PRAWA I PRZEPISY REGULUJĄCE BEZPIECZEŃSTWO CYBERNETYCZNE

Publikacja sfinansowana z funduszy Komisji Europejskiej w ramach programu Erasmus+. Publikacja została zrealizowana przy wsparciu finansowym Komisji Europejskiej. Publikacja odzwierciedla jedynie stanowisko jej autorów i Komisja Europejska oraz Narodowa Agencja Programu Erasmus+ nie ponoszą odpowiedzialności za jej zawartość merytoryczną. PUBLIKACJA BEZPŁATNA

WYKŁADY

1. wprowadzenie do przedmiotu, system prawa, norma prawna, prawo i Internet
2. Odpowiedzialność w cyberprzestrzeni
3. podstawa prawna działalności ISP (dostawcy usług internetowych)
4. Cyberbezpieczeństwo i jego regulacje prawne
5. ISMS
6. Ochrona danych osobowych w cyberprzestrzeni
7. Prywatność i bezpieczeństwo w ICT, ochrona danych w cyberprzestrzeni

WARSZTATY

1. Określenie zakresu obowiązywania prawa w cyberprzestrzeni (granice, możliwości itp.)
2. Odpowiedzialność prywatna i publiczna za działania użytkownika lub firmy w środowisku online
3. Charakterystyka i definicja poszczególnych dostawców usług internetowych oraz ich prawa i obowiązki w odniesieniu do bezpieczeństwa cybernetycznego
4. ISMS i związek z prawem dotyczącym bezpieczeństwa cybernetycznego
5. Pozyskiwanie podstawowych praw i obowiązków dla podmiotów indywidualnych z dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. dotyczącej środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w całej Unii, a także z przepisów krajowych.
6. Stosowanie praw i obowiązków wynikających z GDPR w cyberprzestrzeni
7. Praktyczna analiza warunków umów z dostawcami usług internetowych w odniesieniu do ochrony prywatności

Spis treści

1. Wprowadzenie do przedmiotu, system prawa, norma prawna, prawo i Internet

Prawo jest jednym z najważniejszych środków stabilizacji stosunków społecznych i regulacji społeczeństwa.

Prawo jest konieczne i obecnie niedostępne, ponieważ tam, gdzie jest społeczeństwo, jest i prawo. Społeczeństwo nie jest w stanie długo istnieć bez porządku i zasad. Prawo jako takie znacząco zmniejsza poziom chaosu (entropii) w społeczeństwie i stabilizuje warunki.

Wszystkie powyższe stwierdzenia są prawdziwe, ale tylko przy założeniu, że prawo jest przestrzegane, a także przy założeniu, że samo prawo jest stabilne (przynajmniej względnie).

Prawo, podobnie jak społeczeństwo, ewoluuje i zmienia się.

Prawo to zbiór powszechnie obowiązujących zasad postępowania w żyjących społeczeństwach, określonych przez państwo lub organy, którym państwo powierzyło to zadanie. Aby prawo było trwałe, musi być egzekwowalne. Prawo bez warunku wykonalności jest nadal prawem, ale w rzeczywistości jest to raczej zbiór zaleceń, których przestrzeganie jest obowiązkiem każdego.

Aby móc skutecznie wykonywać lub chronić swoje prawa oraz być świadomym swoich obowiązków, które są ściśle związane z rządzeniem, obywatel lub podmiot, do którego będzie miało zastosowanie prawo, musi posiadać przynajmniej minimalną wiedzę na temat podstawowych przepisów porządku prawnego.

We współczesnym społeczeństwie prawo można scharakteryzować jako względnie dobrze zdefiniowany system norm prawnych, zabezpieczony przez władzę państwową i egzekwowany za pomocą przymusu państwowego. Aby osoba fizyczna lub prawna mogła skutecznie korzystać ze swoich praw lub je chronić, a także aby była świadoma swoich obowiązków wynikających bezpośrednio z przepisów prawa, musi wykazać się przynajmniej minimalną znajomością podstawowych przepisów porządku prawnego.

Samo pojęcie prawa jest stosunkowo trudne do zdefiniowania, ponieważ jest ono zjawiskiem multimedialnym i nie da się go określić jedną definicją:

- **prawo naturalne** (*ius naturale*). Istnieje ona niezależnie od państwa, powstaje i rozwija się w społeczeństwie. Ogólnie rzecz biorąc, jest to zbiór zasad, które są adekwatne do etapu rozwoju społeczeństwa.
- **prawo pozytywne** (*ius positivum*). Prawo to jest nadawane przez państwo, a raczej przez ustanowienie władzy. Prawo pozytywne jest zatem z góry ustalone, jest przewidywalne, reguły są egzekwowane, tzn. że czyny bezprawne są karane.
- **prawo obiektywne** - (odpowiadające angielskiemu terminowi "*law*"). W przypadku prawa obiektywnego, prawo rozumiemy jako zbiór norm prawnych jako ogólnie obowiązujących zasad postępowania ustanowionych lub uznanych przez państwo i egzekwowanych przez państwo.
- **prawo podmiotowe** - (odpowiadające angielskiemu terminowi "*right*"). W tym przypadku pod pojęciem prawa rozumiemy możliwość zachowania się podmiotów prawnych gwarantowaną przez normę prawną, która zwykle odpowiada obowiązkowi prawnemu innego podmiotu prawnego. Prawo w tym sensie odpowiada na przykład stwierdzeniu podmiotu, że "ma on prawo do czegoś".

1.1 Normy prawne

Praworządność jest podstawowym elementem państwa prawa.

Norma prawna to powszechnie obowiązująca reguła postępowania, która reguluje prawa i obowiązki podmiotów. Ta reguła postępowania jest wyrażona w określonej formie prawnej uznanej przez państwo (lub Unię), a jej przestrzeganie jest zapewnione przez przymus państwowy.

Z powyższej definicji normy prawnej wynikają dwie cechy obligatoryjne, które są dalej wyszczególnione. Są to:

1. **Formalne**

   Z punktu widzenia spełnienia formalnej cechy normy prawnej konieczne jest, aby norma prawna została wydana przez uprawniony podmiot i aby jednocześnie został spełniony przewidziany prawem sposób jej publikacji.

2. **Materialne**

   Do cech materialnych normy prawnej można zaliczyć:

   - regulatywność - reguluje stosunki społeczne,
   - wiążący prawnie - reguła postępowania reguluje stosunki społeczne w sposób wiążący,
   - ogólność - zarówno jeśli chodzi o podmiot regulacji prawnej, jak i przedmiot normy prawnej,
   - egzekwowalność przez władzę państwową - "przymus państwowy", jeśli prawo nie jest przestrzegane.

Standardowa **struktura normy prawnej składa się z trzech części**: **hipotezy, dyspozycji i sankcji**.

Hipoteza określa warunki, w jakich norma prawna jest realizowana. W szczególności hipoteza określa fakty prawne, podmioty i przedmioty normy, do których odnoszą się upoważnienia i obowiązki.

Dyspozycja stanowi własną regułę postępowania, ponieważ ustanawia i precyzuje, komu i jakie prawa i obowiązki powstają w przypadku wystąpienia warunków określonych w hipotezie.

Sankcja jest wyrazem konsekwencji naruszenia obowiązku prawnego wynikającego z dyspozycji normy prawnej.

Podział norm prawnych

Normy prawne można podzielić według różnych kryteriów. Należą do nich:

1. *Charakter zasad ustanowionych przez normę prawną.* Ze względu na charakter przepisów, normy prawne dzielą się na:

- Rozstrzygające. Dyspozytywna norma prawna nie ustanawia w ogóle podstawowej reguły postępowania lub ustanawia ją tylko alternatywnie. Ustalenie zasad pozostawia się adresatom. Jeśli adresaci tego nie zrobią, przepisy normy służą jako wskazówki dla sędziego, który powinien wiedzieć, jak podjąć decyzję. Normy dyspozytywne są najczęściej stosowane w prawie cywilnym lub w stosunkach cywilnoprawnych, które pozwalają na większą zmienność w rozwiązywaniu różnych sytuacji (samoregulacja).
- Kogentne (kategoryczne). Bezwzględnie obowiązująca norma prawna w sposób wiążący ustanawia regułę postępowania, nie pozostawiając miejsca na wolę adresata.

