Kwestie prawne związane z IoT

Platforma Przemysłu Przyszłości

MARCIN SIKORSKI

Ekspert współpracujący z Platformą Przemysłu Przyszłości

W opracowaniu zawarto zestawienie najważniejszych informacji prawnych, które należy mieć na uwadze w przypadku kwestii związanych z Internetem Rzeczy IoT (ang. *Internet of Things*). W związku z tym, że prawo (unijne, jak i polskie) nadal borykają się z wieloma zagadnieniami dotyczącymi odpowiedzialności w zakresie dóbr intelektualnych oraz sposobem interpretacji aktów prawnych, poniższe zestawienie stanowi zbiór aktualnej wiedzy i należy mieć na uwadze, że dane te mogą z czasem ulec zmianie lub aktualizacji.

Niniejsze opracowanie ma jedynie charakter informacyjny i nie może stanowić podstawy do jakichkolwiek roszczeń związanych z decyzjami gospodarczymi podejmowanymi w związku z powyższymi treściami. Autor ani Fundacja Platforma Przemysłu Przyszłości nie ponosi odpowiedzialności za konsekwencje decyzji biznesowych podejmowanych przez podmioty korzystające z opracowania, a wszelkie ryzyko związane z takimi decyzjami ponosi podmiot je podejmujący.

1. IoT można rozważać jako rozwiązanie technologiczne, architektoniczne oraz biznesowe:
   1.1. IoT to sieć łącząca przewodowo lub bezprzewodowo urządzenia charakteryzujące się autonomicznym działaniem w zakresie pozyskiwania, udostępniania, przetwarzania danych oraz wchodzenia w interakcje z otoczeniem; z drugiej strony to koncepcja mająca na celu utworzenie inteligentnych systemów kontrolno-pomiarowych, analitycznych oraz układów sterowania,
   1.2. IoT to architektura informatyczna oparta o cztery warstwy:
      – sprzęt,
      – komunikację,
      – oprogramowanie,
      – integrację usług informatycznych,
   1.3. IoT to ekosystem usług biznesowych, wykorzystujących rzeczy, które służą do zbierania oraz przetwarzania danych, wysuwania wniosków i podejmowania decyzji, w celu optymalizacji zasobów oraz środowiska,

2. Jeśli chcemy zasięgnąć prawnej definicji IoT, sugerowana jest rekomendacja Sektora Normalizacji Telekomunikacji ITU (ang. *International Telecommunication Union – Telecommunication Standardisation Sector*) ITU-T Y.2060 (06/2012) (pt. "Przegląd Internetu Rzeczy IoT"), który wyjaśnia koncepcję i zakres IoT, identyfikując podstawowe cechy i wymagania wysokiego poziomu IoT, oraz opisuje model referencyjny IoT; w pkt. 3.2.2 zaprezentowano następujące stwierdzenie: „Globalna infrastruktura społeczeństwa informacyjnego, umożliwia zaawansowane usługi, poprzez łączenie (fizycznych i wirtualnych) rzeczy, w oparciu o istniejące i rozwijające się interoperacyjne technologie informacyjne i komunikacyjne."; w pkt. 3.2.3 zdefiniowano pojęcie rzeczy w kontekście IoT, jako „obiektu fizycznego lub wirtualnego, który można zidentyfikować i zintegrować w sieciach komunikacyjnych".

3. Podstawowe typy bezpieczeństwa, które należy uwzględnić w procesie wytwórczym IoT (omawiane w kolejnych punktach) można ująć w następujących odmianach:
   3.1. **cyberbezpieczeństwo produktu** – zarówno na odpowiednim poziomie i jakości wykonania produktu oraz wyposażenia go w narzędzia i mechanizmy przeciwdziałające cyber niebezpieczeństwom,
   3.2. **bezpieczeństwo fizyczne** – dotyczące wpływu technologii IoT na świat fizyczny (oddziaływanie bezpośrednie i pośrednie), jej zastosowania,
   3.3. **bezpieczeństwo danych** oraz ekosystemu informacji dotyczących otoczenia, a także danych osobowych i technicznych (tj. telemetrycznych).

