Katarzyna Biczysko-Pudełko

Student w otoczeniu Internetu Rzeczy, czyli o jego bezpieczeństwie cybernetycznym

Katarzyna Biczysko-Pudełko

Doktor nauk prawnych, adiunkt w Instytucie Nauk Prawnych Uniwersytetu Opolskiego. Współpracownik Centrum Prawnych Problemów Techniki i Nowych Technologii UO.

kbiczysko@uni.opole.pl

https://orcid.org/0000-0002-4724-1851

Students in the Internet of Things: Remarks on Their Cybersecurity

The article seeks to answer the question whether the current norms of Polish civil law provide effective mechanisms for protecting the rights of students as users of Internet of Things products/devices. Hence, in addition to explaining basic concepts such as the Internet of Things or cybersecurity, the paper provides an exegesis of legally relevant norms of the Polish Civil Code, including in particular provisions on liability for a dangerous product or the possibility for the student to assert his/her claims under the warranty for defects of Internet of Things products/devices. The analysis identifies various legislative shortcomings, the recognition of which is the first step towards formulating postulates de lege ferenda.

Słowa kluczowe: Internet Rzeczy, bezpieczeństwo cybernetyczne, student, kodeks cywilny

Key words: Internet of Things, cybersecurity, student, Civil Code

https://doi.org/10.32082/fp.5(79).2023.1218

1. Wprowadzenie

W roku 2010 w jednej z pierwszych prawniczych prac naukowych poświęconych zjawisku Internetu Rzeczy (ang. *Internet of Things* – IoT), Rolf H. Weber i Romana Weber zwrócili uwagę na konieczność stworzenie ram prawnych dla tej – wówczas jeszcze „raczkującej" – technologii[1]. Jak słusznie wówczas zauważono, to dzięki odpowiedniemu otoczeniu regulacyjnemu możliwe będzie zapewnienie odpowiedniego poziomu bezpieczeństwa całej struktury IoT, jak również prywatności jego użytkowników[2]. Dekadę później, tj. w roku 2020, Rada Unii Europejskiej zatwierdziła konkluzje, w których dostrzegła „rosnące użytkowanie produktów konsumpcyjnych

1 R.H. Weber, R. Weber, *Internet of Things. Legal Perspective*, Zürich 2010, s. III.

2 Tamże.

i urządzeń przemysłowych podłączonych do Internetu oraz powiązane z tym nowe zagrożenia dla prywatności, bezpieczeństwa informacji i cyberbezpieczeństwa"[3], natomiast Komisja Europejska w sprawozdaniu na temat wpływu sztucznej inteligencji, Internetu Rzeczy i robotyki na bezpieczeństwo i odpowiedzialność odnotowała, że „pojawienie się nowych technologii cyfrowych, takich jak AI, IoT i robotyka, stwarza nowe wyzwania w zakresie bezpieczeństwa produktów i odpowiedzialności za produkt, i oceniła, że w obecnie obowiązujących przepisach dotyczących bezpieczeństwa produktów istnieje szereg luk, którymi „należy się zająć"[4].

Powyższe niemal od razu skłania więc do refleksji nad istniejącym obecnie otoczeniem regulacyjnym dla bezpieczeństwa cybernetycznego korzystających z Internetu Rzeczy i dalej poszukiwania odpowiedzi na pytanie, czy obowiązujące obecnie normy prawa cywilnego[5] zapewniają skuteczne mechanizmy ochrony praw tychże podmiotów. Biorąc jednakże pod uwagę fakt, że samo pojęcie „bezpieczeństwo cybernetyczne" – rozumiane jako zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni[6] – w kontekście Internetu Rzeczy zawiera w sobie kilka podkategorii[7], tj.: bezpieczeństwo samego produktu[8], cyberbezpieczeństwo produktu, bezpieczeństwo danych przetwarzanych[9],

„Bezpieczeństwo cybernetyczne" – rozumiane jako zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni – w kontekście Internetu Rzeczy zawiera w sobie kilka podkategorii: bezpieczeństwo samego produktu, cyberbezpieczeństwo produktu, bezpieczeństwo danych przetwarzanych, bezpieczeństwo fizyczne czy też bezpieczeństwo narodowe, militarne.

3 *Komunikat prasowy: Cyberbezpieczeństwo urządzeń podłączonych do internetu – Rada przyjmuje konkluzje*, https://www.consilium.europa.eu/pl/press/press-releases/2020/12/02/cybersecurity-of-connected-devices--council-adopts-conclusions/# (dostęp: 19.09.2021).

4 *Sprawozdanie Komisji dla Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego*, COM(2020)64 final, s. 19.

5 Ściślej przepisy ustawy z 23 kwietnia 1964 r. – Kodeks cywilny (tekst jedn.: Dz.U. z 2023 r. poz. 1610 ze zm.).

6 B. Kaczmarczyk, P. Szczepański, M. Dąbrowska, *Wybrane zagadnienia cyberbezpieczeństwa*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2019, nr 32, s. 203.

7 *IoT w polskiej gospodarce*, Raport Grupy Roboczej ds. Internetu Rzeczy przy Ministerstwie Cyfryzacji, Warszawa 2019, s. 21.

8 W tym zakresie bezpieczeństwo produktu identyfikować należy z punktu widzenia norm dotyczących higieny, toksyczności, funkcjonalności, ergonomii itp., które gwarantują bezpieczne użytkowanie produktu.

9 Cyberbezpieczeństwo danych związane będzie z przetwarzaniem przez produkt lub ekosystem informacji dotyczących otoczenia, zarówno osobowych, jak i technicznych (np. nieosobowych).

bezpieczeństwo fizyczne czy też bezpieczeństwo narodowe, militarne[10].

Z uwagi na ograniczenia redakcyjne, ale też dla jasności wywodu, przedmiotową analizę ograniczono tylko do wybranych aspektów, tj. bezpieczeństwa cybernetycznego i fizycznego tychże urządzeń. Co więcej, pole badawcze niniejszej pracy zawężone zostało także w ujęciu podmiotowym, tj. odpowiedzi na zadanie wcześniej pytanie badawcze poszukiwać będzie się z perspektywy studenta jako użytkownika urządzeń IoT. Powodów ku temu jest niewątpliwie kilka.

Otóż po pierwsze, odnotowania wymaga fakt, iż w literaturze przedmiotu próżno doszukiwać się prac traktujących o tejże tematyce, choć w rzeczywistości Internet Rzeczy coraz śmielej wkracza pod strzechy akademickie, a sami studenci – często nieświadomie – korzystają z urządzeń tenże Internet Rzeczy tworzących. I jakkolwiek oczywiście opisany powyżej trend obecnie bardziej widoczny jest poza granicami kraju (tj. w zagranicznych ośrodkach naukowych), to naturalną koleją rzeczy zdaje się upowszechnienie tejże technologii w niedalekiej perspektywie także w Polsce, co przedmiotowym rozważaniom nadać może walor praktyczny.

Po drugie, nie można tracić z pola widzenia także okoliczności, iż ocena tego, na ile obecnie obowiązujące normy prawne stanowią skuteczne mechanizmy zapewnienia szeroko rozumianego bezpieczeństwa cybernetycznego studenta jako użytkownika IoT determinowana będzie innymi prawnie relewantnymi okolicznościami, a związanymi chociażby z koniecznością rozstrzygnięcia, czy dla zapewnienia studentowi jako użytkownikowi urządzeń Internetu Rzeczy skutecznej ochrony na gruncie przepisów k.c. (a zwłaszcza możliwości dochodzenia roszczeń odszkodowawczych w reżimie odpowiedzialności za produkt niebezpieczny) znaczenie może mieć kwalifikacja studenta w stosunku cywilnoprawnym z uczelnią wyższą jako konsumenta. Dodatkowo rozstrzygnąć trzeba, czy – a jeśli tak, to kiedy – student będzie uprawnionym do kierowania wobec producenta urządzeń IoT roszczeń z tytułu rękojmi. To zaś wskazuje na pewien brak „oczywistości" podjętego tematu.

Tytułem wprowadzenia odnotować jeszcze należy, jak się zdaje, zupełnie zrozumiałą kwestię, a mianowicie: przedmiotowa analiza (chociażby z uwagi na ograniczenia redakcyjnie) nie ma charakteru wyczerpującego, a odnosi się jedynie do tych zagadnień, które w kontekście zaproponowanego tematu *in primo aspectu* zdają się nurtujące.

2. *Pojęcie* Internet of Things

Wobec braku jednej legalnej definicji pojęcia IoT w nauce prezentowane są różne koncepcje ujmowania tego zjawiska, przy czym – co oczywiste – ich kształt w dużej mierze determinowany jest profesją podmiotu definiującego. Inne rozumienie tejże technologii prezentować będą bowiem przedstawiciele biznesu, a jeszcze inne przedstawiciele nauk technicznych (informatyki), ekonomicznych czy prawnych.

I tak dla przykładu wskazać można, że z perspektywy biznesowej Internet Rzeczy to ekosystem usług biznesowych wykorzystujących przedmioty zdolne do zbierania i przetwarzania informacji (interakcji), połączone w sieć, zapewniające interoperacyjność i synergię zastosowań. Łączenie produktów/usług Internetu Rzeczy pozwala na lepsze zrozumienie konsumenta, środowiska, produktów oraz procesów, identyfikację istotnych zdarzeń i reagowanie w celu natychmiastowego optymalizowania czy precyzyjniejszej personalizacji[11].

Natomiast w ujęciu technologicznym[12] IoT to koncepcja architektury informatycznej, która umożliwia współpracę (interoperacyjność) różnorodnych systemów teleinformatycznych wspierających rozmaite zastosowania dziedzinowe, oparta na następujących

10 Bezpieczeństwo militarne rozumiane jako potencjalna możliwość wykorzystania infrastruktury IoT m.in. do szpiegowania poprzez zbieranie informacji, nieautoryzowanego wykorzystania metadanych, spowodowania celowego unieruchomienia ważnych komponentów infrastruktury krytycznej czy awarii masowej, możliwości wykorzystania narzędzi IoT jako bezpośredniego narzędzia do ataku lub spowodowania katastrofy (np. dron czy pojazd autonomiczny).