2. *Sformułowania.* Zgodnie z brzmieniem, normy prawne dzielą się na:

- Autoryzacyjne. W tych normach prawnych wyraźnie sformułowano jedynie upoważnienia.
- Wiążące. Te normy prawne wyraźnie formułują obowiązek, czy to w formie nakazu, czy zakazu.

3. *Status uczestników.* Ze względu na status podmiotów, normy prawne dzielą się na:

- Publiczne. Te normy prawne mają zastosowanie tam, gdzie sprawowana jest władza publiczna. Władza publiczna jest sprawowana przez państwo za pośrednictwem władzy ustawodawczej, wykonawczej i sądowniczej. Za prawo publiczne uważamy tę dziedzinę prawa, w której stosunki opierają się na nierówności podmiotów, gdzie jeden z nich reprezentuje władzę publiczną, która działa wobec osób prywatnych za pomocą nakazów, zakazów i przymusu.
- Prywatne. Te normy prawne są stosowane w sferze prawa prywatnego, tzn. tam, gdzie podmioty występują w równej pozycji i żaden z nich nie może autorytatywnie decydować o prawach i obowiązkach drugiego. Podmioty regulują swoje wzajemne prawa i obowiązki za pomocą umów i porozumień.

4. *Przedmiot regulacji.* Ze względu na przedmiot regulacji, normy prawne dzielą się na:

- Międzynarodowe. Te normy prawne regulują stosunki między państwami lub ich mieszkańcami, ewentualnie na poziomie Unii.
- Krajowe. Krajowe normy prawne regulują stosunki między podmiotami podlegającymi jurysdykcji danego państwa lub, co do zasady, znajdującymi się na jego terytorium.

5. *Metoda regulacji*. Zgodnie z metodą regulacji prawnej normy prawne dzielą się na:

- Merytoryczne. Te normy prawne definiują stosunki prawne w ogólności, określają prawa i obowiązki podmiotów.
- Proceduralne. Te normy prawne regulują tryb postępowania organów władzy publicznej w zakresie stosowania norm prawa materialnego, co może skutkować wydaniem aktu publicznego.

6. *Zakres obowiązywania przepisów.* Ze względu na zakres regulacji prawnej, normy prawne dzielą się na:

- Ogólne. Te normy prawne obowiązują na całym terytorium Państwa lub UE, odnoszą się do wszystkich podmiotów i nie są ograniczone w czasie.
- Szczególne. Te normy prawne funkcjonują tylko na określonym terytorium lub mają zastosowanie tylko do określonej kategorii podmiotów albo przez określony czas.

Skuteczność norm prawnych

Skuteczność normy prawnej oznacza, że rodzi ona prawa i obowiązki dla jej adresatów. Warunkiem skuteczności normy prawnej jest jej obowiązywanie. Oznacza to, że dana norma prawna może wejść w życie najwcześniej w dniu jej obowiązywania. Norma prawna może jednak zacząć obowiązywać później. Tak więc między datą, w której przepis prawny stał się ważny, a datą jego wejścia w życie może upłynąć pewien czas (tzw. *vacatio legis*). Celem tego jest umożliwienie adresatom normy prawnej właściwego zapoznania się z nią i dostosowania się do niej. Data wejścia w życie jest zwykle określona w ostatnim przepisie normy prawnej.

Przykłady prawa wokół nas:

- Umowa kupna
- Umowa o dzieło
- Umowa kredytowa
- Umowa o pracę/umowa o dzieło/umowa o dzieło
- Umowa o świadczenie usług doradczych

- Umowa licencyjna
- Umowa o zarządzanie
- Umowa o zachowaniu poufności
- Umowa sprzedaży udziałów w przedsiębiorstwie
- Czyny niedozwolone (zniesławienie, naruszenie umowy)
- Przestępstwa kryminalne (np. kradzież, oszustwo, naruszenie praw autorskich itp.)

1.2 Związek między prawem a cyberprzestrzenią

Wiele opublikowano na temat relacji między prawem a nowymi technologiami, zwłaszcza Internetem, w tym jego zmian i przekształceń, ale wiele kluczowych kwestii pozostaje nierozwiązanych, wiele innych problemów znajduje się dopiero na etapie identyfikacji lub analizy, ale poszukiwanie rozsądnych rozwiązań jest w najlepszym razie na dobrej drodze, w najgorszym - poza zasięgiem wzroku. Internet jest niewątpliwie zjawiskiem *sui generis* i jako taki nie jest samodzielny, a jego regulacja polega głównie na regulowaniu zachowań jego użytkowników.

Prawo jest jednym z jego możliwych regulatorów w postaci niedoskonałych konstrukcji normatywnych, gdzie bardziej niż gdzie indziej prawdziwe jest twierdzenie, że nie ma zgodności między rzeczywistością, czyli tym, co faktycznie realizuje się w środowisku internetowym, a normatywnością, czyli tym, co powinno być (z woli regulatora i naszej). Tak więc rzeczywistość Internetu i jego normatywna regulacja to dwie stosunkowo odrębne kategorie. Założenie to nie zostanie zanegowane w niniejszej publikacji, wręcz przeciwnie, będzie jednym z jej filarów.

Większość kwestii prawnych związanych z Internetem należy rozpatrywać w ogólnym kontekście prawnym i technologicznym, a nie tylko przez pryzmat utartych schematów czy poszczególnych dyscyplin prawnych *per se*.[1]

[1] MATEJKA, Ján. *Internet jako przedmiot prawa: poszukiwanie równowagi między autonomią a prywatnością.* Praga: CZ.NIC, 2013. ISBN 978-80-904248-7-6 s. 25

2. Odpowiedzialność w cyberprzestrzeni

2.1 Cyberprzestrzeń

"Zgodna halucynacja, której codziennie doświadczają miliardy prawowitych operatorów wszystkich narodów, dzieci uczące się podstaw matematyki... Graficzna reprezentacja danych wyabstrahowanych z banków wszystkich komputerów ludzkiego systemu. Niewyobrażalna złożoność. Linie światła ułożone w przestrzeni umysłu, skupiska i konstelacje danych. Jak światła miasta, ...".

William Gibson: Neuromancer (1984)

Cyberprzestrzeń to wyimaginowana piaskownica, w której się poruszamy, ale jest ona również kluczowym elementem definicji bezpieczeństwa cybernetycznego. Aby zdefiniować cyberprzestrzeń, należy przede wszystkim zdefiniować pojęcie Internetu, które jest bezpośrednio związane z cyberprzestrzenią.