4. Istnieją formalnie dwa sposoby pociągnięcia do odpowiedzialności (producenta lub dystrybutora) za wady IoT, tj. odpowiedzialność wynikająca z tytułu:
   - sprzedaży rzeczy,
   - wad oprogramowania,

5. Podstawę ochrony praw autorskich i odpowiedzialności za oprogramowanie w prawie polskim stanowi art. 55 prawa autorskiego (Ustawa o prawie autorskim i prawach pokrewnych; Dz.U.2019.0.1231 t.j. – Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych) w brzmieniu: "Jeżeli zamówiony utwór ma usterki, zamawiający może wyznaczyć twórcy odpowiedni termin do ich usunięcia, a po jego bezskutecznym upływie może od umowy odstąpić lub żądać odpowiedniego obniżenia umówionego wynagrodzenia, chyba że usterki są wynikiem okoliczności, za które twórca nie ponosi odpowiedzialności. Twórca zachowuje w każdym razie prawo do otrzymanej części wynagrodzenia, nie wyższej niż 25% wynagrodzenia umownego"

   Przepis ten utworzono w celu ochrony praw autora indywidualnego dzieła; co prawda przepisy te nie zostały opracowane w zakresie programów komputerowych, stosowane są jednak odpowiednio, gdyż program komputerowy traktowany jest zgodnie z polskim prawem jak utwór literacki.

6. Wady fizyczne, które mogą wystąpić w przypadku obiektów Internetu Rzeczy można podzielić na:
   - nieistnienie/brak uzgodnionych modułów,
   - brak ergonomii,
   - niewykonywanie lub nienależyte wykonywanie funkcji,
   - brak bezbłędności wykonywanych funkcji,

- niezdolność programu do pracy w określonym systemie operacyjny/wymaganiach sprzętowych.

6.1. W przypadku oprogramowania art. 55 UoPa (Ustawa o prawie autorskim i prawach pokrewnych; Dz.U.2019.0.1231 t.j. – Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych) stanowi samodzielną podstawę odpowiedzialności autora za oprogramowanie i wyłącza przepisy z tytułu rękojmi.

7. Regulacja i prawo odpowiedzialności za szkodę, która wynika z wady fizycznej oprogramowania – a w efekcie, która ma efekt na otoczenie, w którym program i dane urządzenie działają – zgodnie z art. 55 ust. 1 UoPa jest niedostateczne, co więcej, w przypadku równoczesnego istnienia umowy licencyjnej, jej treść (tzw. umowny zakres odpowiedzialności) narzuca dostawca oprogramowania za pomocą tzw. umowy celofanowej (tzw. *shrink wrap licence*) czyli "rodzaju licencji związanej z udostępnianiem masowym odbiorcom utworów niematerialnych, które zostały utrwalone na nośniku materialnym. Specyfika tej umowy polega na sposobie, w jaki zostają zaakceptowane warunki umowy licencyjnej. Umowa zostaje zawarta w wyniku i w momencie rozerwania foliowej lub plastikowej powłoki, która zabezpiecza nośnik lub poprzez zerwanie naklejki umieszczonej na opakowaniu"

   Drugim sposobem jest zastosowanie postanowień umowy licencji sieciowej/foliowej (ang. *click wrap licence*) w następującym brzmieniu: "istota tej licencji sprowadza się do akceptacji warunków licencji przez kliknięcie w odpowiednią ikonę „akceptuję" lub „zgadzam się". Oświadczenie woli jest składane poprzez kliknięcie myszką na odpowiednią ikonę, która jest umieszczona na interaktywnej stronie internetowej. Warunki umowy licencyjnej przed zawarciem umowy są udostępnione potencjalnemu licencjobiorcy, a ich akceptacja jest równa z zawarciem umowy licencyjnej".

   W praktyce producenci i dostawcy oprogramowania stosują licencjonowanie oprogramowania, co skutkuje brakiem możliwości zastosowania przepisów dotyczących sprzedaży rzeczy (w tym rękojmi); Pamiętajmy – program nie jest rzeczą! Licencja nie przenosi praw do programu! Jest to o tyle ważne, że istotą smart urządzeń jest w głównej mierze oprogramowanie.

8. Ochrona użytkownika produktów obszaru IoT obowiązuje bez względu na to, czy nabywcą jest osoba fizyczna, czy jakikolwiek inny podmiot; preambuła dyrektywy 85/374/EWG ("art. 6.1 w brzmieniu: Produkt jest wadliwy, jeżeli nie zapewnia bezpieczeństwa, jakiego osoba ma prawo oczekiwać, biorąc pod uwagę wszystkie okoliczności, w szczególności: a) wygląd produktu; b) sposób użycia produktu, którego można rozsądnie oczekiwać; c) czasu, w którym produkt został wprowadzony do obrotu."), mimo że odwołuje się do ochrony konsumenta, to co do zasady wskazuje na konieczność ustanowienia niezależnej od winy odpowiedzialności ze strony producenta.

