GOŹDZIASZEK
PRAWO INTERNETU I TECHNOLOGII

Perspektywy Internetu Rzeczy

RAPORT PRAWNY

Za rozwojem przedsięwzięć związanych z Internetem Rzeczy przemawia szereg argumentów. Po pierwsze, jest to biznes jednoznacznie kojarzony z innowacyjnością i nowoczesnością. Po drugie, opiera się na „wkładzie" dostarczanym przez klientów. To oni dostarczają danych do działania systemów, producent nie musi ich tworzyć, a jedynie je przetwarza. Po trzecie, są relatywnie mało kapitałochłonne.

Internet Rzeczy zacznie jednak odgrywać istotniejszą rolę dopiero w sytuacji działania na dużą skalę, co spowoduje, że problemy prawne zaistnieją bez okresu przejściowego na wypracowanie najlepszym rozwiązań z punktu widzenia prawa. W relacjach z użytkownikami najważniejsze problemy prawne dotyczą kwestii danych osobowych, w szczególności wrażliwych danych osobowych. Z kolei w kontekście konkurencji rynkowej ważnym zagadnieniem prawnym jest możliwość współpracy pomiędzy producentami sprzętu i oprogramowania.

W niniejszej analizie przedstawiono jedynie generalne kwestie. Są one z zasady miarodajne dla każdego rozwiązania z zakresu Internetu Rzeczy. Zarysowano zatem **otoczenie prawne dla różnego rodzaju aplikacji i urządzeń** związanych z Internetem Rzeczy. Dla pełnej analizy prawnej należałoby również odwołać się do regulacji sektorowych, przykładowo w przypadku wykorzystywania Internetu Rzeczy w energetyce należałoby sięgnąć do regulacji szczegółowo regulujących rynek energii, a w przypadku rozwiązań zdrowotnych do przepisów dotyczących funkcjonowania rynku ochrony zdrowia.

SPIS TREŚCI

1. Zakres informacji podlegających ochronie jako dane osobowe

Internet Rzeczy bazuje na różnych informacjach związanych z człowiekiem, w tym na jego zainteresowaniach, „parametrach" organizmu i przyzwyczajeniach. Informacje te, jako dane osobowe, mogą podlegać ochronie przewidzianej przez ustawę o ochronie danych osobowych. Wprawdzie sednem Internetu Rzeczy są przedmioty, a nie ludzie, to jednak przedmioty te służą ludziom, dlatego w ostatecznym rozrachunku dane osobowe dotyczące poszczególnych ludzi są kluczowe.

W pierwszej kolejności należy zatem określić kiedy informacje są w świetle prawa „danymi osobowymi". Zgodnie z art. 6 ust. 1 tej ustawy dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przywołana definicja danych osobowych jest zatem szeroka, a jej kluczowym elementem jest identyfikacja osoby. Najczęściej konieczność logowania w aplikacji komputerowej będzie równoznaczna ze zidentyfikowaniem. Zwrócić należy uwagę, że zakres danych osobowych obejmuje nie tylko informacje dotyczące zidentyfikowanej, ale też **możliwej** do zidentyfikowania. Przepisy doprecyzowują, że osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio. Ustawa o ochronie danych osobowych przykładowo wymienia takie metody ustalenia tożsamości, wskazując na powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej **cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne** (tak art. 6 ust. 2 ustawy o ochronie danych osobowych). Jednak informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań (tak art. 6 ust. 3 ustawy o ochronie danych osobowych). Reguła ta stanowi zatem swoisty bufor bezpieczeństwa. Dzięki niej kwestia możliwych do wykorzystania narzędzi technicznych służących do ustalenia tożsamości, w kontekście biznesowej opłacalności, nabiera znaczenia prawnego.

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Aby dane przedsięwzięcie podlegało reżimowi ustawy o ochronie danych

dr Łukasz Goździaszek
Adiunkt w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Adwokat. Specjalizuje się w Prawie Internetu i Technologii. Autor książek „Prawo blogosfery" i „Elektroniczne postępowanie upominawcze".