Światowe początki Internetu, który jest podstawową substancją materialną cyberprzestrzeni, sięgają lat 50. ubiegłego wieku. W tym czasie budowano i testowano sieci połączonych ze sobą komputerów, głównie do celów badań naukowych i wojskowych. Chociaż Internet został zbudowany na fundamentach sieci ARPANET i NSFNET[2] , dziś nikt nie jest właścicielem Internetu, nie ma też centralnego organu ani instytucji, która by nim zarządzała. "*Istnieją jednak instytucje, które odgrywają istotną rolę w funkcjonowaniu i dalszym rozwoju Internetu. Pierwszą z nich jest Internet Society (ISOC), która zrzesza użytkowników Internetu. ISOC składa się z dwóch głównych komponentów: Internet Activities Board (IAB) oraz Internet Engeneering Task Force (IETF). Obie te instytucje współpracują z największymi firmami komputerowymi w celu opracowania standardów niezbędnych do dalszego rozwoju Internetu.*" [3]

ICANN[4] (Internet Corporation for Assigned Names and Numbers) ma wyłączną pozycję w Internecie. Stowarzyszenie to jest odpowiedzialne za ustalanie zasad działania systemu nazw domen. Obecnie jednak dostawcy usług internetowych coraz częściej wysuwają się na pierwszy plan i odgrywają coraz większą rolę.[5]

Materialną (namacalną) istotą Internetu jest jego sieć szkieletowa, która przenosi sygnał (dane) przez powietrze, kable lub inne media transmisyjne. Z technicznego punktu widzenia jest to ogólnoświatowa rozproszona sieć komputerowa składająca się z poszczególnych mniejszych sieci połączonych ze sobą za pomocą protokołów IP w celu umożliwienia komunikacji, przesyłania danych, informacji i usług między podmiotami. W efekcie powstaje dynamiczny, stale zmieniający się i ewoluujący system, związany ze sprzętem, ale jednocześnie tworzący trudną do zdefiniowania i praktycznie nieograniczoną cyberprzestrzeń. Można powiedzieć, że cyberprzestrzeń to wirtualna rzeczywistość bez końca i początku. Ta wirtualna rzeczywistość jest jednak całkowicie zależna od substancji materialnej, tj. technologii występujących w świecie rzeczywistym. Tworzy to interesujący paradoks, który pozwala na istnienie niematerialnego medium (cyberprzestrzeni), zdolnego do adaptacji i zmian w przypadku uszkodzenia medium materialnego (elementów sieci, pojedynczych systemów komputerowych, pamięci masowych w chmurze, połączonych usług itp.), ale w przypadku całkowitego załamania się medium materialnego (lub wszystkich jego elementów) cyberprzestrzeń jako taka zostanie nieodwracalnie uszkodzona lub zniknie.

---

[2] Por. *Internetowa historia lat 80.* [online]. [cyt. 2016 Jun 7]. Dostępne od: http://www.computerhistory.org/internethistory/1980s/

[3] *Internet, łączność i możliwy rozwój (Część 2 - Historia i rozwój Internetu).* [online]. [cyt. 2008-02-10]. Dostępny pod adresem: http://www.internetprovsechny.cz/clanek.php?cid=163

[4] Więcej informacji można znaleźć na stronie https://www.icann.org/.

[5] ISP - Internet Service Provider (dostawca usług internetowych).

Cyberprzestrzeń można również zdefiniować jako przestrzeń działań w sieci lub jako przestrzeń stworzoną przez technologie informacyjno-komunikacyjne, która tworzy wirtualny świat (lub przestrzeń) równolegle do przestrzeni rzeczywistej.

Pojęcie cyberprzestrzeni stało się powszechnie znane po ogłoszeniu przez Johna Barlowa (założyciela Electronic Frontier Foundation) deklaracji "A Declaration of the Independence of Cyberspace" (Deklaracja niepodległości cyberprzestrzeni):

Rządy Uprzemysłowionego Świata, wy zmęczone olbrzymy z ciała i stali, przybywam z Cyberprzestrzeni, nowego domu Umysłu. W imieniu przyszłości proszę was z przeszłości, abyście zostawili nas w spokoju. Nie jesteście wśród nas mile widziani. Nie macie władzy nad tym, gdzie się gromadzimy.

Nie mamy rządu pochodzącego z wyboru, ani też nie zanosi się na to, abyśmy go mieli, dlatego zwracam się do was z autorytetem nie większym niż ten, którym zawsze przemawia sama wolność. Ogłaszam, że globalna przestrzeń społeczna, którą budujemy, jest naturalnie niezależna od tyranii, które chcecie nam narzucić. Nie macie moralnego prawa, by nami rządzić ani nie dysponujecie metodami egzekwowania prawa, których moglibyśmy się obawiać.

Rządy czerpią swoje słuszne uprawnienia z przyzwolenia rządzonych. Nie prosiliście o nasze ani nie otrzymaliście. Nie zaprosiliśmy cię. Nie znacie nas ani nie znacie naszego świata. Cyberprzestrzeń nie leży w granicach państwa. Nie myślcie, że możecie go zbudować, tak jakby to był publiczny projekt budowlany. Nie można. Jest to akt natury, który rozwija się dzięki naszym wspólnym działaniom.

Nie uczestniczyliście w naszej wielkiej i gromadzącej rozmowie, ani nie tworzyliście bogactwa naszych rynków. Nie znacie naszej kultury, naszej etyki ani niepisanych kodeksów, które już teraz zapewniają naszemu społeczeństwu więcej porządku, niż można by uzyskać poprzez jakiekolwiek wasze narzucenie.

Twierdzicie, że są wśród nas problemy, które musicie rozwiązać. Używacie tego twierdzenia jako pretekstu do wtargnięcia do naszych dzielnic. Wiele z tych problemów nie istnieje. Tam, gdzie są prawdziwe konflikty, gdzie są krzywdy, zidentyfikujemy je i zajmiemy się nimi za pomocą naszych środków. Tworzymy naszą własną umowę społeczną. Ten sposób zarządzania będzie wynikał z warunków panujących w naszym świecie, a nie w waszym. Nasz świat jest inny.

Cyberprzestrzeń składa się z transakcji, relacji i samej myśli, ułożonych jak fala stojąca w sieci naszej komunikacji. Nasz świat jest jednocześnie wszędzie i nigdzie, ale nie jest tam, gdzie żyją ciała.

Tworzymy świat, do którego wszyscy mogą wejść bez przywilejów i uprzedzeń wynikających z rasy, potęgi ekonomicznej, siły militarnej czy miejsca urodzenia.

Tworzymy świat, w którym każdy i wszędzie może wyrażać swoje przekonania, niezależnie od tego, jak bardzo są one osobliwe, bez obawy, że zostanie zmuszony do milczenia lub podporządkowania się.

Twoje prawne pojęcia własności, ekspresji, tożsamości, ruchu i kontekstu nie mają do nas zastosowania. Wszystkie one opierają się na materii, a tu jej nie ma.

Nasze tożsamości nie mają ciał, więc - w przeciwieństwie do was - nie możemy uzyskać porządku za pomocą przymusu fizycznego. Wierzymy, że nasz sposób zarządzania wyłoni się z etyki, oświeconego interesu własnego i dobra wspólnego. Nasza tożsamość może być rozproszona w wielu jurysdykcjach. Jedynym prawem, które wszystkie tworzące nas kultury uznają, jest Złota Reguła. Mamy nadzieję, że na tej podstawie będziemy mogli budować nasze konkretne rozwiązania. Nie możemy jednak zaakceptować rozwiązań, które próbujecie nam narzucić.

W Stanach Zjednoczonych stworzyliście dziś ustawę, Telecommunications Reform Act, która odrzuca waszą własną Konstytucję i obraża marzenia Jeffersona, Waszyngtona, Milla, Madisona, DeToqueville'a i Brandeisa. Te marzenia muszą teraz narodzić się w nas na nowo.

Boicie się własnych dzieci, ponieważ są one tubylcami w świecie, w którym wy zawsze będziecie imigrantami. Ponieważ się ich boicie, powierzacie biurokratom obowiązki rodzicielskie, z którymi sami jesteście zbyt tchórzliwi, by się zmierzyć. W naszym świecie wszystkie uczucia i przejawy człowieczeństwa, od tych poniżających po anielskie, są częściami jednolitej całości, globalnej rozmowy bitów. Nie można oddzielić powietrza, które dusi, od powietrza, w którym trzepocą skrzydła.

W Chinach, Niemczech, Francji, Rosji, Singapurze, Włoszech i Stanach Zjednoczonych próbuje się odeprzeć wirusa wolności, stawiając posterunki strażnicze na granicach cyberprzestrzeni. Mogą one na jakiś czas powstrzymać epidemię, ale nie sprawdzą się w świecie, który wkrótce zostanie pokryty nośnikami bitowymi.