9. W przypadku produktów IoT istotny jest wyrok TSUE (Trybunał Sprawiedliwości Unii Europejskiej) w sprawie C-285/08 (Wyrok TSUE z 4.06.2009 r. w sprawie C-285/08 Moteurs Leroy Somer v. Dalkia France Ace Europe, ECR 2009, s. I-4733.) tzn. wykładnia dyrektywy powinna być dokonywana tak, by w żaden sposób nie ograniczać poszkodowanemu żądania naprawienia szkody rzeczy przeznaczonej do profesjonalnego użytku na podstawie regulacji krajowych (tj. odpowiedzialności za produkt niebezpieczny). Innymi słowy osoba poszkodowana z tytułu używania produktów IoT może dochodzić swoich praw nawet jeśli produkt był przeznaczony do profesjonalnego użytku.

10. Jeśli sprzedaż produktów z obszaru IoT uznamy za cywilnoprawną umowę sprzedaży rzeczy to wówczas odpowiedzialność za wady urządzenia regulować może art. 556 KC Dz.U.2020.0.1740 tj. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny ("art. 556§ 2 – Domniemanie o chwili powstania lub istnienia wady rzeczy. Jeżeli kupującym jest konsument, a wada fizyczna została stwierdzona przed upływem roku od dnia wydania rzeczy sprzedanej, domniemywa się, że wada lub jej przyczyna istniała w chwili przejścia niebezpieczeństwa na kupującego").

11. Dodatkowo przyjmując, że zakup urządzenia z obszaru Internetu Rzeczy służy wykorzystaniu funkcjonalności objętych specyfikacją, to producent urządzeń ponosi odpowiedzialność kontraktową wynikającą z braków oraz wadliwego/nieprawidłowego działania urządzenia oraz w równym stopniu ponosi odpowiedzialność za szkody spowodowane tymi wadami funkcjonalności; w tym przypadku pod uwagę bierze się art. 354 KC ("Art. 354. Dłużnik powinien wykonać zobowiązanie zgodnie z jego treścią i w sposób odpowiadający jego

celowi społeczno-gospodarczemu oraz zasadom współżycia społecznego, a jeżeli istnieją w tym zakresie ustalone zwyczaje – także w sposób odpowiadający tym zwyczajom.") oraz art. 471 KC ("Art. 471. Odpowiedzialność dłużnika za niewykonanie lub nienależyte wykonanie zobowiązania – odpowiedzialność *ex contractu*. Dłużnik obowiązany jest do naprawienia szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które dłużnik odpowiedzialności nie ponosi."); Dz.U.2020.0.1740 t.j. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny.

12. Odpowiedzialność deliktowa opisana jest w art. 415 KC ("Art. 415. Odpowiedzialność *ex delicto* – zasada winy. Kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia."); istotne jest to, że w żadnym wypadku nie jest powiązane to z zawartym kontraktem, ale oparte jest o umyślną winę, bądź nieumyślne działanie sprawcy.

13. Najlepszym i najbardziej zarazem aktualnym źródłem wiedzy dotyczącej kwestii związanych z prawem i bezpieczeństwem jest tzw. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).

    Możemy przytoczyć tu punkt 20 w/w dokumentu, który mówi wprost: "ENISA powinna rozwijać i utrzymywać wysoki poziom wiedzy fachowej oraz pełnić rolę punktu odniesienia służącego budowie zaufania i wiarygodności na jednolitym rynku z racji swojej niezależności, jakości oferowanego doradztwa, jakości rozpowszechnianych informacji, przejrzystości jej procedur, przejrzystości jej metod działania, a także staranności w realizacji swoich zadań".

    Innymi słowy, jeśli zależy nam na najświeższym dokumencie prawnym, który może wspomóc nas w omawianiu i zrozumieniu kwestii związanych z bezpieczeństwem IoT (certyfikacje, wymogi prawne, procedury, zasady organizacji pracy etc.) to właśnie ten dokument powinien rozwiać wątpliwości (cytując punkt 31: "ENISA powinna gromadzić i analizować dobrowolnie udostępniane raporty krajowe przekazywane przez zespoły CSIRT i międzyinstytucjonalny zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii ustanowiony porozumieniem między Parlamentem Europejskim, Radą Europejską, Radą Unii Europejskiej, Komisją Europejską, Trybunałem Sprawiedliwości Unii Europejskiej, Europejskim Bankiem Centralnym, Europejskim Trybunałem Obrachunkowym, Europejską Służbą Działań Zewnętrznych, Europejskim Komitetem Ekonomiczno-Społecznym, Europejskim Komitetem Regionów i Europejskim Bankiem Inwestycyjnym w sprawie organizacji i funkcjonowania zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE)".