11 *IoT w polskiej gospodarce*, s. 5.

12 Tamże.

warstwach: sprzęt[13], komunikacja[14], oprogramowanie[15], integracja[16].

Wreszcie też pojęcie Internetu Rzeczy prezentowane może być zarówno w ujęciu mikro i wówczas obejmować będzie ono urządzenie lub zespół urządzeń wyposażonych w oprogramowanie i podłączonych do sieci telekomunikacyjnej, z której wykorzystaniem przesyłane są dane, polecenia oraz aktualizacje do i z urządzeń[17], jak i w ujęciu makro, gdzie w ramach Internetu następuje komunikacja w formule rzecz–rzecz[18].

Jakkolwiek jednak definiować zjawisko Internetu rzeczy, istotne jest to, że warunkiem *sine qua non*, aby w ogóle można było w określonym przypadku uznać, że mamy do czynienia z urządzeniem IoT, jest konieczność wyposażenia tegoż urządzenia w oprogramowanie lub dostęp do sieci telekomunikacyjnej[19] i zdolność do łączenia się pomiędzy sobą poszczególnych urządzeń[20].

Aby w ogóle można było w określonym przypadku uznać, że mamy do czynienia z urządzeniem IoT, konieczne jest wyposażenia tegoż urządzenia w oprogramowanie lub dostęp do sieci telekomunikacyjnej i zdolność do łączenia się z innymi urządzeniami.

W rzeczywistości, w zakresie pojęcia Internet rzeczy, mieścić się będzie szereg różnego rodzaju urządzeń, tj. od inteligentnych zegarków (tzw. Smartwatchy) począwszy, poprzez inteligentne lampy, żarówki, kamery do monitoringu (a więc te kwalifikowane do urządzeń *smart home*), urządzenia medyczne (np. rozruszniki serca), a na inteligentnych (autonomicznych) pojazdach skończywszy. Natomiast w szeroko rozumianej edukacji (jako tej, w ramach której dochodzi do wykorzystywania przez studentów urządzeń IoT – co jest przedmiotem niniejszej analizy) Internet rzeczy również znajdować będzie całe spectrum zastosowań[21], tj. np.: interaktywne tablice[22], skanery[23]

13 Pod pojęciem sprzętu rozumieć należy urządzenia (lub przedmioty w nie wyposażone), w szczególności sensory, elementy wykonawcze, ale także sterowniki, smartfony, tablety, laptopy czy komputery, które zdolne są do komunikacji i przetwarzania danych bez zaangażowania człowieka lub w ograniczonej z nim interakcji.

14 Komunikacja, czyli infrastruktura telekomunikacyjna oraz sieć telekomunikacyjna (przewodowa lub bezprzewodowa), pracująca na podstawie dowolnych standardów transmisji danych o dowolnym zasięgu (tu Internet).

15 Oprogramowanie to systemy informatyczne urządzeń IoT oraz oprogramowanie służące do wymiany danych, ich przetwarzania, zarządzania systemem i jego zabezpieczenia.

16 Integracja, czyli zbiory zdefiniowanych usług informatycznych zapewniających interoperacyjność oprogramowania na wszystkich poziomach architektury.

17 P. Marciniak, *Problem odpowiedzialności za błędy w oprogramowaniu*, „Przegląd Ustawodawstwa Gospodarczego" 2020, nr 10, s. 38.

18 L. Tan, N. Wang, *Future internet: The Internet of Things*, https://ieeexplore.ieee.org/document/5579543 (dostęp: 14.02.2024).

19 P. Marciniak, *Problem*…, s. 38.

20 Najczęściej jest to Wi-Fi, Ethernet lub Bluetooth.

21 Zob. więcej: M. Tomas, *The Connected Classroom: 9 Examples of IoT in Education*, https://builtin.com/internet-things/iot-education-examples (dostęp: 19.09.2021).

22 Tablice te łączą w sobie technologię wielodotykową, suchościeralną i naturalnego pisania, a także oparte na chmurze oprogramowanie do prowadzenia lekcji i spersonalizowane szkolenia dla nauczycieli.

23 Użytkownicy takich skanerów mogą szybko skanować edytowalny tekst z książek czy bezpośrednio do telefonu, tabletu

czy też „inteligentne" karty (legitymacje) studenckie, które to *notabene* stały się przyczynkiem do podjęcia rozważań w ramach przedmiotowej pracy, a których to praktyczne wykorzystanie doskonale zobrazować może złożoność samego środowiska IoT i jego wpływ na ocenę prawną bezpieczeństwa cybernetycznego studenta w otoczeniu IoT.

In concreto przywołane wcześniej „inteligentne" karty studenckie są unikatowymi „kluczami", które umożliwiają poszczególnym studentom dostęp do kampusu, wydziałów i poszczególnych sal wykładowych. Student, który chce wejść na teren swojego wydziału, skanuje kartę, która – jak już wspomniano – poza fizycznym umożliwieniem studentowi wejścia do budynku, dokonuje także rejestracji faktu jego przybycia na określone zajęcia (odnotowuje jego obecność w określonym czasie i określonym miejscu, a następnie zestawia to z harmonogramem zajęć), natomiast w przypadku scenariusza mobilizacji w nagłych wypadkach dane zapisane na karcie, a następnie przetworzone przez obsługujące je oprogramowanie mogą pomóc zweryfikować, kto znajdował się w określonym czasie w danej części budynku.

Co więcej, przy pomocy owych „inteligentnych" kart placówki edukacyjne mogą udzielać dostępu, a następnie monitorować wykorzystanie danych dotyczących zajęć, zasobów e-learningowych, z których korzystają studenci, a także umożliwiać zapisy na poszczególne przedmioty. Często karty identyfikacyjne są używane także jako karty biblioteczne czy karty członkostwa w klubach sportowych i stowarzyszeniach. W praktyce przedmiotowe karty wykorzystywane mogą być również jako swoistego rodzaju „karty płatnicze", dzięki którym student – w sposób bezgotówkowy – może dokonywać transakcji zakupu w automatach, opłacać usługę kserowania czy drukowania bądź opłacać posiłki na stołówkach akademickich – po czym dochodzi do automatycznego pobrania określonych kwot pieniężnych z kont indywidualnych studentów. Wreszcie też warto zauważyć, że karty te mogą być używane do przechowywania ważnych danych osobowych poszczególnych studentów, w tym dotyczących ich krewnych i kontaktów do nich w nagłych przypadkach czy też danych o stanie zdrowia, jak np. grupie krwi, zażywanych lekach czy alergenach[24].

3. Bezpieczeństwo fizyczne i cyberbezpieczeństwo urządzeń IoT a przepisy Kodeksu cywilnego

Jak zauważono już wcześniej, w ogólnym pojęciu bezpieczeństwa cybernetycznego wyróżnić można różnego rodzaju podkategorie, w tym te dotyczące bezpieczeństwa fizycznego i cyberbezpieczeństwa samych urządzeń tworzących Internet rzeczy. Pierwsza z wymienionych kategorii (bezpieczeństwo fizyczne), jak wskazała w swoim raporcie *IoT w polskiej gospodarce* Grupa Robocza ds. Internetu Rzeczy działająca przy Ministerstwie Cyfryzacji, dotyczyć będzie wpływu technologii IoT i jej zastosowania na świat fizyczny (oddziaływanie bezpośrednie i wpływ świata IoT na codzienne życie obywateli, np. funkcje blokady drzwi, skrętu auta autonomicznego, kontroli przepływu w wodociągach czy prawidłowe działanie urządzenia telemedycznego, takiego jak stymulator serca), natomiast cyberbezpieczeństwo produktów sprowadzać będzie się do zagadnienia zapewnienia odpowiedniego poziomu wykonania produktu oraz wyposażenia go w narzędzia i mechanizmy przeciwdziałające zagrożeniom teleinformatycznym. Przekładając powyższe na stanowiący przedmiot niniejszej pracy kazus wykorzystania przez studenta urządzenia IoT w postaci „inteligentnej" karty, można stwierdzić, że zagadnienie bezpieczeństwa fizycznego owej karty w kontekście cyberbezpieczeństwa studenta identyfikowane może być np. z przypadkiem niekontrolowanej przez studenta blokady drzwi po jego wejściu do sali, natomiast cyberbezpieczeństwo produktu (karty) np. z możliwością użycia karty i przypisanego do niego konta przez nieuprawnione osoby trzecie i dalej wykorzystanie luki znajdującej się w oprogramowaniu do dokonania ataku na indywidualne konto studenta (a nawet szerzej: na cały system informatyczny danej uczelni). Powstaje więc pytanie: czy w tego typu przypadkach możliwe będzie zastosowanie przepisów k.c.,

lub komputera. Tekst ten można następnie przetłumaczyć na ponad czterdzieści języków. Dostępna jest także funkcja, która pozwala słuchać podczas skanowania.

24 Zob. więcej o inicjatywie MagiCard, która wykorzystywana jest np. w Wielkiej Brytanii w Weymouth: https://magicard.com/solutions/by-industry/education/ (dostęp: 1.10.2021).

a jeśli tak, to które z nich stanowić mogą podstawę formułowania wobec producenta urządzeń IoT roszczeń odszkodowawczych?