Wasz coraz bardziej przestarzały przemysł informacyjny utrwaliłby się, proponując w Ameryce i innych krajach prawa, które rościłyby sobie prawo do posiadania mowy całego świata. Przepisy te uznałyby idee za kolejny produkt przemysłowy, nie bardziej szlachetny niż stalowa surówka. W naszym świecie wszystko, co stworzy ludzki umysł, może być powielane i rozpowszechniane w nieskończoność bez żadnych kosztów. Globalne przekazywanie myśli nie wymaga już istnienia fabryk.

Te coraz bardziej wrogie i kolonialne działania stawiają nas w tym samym położeniu, co wcześniejszych miłośników wolności i samostanowienia, którzy musieli odrzucić władze odległych, nieświadomych mocarstw. Musimy zadeklarować, że nasze wirtualne jaźnie nie podlegają waszej władzy, nawet jeśli nadal zgadzamy się na wasze panowanie nad naszymi ciałami. Rozprzestrzenimy się po całej planecie, aby nikt nie mógł zatrzymać naszych myśli.

Stworzymy cywilizację umysłu w cyberprzestrzeni. Niech będzie on bardziej ludzki i sprawiedliwy niż świat, który wasze rządy stworzyły wcześniej.

Davos,
Szwajcaria8 lutego
1996 r.[6]

Prawie dwadzieścia lat po wydaniu Deklaracji jej tekst jest nadal bardzo aktualny. Współczesne społeczeństwo stara się reagować na ogromny rozwój technologii informacyjnych i komunikacyjnych, ich wzajemne przenikanie się i łączenie, pojawianie się nowych trendów itp. Jednak reakcja ta często opiera się przede wszystkim na egzekwowaniu przepisów i wprowadzaniu ograniczeń, a nie na zrozumieniu i edukacji użytkowników.

Cyberprzestrzeń, w porównaniu ze światem rzeczywistym, jest bardzo specyficzna i zdecydowanie błędne jest zakładanie, że będą w niej obowiązywać te same zasady, co w świecie rzeczywistym. Ogólnie można stwierdzić, że w cyberprzestrzeni można stosować standardowe kryteria, które są stosowane w odniesieniu do rzeczywistej fizycznej lokalizacji danych lub informacji. Drugą możliwością jest stworzenie nowych kryteriów stosowania zasady właściwości miejscowej (chodzi o wirtualną lokalizację stosunków prawnych).[7]

Cyberprzestrzeń charakteryzuje się tym, że jest z nią połączona duża część społeczeństwa (szacuje się, że jest w nią zaangażowanych 3,6 miliarda osób, przy populacji globalnej wynoszącej około 7,4

[6] BARLOW, Perry John. *Deklaracja niepodległości cyberprzestrzeni.* [online]. [cyt. 23.9.2014]. Dostępny pod adresem: https://www.eff.org/cyberspace-independence.
[7] Więcej szczegółów w: REED, Chris. *Prawo internetowe*. Cambridge: Cambridge University Press, 2004, s. 218.

miliarda).[8] Jednocześnie należy zauważyć, że masowe zaangażowanie społeczeństwa zaczęło się pojawiać dopiero około 15-20 lat temu.

Cechami charakterystycznymi cyberprzestrzeni są decentralizacja, globalność, otwartość, bogactwo informacji (w tym informacji w postaci "smogu informacyjnego", bzdur, półprawd i kłamstw), interaktywność oraz możliwość wpływania na opinię poprzez użytkowników (awatary[9]). Istotną cechą cyberprzestrzeni jest to, że główną rolę odgrywa w niej technologia i związane z nią usługi. Ostatnio coraz wyraźniej widać, że przejawy świata wirtualnego mogą mieć i mają reperkusje w świecie rzeczywistym.

Szybkość, a zwłaszcza dostępność przesyłanych danych staje się dziś kluczowym elementem. Użytkownik zazwyczaj nie chce, a nawet nie zadaje sobie trudu, aby dowiedzieć się, jak i gdzie są przesyłane dane, które są wprowadzane do sieci informacyjnych. Nie obchodzi ich także, gdzie znajduje się odbiorca przesyłanych danych ani gdzie są one przechowywane, co powoduje oderwanie treści od fizycznej struktury sieci informacyjnych.

Z jednej strony można zaobserwować sytuację, w której **stosunki społeczne w cyberprzestrzeni ulegają delokalizacji**[10] , co stwarza problemy w zakresie stosowania prawa, ale z drugiej strony ta delokalizacja pozwala użytkownikom na swobodne komunikowanie się, wysyłanie, przechowywanie, zmienianie danych ("swobodnie" i bez ograniczeń w postaci granic).

Cechami charakterystycznymi cyberprzestrzeni są **decentralizacja**, **globalność**, **otwartość**, **bogactwo informacji**, **interaktywność** oraz możliwość wpływania na opinię publiczną poprzez użytkowników. Zasadniczą cechą cyberprzestrzeni jest to, że główną rolę odgrywa w niej technologia i związane z nią usługi. Ostatnio coraz wyraźniej widać, że przejawy świata wirtualnego mogą mieć i mają reperkusje w świecie rzeczywistym.

Jeśli chodzi o definicję prawną cyberprzestrzeni, można posłużyć się np. brzmieniem art. 2 lit. a) ustawy nr 181/2014 Coll., o bezpieczeństwie cybernetycznym[11] , który stanowi, że "*cyberprzestrzeń to środowisko cyfrowe umożliwiające tworzenie, przetwarzanie i wymianę informacji, składające się z systemów informatycznych oraz usług i sieci łączności elektronicznej"*.

Naszym zdaniem jedną z najbardziej udanych definicji cyberprzestrzeni jest dokument Cyberspace Operations: Concept Capability Plan 2016-2028, który definiuje **cyberprzestrzeń jako przestrzeń składającą się z trzech warstw:** [12]

1. **fizyczne,**
2. **logiczne** i
3. **społeczne**.

Warstwy te składają się w sumie z pięciu komponentów.

---

[8] Patrz np. *World Internet Users and 2015 Population Stats.* [online]. [cyt. 2015-08-09]. Dostępny pod adresem: http://www.internetworldstats.com/stats.htm

[9] Celowo używam tu terminu awatar, ponieważ jest on wyrazem wirtualnej tożsamości stworzonej przez prawdziwą osobę. Pojęcie awatara pochodzi z hinduizmu, gdzie termin ten odnosił się do materializacji boga lub wyzwolonej duszy w formie fizycznej na ziemi (ziemskie wcielenie istoty duchowej).
Obecnie termin ten jest używany jako wizualna reprezentacja (ikona lub postać) użytkownika w świecie wirtualnym (w grze, blogu, na forum, w Internecie itp.), czyli w cyberprzestrzeni.

[10] *Delokalizacja stosunków prawnych w Internecie* [online]. [cit.15.4.2012]. Dostępny pod adresem: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html

[11] Zwany dalej ZKB

[12] TRADOC. Operacje w cyberprzestrzeni: Plan Zdolności Koncepcyjnych na lata 2016-2028 [online]. [cited 2018 Feb 18], pp. 8-9 Available from: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

Ad 1) Warstwa fizyczna

Warstwa ta obejmuje pojęcie "**komponentu geograficznego**" oraz pojęcie **fizycznych komponentów sieci**. Termin "element geograficzny" nie ma dokładnego odpowiednika w naszym języku, ale odnosi się do dokładnej lokalizacji elementów sieci w świecie fizycznym. Fizyczny element sieci obejmuje infrastrukturę w postaci kabli, kontrolerów sieciowych (przełączników, routerów) i innego sprzętu.

Taki podział warstwy fizycznej ma swoją logikę. Podczas gdy w cyberprzestrzeni można z łatwością przekraczać geopolityczne granice między państwami, w świecie rzeczywistym nadal istnieją ograniczenia wynikające z natury naszego świata fizycznego.