14. Akt o cyberbezpieczeństwie (ang. *The EU Cybersecurity Act*) jako rozporządzenie nie posiada widocznych wskazań do obowiązkowego certyfikowania poszczególnych kategorii rozwiązań; Jest to dobrowolny akt, który jednak w nadchodzących latach (2021-2022) może przekształcić się w wymóg; Wszystko zależne jest od kierunku dyskusji, która odbędzie się z chwilą, gdy miną dwa lata od wejścia w życie aktu o cyberbezpieczeństwie.

15. W kwestii wymogów prawnych narzuconych na twórcę oprogramowania/osprzętu IoT Unia Europejska określa tzw. poziom uzasadnienia zaufania; Jak można przeczytać w punkcie 86 ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 – Akt o cyberbezpieczeństwie): "Poziom uzasadnienia zaufania europejskiego programu certyfikacji stanowi podstawę dla pewności, że produkt ICT, usługa ICT lub proces ICT spełniają wymogi bezpieczeństwa danego europejskiego programu certyfikacji cyberbezpieczeństwa. (...) Każdy europejski certyfikat cyberbezpieczeństwa mógłby wskazywać jeden z poziomów uzasadnienia zaufania: „podstawowy", „istotny" lub „wysoki", natomiast unijne deklaracje zgodności mogłoby jedynie wskazywać poziom uzasadnienia zaufania „podstawowy". Poziomy uzasadnienia zaufania zapewniłyby odpowiadającą im rygorystyczność i wnikliwość oceny produktu ICT, usługi ICT lub procesu ICT oraz byłyby określane przez odesłanie do powiązanych z nimi specyfikacji technicznych, norm i procedur, w tym kontroli technicznych, których celem jest zapobieganie incydentom lub łagodzenie ich skutków".

16. W zakresie kwestii produktów niebezpiecznych, które mogą zagrozić konsumentowi – posłużyć się można dyrektywą 85/374/EWG (Dyrektywa Rady 85/374/EWG z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących odpowiedzialności za produkty wadliwe), która definiuje nie tylko odpowiedzialność producenta, ale również to czym jest szkoda (m.in. "Artykuł 9 do celów art. 1 definiuje – „szkoda" oznacza: a) szkodę spowodowaną przez śmierć lub przez uszkodzenia ciała; b) uszkodzenie lub zniszczenie każdej rzeczy innej niż produkt wadliwy o wartości powyżej 500 ECU, pod warunkiem, że rzecz ta: i) jest zwykle przeznaczona do prywatnego użytku lub konsumpcji; i ii) była używana przez osobę poszkodowaną głównie do jej prywatnego użytku lub konsumpcji.")

    Oczywiście w Polskim prawie (tj. prawie krajowym) ma to odniesienie do art 491 KC ("Art. 449[1]. Odpowiedzialność za produkt niebezpieczny – ryzyko producenta. § 1. Kto wytwarza w zakresie swojej działalności gospodarczej (producent) produkt niebezpieczny, odpowiada za szkodę wyrządzoną komukolwiek przez ten produkt. § 2. Przez produkt rozumie się rzecz ruchomą, choćby została ona połączona z inną rzeczą. Za produkt uważa się także zwierzęta i energię elektryczną. § 3. Niebezpieczny jest produkt niezapewniający bezpieczeństwa, jakiego można oczekiwać, uwzględniając normalne użycie produktu. O tym, czy produkt jest bezpieczny, decydują okoliczności z chwili wprowadzenia go do obrotu, a zwłaszcza sposób zaprezentowania go na rynku oraz podane konsumentowi informacje o właściwościach produktu. Produkt nie może być uznany za nie zapewniający bezpieczeństwa tylko dlatego, że później wprowadzono do obrotu podobny produkt ulepszony."; Dz.U.2020.0.1740 t.j. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny) – przy czym przez produkt rozumie się w tym przypadku zarówno rzecz ruchomą, nawet jeśli została połączona z inną rzeczą, jak również zwierzę czy energię elektryczną.

17. Przepisy określają więc, że wszyscy twórcy produktów obszaru Internetu Rzeczy odpowiadają solidarnie za wprowadzenie produktu do obrotu tj. producenci, twórcy, importerzy, dostawcy etc., a ustalenie odpowiedzialności oprzeć można na domniemaniu faktycznym, które jest oparte o oświadczenie; Co więcej wykazanie przez poszkodowanego zaniedbań z tytułu wady wynikającej z przyjętej technologii i braku nadzoru oraz weryfikacji jakości jest wystarczającym działaniem, by określić winę po stronie producenta.