BLOG:
www.prawo-internetu.pl

KONTAKT:
adwokat@gozdziaszek.pl

osobowych konieczne jest również spełnienie przesłanek o charakterze **podmiotowym**. W przeciwnym przypadku podmiot może w ogóle być nie związany przepisami polskiej ustawy. Kluczowymi kryteriami oceny w tym zakresie jest:

1. albo siedziba podmiotu,
2. albo umiejscowienie środków technicznych, za pomocą których następuje przetwarzanie danych (chyba że takie środki techniczne służą wyłącznie do przekazywania danych).

Ustawę o ochronie danych osobowych **stosuje się** m.in.:	Ustawy o ochronie danych osobowych **NIE stosuje się** jednak m.in.:
do osób i podmiotów przetwarzających dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych, które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej (tak art. 3 ust. 2 pkt 2 ustawy o ochronie danych osobowych).	do podmiotów mających siedzibę w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych (tak art. 3a ust. 1 pkt 2 ustawy o ochronie danych osobowych).

W odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5 ustawy o ochronie danych osobowych, czyli dotyczące zabezpieczenia danych osobowych (tak art. 2 ust. 3 ustawy o ochronie danych osobowych). Wydaje się jednak, że takie ograniczenia zakresu zastosowania polskiej ustawy rzadko będzie występowało przy rozwiązaniach z zakresu Internetu Rzeczy.

Zbiór danych to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Przetwarzania danych zazwyczaj wiąże się z **tworzeniem zbiorów danych** osobowych, które z zasady wymagają rejestracji u Generalnego Inspektora Ochrony Danych Osobowych (dalej: „GIODO"). Jednak powołanie w firmie Administratora Bezpieczeństwa Informacji (tzw. „ABI") może ten obowiązek wyeliminować. Wyjątek dotyczy wrażliwych danych osobowych, które zawsze wymagają rejestracji. Szerzej o danych wrażliwych w dalszej części niniejszego opracowania.

Z punktu widzenia prawa **najlepszym rozwiązaniem** byłoby, aby Internet Rzeczy posługiwał się informacjami innymi niż dane osobowe, ponieważ nie byłoby potrzeby przestrzegania rygorów przywołanej ustawy o ochronie danych osobowych. Jednak wtedy Internet Rzeczy utraciłby główny cel swojego funkcjonowania jakim jest wspieranie konkretnych ludzi poprzez wykorzystywanie rozwiązań technicznych. Można jednak wyobrazić sobie takie rozwiązania, w których urządzenia są powiązane nie z konkretnymi osobami, lecz innymi urządzeniami, przykładowo kiedy jedno urządzenie uruchamia się w reakcji na znalezienie się w obszarze oddziaływania drugiego urządzenia, a przy tym żadna z czynności nie byłaby wiązana z danymi osobowymi. Istnieje też możliwość, że dane osobowe nie byłyby przesyłane z urządzenia (nie opuszczałyby urządzenia będącego w wyłącznej dyspozycji użytkownika), a przez to nie były przetwarzane przez podmiot zewnętrzny, ale takie rozwiązanie nie byłoby realizacją koncepcji Internetu Rzeczy, ponieważ nie byłoby w nim Internetu. Jak wynika z powyższego, Internet Rzeczy zazwyczaj będzie musiał uwzględniać wymogi prawne związane z ochroną danych osobowych, chyba że urządzenia nie byłyby wiązane z konkretnymi (zidentyfikowanymi) ludźmi. Regułą jednak przy projektowaniu rozwiązań z zakresu Internetu Rzeczy powinno być liczenie się z wymogami prawnymi służącymi ochronie danych osobowych.

2. Podstawy prawne przetwarzania danych osobowych

Restrykcyjny charakter ochrony danych osobowych nie polega jedynie na dbaniu o zapewnienie bezpieczeństwa danych i ewentualnej rejestracji zbiorów danych osobowych, lecz na ściśle określonych podstawach przetwarzania danych, czyli sytuacjach w których przetwarzanie jest w ogóle dopuszczalne przez prawo. Jeśli rozwiązania z zakresu Internetu Rzeczy mają korzystać z danych osobowych, to muszą bazować przynajmniej na jednej z poniżej wskazanych podstaw przetwarzania.