Jeśli przeniesiemy tę ideę na świat cyberataków i incydentów, oznacza to, że jako atakujący mogę albo uszkodzić element warstwy fizycznej zdalnie, na przykład znając jego konkretną podatność, którą można zaatakować zdalnie, albo mogę go uszkodzić bezpośrednio w świecie rzeczywistym, jeśli mogę się do niego fizycznie dostać i zaatakować go, na przykład używając siły fizycznej. Oddziaływanie w cyberprzestrzeni będzie takie samo, ale sam sposób przeprowadzenia ataku jest zupełnie inny.

Ad 2) Warstwa logiczna

Ta warstwa zawiera **logiczne elementy sieci**, czyli logiczne połączenia między węzłami sieci. Są one realizowane za pomocą protokołów komunikacji sieciowej. Węzłami mogą być komputery, telefony i inne urządzenia sieciowe.

Ad 3) Klasa społeczna

Warstwa ta składa się z elementów zwanych "**cyberosobowością**" i **osobowością**.

Element "tożsamości cybernetycznej" obejmuje identyfikację osoby w sieci, np. adres e-mail, adres IP, numer telefonu i inne. Komponent osobowościowy składa się z rzeczywistych osób podłączonych do sieci. Jedna osoba może mieć wiele "cyberosobowości", na przykład różne e-maile na różnych urządzeniach, a jedna "cyberosobowość" może być w rzeczywistości wieloma różnymi rzeczywistymi osobami korzystającymi na przykład z jednego wspólnego konta.

Cyberprzestrzeń można również zdefiniować poprzez dostępność i możliwość śledzenia danych dla przeciętnego użytkownika. Zgodnie z tym podziałem cyberprzestrzeń można podzielić na usługi i dane dostępne przez Internet, usługi i dane dostępne tylko w ramach określonych sieci i urządzeń oraz usługi i dane celowo ukryte i dostępne za pomocą specjalnych narzędzi.

Zwykle stosuje się następujące nazwy dla tych kategorii:

1. **Surface Web,**
2. **Głęboka sieć** i
3. **Ciemna sieć**.

Deep i Dark Weby są również określane wspólną nazwą **D4rkN3ts - Darknets**. Wszystkie te elementy łączą się, tworząc prawdziwą cyberprzestrzeń.[13]

Terminologia, w której używa się terminu "*sieć"* do podziału cyberprzestrzeni, jest niestety uwarunkowana faktem, że dla większości społeczeństwa obowiązuje proste równanie:

---

[13] Por. *Np. Ciemna sieć - wyjaśnienie.* [online]. [cyt. 2016-07-20]. Dostępny pod adresem: https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html
lub .
Surface Web, Deep Web, Dark Web - na czym polega różnica. [online]. [cyt. 2016-07-20]. Dostępny pod adresem: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

CYBERPRZESTRZEŃ = INTERNET = **SIEĆ**

Cyberprzestrzeń to jednak nie tylko strony internetowe, ale wszystkie systemy komputerowe, usługi, użytkownicy i dane, które poruszają się w tej przestrzeni.

2.2 Zakres obowiązywania prawa w cyberprzestrzeni

Cyberprzestrzeń jest otwarta i łatwo dostępna dla wszystkich, ***"...nie obowiązują w niej żadne specjalne prawa i należy przestrzegać ogólnie obowiązujących norm".*** [14]

Jest faktem bezspornym, że realizacja coraz większej liczby stosunków społecznych i gospodarczych przenosi się do środowiska sieci informacyjnych, a tym samym powstaje potrzeba pewnej regulacji prawnej tych zachowań. W związku z delokalizacją podmiotów prawnych w różnych krajach świata pojawia się pytanie, jaki system prawny (jeśli w ogóle) będzie miał zastosowanie do ewentualnych czynów (lub naruszeń) popełnionych w Internecie.

Przede wszystkim należy zająć się dwiema kwestiami. Po pierwsze, czy prawo obowiązuje w Internecie, a jeśli tak, to jakie normy prawne mają zastosowanie. Po drugie, w jaki sposób prawo to może być stosowane, w tym ewentualne sankcje i inne środki. Przykładem trudności w stosowaniu prawa jest sytuacja, w której w 2005 r. w Chinach jeden z graczy gry internetowej *"The Legend of Mir 3"* **zabił innego gracza za kradzież wirtualnej broni**. Między graczami funkcjonuje nie tylko sprzedaż wirtualnych dóbr, ale także system pożyczek. W szczególności zdarza się to wśród graczy, którzy znają się bardzo blisko, ale nie jest wymagane, aby znali się w świecie rzeczywistym. To właśnie ta pożyczka była przyczyną wspomnianego morderstwa. Gracz Qui Chengwei pożyczył wirtualną szablę, *"Smoczą szablę"*, swojemu wirtualnemu przyjacielowi Zhu Caoyuanowi. Zhu uległ jednak wizji łatwych pieniędzy i sprzedał broń za 7 200 juanów (co przekłada się na około 19 000-20 000 koron czeskich) na aukcji internetowej. Dowiedziawszy się o sprzedaży, Qui skontaktował się z policją i zgłosił kradzież wirtualnej szabli. Policja odmówiła zajęcia się tą sprawą, twierdząc, że własność wirtualna (de facto nieistniejące przedmioty) nie jest objęta prawem. Qui stracił cierpliwość, zaatakował Zhu w jego domu i zadźgał go na śmierć.[15]

Oczywiście jest to przypadek bardzo skrajny, ale trafnie pokazuje, że świat wirtualny nie jest oderwany od świata rzeczywistego i dlatego należy zająć się kwestią odpowiedzialności prawnej w tym świecie.[16] De facto od początku rozwoju Internetu doszło do konfrontacji między światem techniki a światem prawa. Z technicznego punktu widzenia Internet jest zaprojektowany w sposób logiczny, z wyraźną hierarchią i strukturą. Jednak prawo, a zwłaszcza prawo lokalne, często wprowadzało i nadal wprowadza "chaos" do tej logiki. Termin "chaos" być może najtrafniej opisuje wysiłki ustawodawstwa zmierzające do uregulowania tego czysto technicznego świata, ponieważ w cyberprzestrzeni użytkownik ma wiele możliwości "obejścia" konkretnego zakazu lub ograniczenia. W kolejnych przykładach postaram się pokazać wpływ świata rzeczywistego i wirtualnego.

LICRA vs. Yahoo

Jedna z pierwszych spraw dotyczących możliwości stosowania prawa w Internecie miała miejsce w 2000 roku we Francji. W lutym 2000 roku Marc Knobel (francuski Żyd, który poświęcił swoje życie walce z nazizmem) odwiedził stronę aukcyjną www.yahoo.com i odkrył, że na stronie tej można

---

[14] SMEJKAL, Vladimir. *Internet i §§* 2. aktualizacji. wyd. 2 i rozszerzone. Praga: Grada, 2001, s. 32.

[15] Por. HAINES, Lester. *Gracz internetowy dźgnięty nożem z powodu "skradzionego" cyberhasła.* [online]. [cyt. 3.10.2006]. Dostępny pod adresem: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

[16] Por. Postanowienie Sądu Najwyższego 4 Tz 265/2000 z dnia 16 stycznia 2001 r. [online]. [cyt. 13.3.2008]. Dostępny pod adresem: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/B82A96F8E1B60D3AC1257A4E00694707?openDocument&Highlight=0

znaleźć wiele przedmiotów związanych z nazizmem lub z niemieckimi działaniami wojennymi w czasie II wojny światowej. Po tym odkryciu Marc Knobel skontaktował się z firmą Yahoo! Inc. z prośbą o zablokowanie tych witryn. Yahoo! Inc. nie spełniło jego prośby. W dniu 11 kwietnia 2000 r. Marc Knobel, za pośrednictwem L.I.C.R.A. (Ligue Internationale Contre Le Racisme et l'Antisémitisme), wniósł powództwo przeciwko Yahoo! Inc. przed sądem francuskim za naruszenie prawa francuskiego, ponieważ propagowanie i popieranie nazizmu w telewizji, radiu i na piśmie jest we Francji zabronione. Yahoo! Inc. broniła się, argumentując, że serwery, na których działa portal aukcyjny, fizycznie znajdują się w USA, a zatem nie można pozwolić, aby prawo francuskie miało zastosowanie do sprzętu i stron internetowych działających w Ameryce. Obrona argumentowała ponadto, że zawartość stron jest przeznaczona przede wszystkim dla mieszkańców USA, którym Pierwsza Poprawka do Konstytucji USA gwarantuje wolność słowa. Wszelkie działania zmierzające do usunięcia tych stron naruszałyby tę poprawkę.