    Jako przykład może posłużyć wyrok sądowy III CSK 174/06 w sprawie z powództwa N.T. przeciwko A.G. i in., o odszkodowanie i rentę z dnia 27 lipca 2005 r., w brzmieniu: "Zarysowała się wyraźnie tendencja do obiektywizacji kryterium winy przy odpowiedzialności za szkodę spowodowaną przez produkt niebezpieczny oraz wykładni art. 415 KC przy uwzględnieniu zasady ochrony konsumenta. W literaturze przyjmowano, że dla wykazania winy na tle odpowiedzialności deliktowej za produkt niebezpieczny wystarczające jest wykazanie przez poszkodowanego zaniedbań typu organizacyjnego u przedsiębiorcy (producenta). Z kolei z uwagi na fakt, że sposób organizacji przedsiębiorstwa (procesu technologicznego, sposobu kontroli jakości, czy magazynowania i transportu wyrobów) nie jest znany poszkodowanemu przyjmowano, że należy dopuścić skuteczność dowodu prima facie w odniesieniu do wnioskowania co do istnienia winy organizacyjnej, w oparciu o stwierdzony rodzaj szkodliwości wyrobu.".

18. Co do zasady w kwestii odpowiedzialności za szkody wynikające i wykryte w obszarze produktów Internetu Rzeczy stosuje się ogólne zasady, tj. odpowiedzialność za niewykonanie (lub nienależyte wykonanie) umowy oraz odpowiedzialność z tytułu rękojmi za wady i gwarancji jakości.

    Dodatkowo istotne są przepisy dotyczące odpowiedzialności za produkty niebezpieczne (ogólne przepisy dotyczące odpowiedzialności za produkt niebezpieczny).

    Co do wad uznać możemy szkody wynikające z wad urządzenia, danych usług dostępnych, danych przetwarzanych przez aplikację, autonomiczne decyzje podejmowane na podstawie rzeczywistych i odpowiednio zebranych danych.

19. Regulacje prawne o cyberbezpieczeństwie określa również ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (KSC). Jest to wdrożenie dyrektyw unijnej w sprawie środków na rzecz wysokiego poziomu bezpieczeństwa, tak sieci jak i systemów informatycznych ulokowanych na terenie Unii Europejskiej.

Ważna uwaga! Ustawa ta nie odnosi się wprost do Internetu Rzeczy, niemniej podmioty, które korzystają z takich rozwiązań (produkcja, świadczenie usług) mogą być jednocześnie operatorami usług kluczowych, jak i dostawcami usług cyfrowych.

Za niedostosowanie się do obowiązków opisanych i określonych w ustawie o krajowym systemie cyberbezpieczeństwa mogą grozić kary finansowe; Do tych obowiązków należą m.in.:

- przygotowanie i zorganizowanie narzędzi niezbędnych do zapobiegania i minimalizowania wpływu incydentów na świadczoną usługę cyfrową (zachowanie ciągłości świadczenia dotychczasowej usługi),
- regularna kontrola skierowania na wczesne wykrywanie, reagowanie, analizowanie oraz priorytetowanie zachodzących incydentów,
- natychmiastowe zgłaszanie wykrytych incydentów do właściwych podmiotów (nie dłużej jak 24 godziny od momentu wystąpienia).

20. W ramach europejskich działań, których efekty mogą wpłynąć na działanie polskich przedsiębiorców, warto zaznajomić się z dokumentem „Cybersecurity Certification: EUCC Candidate Scheme", który powstał na podstawie Common Criteria, wspólnej i ogólnej metodologii oceny bezpieczeństwa informatycznego, oraz norm ISO/IEC 15408 (ISO/IEC 15408–1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model), która ustanawia ogólne koncepcje i zasady oceny bezpieczeństwa IT oraz określa ogólny model oceny podawany przez różne części ISO/IEC 15408–…, który w całości ma służyć jako podstawa oceny bezpieczeństwa właściwości produktów IT) i ISO/IEC 18045, a który to dokument również uszczegóławia kwestie oraz wątpliwości związane z tematyką cyberbezpieczeństwa Internetu Rzeczy.

    W przypadku dostawców usług chmurowych programem, który uspójnia zagadnienie jest program CSPCert (ang. *Certified Safety Professional Education Requirements and Career*).

21. Skoro poruszamy już kwestię dotyczącą bezpieczeństwa, istotne jest przywołanie artykułu 269 KK ("Art. 269. Niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych."), który jasno wskazuje, że niedostateczne zabezpieczenie produktów obszaru Internetu Rzeczy może skutkować karami wynikającymi z „sabotażu" i działania przeciw krajowi.

22. Istotne jest to, że w zakresie dóbr intelektualnych w literaturze dominuje pogląd, że oprogramowanie komputerowe nie jest „produktem" w rozumieniu przepisów o odpowiedzialności za produkt niebezpieczny (Art 45 KC, "Art. 45. Definicja rzeczy. Rzeczami w rozumieniu niniejszego kodeksu są tylko przedmioty materialne"; Dz.U.2020.0.1740 t.j. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny).