Przetwarzanie danych to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Przetwarzanie danych jest możliwe tylko i wyłącznie wtedy, gdy zachodzi co najmniej jeden z przypadków, o których mowa w art. 23 ust. 1 ustawy o ochronie danych osobowych, tj.:

1. osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
2. jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
3. jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

4. jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

5. jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Za prawnie usprawiedliwiony cel, o jakim mowa w powyższym punkcie piątym, uważa się w szczególności:

- marketing bezpośredni własnych produktów lub usług administratora danych,

- dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej (tak art. 23 ust. 4 pkt 1-2 ustawy o ochronie danych osobowych).

Nie jest jasne jak w przypadku Internetu Rzeczy traktować pojęcie **rozstrzygnięcia indywidualnej sprawy** na gruncie art. 26a ustawy o ochronie danych osobowych. Zgodnie z tym przepisem z zasady niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym. Zakazu ten nie obowiązuje jedynie, jeżeli rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia wniosek osoby, której dane dotyczą, albo jeżeli zezwalają na to przepisy prawa, które przewidują również środki ochrony uzasadnionych interesów osoby, której dane dotyczą. Gdyby uznać, że w poprzez kontakt maszyn w ramach Internetu Rzeczy dochodziło do rozstrzygania indywidualnych spraw osobowych, to wtedy rozwój branży byłby ograniczony.

Dane osobowe mogą być zbierane tylko dla oznaczonego celu i w zakresie do niego adekwatnym.

Co istotne, nie wystarczy dobrze określić cel przetwarzania oraz działań w oparciu o jedną z podstaw przetwarzania informacji, aby móc przetwarzać, w tym przede wszystkim pozyskiwać, dowolne dane osobowe. W myśl art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych konieczne jest **zachowanie proporcjonalności środków** do celów. Adekwatność wiąże się przede wszystkim z ograniczeniem zakresu kategorii danych możliwych do przetwarzania. Nie można zatem zbierać danych, które niczemu nie służą i jako takie są zbędne lub też można cele te zrealizować poprzez inne - mniej szczegółowe - dane osobowe. Kwestia ta będzie szczególnie istotna w przypadku posługiwania ja się danymi biometrycznymi. Wymóg proporcjonalności środków może również czasami stanowić element hamujący rozwój innowacyjnych przedsięwzięć związanych z przetwarzaniem danych osobowych. Z natury innowacyjnych rozwiązań wynika ich nowatorskość, co zawsze rodzi obawę, że dotychczas stosowany tradycyjny odpowiednik tego rozwiązania - choć nie tak efektywny lub z innych względów mniej atrakcyjny - to jednak pozwalający osiągną identyczny cel przy mniejszym zakresie przetwarzanych danych osobowych. Udoskonalenie narządzi i urządzeń poprzez „zasilenie" ich danymi osobowymi, w świetle konieczności zachowania adekwatności środków do celu, może okazać się prawnie niedo-

puszczalne lub przynajmniej wątpliwe, jeśli używanie tradycyjnych narzędzi i urządzeń pozwala osiągną identyczny cel.

3. Wrażliwe dane osobowe

Szczególną kategorią danych osobowych są tzw. dane wrażliwe. W ustawie wprost wskazano jakie dane zaliczają się do takiej kategorii. W szczególności danymi wrażliwymi są dane zdrowotne. Przedstawiony poniżej w dymku **katalog** wrażliwych danych osobowych jest zamknięty. Tylko takie dane mają charakter wrażliwy. Nie ma możliwości, aby katalog ten uzupełnić w drodze praktyki lub wykładni. Odrębną kwestią jest nieprecyzyjność wielu z przytoczonych pojęć. W przypadkach wątpliwych należałoby przyjąć z ostrożności szeroką interpretację poszczególnych typów danych wrażliwych.

Do katalogu danych wrażliwy należą dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie wrażliwych danych osobowych z zasady jest **zabronione**. Jest jednak dopuszczalne, jeżeli:

1. osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,
2. przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,
3. przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
4. jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,
5. przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

6. przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

7. przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

8. przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

9. jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,

10. przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym (art. 27 ust. 2 ustawy o ochronie danych osobowych).