Wśród przedstawicieli nauki wyrażony został pogląd, że z cywilnoprawnego punktu widzenia korzystanie z IoT obejmuje korzystanie z rzeczy (urządzenie podłączone do sieci), oprogramowania (aplikacje i systemy IoT) oraz usługi (np. dostęp do sieci, dostarczanie danych)[25]. Natomiast Piotr Marciniak w swojej analizie problemu odpowiedzialności za błędy w oprogramowaniu IoT doprecyzowuje, że „istnieją formalnie dwa sposoby pociągnięcia do odpowiedzialności producenta lub dystrybutora za wady IoT, tj. odpowiedzialność z tytułu sprzedaży rzeczy oraz odpowiedzialność z tytułu wad oprogramowania" i dalej konstatuje, że „gdy elementy rozwiązań IoT są sprzedawane jako rzecz, zastosowanie ma rękojmia i bardzo często – gwarancja"[26]. To pozornie niewymagające głębszej analizy zagadnienie w przypadku Internetu rzeczy skłania jednak do refleksji i kilku słów komentarza.

Otóż zważyć należy, że w opisanym powyżej kazusie „inteligentnych kart" (podobnie jak to miało do tej pory miejsce w przypadku legitymacji studenckich) w założeniu uczelnia, a nie poszczególni studenci, będzie – jako kupująca – zgodnie z art. 556 k.c. miała wyłącznie legitymację czynną wobec sprzedawcy (jako legitymowanym biernie) formułowania roszczeń z tytułu wad tego typu kart „inteligentnych". Natomiast ocena, czy – a jeśli tak, to kiedy – to student miałby przysługujące wobec pierwotnego sprzedawcy uprawnienia wynikające z przepisów o rękojmi, poprzedzona musi zostać wcześniej oceną, kiedy uprawnienia z tytułu rękojmi mogą być przeniesione na kolejnego nabywcę. I choć w tym zakresie niejednokrotnie wypowiadali się przedstawiciele doktryny[27], a także przedstawiciele judykatury, to nadal jednak nie wypracowano jednolitego stanowiska. W pierwszych wypowiedziach judykatury w tym temacie[28] optowano za twierdzeniem, że uprawnienia z tytułu rękojmi „idą" za rzeczą, a zmiana właściciela nabytej rzeczy w drodze umowy sprzedaży, zamiany i darowizny lub spadkobrania nie eliminuje więzi prawnej ze sprzedawcą (producentem). Następcy prawni kupującego są tylko kontynuatorami jego uprawnień[29]. Z czasem stanowisko to zrewidowano[30] na rzecz koncepcji, w myśl której sprzedaż rzeczy przez kupującego nie powoduje przejścia na nabywcę uprawnień z tytułu rękojmi za wady fizyczne rzeczy; kupujący może jednak przelać

Z cywilnoprawnego punktu widzenia korzystanie z IoT obejmuje korzystanie z rzeczy (urządzenie podłączone do sieci), oprogramowania (aplikacje i systemy IoT) oraz usługi (np. dostęp do sieci, dostarczanie danych).

25 X. Konarski, *Internet Rzeczy – najważniejsze regulacje prawne w Polsce*, https://www.traple.pl/2020/06/17/internet-rzeczy-najwazniejsze-regulacje-prawne-w-polsce/ (dostęp: 2.10.2020).

26 P. Marciniak, *Problem*…, s. 39.

27 Zob. m.in. A. Pawlikowska, *Przejście uprawnień z tytułu rękojmi, niezgodności towaru konsumpcyjnego z umową i gwarancji na dalszych nabywców – rozważania na podstawie prawa polskiego i wybranych systemów europejskich*, „Transformacje Prawa Prywatnego" 2008, nr 3–4, s. 53 i n.

28 Jako cezurę czasową wskazuje się rok 2004 i wydaną wówczas uchwałę SN z 5 lutego 2004 r., III CZP 96/03, Legalis nr 61423.

29 Uchwała SN z 30 grudnia 1988 r., III CZP 48/88, Lex nr 3429; wyrok SN z 2 października 1997 r., II CKN 361/97, Legalis nr 343232.

30 Zob. więcej: K. Koch, *Przejście uprawnień z tytułu rękojmi na kolejnego nabywcę rzeczy – glosa – III CZP 96/03*, „Monitor Prawniczy" 2007, nr 3, s. 156 i n.

na nabywcę uprawnienia do żądania obniżenia ceny, usunięcia wady lub dostarczenia rzeczy wolnej od wad[31]. Przychylenie się do drugiego, aktualnie forsowanego w orzecznictwie stanowiska prowadzi do konkluzji, że ewentualna możliwość dochodzenia przez studenta roszczeń z tytułu rękojmi wymagać będzie po stronie uczelni po pierwsze, dostrzeżenia konieczności zabezpieczenia interesów studenta w tym zakresie, a po drugie, cesji na jego rzecz wskazanych wyżej uprawnień.

W przypadku poszukiwania odpowiedzi na pytanie o ochronę na gruncie przepisów Kodeksu cywilnego studenta jako użytkownika urządzeń Internetu rzeczy nasuwa się także kwestia możliwości (czy też braku) zastosowania przepisów dotyczących odpowiedzialności za produkt niebezpieczny, a więc przepisów art. 449^1–449^{10} k.c.

W przypadku poszukiwania odpowiedzi na pytanie o ochronę na gruncie przepisów k.c. studenta jako użytkownika urządzeń Internetu rzeczy nasuwa się także kwestia możliwości (czy też braku) zastosowania przepisów dotyczących odpowiedzialności za produkt niebezpieczny, a więc przepisów art. 449^1–449^{10} k.c. Wspomnieć należy, że zgodnie z treścią pierwszej z norm, tj. art. 449^1 § 1 k.c., „kto wytwarza w zakresie swojej działalności gospodarczej (producent) produkt niebezpieczny, odpowiada za szkodę wyrządzoną komukolwiek przez ten produkt”[32]. Jednoznacznie więc odpowiedzialność za szkodę wyrządzoną przez produkt ponosi ten, kto ma wpływ na jego bezpieczeństwo, a zatem co do zasady jego producent, czyli wytwórca wyrobu finalnego, choć na warunkach określonych w treści art. 449^5 k.c. odpowiedzialność tą ponoszą także inne podmioty, które jako profesjonaliści uczestniczą w procesie wytwarzania lub wprowadzania tego produktu do obrotu, przy czym odpowiedzialność tych podmiotów nie jest jednakowa, co łączy się z różną postacią okoliczności egzoneracyjnych[33]. Natomiast uprawnionym, który na zasadach określonych w art. 449^1–449^{10} k.c. może dochodzić naprawienia szkody, jest każdy, kto został poszkodowany przez produkt niebezpieczny, a więc nie tylko np. konsument. Co więcej, jak wskazuje się w doktrynie, użyte w art. 449^1 k.c. określenie „komukolwiek” obejmuje nie tylko bezpośredniego nabywcę produktu niebezpiecznego, ale też i każdego jej następnego posiadacza, a nawet osobę, która przypadkowo dotknięta została przez szkodliwe oddziaływanie tego przedmiotu. Poszkodowanym może być zarówno ten, kto nabył wprowadzony do obrotu produkt niebezpieczny na własny użytek, jak i ten, kto jako osoba postronna znalazł się

31 Uchwała SN z 5 lutego 2004 r., III CZP 96/03, Legalis nr 61423 oraz wyrok SN z 18 stycznia 2017 r., V CSK 223/16, Legalis nr 1603877.

32 Zagadnienie odpowiedzialności za produkt niebezpieczny w polskim piśmiennictwie doczekało się wielu opracowań. Zob. m.in.: M. Jagielska, *Odpowiedzialność za produkt*, „Monitor Prawniczy” 2000, nr 8, s. 495 i n.; B. Gnela, *Odpowiedzialność za produkt (uwagi o polskiej regulacji)*, „Państwo i Prawo” 2009, nr 9, s. 33–47.

33 W. Dubis, *Art. 449^1 [Ryzyko producenta]*, w: *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, Warszawa 2021, nb. 1.

w obszarze szkodliwego oddziaływania takiego produktu[34], czyli tzw. osoba trzecia (*by-stander*)[35]. Tego typu okoliczność w przypadku rozpatrywania możliwości dochodzenia przez studenta roszczeń z tytułu szkody wyrządzonej przez produkt IoT – na podstawie treści art. 449^1 i nast. k.c. – zdaje się czynić go czynnie legitymowanym w tym zakresie. Niemniej powyższa teza wymaga doprecyzowania, jeżeli weźmie się pod uwagę fakt, że jakkolwiek uprawnionym jest – w myśl komentowanego artykułu – każdy, komu produkt niebezpieczny wyrządza szkodę, to jednak ustawodawca, definiując produkt niebezpieczny (art. 449^1 § 3 k.c.), odwołuje się do pojęcia konsumenta[36]. To też, jak się wydaje, może być przyczyną formułowania twierdzeń, że odpowiedzialność za produkt niebezpieczny dotyczy tylko relacji z konsumentem[37] lub też – jak wskazuje P. Marciniak – w kontekście treści art. 449^2 k.c., że na podstawie przedmiotowej normy w odniesieniu do reżimu odpowiedzialności za produkt niebezpieczny „wywodzi się przede wszystkim ochronę konsumenta[38]. Gdyby więc przyjąć powyższy punkt widzenia za trafny – co *notabene* będzie jeszcze przedmiotem późniejszych rozważań – należałoby się zastanowić, czy student może być uznany za konsumenta. W odpowiedzi na powyższe warto w pierwszym rzędzie wskazać, że w myśl art. 425 Ustawy z dnia 20 lipca 2018 roku Prawo o szkolnictwie wyższym i nauce (p.s.w.n.)[39] wykonywanie przez uczelnię zadań, o których mowa w art. 11[40], oraz prowadzenie działalności sportowej, rehabilitacyjnej lub diagnostycznej nie stanowi działalności gospodarczej w rozumieniu przepisów Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców[41]. Jak jednak słusznie wskazuje Jan Michał Zieliński: „powyższe nie oznacza, że uczelnie w zakresie wymienionej w przepisie działalności odwołującej się do art. 11 p.s.w.n. nie są przedsiębiorcami. Uczelnie nie są bowiem przedsiębiorcami w rozumieniu powołanej w przepisie Ustawy z 6.03.2018 r. – Prawo przedsiębiorców", lecz nie stoi to na przeszkodzie uznaniu ich za przedsiębiorców w rozumieniu innych przepisów prawa. Powyższemu wtóruje także Marek Salamonowicz, który wskazuje, iż: „z praktyki wynika, że działalność uczelni w zakresie określonym w art. 11 p.s.w.n. może być kwalifikowana jako działalność gospodarcza przedsiębiorcy w rozumieniu innych ustaw"[42].