23. Należy także pamiętać, że zgodnie z wyrokiem TSUE z dnia 4 czerwca 2009 r. w sprawie C-285/08 (Moteurs Leroy Somer v. Dalkia France i Ace Europe, ECR 2009, s. I-4733) przepisy dyrektywy 85/374/EWG nie mogą być interpretowane zawężająco, tj. prawo krajowe może regulować inne przypadki odpowiedzialności za produkt niebezpieczny.

24. Warto również mieć na uwadze kwestie związane ze zgodnością towaru, czyli z tzw. „wbudowaną treścią cyfrową". W tym przypadku zastosowanie mają poniższe regulacje unijne:
    - dyrektywa 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 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów sprzedaży towarów, zmieniającej rozporządzenie (UE) 2017/2394 (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z dnia 12 grudnia 2017 r. w sprawie współpracy między organami

krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004,

- dyrektywa Parlamentu Europejskiego i Rady 2009/22/WE z dnia 23 kwietnia 2009 r. w sprawie nakazów zaprzestania szkodliwych praktyk w celu ochrony interesów konsumentów (Wersja skodyfikowana) i uchylająca dyrektywę 1999/44/WE

oraz

- dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych.

Unia Europejska rozważa, aby dyrektywy te obejmowały swym działaniem towary niematerialne (w tym oprogramowanie).

25. Kwestie dotyczące standaryzacji wyznacza europejski dokument ETSI EN 303 645 CYBER – *Cyber Security for Consumer Internet of Things: Baseline Requirements*, który określa normy jakie musi spełniać produkt konsumencki z obszaru Internetu Rzeczy, aby można było określić jego poziom i stopień przystosowania w kwestiach cyberbezpieczeństwa.

26. Istotne jest ustalenie, że certyfikacja sama w sobie nie może gwarantować 100% skutecznego bezpieczeństwa od wszystkich znanych rodzajów ataków; Certyfikacja poświadcza jednak, że sprzedawane urządzenie obszaru Internetu Rzeczy przygotowane jest w sposób staranny i należyty co oznacza, że realizuje zaprojektowane funkcjonalności i robi to zgodnie z istniejącymi, znanymi i aktualnymi modelami zagrożeń; Im bardziej produkt będzie rozmijać się z liczbą zaplanowanych funkcjonalności (tj. możliwe będzie wprowadzenie dodatkowych elementów), tym poziom zaufania będzie znacząco mniejszy.

27. Wszystkie wymienione akty prawne i dokumenty mają za zadanie określić i wypracować pewne modele, wymagania, zachowania oraz nawyki, które mają zagwarantować bezpieczeństwo zarówno producentowi jak i konsumentowi.

Kwestia AI a prawo (informacje w oparciu o EU JURI Artificial Intelligence and Civil Liability Legal Affairs)

Poniższe informacje stanowią punkt wyjścia do dyskusji na temat sztucznej inteligencji AI (ang. *Artificial Intelligence*) i jej prawnych konsekwencji. Przedstawione informacje stanowią raczej wytyczne niż wskazania konkretnych rozwiązań. Jednocześnie przedstawione fakty obrazują stopień skomplikowania i wieloaspektowość poruszanej w opracowaniu tematyki:

1. Ogólna definicja sztucznej inteligencji AI jest niemożliwa do utworzenia:
   - z jednej strony to „słowo-wytrych", które stało się modne i opisywany jest nim każdy podmiot, który spełnia minimalne wymagania „myślącego" systemu,
   - w praktyce jest to ciągle ewoluujące określenie, które obejmuje rozległy typ urządzeń, aplikacji i logiki,
   - społeczeństwo postrzega i rozumie AI jako „tworzenie i obdarzanie maszyn oraz programów cechami zbliżonymi do ludzkich",
   - w praktyce większość AI ma charakter „lekkiego AI", tj. wykonującego bardzo precyzyjne, wąskie, określone zadanie niezwiązane z cechami ludzkimi,
   - AI jest ciągle ewoluującym bytem, który przenika do najróżniejszych dziedzin życia ludzkiego,
   - co więcej, to co uznane zostaje za „myślące", wraz z rozwojem technologii i z upływem czasu uważane jest jednak za niedoskonałe i ta etykietka zostaje mu odebrana,
   - w związku z tym nawet prawnicy mają trudność w określeniu jasnych i przejrzystych norm prawnych dotyczących tego zagadnienia, które mogłyby być spójne tak w czasie, jak i w rozumieniu,
   - oznacza to, że w zależności od typu AI pojawiają się nowe wątpliwości społeczne, prawne, etyczne i ekonomiczne.

