawo autorskie,* t. 13, 752–765. Warszawa: C.H. Beck.

Barta, J., Markiewicz, R. (2019). *Prawo autorskie i prawa pokrewne*. Warszawa: Wolters Kluwer.

Falkowska A. (2010). *Odpowiedzialność sprzedawcy z tytułu rękojmi za wady fizyczne rzeczy*. Warszawa: Wolters Kluwer.

Hoffmann, R., Stanik, J., Napiórkowski, J. (2017). Modele wykrywania podatności oprogramowania w ujęciu dynamiki systemowej. *Roczniki Kolegium Analiz Ekonomicznych SGH*, (45), 201–212.

KBZ Żuradzka & Wspólnicy (2001). Program komputerowy i jego wady. *Gazeta Prawna* (33), dodatek *Prawo na Zamówienie*.

Krupanek, B., Bogacz, R. (2018). Węzły końcowe systemów internetu rzeczy. *Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej*, (59), 111–116.

Kwasiński, O., Łanowy, T. (2018). Rękojmia i gwarancja jako instytucje zabezpieczające interes kupującego, a odpowiedzialność z nich wynikająca. *Rynek-Społeczeństwo-Kultura, 1*(27), 128–132.

Podrecki, P. (red.) (2004). *Prawo Internetu*. Warszawa: Wydawnictwo Prawnicze LexisNexis.

Radoniewicz, F. (2016). *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*. Warszawa: Wolters Kluwer.

Wojdył, S. (2005). Wadliwość oprogramowania komputerowego jako przedmiotu obrotu prawnego, 49, nieopublikowana praca magisterska, Uniwersytet Gdański.

Zoll, F. (2018). *Rękojmia. Odpowiedzialność sprzedawcy*. Warszawa: C.H. Beck.

Orzecznictwo/Judgments

Wyrok SN z 12.07.2002 r., V CKN 1112/00.

Wyrok SN z 30.08.2006 r., II CSK 89/2006.

Wyrok SN z 8.11.2006 r., III CSK 174/06.

Wyrok SN z 5.12.2008 r., III CSK 211/08.

Wyrok SN z 25.06.2009 r., III CZP 39/09.

Wyrok SN z 2.10.2015 r., II CSK 818/14.

Wyrok SO w Poznaniu z 30.05.2017 r., XVIII C 606/15.

Wyrok TSUE z 4.06.2009 r. w sprawie C-285/08 Moteurs Leroy Somer v. Dalkia France i Ace Europe, ECR 2009, s. I–4733.

Akty prawne/Legal acts

Dyrektywa 85/374/EWG z 25.07.1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz.Urz. WE L 210 z 7.08.1985 r.)

Dyrektywa Rady w spawie ochrony prawnej programów komputerowych 91/250/EWG z 14.05.1991 r.

Rekomendacja ITU-T Y. 2060 (06/2012).

Ustawa z 23.04.1964 r. — Kodeks cywilny (Dz.U. 1964 nr 16 poz. 93 z późn. zm.).

Ustawa z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24 poz. 83 z późn. zm.).

Ustawa z 6.06.1997 r. — Kodeks karny (Dz.U. 1997 nr 88 poz. 553 z późn. zm.).

Mgr Piotr Marciniak

Doktorant w Instytucie Nauk Prawnych Polskiej Akademii Nauk, absolwent Wydziału Prawa i Administracji Uniwersytetu Łódzkiego. Studiował ponadto na Universiteit Antwerpen oraz York University w Toronto. W działalności naukowej specjalizuje się w problematyce samorządu gospodarczego i nowych technologii. Ekspert rynku telekomunikacyjnego. Od 1999 r. udziałowiec i prezes zarządu firm telekomunikacyjnych. W 2008 r. współtwórca i do 2017 r. członek władz, w tym prezes, Krajowej Izby Komunikacji Ethernetowej. Autor lub współautor przeszło 100 stanowisk, raportów i analiz na temat rynku telekomunikacyjnego. Członek i kierownik kilku resortowych zespołów eksperckich.

Mgr Piotr Marciniak

PhD candidate at the Institute of Legal Sciences of the Polish Academy of Sciences. Graduate of the Faculty of Law and Administration at the University of Lodz. Studied also at Universiteit Antwerpen and York University in Toronto. In his scientific activity, he specializes in chambers of commerce and new technologies. Telecommunications market expert. From 1999, shareholder and CEO of telecommunications companies. In 2008 a co-founder and until 2017 a member of the authorities, including the president, of the National Chamber of Ethernet Communications. Author or co-author of over 100 positions, reports and analyzes on the telecommunications market. Member and head of several departmental expert grups.