Tym samym „bez wątpienia uczelnie są zatem przedsiębiorcami w rozumieniu ustawy z 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2021 r., poz. 275). Artykuł 4 pkt 1 tej ustawy przez przedsiębiorcę rozumie bowiem nie tylko przedsiębiorcę w rozumieniu przepisów ustawy Prawo przedsiębiorców, lecz także m.in. osobę prawną organizującą lub świadczącą usługi o charakterze użyteczności publicznej, które nie są działalnością gospodarczą w rozumieniu przepisów Ustawy z 6 marca 2018 r. – Prawo przedsiębiorców. Potraktowanie w tym zakresie uczelni jako przedsiębiorcy powoduje, że studenci i doktoranci traktowani są jak konsumenci, ze wszystkimi konsekwencjami wynikającymi z tego faktu – a więc i z decyzjami Prezesa Urzędu Ochrony Konkurencji i Konsumentów w przypadku uznania, że naruszone zostały prawa konsumenckie"[43]. *Notabene* powyższa argu-

34 Tamże.

35 E. Rutkowska, B. Trabszys, *Odpowiedzialność zbywcy za produkt niebezpieczny sprowadzony przez niego do Polski z innego państwa członkowskiego Unii Europejskiej*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2016, nr 8, s. 84.

36 Z. Banaszczyk, *Art. 449^1 [Ryzyko producenta]* w: *Kodeks cywilny. Komentarz*, t. 1, red. K. Pietrzykowski, Warszawa 2020, nb. 20.

37 X. Konarski, *Internet Rzeczy...*, dz.cyt.

38 P. Marciniak, *Problem...*, s. 42.

39 Ustawa z 20 lipca 2018 roku – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2018 r., poz. 1668 ze zm.).

40 Art. 11 Ustawy prawo o szkolnictwie wyższym i nauce wskazuje katalog podstawowych zdań uczelni, tj. m.in.: prowadzenie kształcenia na studiach, prowadzenie kształcenia na studiach podyplomowych lub innych form kształcenia, prowadzenie działalności naukowej, świadczenie usług badawczych oraz transfer wiedzy i technologii do gospodarki, prowadzenie kształcenia doktorantów, kształcenie i promowanie kadr uczelni.

41 Dz.U. z 2021 r., poz. 162 ze zm.

42 M. Salamonowicz, *Art. 425 [Działalność uczelni niestanowiąca działalności gospodarczej]*, w: *Prawo o szkolnictwie wyższym i nauce. Komentarz*, red. A. Jakubowski, Warszawa 2023, nb. 2.

43 J.M. Zieliński, *Art. 425 [Działalność uczelni niestanowiąca działalności gospodarczej]*, w: *Prawo o szkolnictwie wyższym i nauce. Komentarz*, red. H. Izdebski, J.M. Zieliński, LEX/el. 2021, nt. 3.

mentacja zdaje się mieć rację bytu także w odniesieniu do pojęcia przedsiębiorcy wskazanego w art. 43^1 k.c., zgodnie z którym przedsiębiorcą jest osoba fizyczna, osoba prawna i jednostka organizacyjna, o której mowa w art. 33^1 § 1, prowadząca we własnym imieniu działalność gospodarczą lub zawodową. Przede wszystkim podkreślić bowiem trzeba, że w przypadku stosowania norm wyznaczających stosunki cywilnoprawne zasadniczo prawnie irrelewantne pozostają przepisy wspomnianej powyżej ustawy Prawo przedsiębiorców jako aktu z zakresu prawa publicznego[44]. Dodatkowo zwrócić należy także uwagę na fakt, że w przypadku uczelni niepaństwowych fakt prowadzenia przez nie działalności gospodarczej w rozumieniu przepisów k.c. został jednolicie przyjęty nie tylko w doktrynie[45], ale także i potwierdzony przez Trybunał Konstytucyjny[46]. Jednocześnie, na co słusznie uwagę zwraca Natalia Miłostan, choć w piśmiennictwie podkreśla się, że nieco odmiennie kształtuje się sytuacja uczelni publicznych, które kształcą studentów na mocy decyzji administracyjnej będącej podstawą przyjęcia na studia, to ostatecznie jednak, zgodnie z poglądem wyrażonym przez Sąd Najwyższy w postanowieniu z 21 listopada 2000 r.[47], powstanie stosunku cywilnoprawnego może łączyć się z różnymi działaniami i zaniechaniami, w tym z aktami administracyjnymi wywołującymi skutki w zakresie prawa cywilnego[48].

Jednoznacznie więc, nawet gdyby reżim odpowiedzialności za produkt niebezpieczny limitowany był wyłącznie do roszczeń konsumenckich, to w świetle powyższych rozważań również i student z takiej ochrony mógłby skorzystać. W tym miejscu jednak podkreślić należy, że posłużenie się przez ustawodawcę sformułowaniem „konsument" w treści art. 449^1 § 3 zd. 2 w istocie służyć ma jedynie określeniu wzorca osoby, której oczekiwania powinny być brane pod uwagę przy dokonywaniu oceny niebezpiecznych właściwości produktu, a nie zdefiniowaniu grupy podmiotów uprawnionych do dochodzenia odszkodowania, stąd niezasadne wydaje się ograniczenie kręgu uprawnionych do dochodzenia roszczeń z tytułu produkt niebezpiecznego. Stąd w tym zakresie prawnie irrelewantna będzie także ocena, czy student może być uznany za konsumenta. Bez znaczenia dla omawianego problemu pozostaje także to, czy studenta jako poszkodowanego łączyły z producentem jakieś

W odniesieniu do urządzeń Internetu rzeczy problematyczne może okazać się ich zakwalifikowanie jako produktów niebezpiecznych rozumianych jako rzeczy ruchome, choćby zostały one połączone z innymi rzeczami. Za produkt uważa się także zwierzęta i energię elektryczną.

44 R. Strugała, *Art. 43^1 [Pojęcie przedsiębiorcy]*, w: *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, Warszawa 2023, nb. 1.

45 N. Miłostan, *Szkoła wyższa jako przedsiębiorca w warunkach społecznej gospodarki rynkowej*, w: *Zarządzanie szkołą wyższą*, red. J. Blicharz, A. Chrisidu-Budnik, A. Sus, Wrocław 2014, s. 61 i n.

46 Zob. więcej: wyrok TK z 5 października 2005 r., SK 39/05, Legalis nr 70595.

47 Postanowienie SN z 21 listopada 2000 r., III CKN 1048/00, Legalis nr 76569.

48 N. Miłostan, *Szkoła wyższa…*, s. 64.

stosunki prawne, czy też nie, albowiem odpowiedzialność za produkt powstaje *ex lege* w reżimie deliktowym i już samo ziszczenie się jej przesłanek rodzi pierwotny obowiązek naprawienia szkody[49].

Powyższe ustalenia, jakkolwiek prawnie relewantne, *per se* stanowią jedynie pewnego rodzaju preludium do dalszych rozważań dotyczących możliwości zastosowania przepisów o odpowiedzialności za produkt niebezpieczny w przypadku Internetu rzeczy, a ocena w tym zakresie jedynie pozornie wydaje się oczywista. Przede wszystkim – w odniesieniu do urządzeń Internetu rzeczy – problematyczne może okazać się ich zakwalifikowanie jako produktów niebezpiecznych w rozumieniu art. 449^1 § 2 k.c, który to wprost stanowi, iż przez produkt rozumie się rzecz ruchomą, choćby została ona połączona z inną rzeczą. Za produkt uważa się także zwierzęta i energię elektryczną.

Wobec takiej konstrukcji ww. przepisu i w związku z treścią art. 45 k.c., który stanowi, iż rzeczami w rozumieniu k.c. są tylko przedmioty materialne, wątpliwości nie budzi fakt, iż produktem niebezpiecznym mogą być rzeczy materialne. Bardziej problematyczne, a przy tym w kontekście produktów Internetu rzeczy niezwykle istotne, wydaje się rozstrzygnięcie, czy w pojęciu rzeczy ruchomej, jak uważają niektórzy, mieścić mogą się dobra intelektualne, tj. m.in. oprogramowania komputerowe. Okoliczność ta jest zaś niezmiernie istotna, albowiem immanentną cechą urządzeń tworzących IoT, poza sprzętem, są przecież oprogramowania owe urządzenia „obsługujące".

W doktrynie jak dotąd nie wypracowano jednego spójnego stanowiska[50] co do możliwości objęcia zakresem przedmiotowym pojęcia produktu niebezpiecznego także dóbr niematerialnych (oprogramowania komputerowego)[51]. I tak część przedstawicieli doktryny prezentuje pogląd, w myśl którego dobra niematerialnie nie mogą być traktowane jako produkt niebezpieczny, a to z uwagi na ich niematerialny charakter. Jak się konkluduje, dobra niematerialne nie mieszczą się w kategorii „produkt" w rozumieniu art. 449^1 § 2 w zw. z art. 45 k.c., gdyż nie mają wymaganej dla rzeczy postaci materialnej nawet wtedy, kiedy staną się elementem umożliwiającym stworzenie określonej rzeczy czy zapewnią możliwość jej wykorzystywania, tak jak to ma miejsce szczególnie w przypadku oprogramowania informatycznego[52]. Tego typu stanowisko z punktu widzenia interesów studenta i dalej możliwości zapewnienia mu ochrony na podstawie przepisów o produkcie niebezpiecznym nie jest korzystne.