2. Wszystkie aplikacje i maszyny używające AI są produktem. Nie ma technicznego, filozoficznego czy prawnego względu, który uzasadniałby uznanie maszyn za „moralnie aktywnych" agentów (byty) pomimo posiadania

przez nie wewnętrznych charakterystyk (autonomiczne zachowanie, zdolność uczenia się i rozwoju w czasie, zdolność do realizacji określonego celu niezależnie od nadzoru i kontroli człowieka itp.).

3. Zgodnie z unijnym prawem nie istnieje pojęcie luki wynikającej z odpowiedzialności. Zawsze można zidentyfikować człowieka, który mógłby być odpowiedzialny za wyrządzoną szkodę powstałą w wyniku produkcji, obsługi i użytkowania. Oznacza to, że nie można klasie aplikacji AI przypisać osobowości prawnej i uznać ją za „czarnoskrzynkowe niewiadome".

4. W uznaniu do aktualnie istniejącego prawa, bezpieczeństwo produktu i odpowiedzialność za produkt są spójnym i gwarantowanym prawem konsumenckim. Oznacza to, że produkt można uznać za bezpieczny i wprowadzić do obrotu w momencie, gdy prawo identyfikuje kto ponosi odpowiedzialność za następstwa szkody wyrządzonej przez sam produkt. Równoważąc tym samym potrzebę zapewnienia ochrony użytkowników i umożliwienie dystrybucji produktów w celach zarobkowych.

5. Dyrektywa w sprawie odpowiedzialności za produkt PLD (ang. *Product Liability Directive*) ustanawia horyzontalny, neutralny technologicznie system odpowiedzialności, w przypadku których producent ponosi bezwzględną odpowiedzialność za szkody spowodowane wadą swojego produktu, przy czym ofiara jest zobowiązana do udowodnienia poniesionej szkody, wady i przyczyny powiązania między nimi bez obowiązku ujawniania odpowiednich informacji na temat swojej domeny.

6. Rozróżnienie między aplikacjami i urządzeniami opartymi na AI (niskiego i wysokiego ryzyka) jest niemożliwe do określenia z powodu braku istotnych statystycznie danych dotyczących wielkości i częstotliwości spodziewanych szkód.

7. Podobne znaczenie ma fakt, że wybór przestrzeni zastosowania technologii (przestrzeń prywatna lub publiczna) nie ma pierwszorzędnego znaczenia przy określaniu poziomu ryzyka jakie powoduje użycie AI.

8. UE nie będzie próbować regulować „technologii opartych na sztucznej inteligencji" w sposób jednolity, nawet z szacunkiem do odpowiedzialności. Ze względu na to, że zastosowanie szerokich pojęć, takich jak „systemy AI" może powodować komplikacje (tzw. rozmyta odpowiedzialność).

9. Strona, która ma zostać pociągnięta do odpowiedzialności, powinna być tą, która jest w najlepszej pozycji do identyfikacji, kontroli i zarządzania ryzykiem, niezależnie od okoliczności dotyczących winy.

10. To, która spośród możliwych stron odpowiedzialnych (producent, właściciel, użytkownik, operator) powinna być pociągnięta do odpowiedzialności prawnej, będzie oceniane w odniesieniu do specyfiki klasy zastosowań, które ustawodawca zamierza regulować. Tylko jeden podmiot powinien być *prima facie* odpowiedzialny wobec zaistniałej szkody.

11. Podejście do zarządzania ryzykiem poprzez tzw. stowarzyszenia zarządzania ryzykiem (ang. *Risk Management Association*), jako specyficzna w zakresie technologii metoda stosowana do celów zarządzania ryzykiem w obszarze zaawansowanych technologii, jest alternatywą w odniesieniu do neutralnego technologicznie podejścia związanego z regulowaniem odpowiedzialności cywilnej technologii AI.

12. Zasady odpowiedzialności powinny obciążać podmiot, który jest w stanie najlepiej:
    - zidentyfikować ryzyko,
    - kontrolować ryzyko,
    - zarządzać nim, zapewniając ofierze łatwe, szybkie i pełne odszkodowanie, niezależnie od okoliczności dotyczących winy.

13. Strona, która ma zostać pociągnięta do odpowiedzialności, różni się w zależności od rodzaju technologii rozpatrywanych aplikacji, biorąc pod uwagę ich złożoność i działanie, a także w zależności od domeny np. operator dronów, producent lub właściciel autonomicznych pojazdów etc. Mechanizm ten jest zgodny z niektórymi już uchwalonymi przepisami UE, takimi jak dyrektywy konsumenckie, które zapewniają konsumentom natychmiastowe

zadośćuczynienie poprzez obciążenie sprzedawcy, prima facie, i tym samym unikając skomplikowanych sporów.