Choć zatem przetwarzania wrażliwych danych osobowych dopuszczalne jest na zasadzie wyjątku od reguły, to jednak przesłanki zastosowania wyjątku są szczególnie rygorystyczne. Zwraca uwagę, że nawet uzyskanie zgody - najprostsza i najpopularniejsza podstawa przetwarzania danych osobowych - jest utrudnione w świecie Internetu oraz Internetu Rzeczy, ponieważ musi mieć **formę pisemną**. Można nawet stwierdzić, że uzyskanie zgody na piśmie jest nierealne i podważałoby model biznesowy przedsięwzięcia.

Tematy pokrewne do poruszonych w tym rozdziale dostępne są na blogu "Prawo Internetu" m.in. we wpisach: „Wrażliwe dane osobowe", „Aplikacje zdrowotne a dane osobowe", „Dane zdrowotne jako WRAŻLIWE dane osobowe".

4. Dane biometryczne

Do danych biometrycznych zaliczyć należy przede wszystkim odciski palców, cechy charakterystyczne twarzy i głos. Część danych biometrycznych to również **dane wrażliwe** w rozumieniu przedstawionym w poprzednim rozdziale. Największa jednak przeszkodą w przypadku wykorzystywania danych biometrycznych jest konieczność przestrzegania, wyżej opisanej, **zasady proporcjonalność** zakresu przetwarzanych danych do celów przetwarzania. Najczęściej podobne cele jak poprzez użycie biometrii można osiągnąć poprzez mniej zaawansowane metody identyfikacji. Dotyczy to zwłaszcza przestrzeni publicznej. Z tych powodów kwestionowana jest przykładowo możliwość identyfikowania pracowników przez pracodawcę za pomocą urządzeń biometrycznych.

5. Przekazanie danych osobowych do państwa trzeciego

Internet Rzeczy opiera się na ciągłej wymianie informacji. Trzeba jednak przestrzegać granic państwowych. Przekazanie danych osobowych do państwa trzeciego (co do definicji państwa trzeciego zobacz wyjaśnienie w dymku obok) może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli:

Państwo trzecie to państwo nienależące do Europejskiego Obszaru Gospodarczego. Co oczywiste, do tego obszaru nie należą Stany Zjednoczone Ameryki, dlatego przekazywanie tam danych osobowych podlega szczególnym zasadom.

1. osoba, której dane dotyczą, udzieliła na to zgody na piśmie,
2. przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie,
3. przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem,
4. przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych,
5. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,
6. dane są ogólnie dostępne (art. 47 ust. 1 i 3 pkt 1-6 ustawy o ochronie danych osobowych).

W przypadkach innych niż wymienione powyżej przekazanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych, może nastąpić po uzyskaniu zgody GIODO, wydanej w drodze decyzji administracyjnej, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. Zgoda GIODO nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez:

1. standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską,
2. prawnie wiążące reguły lub polityki ochrony danych osobowych (tzw. wiążące reguły korporacyjne), które zostały zatwierdzone przez GIODO (art. 48 ust. 1-2 ustawy o ochronie danych osobowych).

6. Ochrona dóbr osobistych i prywatności

Dochowanie wymagań związanych z ochroną danych osobowych nie oznacza **bezpieczeństwa prawnego** w zakresie dóbr osobistych. Przedstawiony poniżej w dymku katalog dóbr osobistych jest jedynie przykładowy. Nie ma jednoznacznej definicji dóbr osobistych. Dane osobowe, pomimo podobnej nazwy, to odrębna kategoria prawna. Może zdarzyć się, co więcej - najczęściej właśnie taka sytuacja będzie miała miejsce, że ta sama informacja będzie daną osobową i może być traktowana w kontekście dóbr osobistych. Innymi słowy, niewłaściwe posługiwanie się konkretną informacją może prowadzić do konsekwencji zarówno na gruncie ochrony danych osobowych, jak i w zakresie ochrony dóbr osobistych. Może być też tak, że choć nie będzie dochodziło do naruszeń w zakresie ochrony danych osobowych (czyli wszystko będzie zgodne z ustawą o ochronie danych osobowych), to jednak dojdzie do naruszenia dóbr osobistych.

Dobra osobiste człowieka to m.in. zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska.