W doktrynie jak dotąd nie wypracowano spójnego stanowiska co do możliwości objęcia zakresem przedmiotowym pojęcia produktu niebezpiecznego także dóbr niematerialnych (oprogramowania komputerowego).

Jednocześnie w doktrynie wskazuje się, że oprogramowanie komputerowe w momencie zintegrowania

49 Z. Banaszczyk, *Art. 449^1*..., nb. 20.

50 Zob. więcej: J.M. Kondek, *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję (uwagi de lege lata i de lege ferenda)*, Warszawa 2021, s. 6 i n.

51 Zob. więcej: J. Kuźmicka-Sulikowska, *Pojęcie produktu niebezpiecznego na gruncie przepisów kodeksu cywilnego dotyczących odpowiedzialności za szkodę wyrządzoną przez ten produkt*, w: *Księga dla naszych kolegów. Prace prawnicze poświęcone pamięci doktora Zygmunta Masternaka, doktora Andrzeja Ciska, doktora Marka Zagrosika*, red. J. Mazurkiewicz, Wrocław 2013, s. 252–254.

52 Zob. W. Dubis, *Art. 449^1*..., nb. 11.

go z pewną rzeczą, choćby komputerem czy innym urządzeniem, staje się „swoistego rodzaju częścią składową produktu" i wówczas jako takie powinno podlegać reżimowi odpowiedzialności za produkt[53]. Jeszcze inni uznają natomiast, że oprogramowanie powinno być traktowane jako produkt[54]. Oczywiście z punktu widzenia interesów studenta i dalej zapewnienia mu jako potencjalnie poszkodowanemu ochrony odpowiedzenie się za możliwością zakwalifikowania oprogramowania komputerowego jako produktu niebezpiecznego jest niewątpliwie pożądane i trafne, jeżeli nie *de lege lata*, to z całą pewnością *de lege ferenda*[55].

Z punktu widzenia interesów studenta i dalej zapewnienia mu jako potencjalnie poszkodowanemu ochrony odpowiedzenie się za możliwością zakwalifikowania oprogramowania komputerowego jako produktu niebezpiecznego jest niewątpliwie pożądane i trafne, jeżeli nie *de lege lata*, to z całą pewnością *de lege ferenda*.

Kilka słów komentarza warto poświęcić zagadnieniu przesłanek egzoneracyjnych, których wykazanie może zwolnić producenta urządzeń Internetu rzeczy od odpowiedzialności za produkt niebezpieczny. Ustawodawca w treści art. 449^3 k.c. przewidział pięć takich przesłanek, przy czym w kontekście IoT szczególnego znaczenia nabiera ta związana z właściwościami niebezpiecznego produktu, które ujawniły się po wprowadzeniu go do obrotu. Jak stanowi art. 449^3 § 2 zd. 2 k.c., producent nie odpowiada za szkodę wyrządzoną przez produkt niebezpieczny także wtedy, gdy nie można było przewidzieć niebezpiecznych właściwości produktu, uwzględniając stan nauki i techniki w chwili wprowadzenia produktu do obrotu[56]. Na tej podstawie, w odniesieniu do urządzeń IoT i perspektywy ich wykorzystania przez studenta, a także uwzględniając specyfikę Internetu rzeczy, nietrudno sobie wyobrazić, że niebezpieczne właściwości produktu ujawnią się dopiero po wprowadzeniu produktu do obrotu, a stan nauki i techniki[57] w chwili wprowadzenia nie pozwalała na przewidzenie owej niebezpiecznej cechy. Właściwie w przypadku urządzeń IoT można byłoby zaryzykować twierdzenie, że immanentną cechą tych

53 Zob. M. Jagielska, *Odpowiedzialność*..., s. 495 i n. oraz cytowana tam literatura.

54 J. Kuźmicka-Sulikowska, *Pojęcie produktu niebezpiecznego*..., s. 252–254.

55 Tamże.

56 Jest to tzw. ryzyko rozwoju. Zob. więcej: J. Kuźmicka-Sulikowska, *Okoliczności wyłączające odpowiedzialność za szkodę wyrządzoną przez produkt niebezpieczny*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2015, t. 100, nr 1, s. 492–497.

57 W świetle orzecznictwa TSUE (wyr. TSUE z 29 maja 1997 r. C-300/95, *Komisja v. Wielka Brytania*, ECLI:EU:C:1997:255) w ramach tzw. ryzyka rozwojowego należy brać pod uwagę stan wiedzy naukowej i technicznej na poziomie najbardziej zaawansowanym, który istniał w momencie wprowadzenia produktu do obrotu. Punktem odniesienia jest obiektywny stan tej wiedzy, nie zaś wiedza, którą konkretny producent posiadał lub mógł posiąść. Wymagana wiedza powinna być jednak dostępna w momencie wprowadzenia produktu do obrotu. Zob. P. Mikłaszewicz, *Art. 449^3 [Okoliczności zwalniające]*, w: *Kodeks cywilny. Komentarz*, red. K. Osajda, Warszawa 2021, nb. 4.

produktów jest ryzyko braku przewidzenia w momencie wprowadzenia do obrotu wynikającego z ich użytkowania niebezpieczeństwa. Tymczasem jeśli niebezpieczna cecha produktu ujawniła się później, po wprowadzenia go do obrotu, ale wynikała z przyczyny tkwiącej w produkcie[58], musi to wykazać poszkodowany[59], a więc w przypadku przedmiotowej analizy – który *notabene* stanowi implementację do polskiego porządku prawnego szeregu aktów unijnych[61], reguluje kwestie związane z prawami konsumentów i obowiązkami przedsiębiorców w tym zakresie, a więc ma istotne znaczenie także w kontekście przedmiotu niniejszej pracy. Jeżeli chodzi o samo pojęcie konsumenta czy przedsiębiorcy, to w świetle przepisów wspo-

Czyniąc uwagi na temat otoczenia regulacyjnego dla bezpieczeństwa cybernetycznego studenta w „świecie" Internetu rzeczy, warto pochylić się jeszcze nad przepisami pozakodeksowymi, a zwłaszcza przepisami Ustawy o prawach konsumenta.

student. Okoliczność ta okazać może się zniechęcająca chociażby z uwagi na znaczące koszty ekspertyz (opinii biegłych) powyższe wykazujących.

Dodatkowo z praktycznego punktu widzenia także fakt, że w środowisku IoT zachodzą interakcje wielu różnych urządzeń i usług podłączonych do sieci może, o ile nie uniemożliwiać, to znacznie utrudniać ustalenie, gdzie powstała szkoda i kto (który z producentów różnych urządzeń) ponosi za nią odpowiedzialność.

4. Regulacje pozakodeksowe

Czyniąc uwagi na temat otoczenia regulacyjnego dla bezpieczeństwa cybernetycznego studenta w „świecie" Internetu rzeczy, warto pochylić się jeszcze nad przepisami pozakodeksowymi, a zwłaszcza przepisami Ustawy o prawach konsumenta[60]. Akt ten, mnianej ustawy wykładane powinno być z uwzględnieniem definicji konsumenta zawartej w art. 2 pkt 1 dyrektywy 2011/83/UE oraz definicji przedsiębiorcy w rozumieniu art. 2 pkt 2 tej dyrektyw, tj. jako każdą osobę fizyczną, która w umowach objętych dyrektywą działa w celach niezwiązanych z działalnością handlową, gospodarczą, rzemieślniczą ani wykonywaniem

58 Wyrok SA w Warszawie z 4 listopada 2008 r., I ACa 526/08, LEX nr 1641212.

59 Jeżeli producent powołuje się na ryzyko rozwoju jako okoliczność egzoneracyjną, musi wykazać, że stan wiedzy istniejący w momencie wprowadzania produktu do obrotu nie pozwalał na wykrycie jego niebezpiecznych właściwości.

60 Ustawa z 30 maja 2014 r. o prawach konsumenta (tekst jedn.: Dz.U. z 2023 r., poz. 2759 ze zm).

61 Są to np.: Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z 25 października 2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady z 25 października 2011 r. (Dz.Urz. UE L 304, s. 64–88), Dyrektywa 2002/65/WE Parlamentu Europejskiego i Rady z 23 września 2002 r. dotycząca sprzedaży konsumentom usług finansowych na odległość oraz zmieniająca dyrektywę Rady 90/619/EWG oraz dyrektywy 97/7/WE i 98/27/WE z 23 września 2002 r. (Dz.Urz UE L 271, s. 16–24), Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/2161 z 27 listopada 2019 r. zmieniająca dyrektywę Rady 93/13/EWG i dyrektywy Parlamentu Europejskiego i Rady 98/6/WE, 2005/29/WE oraz 2011/83/UE w odniesieniu do lepszego egzekwowania i unowocześnienia unijnych przepisów dotyczących ochrony konsumenta (Dz.Urz. UE L 328, s. 7–28).

wolnego zawodu. Przedsiębiorcą jest każda osoba fizyczna i każda osoba prawna, niezależnie od tego, czy jest to podmiot publiczny, czy prywatny, która działa – w tym również za pośrednictwem każdej innej osoby działającej w jej imieniu lub na jej rzecz – w celach związanych z jej działalnością handlową, gospodarczą, rzemieślniczą lub wykonywaniem wolnego zawodu, w związku z umowami objętymi zakresem dyrektywy 2011/83/UE[62].