LICRA zauważyła jednak, że jeśli Yahoo! Inc. prowadzi działalność we Francji, jest zobowiązana do przestrzegania tamtejszego prawa, a Internet nie jest tu wyjątkiem. Yahoo! Inc. odpowiedziała na ten argument, stwierdzając, że nie jest w stanie określić, skąd jej klienci wchodzą na portal aukcyjny. Dlatego usunięcie tej strony byłoby nie tylko naruszeniem Pierwszej Poprawki do Konstytucji USA, ale także uniemożliwiłoby dostęp do niej wszystkim użytkownikom, bez względu na granice państwowe. W ten sposób prawo francuskie stałoby się de facto prawem światowym. 22 maja 2000 r. sędzia Jean-Jacques Gomez wydał orzeczenie nakazujące firmie zablokowanie francuskim użytkownikom dostępu do amerykańskich serwisów aukcyjnych z pamiątkami po nazistach. Swoją decyzję uzasadnił m.in. tym, że Yahoo! Inc. może zidentyfikować użytkowników francuskich na tyle dobrze, aby umieszczać reklamy w języku francuskim w odwiedzanych przez nich witrynach. Sędzia przyznał Yahoo! Inc. 90 dni na zainstalowanie reklam na francuskich stronach Yahoo! Inc. system filtrowania oparty na słowach kluczowych. "*Sędzia Gomez stwierdził w swoim uzasadnieniu, że możliwe jest zablokowanie dostępu do stron internetowych objętych zarzutami nawet dziewięćdziesięciu procentom francuskich użytkowników. Rozwiązanie techniczne, jakie Yahoo! ma zaproponować po wydaniu orzeczenia, zostanie ocenione przez międzynarodowy zespół składający się z trzech członków. We wcześniejszych ustaleniach panelu stwierdzono, że możliwe jest odblokowanie do siedemdziesięciu procent użytkowników poprzez wskazanie ich dostawcy usług internetowych (ISP), a kolejnych dwadzieścia procent poprzez śledzenie słów kluczowych wpisywanych do wyszukiwarki na Yahoo!*" .[17]

Radca prawny Yahoo! Greg Wrenn z firmy Inc. powiedział: *"Za każdym razem, gdy na stronie upamiętniającej ofiary Holocaustu pojawi się słowo 'Hitler', strona zostanie automatycznie zamknięta. Nie można w ogóle mówić o skutecznej karze, ponieważ jest ona niemożliwa do wyegzekwowania".*

Ówczesne problemy techniczne polegały, a częściowo nadal polegają na tym, że można odfiltrować to, co można jednoznacznie zdefiniować (np. słowa takie jak Nazi, Heil Hitler itp.). Filtr nie jest jednak w stanie wykryć wszystkich możliwych wersji niepożądanego materiału (np. N_A_Z_I, H3Il HiT_L3R itp.). Różnice te mogą zostać rozpoznane przez osoby prywatne (np. pracowników danego dostawcy usług internetowych), które następnie usuwają stronę, ale operator forum lub aukcji glitch może po prostu zmienić adres i kontynuować swoją działalność.

Yahoo! Inc. zrezygnowała z odwołania się od orzeczenia francuskiego sądu i rozpoczęła blokowanie francuskich użytkowników na stronach oferujących treści niezgodne z prawem. Yahoo! Inc. zwróciła się jednak także do lokalnego sądu okręgowego USA[18] o wydanie deklaratywnego orzeczenia

---

[17] ŠTOČEK, Mediolan. *W duchu "Hitler przeciw Hitlerowi".* [online]. [cit.10.7.2016]. Dostępny pod adresem: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325

[18] Sąd Okręgowy Stanów Zjednoczonych dla Północnego Okręgu Kalifornii w San Jose

wykluczającego jurysdykcję sądu francuskiego nad spółką amerykańską. Sąd przyznał Yahoo! Inc. przychylił się do tego wniosku, uznając, że wykonanie francuskiego wyroku na terytorium USA jest niezgodne z konstytucją. Firma LICRA odwołała się od tego wyroku. W odpowiedzi Sąd Apelacyjny Stanów Zjednoczonych odmówił przyznania jurysdykcji w sprawie LICRA. W 2006 roku sprawa trafiła do Sądu Najwyższego Stanów Zjednoczonych[19] , który ostatecznie odmówił jej rozpatrzenia. Wyroki sądów amerykańskich były więc na ogół korzystne dla Yahoo! Inc., ale ta ostatnia dobrowolnie zdecydowała się usunąć ze swoich serwerów strony oferujące przedmioty o tematyce nazistowskiej, nie tylko we Francji.

Gutnick vs. Dow Jones

W 2000 r. Joseph Gutnick (australijski przedsiębiorca z branży diamentowej) przeczytał w internetowym wydaniu Barron's[20] artykuł na swój temat, który uznał za oszczerczy. Gutnick wniósł do australijskiego sądu pozew o zniesławienie przeciwko Dow Jones. Dow Jones użył podobnych argumentów jak Yahoo! Inc. w sporze z firmą LICRA. Argument ten opierał się głównie na fakcie, że drukowana wersja gazety była przeznaczona głównie na rynek amerykański, więc prawo australijskie nie mogło mieć zastosowania w tej sprawie.

Pomimo tej argumentacji, sąd australijski[21] orzekł w 2002 r.[22] w następujący sposób: *"ponieważ materiał (artykuł) jest dostępny również w Australii, miejscu, w którym biznesmen Gutnick jest najbardziej znany, zniesławienie może być dla niego najbardziej szkodliwe. Dow Jones jest zobowiązany do wypłaty odszkodowania na rzecz Gutnicka."* Sąd stwierdził, że nie będzie brał pod uwagę tego, czy Internet ma granice, czy też nie, i weźmie pod uwagę przede wszystkim to, gdzie treści są dostępne, a nie to, gdzie zostały zamieszczone. Sąd stwierdził również, że każdy ma prawo do ochrony prawnej przed podobnymi zachowaniami lub innymi atakami. W swoim wyroku sąd australijski zwrócił również uwagę na transgraniczny charakter Internetu, który odpowiada szerokiemu stosowaniu jurysdykcji.

GoDaddy

GoDaddy[23] jest głównym rejestratorem domen internetowych z siedzibą w USA. W 2016 r. zarządzała ponad 61 milionami domen internetowych, co czyni GoDaddy największym rejestratorem domen. Rejestracja domeny u tego dostawcy usług internetowych jest bardzo prosta i niedroga. Jednocześnie, dzięki lokalizacji firmy (USA), użytkownicy mają zapewnioną ochronę prawną swoich danych osobowych oraz danych umieszczonych na domenie zarejestrowanej w GoDaddy, o ile nie naruszają prawa amerykańskiego. Z tego powodu domeny zarejestrowane w GoDaddy są bardzo często wykorzystywane na przykład przez grupy lub użytkowników o poglądach ekstremistycznych, rasistowskich i innych. Użytkownicy ci powołują się następnie na amerykańskie prawo konstytucyjne i Pierwszą Poprawkę do Konstytucji USA:

"Kongres nie będzie stanowił ustaw dotyczących ustanawiania religii lub zabraniających swobodnego jej praktykowania, ograniczających wolność słowa, prasy lub prawo obywateli do spokojnego gromadzenia się i wnoszenia do rządu petycji w celu uzyskania zadośćuczynienia za doznane krzywdy".[24]

---

[19] Sąd Najwyższy Stanów Zjednoczonych
[20] http://online.barrons.com
[21] Sąd Najwyższy Australii
[22] Wyrok [2002] HCA 56 z 10 grudnia 2002, [online]. [cyt. 24.3.2014]. Dostępne od: http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html
[23] https://uk.godaddy.com/
[24] *Pierwsza poprawka.* [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://www.law.cornell.edu/constitution/first_amendment. Tłumaczenie autora

Problemem w postępowaniu z cyberprzestępczością o powyższej treści jest następnie udowodnienie realności zagrożenia lub przestępstwa, tak aby nie naruszało ono również Pierwszej Poprawki do Konstytucji.