Dobra osobiste również mają podwójną naturę. Ponieważ należy je rozpatrywać zarówno w kontekście prawa cywilnego, jaki prawa karnego. Samo pojęcie dóbr osobistych właściwe jest prawu cywilnemu, jednak najczęściej, to co kryje się pod tym pojęciem może być kwalifikowane na gruncie prawa karnego np. jako przestępstwo przeciwko czci lub przestępstwo przeciwko ochronie informacji.

W tym opracowaniu poruszony zostanie jedynie wątek konsekwencji naruszenia dóbr osobistych w świetle regulacji prawa cywilnego. osobistych. Ten, czyje dobro osobiste zostaje **zagrożone** cudzym działaniem (czyli niekoniecznie już się dokonało, ale jest zagrożenie), może żądać **zaniechania** tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do **usunięcia jego skutków**, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Może on również żądać **zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy** pieniężnej na wskazany cel społeczny. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych (art. 24 § 1-2 Kodeksu cywilnego).

7. Własność przemysłowa

Internet Rzeczy nie ma i raczej nie będzie miał zestandaryzowanej struktury w nieodległej przyszłości, chyba że pojawi się firma, która zdominuje rynek. Rozwiązania z zakresu Internetu Rzeczy może tworzyć sama aplikacja zainstalowana ma smartfonie. Jednak mogą bazować też na specjalnych urządzenia (obecnie najlepszym przykładem są opaski zbierające dane o stanie zdrowia).

W tej ostatniej sytuacji pojawić może się kwestia współdziałania urządzeń różnych firm, również w kontekście używania tzw. „zamienników”. Materia te regulowana jest przez przepisy prawa własności przemysłowej. Niestety prawo to nie ustanawia jednoznacznych wskazówek w przedmiotowym zakresie. Ważne znaczenie, oprócz co oczywiste patentów, odegrać mogą uregulowania dotyczące znaków towarowych (np. loga lub charakterystycznej nazwy), w szczególności w zakresie posługiwania się cudzym znakiem towarowym, ale nie w celu tworzenie „podróbek”, lecz choćby informowania, że dane urządzenia współdziała z urządzeniami innych marek.

W myśl z art. 156 ust. 1 pkt 2-4 oraz ust. 2 Prawa własności przemysłowej, pomimo że konkretnemu podmiotowi przysługuje wyłączne prawo do **znaku towarowego**, to inne podmioty też mogą w obrocie gospodarczym używać:

1. oznaczeń wskazujących w szczególności na cechy i charakterystykę towarów, ich rodzaj, ilość, jakość, przeznaczenie, pochodzenie czy datę wytworzenia lub okres przydatności,

2. zarejestrowanego oznaczenia lub oznaczenia podobnego, jeżeli jest to konieczne dla wskazania przeznaczenia towaru, zwłaszcza gdy chodzi o oferowane części zamienne, akcesoria lub usługi,

3. zarejestrowanego oznaczenia geograficznego, jeżeli prawo do jego używania przez te osoby wynika z innych przepisów ustawy.

Używanie wskazanych oznaczeń jest dozwolone tylko wówczas, gdy odpowiada ono usprawiedliwionym potrzebom używającego i nabywców towarów i jednocześnie jest zgodne z uczciwymi praktykami w produkcji, handlu lub usługach. Posługiwanie się cudzymi oznaczeniami jest jednak prawnie dopuszczalne (w przedstawionych sytuacjach), co pozwalałoby na powstanie infrastruktury współpracujących ze sobą urządzeń różnych producentów.

www.prawo-internetu.pl

WSZYSTKIE UWAGI PRAWNE POCZYNIONE ZOSTAŁY W OPARCIU O STAN PRAWNY OBOWIĄZUJĄCY NA DZIEŃ 20.9.2015 R. ZANIM INTERNET RZECZY ZACZNIE FUNKCJONOWAĆ W WIĘKSZYM ROZMIARACH, ZWŁASZCZA W RELACJACH Z KONSUMENTAMI, A NIE TYLKO POMIĘDZY PRZEDSIĘBIORCAMI LUB WEWNĄTRZ PRZEDSIĘBIORSTWA, REGULACJE PRAWNE MOGĄ ULEC ZMIANIE. PRAWDOPODOBNE SĄ PRZEDE WSZYSTKIM ZMIANY W ZAKRESIE OCHRONY DANYCH OSOBOWYCH.