W odniesieniu do zagadnienia analizowanego w ramach niniejszej pracy uwagę zwrócić należy zaś przede wszystkim na fakt, że w przedmiotowej ustawie – za sprawą implementacji przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/771 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniająca rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE i uchylająca dyrektywę 1999/44/WE[63] – w art. 2 pkt. 5b zdefiniowano towar z elementami cyfrowymi, tj. towar zawierający treść cyfrową lub usługę cyfrową lub z nimi połączony w taki sposób, że brak treści cyfrowej lub usługi cyfrowej uniemożliwiłby jego prawidłowe funkcjonowanie. W treści dyrektywy 2019/771, w jej motywie 15, wskazano przy tym, że niniejsza dyrektywa powinna mieć zastosowanie do umów sprzedaży towarów, w tym towarów z elementami cyfrowymi, w przypadku których brak zawarcia w tych towarach albo wzajemnego z nimi połączenia treści cyfrowych lub usług cyfrowych uniemożliwiłby tym towarom pełnienie ich funkcji oraz w przypadku których te treści lub usługi cyfrowe są dostarczane wraz z towarem na podstawie tej samej umowy sprzedaży dotyczącej tych towarów.

W świetle powyższego wątpliwości nie powinien więc budzić fakt, że pojęciem towaru z elementami cyfrowymi objąć można także urządzenia IoT, w tym także „inteligentne" karty studenta. Zresztą ustawodawca unijny w treści dyrektywy również powołuje jako przykłady towarów z elementami cyfrowymi, np. inteligentny zegarek czy inteligentny telewizor (motyw 15 preambuły). Tym samym już na wstępie rozważań poświęconych zagadnieniu ochrony prawnej studenta korzystającego z urządzeń IoT ocenić można, że fakt odrębnego uregulowania w prawie polskim umowy sprzedaży towaru z elementami cyfrowymi poprawia poziom ochrony korzystających z urządzeń IoT, albowiem wprowadza pewien normatywny wzorzec dla oceny, czy konkretna umowa została ukształtowana w sposób dopuszczalny[64].

Wątpliwości nie powinien więc budzić fakt, że pojęciem towaru z elementami cyfrowymi objąć można także urządzenia IoT, w tym także „inteligentne" karty studenta.

Omawiając więc w dalszej kolejności przepisy Ustawy o prawach konsumenta jako prawnie relewantnej dla kształtowania pozycji studenta korzystającego z urządzeń IoT, zwrócić należy uwagę na te przepisy, które zostały poświęcone zagadnieniu niezgodności

62 P. Mikłaszewicz, *Art. 2 [Objaśnienie terminów]*, w: *Ustawa o prawach konsumenta. Komentarz*, red. P. Mikłaszewicz, Legalis/el. 2022, nb. 3.

63 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/771 z 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniająca rozporządzenie (UE) 2017/2394 oraz dyrektywę 2009/22/WE i uchylająca dyrektywę 1999/44/WE (Dz.Urz. UE L 136, s. 28–50).

64 K. Południak-Gierz, *Wpływ dyrektyw 2019/770 oraz 2019/771 na poziom ochrony konsumenta w ramach reżimu rękojmi w prawie polskim*, „Prawo w działaniu" 2023, nr 54, s. 175–176.

towaru z umową (w ustawie nie posłużono się określeniem rękojmia).

Jak wskazano w art. 43a Ustawy o prawach konsumenta, w razie braku zgodności towaru z umową konsumentowi przysługują uprawnienia określone w rozdziale 5a ustawy. Do umów zobowiązujących do przeniesienia własności towaru na konsumenta, w tym w szczególności umów sprzedaży, umów dostawy oraz umów o dzieło będące towarem, nie stosuje się przepisów księgi trzeciej tytułu XI działu II Ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny. Za sprawą komentowanego przepisu doszło więc do wyłączenia stosowania przepisów k.c. w zakresie rękojmi i gwarancji do „umów zobowiązujących do przeniesienia własności towaru na konsumenta, w tym w szczególności umów sprzedaży, umów dostawy oraz umów o dzieło będące towarem". Konsekwencją powyższych zmian jest swoistego rodzaju rozbicie reżimu rękojmi, tj. odmiennie regulowana jest odpowiedzialność sprzedawcy z tytułu rękojmi w umowach zawieranych w obrocie powszechnym i profesjonalnym (k.c.), a odmiennie w umowach konsumenckich (ustawa o prawach konsumenta) – przy czym, jeśli przedmiotem umowy sprzedaży zawartej przez konsumenta (lub osobę fizyczną, określoną w art. 556^4 k.c.) jest nieruchomość, to zastosowanie znajdują przepisy k.c.[65]

Powstaje więc pytanie: jakie urządzenie IoT będzie zgodne z umową w świetle przepisów Ustawy o prawach konsumenta? Otóż odpowiedzi poszukiwać należy w art. 43b ust. 1 pkt.1, w którym ustawodawca wskazał, że towar będzie zgodny z umową wówczas, gdy w szczególności zgodny z umową pozostaje opis towaru, jego rodzaj, ilość, kompletność i funkcjonalność, a w odniesieniu do towarów z elementami cyfrowymi także kompatybilność, interoperacyjność i dostępność aktualizacji. Dodatkowo, jak wskazano w pkt 2 ust. 1 art. 43b analizowanej ustawy, towar będzie zgodny z umową, jeżeli będzie przydatny do szczególnego celu, do którego jest potrzebny konsumentowi, o którym konsument powiadomił przedsiębiorcę najpóźniej w chwili zawarcia umowy i który przedsiębiorca zaakceptował. Co więcej, w odniesieniu do towarów z elementami cyfrowymi wskazano, że towar będzie zgodny z umową, jeżeli zapewniać będzie taką funkcjonalność i kompatybilność, jakie są typowe dla towaru tego rodzaju i których konsument może rozsądnie oczekiwać, biorąc pod uwagę charakter towaru oraz publiczne zapewnienie złożone przez przedsiębiorcę, jego poprzedników prawnych lub osoby działające w ich imieniu, w szczególności w reklamie lub na etykiecie (art. 43b ust. 2 pkt 2 Ustawy o prawach konsumenta).

Przenosząc powyższe na grunt analizowanego w niniejszym artykule kazusu urządzeń IoT, pozytywnie ocenić trzeba uzupełnienie wymogów zgodności towaru z umową o kryteria funkcjonalności, kompatybilności oraz interoperacyjności[66]. Wraz z upowszechnieniem się urządzeń IoT – także tych wykorzystywanych przez studentów – zupełnie oczywiste zdaje się oczekiwanie, że „ekosystem" tych urządzeń będzie coraz szerszy, a ich „zdolność do wzajemnej interakcji" – coraz większa. Skoro zaś cechą charakterystyczną urządzeń IoT ma być ich wzajemna kompatybilność, to zupełnie racjonalne wydaje się prawne zapewnienie konsumentowi możliwości oczekiwania, że taki towar z elementami cyfrowymi będzie w stanie sprostać również i tym oczekiwaniom – zresztą wpisującym się także w przydatność celu, dla których zazwyczaj używa się towaru tego rodzaju. *In plus* dla ochrony bezpieczeństwa cybernetycznego studenta korzystającego z urządzeń IoT oceniać należy także treść art. 43b ust. 1 pkt 1 Ustawy o prawach konsumenta, który stanowi, że towar jest zgodny z umową, jeżeli zapewnia się dostępność aktualizacji.

Jednocześnie na przedsiębiorcę nakłada się obowiązek poinformowania konsumenta o aktualizacjach, w tym dotyczących zabezpieczeń, niezbędnych do zachowania zgodności towaru cyfrowego z umową. W przypadku gdy konsument nie zainstaluje w rozsądnym czasie aktualizacji dostarczonych przez przedsiębiorcę zgodnie z wymaganiami ust. 3 art. 43k, przedsiębiorca nie będzie ponosi odpowiedzialności za brak zgodności urządzenia IoT z umową wynikający wyłącznie z braku aktualizacji, jeżeli poinformował konsumenta o aktualizacji i konsekwencjach jej niezainstalowania, a także w przypadku, kiedy niezainstalowanie lub niewłaściwa instalacja aktualizacji nie wynikały z błędów w instrukcji instalacji

65 Tamże, s. 179.

66 Tamże, s. 185.

dostarczonej przez przedsiębiorcę. Biorąc pod uwagę fakt, że jednym z warunków zapewnienia bezpieczeństwa cybernetycznego urządzeń IoT jest zapewnienie konsumentowi możliwości korzystania z urządzenia wyposażonego w najnowsze wersje oprogramowania, co pozwala wyeliminować np. ujawnione wcześniej tzw. luki w zabezpieczeniach, tego typu podejście regulacyjne było nie tylko pożądane, co właściwie konieczne dla przyznania konsumentowi ochrony przystającej zarówno do aktualnego postępu technologicznego, jak i płynących z niego zagrożeń. Jednocześnie, co również warte odnotowania, ustawodawca zdecydował się zwiększyć „motywację" konsumenta do aktualizacji oprogramowań urządzeń IoT, a to z uwagi na potencjalną możliwość wyłączenia odpowiedzialności producenta w tym zakresie. To zaś może przyczynić się do zwiększenia bezpieczeństwa całego „ekosystemu" urządzeń IoT, a więc także innych jego użytkowników.