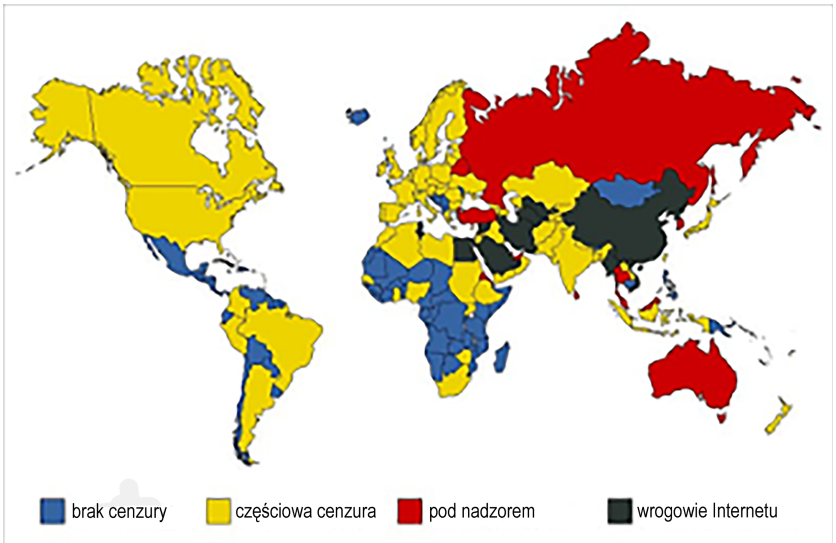
Second Life (i "dziecięce" porno).

Second Life to wirtualne środowisko 3D stworzone przez firmę Linden Lab. Środowisko to umożliwia tworzenie własnych awatarów, ich wzajemną interakcję, w tym generowanie zysków. Second Life jest podzielony na dwa wirtualne światy w zależności od wieku użytkownika.[25] Użytkownicy mogą zmieniać swoją tożsamość i modyfikować wygląd swojego awatara zgodnie z własnymi upodobaniami. W 2007 roku niemiecka stacja telewizyjna ARD, a następnie CNN zwróciły uwagę na istnienie "wyspy pedofilów". [26]

W raporcie podkreślono fakt, że niektórzy użytkownicy MainGrid (tj. użytkownicy powyżej 18 roku życia) tworzyli awatary w postaci dzieci, podczas gdy inni podawali się za dorosłych. Awatary dzieci były następnie maltretowane przez awatary dorosłych w ich wzajemnych interakcjach. Organy ścigania w Niemczech wszczęły dochodzenie, ponieważ zgodnie z niemieckim prawem karnym posiadanie wirtualnej pornografii dziecięcej jest przestępstwem.[27] Linden Lab udzieliło władzom niemieckim pomocy w ustaleniu tożsamości użytkowników i właścicieli wirtualnych stron, na których dochodziło do wirtualnej pornografii dziecięcej. W Republice Federalnej Niemiec i Zjednoczonym Królestwie przedmiotowe postępowanie było karalne, natomiast w Stanach Zjednoczonych nie.

Nie ma dziś na świecie państwa, które zrzekłoby się prawa do karania wykroczeń naruszających chronione przez nie interesy. Poza wymienionymi przypadkami istnieje wiele innych przykładów regulacji Internetu i usług internetowych przez organizacje lub państwa. Taka regulacja nieuchronnie wiąże się z problemami dotyczącymi stosowania i egzekwowania prawa.

Z przedstawionej mapy (patrz Rys. 1)[28] wynika, że większość krajów na świecie przyjęła instrumenty prawne, które mają wpływ na Internet lub świadczone przez niego usługi.



Rys. 1 - Rozkład krajów według cenzury Internetu

Z punktu widzenia użytkownika należy zauważyć, że zasada terytorialności traci na znaczeniu w kontekście Internetu, ponieważ w każdej chwili można być w dowolnym miejscu na świecie, a użytkownik nie musi wiedzieć, gdzie znajduje się serwer, z którym aktualnie się komunikuje. Z tego punktu widzenia Internet ma charakter globalny i nie zna granic.

[25] **MainGrid** - przeznaczony dla użytkowników w wieku 18 lat i starszych; **TeenGrid** - przeznaczony dla użytkowników w wieku od 13 do 18 lat.

[26] Więcej informacji *na ten temat można znaleźć w serwisie CNN na temat pedofilskiego seksu w Second Life.* [online]. [cyt. 18.6.2009]. Dostępny pod adresem: http://www.youtube.com/watch?v=AQM-SiiaipE

[27] *Pozew o "molestowanie dzieci" w Second Life.* [online]. [cyt. 2009, 16 czerwca]. Dostępne: http://news.bbc.co.uk/2/hi/technology/6638331.stm

[28] *Cenzura Internetu* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://www.deliveringdata.com/2010_10_01_archive.html

"O ile prawdą jest, że można prześledzić fizyczną lokalizację konkretnej informacji w dowolnym momencie - o tyle odpowiednia lokalizacja jest często przypadkowa, bardzo krótkotrwała i zazwyczaj zupełnie nieistotna dla samej informacji i jej skutków prawnych".[29]

Prawo powinno nadążać za światem wirtualnym, ale niestety nie zawsze tak się dzieje, ponieważ państwa (zamknięte na stałych terytoriach) często nie dysponują środkami umożliwiającymi skuteczne egzekwowanie prawa w cyberprzestrzeni.[30] Zasadniczo istnieją dwa możliwe rozwiązania tego problemu. Jedną z opcji jest przestrzeganie zasad terytorialności państw w ich obecnym kształcie. Takie podejście oznaczałoby de facto, że jeśli ktoś narusza prawa, których ochronę zagwarantowało państwo, trzeba czekać, aż napastnik znajdzie się w zasięgu fizycznej jurysdykcji państwa[31] , lub skorzystać z międzynarodowej pomocy prawnej.

Druga opcja polega na stworzeniu specjalnego systemu prawnego, tzw. jurysdykcji internetowej, który miałby zastosowanie do świata online. Pozostaje pytanie, jak to nowe prawo zostanie przyjęte przez poszczególne kraje. Osobiście uważam, że w obecnych warunkach nie jest możliwe globalne ujednolicenie wszystkich sektorów prawa (cywilnego, handlowego, karnego, administracyjnego itd.), w które w jakiś sposób ingeruje Internet. Swoje twierdzenie opieram m.in. na tym, że Konwencja o cyberprzestępczości, określająca podstawowe grupy przestępstw, które powinny być ścigane w cyberprzestrzeni, została przyjęta w 2001 r., ale na dzień 1 sierpnia 2016 r. ratyfikowało ją tylko 49 państw.

Ponadto, biorąc pod uwagę globalny charakter Internetu, wydaje się być problematyczne ustalenie:

1. **prawa właściwego** (prawa kraju, na podstawie którego zostanie rozstrzygnięty spór),
2. **organu uprawniony do wydawania decyzji**,
3. **organu, który może wyegzekwować lub bezpośrednio wykonać decyzję.**[32]

Oprócz klasycznych norm prawnych, *organy definiujące uczestniczą w* tworzeniu prawa lub zasad w Internecie poprzez tworzenie *norm definicyjnych*.