14. Gdy wiele stron przyczynia się do świadczenia usługi opartej na sztucznej inteligencji, utrudniając określenie wprost ich roli i zidentyfikowanie optymalnych winnych można wówczas rozważyć tzw. fikcyjną „osobę elektroniczną" jeżeli żadna inna opcja nie jest preferowana.

15. Zgodnie z RMA odpowiedzialność jest raczej rygorystyczna (jeśli nie bezwzględna), a nie oparta na winie. Rzeczywiście, *ex ante*, bezpieczeństwo powinno zostać oddzielone od odszkodowania *ex post*, pozostawiając inne mechanizmy (takie jak przepisy bezpieczeństwa) zachęcające do pożądanych standardów postępowania. Ramy bezpieczeństwa produktów będą dalej wykorzystywane poprzez przyjęcie szczegółowych regulacji i standardów technicznych w celu lepszego dostosowania do pojawiających się technologii.

16. Osoba odpowiedzialna niekoniecznie poniesie koszty ekonomiczne wypadku. Przez mechanizmy ubezpieczeniowe i cenowe może przenosić koszt na wszystkich użytkowników danej technologii (efekt kumulacji i rozprzestrzeniania się).

17. Osobie odpowiedzialnej należy przyznać prawo do regresu innych agentów (tzw. bytów), którzy mogliby przyczynić się do wyrządzenia szkody. Gdy wiele stron współtworzy złożone aplikacje i usługi oparte na sztucznej inteligencji, a określenie optymalnego miejsca rozpoczęcia sporu jest trudne, szybkie odszkodowanie można alternatywnie osiągnąć poprzez nadanie osobowości prawnej określonej grupie zgłoszeń, gdzie procentowo wszystkie zaangażowane strony poniosłyby koszty odpowiedzialności zgodnie z ich udziałem w projekcie.

Regulacje prawne i ustawy w Polskim prawie:

- Ustawa z dnia 5 lipca 2018 r. (Dz.U. 2018 poz. 1560) o Krajowym Systemie Cyberbezpieczeństwa KSC (implementacja dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych, tzw. Dyrektywa NIS)
- Dz.U. 2016 poz. 542 – Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku,
- Akt o cyberbezpieczeństwie z dnia 7 czerwca 2019 r. tj. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 – Akt o cyberbezpieczeństwie),
- Ustawa z 06 czerwca 1997 r. Kodeks karny (Dz. U. 1997 Nr 88 poz. 553 z późn. zm.),
- Dyrektywa 85/374/EWG z dnia 25 lipca 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.),
- Dyrektywy Rady ws. ochrony prawnej programów komputerowych 91/250/EWG z dnia 14.05.1991 r.,
- Ustawa z 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 1964 nr 16 poz. 93 z późn. zm.),
- Ustawa z 04 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24 poz. 83 z późn. zm.)

Dokumentami prawnymi, które na arenie międzynarodowej stosuje się do obiektów Internetu Rzeczy są m.in.:

- **UE** – GDPR, ETSI EN 303 645 CYBER – Cyber Security for Consumer Internet of Things:Baseline Requirements, Article 83: General conditions for imposing administrative fines, Data Protection by Design and by Default (679/2016), EU DPR-2012: European Data Protection Regulation, EU Directive-2013/40 about Cybercrime, EU NIS Directive-2016, EU Directive 2014/53, EU Connected Communities Initiative, Product Liability Directive,

- **USA** – Federal Trade Commission Act, które ma przeciwdziałać nieuczciwym praktykom pokroju fałszywej reklamy, Cyber Security Information Sharing Act, który jest odpowiednikiem RODO czy Children's Online Privacy Protection Act, które chroni najmłodszych,
- **UK** – Digital Economy Act, Data Protection Act 2018, Consumer Rights Act, Digital Economy Act,
- **Australia** – Privacy Act 1988 and Notifiable Data Breaches Acts,
- **Singapur** – Application of English Law Act, Energy Conservation Act, Health Products Act

Literatura uzupełniająca:

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

Hoffmann R., Stanik J., Napiórkowski J. (2017). Modele wykrywania podatności oprogramowania w ujęciu dynamiki systemowej, Roczniki KAE, z 45/2017

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

Radoniewicz F. (2016). Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym (271 i nast.), Wolters Kluwer

Ruchała P., Sikorski M. Kodeks cywilny. Tom II, M. Gutowski (red.), 2019 r. wydanie 2, Legalis