W sytuacji, gdy urządzenie IoT nie zbyło zgodne z umową, konsumentowi przysługiwać będzie roszczenie o jego naprawienie lub wymianę (art. 43d Ustawy o prawach konsumenta). Natomiast oświadczenie o obniżeniu ceny konsument lub o odstąpienie od umowy konsument będzie mógł złożyć dopiero w momencie spełnienia się którejś z przesłanek wskazanych w art. 43 e ust. 1 analizowanej ustawy, tj. jeżeli przedsiębiorca odmówił naprawy lub wymiany z uwagi na nadmierne dla niego koszty czy np. jeżeli brak zgodności towaru z umową występuje nadal, mimo że przedsiębiorca próbował doprowadzić towar do zgodności z umową – co wskazuje na hierarchię środków ochrony prawnej przysługujących w tym względzie konsumentowi. W literaturze przedmiotu wskazuje się, że „w porównaniu z regulacją art. 560 k.c. jest to osłabienie praw konsumenta w zakresie wyboru jednego z czterech uprawnień z rękojmi w celu doprowadzenia do ekwiwalentności świadczeń i ma przede wszystkim na celu utrzymanie umowy oraz realne i należyte jej wykonanie, co służy ochronie interesu sprzedawcy"[67]. Autorka zgadza się jednak z oceną zaprezentowaną przez Ewę Łętowską i Konrada Osajdę, że „w Polsce ciągle brak świadomości, że założeniem europejskiego standardu ochrony konsumenta nie jest odpowiedzialność ujęta w kategoriach utrzymania ekonomicznej równowagi w majątku konsumenta (odszkodowanie), ale zaspokojenia potrzeby będącej celem zawarcia umowy. Sankcja ma więc sprzyjać zaspokojeniu rzeczywistego gospodarczego interesu wierzyciela, a nie tylko zapewniać zachowanie rachunkowego bilansu jego majątku"[68]. Nie ma więc większych powodów ku temu, aby zmiany wprowadzone do przepisów Ustawy o prawach konsumenta w zakresie pewnej hierarchiczności uprawnień przysługujących konsumentowi ocenić jako te osłabiającego jego ochronę prawną.

In plus dla ochrony bezpieczeństwa cybernetycznego studenta korzystającego z urządzeń IoT oceniać należy także treść art. 43b ust. 1 pkt 1 Ustawy o prawach konsumenta, który stanowi, że towar jest zgodny z umową, jeżeli zapewnia się dostępność aktualizacji.

67 A. Kołodziej, *Harmonizacja pełna uprawnień konsumenta w razie niezgodności towaru z umową w dyrektywie 2019/771 o sprzedaży towarów – część II*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2022, t. 128, s. 157.

68 K. Osajda, E. Łętowska, *Wprowadzenie do części ogólnej zobowiązań*, w: *System Prawa Prywatnego*, t. 5. *Prawo zobowiązań. Część ogólna*, red. K. Osajda, Warszawa 2019, s. 64.

5. Przyszłość regulacyjna

Oceniając adekwatność przepisów prawa cywilnego w zakresie ochrony studentów jako użytkowników urządzeń IoT, nie można tracić z pola widzenia faktu, że obowiązujące w Polsce czy w innych krajach UE przepisy dotyczące odpowiedzialności za produkt są implementacją prawa unijnego, a zatem to prawodawca unijny ma istotny wpływ na to, jak kształtować się będzie poziom przedmiotowej ochrony. W momencie rozpoczęcia prac nad przepisami dyrektywy 85/374/EWG z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe, w poszczególnych państwach członkowskich UE istniały już podstawy prawne do dochodzenia odszkodowania od producenta wadliwego towaru. Przybierały one postać odpowiedzialności deliktowej lub kontraktowej, z różnymi modyfikacjami i ograniczeniami. Przyjęcie dyrektywy nie wyrównało jednak w pełni poziomu ochrony poszkodowanych, z uwagi na oczywisty fakt pozostawienia ustawodawcy krajowemu kompetencji do uregulowania w ramach swoich wewnętrznych porządków prawnych różnych regulacji, np. kwestii odpowiedzialności regresowej między współodpowiedzialnymi.

W odniesieniu do kwestii odpowiedzialności za produkty wadliwe ustawodawca unijny zapowiedział pewne zmiany legislacyjne, których nie można pominąć. I tak 28 września 2022 r. opublikowano Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za produkty wadliwe[69], którego celem jest ustanowienie na poziomie UE systemu rekompensat dla osób, które doznały uszczerbku na zdrowiu lub majątku spowodowanego przez wadliwe produkty. Z punktu widzenia użytkowników urządzeń Internetu rzeczy istotne wydaje się dostrzeżenie przez ustawodawcę unijnego konieczności przedefiniowania samego pojęcia produktu[70] i dalsze przyjęcie, że odpowiedzialność na zasadzie ryzyka za produkty wadliwe powinna dotyczyć wszystkich rzeczy ruchomych, w tym również wtedy, gdy są one wbudowane w inne rzeczy ruchome lub na nich zainstalowane[71], a także konieczność zmniejszenia ciężaru dowodu spoczywającego na powodzie – projekt po raz pierwszy zawiera przepisy zobowiązujące producentów do ujawniania dowodów, które mają zmniejszyć ciężar dowodu spoczywający na konsumentach w skomplikowanych sprawach. Z punktu widzenia wykorzystywania urządzeń IoT przez studentów (ale też szerzej: konsumentów) istotne jest także rozszerzenie odpowiedzialności importerów i dystrybutorów w sytuacji, gdy nie będzie można ustalić producenta, to oni będą ponosić odpowiedzialność, a także brak możliwości zwolnienia z odpowiedzialności w sytuacji, gdy nie dostarczono poprawek do oprogramowania. W celu lepszej ochrony powodów, a jednocześnie uzyskania większej pewności, projekt wprowadza okres przedawnienia wynoszący piętnaście lat (zamiast dziesięciu lat) w przypadku przedawnienia szkody na osobie.

W odniesieniu do kwestii odpowiedzialności za produkty wadliwe ustawodawca unijny zapowiedział pewne zmiany legislacyjne, których nie można pominąć.

69 Wniosek o przyjęcie dyrektywy Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za produkty wadliwe, COM(2022)495 final, 2022/0302(COD).

70 W projekcie wskazano, że pojęcie „produkt" oznaczać ma każdą rzecz ruchomą, nawet jeżeli jest ona zintegrowana z inną rzeczą ruchomą lub nieruchomą. „Produkt" obejmuje energię elektryczną, cyfrowe pliki produkcyjne i oprogramowanie.

71 Motyw 6 preambuły projektu.

Oczywiście ostateczna ocena zapowiadanych zmian na poziomie prawa Unii Europejskiej powinna nastąpić dopiero po ich wejściu w życie, jednak na chwilę obecną można stwierdzić, że zapowiadane zmiany w pewnym stopniu zaspokoją potrzeby kreowane przez technologię Internetu rzeczy.

In plus oceniać należy także zmiany, do jakich dojść może na skutek przyjęcia będących obecnie w fazie procedowania przepisów projektu Rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020[72]. Przedmiotowy akt prawny ma na celu wypełnienie luk prawnych, z jakimi obecnie mamy do czynienia w zakresie obowiązkowych wymogów dotyczących bezpieczeństwa produktów z elementami cyfrowymi. W projekcie rozporządzenia znalazły się przepisy dotyczące wprowadzania do obrotu produktów z elementami cyfrowymi w celu zapewnienia cyberbezpieczeństwa takich produktów; zasadnicze wymogi dotyczące projektowania, opracowywania i produkcji produktów z elementami cyfrowymi oraz obowiązki podmiotów gospodarczych w odniesieniu do tych produktów w zakresie cyberbezpieczeństwa; zasadnicze wymogi dotyczące procedur postępowania w przypadku wykrycia podatności wprowadzonych przez producentów w celu zapewnienia cyberbezpieczeństwa produktów z elementami cyfrowymi w całym cyklu życia oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procedur; przepisy dotyczące nadzoru rynku i egzekwowania wyżej wymienionych przepisów i wymogów. W związku z tym, że proponowane rozporządzenie będzie miało zastosowanie do wszystkich produktów z elementami cyfrowymi, których przeznaczenie i racjonalnie przewidywalne wykorzystanie obejmuje bezpośrednie lub pośrednie logiczne lub fizyczne połączenie danych z urządzeniem lub siecią w bezpośredni sposób dotyczyć będzie ono urządzeń IoT, także tych, które są wykorzystywane przez studentów.

Wśród proponowanych zmian na uwagę zasługuje obowiązek wprowadzanie produktów, w odniesieniu do których producenci zapewniają, że zostały one zaprojektowane, opracowane i wyprodukowane zgodnie z zasadniczymi wymaganiami określonymi w sekcji 1 załącznika I do rozporządzenia, co wprost wprowadzi po stronie producentów do obowiązkowej oceny ryzyka ich produktów. Taka ocena ryzyka musi być zawarta w dokumentacji technicznej przy wprowadzaniu produktu na rynek Unii Europejskiej. Na podstawie oceny ryzyka produkty z elementami cyfrowymi m.in.:

- będą dostarczane z bezpieczną konfiguracją domyślną, obejmującą możliwość przywrócenia produktu do stanu pierwotnego;
- zapewniają ochronę przed nieuprawnionym dostępem poprzez odpowiednie mechanizmy kontroli, w tym m.in. systemy uwierzytelniania, zarządzania tożsamością lub systemy zarządzania dostępem;
- będą chronić poufność przechowywanych, przesyłanych lub w inny sposób przetwarzanych danych, osobowych lub innych.

Istotny jest nadto fakt, że także importerzy i dystrybutorzy zaangażowani we wprowadzanie produktów na rynek Unii Europejskiej podlegać będą szczególnym obowiązkom, zwłaszcza w odniesieniu do dokumentacji i oznakowania CE. Co więcej, jeśli na przykład produkt będzie sprzedawany pod nazwą lub znakiem towarowym importera/dystrybutora lub jeśli importer/dystrybutor już dokonał „istotnej modyfikacji" produktu, będą oni podlegać także pełnym obowiązkom producenta.

Oceniając projekt rozporządzenie w obecnym kształcie, można stwierdzić, że przedstawione tam wymagania co do bezpieczeństwa wydają się przyszłościowe i neutralne technologicznie, nieść mogą korzyści dla obu zainteresowanych stron – producentów i konsumentów – jak i przyczynić się do harmonizacja unijnego otoczenia regulacyjnego.

6. Podsumowanie

Doszukując się odpowiedzi na postawione we wstępie do niniejszej pracy pytanie, czy obowiązujące obecnie normy prawna cywilnego zapewniają skuteczne mechanizmy ochrony praw studentów jako użytkowników urządzeń/produktów Internetu rzeczy,

72 Wniosek o przyjęcie rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020, COM(2022)454 final, 2022/0272(COD).

stwierdzić należy, że nie. I jakkolwiek sama możliwość zastosowania przepisów o odpowiedzialności za produkt niebezpieczny także do urządzeń IoT wykorzystywanych przez studentów jest akceptowana, to jednak poszczególne przepisy k.c. kształtujące przedmiotową odpowiedzialność – w kontekście IoT – pozostawią pewne pole do formułowania uwag *de lege ferenda*. Przede wszystkim zwrócić należy uwagę na fakt, że zwiększeniu ochrony studentów korzystających z IoT nie służy uregulowane w art. 449^1 § 2 k.c. rozumienie pojęcia produktu i bliżej problem z oceną urządzeń IoT w świetle art. 45 k.c. Wątpliwości interpretacyjne, jakie w tym zakresie powstają, mogą utrudniać identyfikację podmiotu, który ponosić będzie odpowiedzialność w przypadku, gdy wadą dotknięte będzie oprogramowanie stanowiące część urządzenia IoT[73].

De lege ferenda w kwestii zapewnienia większej adekwatności przepisów o odpowiedzialności za produkt niebezpieczny w kontekście urządzeń IoT wskazać także trzeba na problematyczną interpretację jednej z przesłanek egzoneracyjnych, a konkretniej tej związanej z właściwościami niebezpiecznego produktu, które ujawniły się po wprowadzeniu go do obrotu. Jak słusznie wskazuje Monika Woźniak-Cichuta, to nieostre pojęcie „nie pozwala na jednoznaczną ocenę, kiedy dana zmiana zachodząca w zakresie inteligentnego produktu jest jedynie modyfikacją techniczną, a kiedy jest ona na tyle daleko idąca, że należy ją uznać za ponowne wprowadzenie produktu na rynek"[74], co w konsekwencji rzutuje na zakres odpowiedzialności i dalej ochrony użytkowników tych urządzeń IoT.

Bardziej pozytywnie oceniać należy natomiast przepisy pozakodeksowe, tj. w zwłaszcza przepisy Ustawy o prawach konsumenta w kontekście ochrony prawnej przysługującej studentowi korzystającemu z urządzeń IoT. Jak wskazano wcześniej, już sam fakt dostrzeżenie w przepisach prawa towarów z elementami cyfrowymi stanowi doskonałe preludium do dalszych zmian. I chociaż w szczegółach można by dyskutować o poszczególnych rozwiązaniach prawnych, to jednak nie wyklucza to pozytywnej oceny całości zmian ustawodawczych, jakie w zakresie niezgodności towaru z umową nastąpiły.

Optymistycznie przyjmować należy również zapowiadane zmiany w przepisach prawa Unii Europejskiej, które w bezpośredni sposób kształtować będą sytuację prawną także i studentów korzystających z urządzeń IoT. I choć ostateczny kształt zapowiadanych zmian w chwili obecnej jest nieznany, to już sam fakt, że zajęto się tymi niedostatkami prawnymi, jest dobrym prognostykiem, daje bowiem szansę na stworzenie regulacji na tyle neutralnych technologicznie, że będą one w stanie odpowiadać tak silnie zmieniającej się rzeczywistości.

73 M. Woźniak-Cichuta, *Kto ponosi odpowiedzialność w gospodarce nowych technologii? Bezpieczeństwo produktów w erze sztucznej inteligencji, Internetu Rzeczy i robotyki*, w: *Wyzwania dla prawa konsumenckiego w wymiarze globalnym, regionalnym i lokalnym*, red. M. Namysłowska, K. Podgórski, E. Sługocka-Krupa, Warszawa 2022, s. 135–145.

74 Tamże.

Bibliografia

Banaszczyk Z., *Art. 449[1] [Ryzyko producenta]* w: *Kodeks cywilny. Komentarz*, t. 1, red. K. Pietrzykowski, Warszawa 2020, s. 1641–1654.

Dubis W., *Art. 449[1] [Ryzyko producenta]*, w: *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, Warszawa 2021, s. 1061–1065.

Gnela B., *Odpowiedzialność za produkt (uwagi o polskiej regulacji)*, „Państwo i Prawo" 2009, nr 9, s. 33–47.

IoT w polskiej gospodarce, Raport Grupy Roboczej ds. Internetu Rzeczy przy Ministerstwie Cyfryzacji, Warszawa 2019.

Jagielska M., *Odpowiedzialność za produkt*, „Monitor Prawniczy" 2000, nr 8, s. 495–500.

Kaczmarczyk B., Szczepański P., Dąbrowska M., *Wybrane zagadnienia cyberbezpieczeństwa*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2019, nr 32, s. 201–210.

Koch K., *Przejście uprawnień z tytułu rękojmi na kolejnego nabywcę rzeczy – glosa – III CZP 96/03*, „Monitor Prawniczy" 2007, nr 3, s. 155–168.

Kołodziej A., *Harmonizacja pełna uprawnień konsumenta w razie niezgodności towaru z umową w dyrektywie 2019/771 o sprzedaży towarów – część II*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2022, t. 128, s. 155–176.

Konarski X., *Internet Rzeczy – najważniejsze regulacje prawne w Polsce*, https://www.traple.pl/2020/06/17/internet-rzeczy--najwazniejsze-regulacje-prawne-w-polsce/ (dostęp: 2.10.2020).

Kondek J.M., *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję (uwagi de lege lata i de lege ferenda)*, Warszawa 2021.

Kuźmicka-Sulikowska J., *Okoliczności wyłączające odpowiedzialność za szkodę wyrządzoną przez produkt niebezpieczny*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2015, t. 100, cz. 1, s. 487–505.

Kuźmicka-Sulikowska J., *Pojęcie produktu niebezpiecznego na gruncie przepisów kodeksu cywilnego dotyczących odpowiedzialności za szkodę wyrządzoną przez ten produkt*, w: *Księga dla naszych kolegów. Prace prawnicze poświęcone pamięci doktora Zygmunta Masternaka, doktora Andrzeja Ciska, doktora Marka Zagrosika*, red. J. Mazurkiewicz, Wrocław 2013, s. 245–269.

Marciniak P., *Problem odpowiedzialności za błędy w oprogramowaniu*, „Przegląd Ustawodawstwa Gospodarczego" 2020, nr 10, s. 37–46.

Mikłaszewicz P., *Art. 2 [Objaśnienie terminów]*, w: *Ustawa o prawach konsumenta. Komentarz*, red. P. Mikłaszewicz, Legalis/el. 2022.

Mikłaszewicz P., *Art. 449[3] [Okoliczności zwalniające]*, w: *Kodeks cywilny. Komentarz*, red. K. Osajda, Warszawa 2021, s. 898–900.

Miłostan N., *Szkoła wyższa jako przedsiębiorca w warunkach społecznej gospodarki rynkowej*, w: *Zarządzanie szkołą wyższą*, red. J. Blicharz, A. Chrisidu-Budnik, A. Sus, Wrocław 2014, s. 61–69.

Osajda K., Łętowska E., *Wprowadzenie do części ogólnej zobowiązań*, w: *System Prawa Prywatnego*, t. 5. *Prawo zobowiązań. Część Ogólna*, red. K. Osajda, Warszawa 2019, s. 3–127.

Pawlikowska A., *Przejście uprawnień z tytułu rękojmi, niezgodności towaru konsumpcyjnego z umową i gwarancji na dalszych nabywców – rozważania na podstawie prawa polskiego i wybranych systemów europejskich*, „Transformacje Prawa Prywatnego" 2008, nr 3–4, s. 53–88.

Południak-Gierz K., *Wpływ dyrektyw 2019/770 oraz 2019/771 na poziom ochrony konsumenta w ramach reżimu rękojmi w prawie polskim*, „Prawo w działaniu" 2023, nr 54, s. 172–199.

Rada Unii Europejskiej, Komunikat prasowy: *Cyberbezpieczeństwo urządzeń podłączonych do internetu – Rada przyjmuje konkluzje*, https://www.consilium.europa.eu/pl/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/# (dostęp: 19.09.2021).

Rutkowska E., Trabszys B., *Odpowiedzialność zbywcy za produkt niebezpieczny sprowadzony przez niego do Polski z innego państwa członkowskiego Unii Europejskiej*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2016, nr 8, s. 82–92.

Salamonowicz M., *Art. 425 [Działalność uczelni niestanowiąca działalności gospodarczej]*, w: *Prawo o szkolnictwie wyższym i nauce. Komentarz*, red. A. Jakubowski, Warszawa 2023, s. 1213–1214.

Sprawozdanie Komisji dla Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego, COM(2020)64 final.

Strugała R., *Art. 43[1] [Pojęcie przedsiębiorcy]*, w: *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, Warszawa 2023, s. 104–107.

Tan L., Wang N., *Future Internet: The Internet of Things*, *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, https://ieeexplore.ieee.org/document/5579543 (dostęp: 14.02.2024).

Tomas M., *The Connected Classroom: 9 Examples of IoT in Education*, https://builtin.com/internet-things/iot-education-examples (dostęp: 19.09.2021).

Weber R.H., Weber R., *Internet of Things. Legal Perspective*, Zürich 2010.

Woźniak-Cichuta M., *Kto ponosi odpowiedzialność w gospodarce nowych technologii? Bezpieczeństwo produktów w erze sztucznej inteligencji, Internetu Rzeczy i robotyki*, w: *Wyzwania dla prawa konsumenckiego w wymiarze globalnym, regionalnym i lokalnym*, red. M. Namysłowska, K. Podgórski, E. Sługocka-Krupa, Warszawa 2022, s. 135–145.

Zieliński J.M., *Art. 425 [Działalność uczelni niestanowiąca działalności gospodarczej]*, w: *Prawo o szkolnictwie wyższym i nauce. Komentarz*, red. H. Izdebski, J.M. Zieliński, LEX/el. 2021.