---

[29] POLČÁK, Radim. *Prawo w Internecie. Spam i odpowiedzialność dostawcy usług internetowych.* Brno: Computer Press, 2007, s. 7.

[30] Por. stwierdzenie w **Deklaracji niepodległości cyberprzestrzeni**.
Por. THOMAS, Douglas. *Przestępczość na granicy elektronicznej.* W Cyberprzestępczość. Londyn: Routledge, 2003, s. 17 i nast.
Por. JOHNSON, David R. i David POST. *Powstanie prawa w cyberprzestrzeni.* [online]. [cyt. 10.7.2016]. Dostępne z: http://poseidon01.ssrn.com/delivery.php?ID=797101088103069021099122095084084095061040041017050027018013071117008115007025117112101013061121056036119084118089028085067043023001058093120070084069085089012000019127120091078115090125017120030014000101095031109003094069069113114112102&EXT=pdf

[31] Przykładem takiego podejścia może być przypadek, w którym użytkownik z Republiki Czeskiej publicznie i wielokrotnie atakuje w Internecie jakieś państwo (np. za nieprzestrzeganie praw człowieka w tym kraju itp.) lub angażuje się w inne działania, które są nielegalne w tym państwie (ale nie są nielegalne w Republice Czeskiej). Jeśli kiedyś w przyszłości użytkownik zdecyduje się odwiedzić kraj, przeciwko któremu wystąpił w ten sposób, przy przekraczaniu granic tego państwa może powołać się na swoje prawa terytorialne.

[32] POLČÁK, Radim. *Prawo w Internecie. Spam i odpowiedzialność dostawcy usług internetowych.* Brno: Computer Press, 2007, s. 7.

PODSUMOWANIE ROZDZIAŁU

- Aby zrozumieć ustawy i rozporządzenia regulujące kwestie bezpieczeństwa cybernetycznego, konieczne jest poznanie przynajmniej podstawowych zasad prawa, jego podziału i wdrażania. W pierwszych dwóch rozdziałach przedstawiono jedynie ogólne ramy stosowania prawa w cyberprzestrzeni.
- Norma prawna to powszechnie obowiązująca reguła postępowania, która reguluje prawa i obowiązki podmiotów. Ta reguła postępowania jest wyrażona w określonej formie prawnej uznanej przez państwo (lub Unię), a jej przestrzeganie jest zapewnione przez przymus państwowy.
- Prawo jest jednym z jego możliwych regulatorów w postaci niedoskonałych konstrukcji normatywnych, gdzie bardziej niż gdzie indziej prawdziwe jest twierdzenie, że nie ma zgodności między rzeczywistością, czyli tym, co faktycznie realizuje się w środowisku internetowym, a normatywnością, czyli tym, co powinno być (z woli regulatora i naszej). Rzeczywistość Internetu i jego normatywna regulacja to zatem dwie stosunkowo odrębne kategorie. Założenie to nie zostanie zanegowane w niniejszej publikacji, wręcz przeciwnie, będzie jednym z jej filarów.
- Cyberprzestrzeń jest:
    - przestrzeń działań cybernetycznych lub jako przestrzeń tworzoną przez technologie informacyjne i komunikacyjne, która tworzy świat (lub przestrzeń) wirtualną jako paralelę do przestrzeni rzeczywistej.
    - środowisko cyfrowe umożliwiające tworzenie, przetwarzanie i wymianę informacji, składające się z systemów informatycznych oraz usług i sieci łączności elektronicznej.
    - przestrzeń jako przestrzeń składającą się z trzech warstw: fizycznej, logicznej i społecznej.
- Przykłady stosowania prawa w cyberprzestrzeni zostały przedstawione w poszczególnych studiach przypadków.

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

- prawo
- norma prawna
- cyberprzestrzeń

PYTANIA KONTROLNE

- Czym jest prawo?
- Co to jest norma prawna i jak się ją dzieli?
- Co to jest cyberprzestrzeń?

- Z jakich warstw składa się cyberprzestrzeń?
- Czy prawo obowiązuje w cyberprzestrzeni, a jeśli tak, to jakie normy prawne mają zastosowanie?
- W jaki sposób można stosować prawo w cyberprzestrzeni, w tym ewentualne sankcje i inne środki?
- Podaj kilka przykładów zastosowania prawa w cyberprzestrzeni.

3. Podstawa prawna działalności ISP (dostawcy usług internetowych)

Organy definiujące uczestniczą w tworzeniu prawa w Internecie, w ograniczaniu lub rozszerzaniu jego działalności, poprzez tworzenie *norm definicyjnych*. Aby zrozumieć kwestię potencjalnej odpowiedzialności dostawców usług społeczeństwa informacyjnego, muszę najpierw scharakteryzować normę definicyjną i organ definiujący.

Standardy definiowania są tworzone i wdrażane przez podmioty uprawnione do definiowania środowiska sieci informacyjnej. Są one de facto normami *sui generis,* które definiują sieci informacyjne jako takie. Występują one w warstwach, które są od siebie zależne. *"Standardy definiujące są tworzone przez operatorów telekomunikacyjnych, przez producentów oprogramowania biurowego, ale także np. przez twórców lub operatorów gier online, przez każdego, kto otwiera bloga lub ma skrzynkę pocztową (standardem definiującym tworzonym przez użytkownika tej skrzynki jest np. filtr, który automatycznie wykonuje określoną operację na skrzynce)".* [33]

Organy definiujące są twórcami norm definicyjnych; są podmiotami, które tworzą reguły systemu logicznego, w którym funkcjonuje dany autorytet. Jak wspomniano wcześniej, ICANN zajmuje uprzywilejowaną pozycję wśród tych organów, ponieważ jest organizacją odpowiedzialną za przydzielanie, administrowanie i ustalanie zasad funkcjonowania systemu nazw domen.[34] Innym organem definiującym jest na przykład IETF.[35] Chociaż organy definiujące mogą wydawać się nieograniczonymi zarządcami cyberprzestrzeni, nadal podlegają prawu danego państwa. [36]

Specyfika Internetu polega na tym, że **istnieje** on **tylko dzięki** organom **definiującym. Składa się z nich. Żadna operacja nie odbywa się bez udziału** (wykonania lub pośredniczenia w wykonaniu operacji) **organu definiującego.**

Lawrence Lessig w swojej książce Code and Other Laws of Cyberspace (Code v. 2) stwierdza: *"Możemy budować, projektować lub kodować*[37] *(programować) cyberprzestrzeń, aby chronić wartości, które uważamy za fundamentalne. Ale możemy też zaprojektować lub zaprogramować go tak, aby te wartości zniknęły. Nie ma środka, wszystko w cyberprzestrzeni jest w jakiś sposób zbudowane. My nigdy nie odkrywamy kodu, my go zawsze kształtujemy".*[38]

Kierując się powyższym stwierdzeniem i moim doświadczeniem z cyberprzestrzenią, zaryzykowałbym stwierdzenie, że największym **autorytetem definiującym,** nawet jeśli nie jest nim podmiot tworzący zasady działania systemu logicznego, **jest użytkownik jako taki.** Jego rola definicyjna działa w sposób zastępczy. Użytkownik usług świadczonych przez poszczególnych

---

[33] Por. POLČÁK, Radim. *Prawo w Internecie. Spam i odpowiedzialność dostawcy usług internetowych.* Brno: Computer Press, 2007, s. 42 i nast. oraz s. 88 i nast.
Do standardów definicyjnych można także włączyć **RFC** (*Request For Comments*). Chociaż dokumenty te są raczej zaleceniami niż normami, są one respektowane przez użytkowników tak, jakby były normami. Dokumenty RFC można bezpłatnie uzyskać pod adresem http://www.ietf.org/rfc.html.

[34] Nazwa domeny jest używana do oznaczenia "klasy" systemów komputerowych podłączonych do Internetu, które charakteryzują się pewną jednością geograficzną i organizacyjną: np. wszystkie komputery w domenie **.cz** znajdują się w Republice Czeskiej, wszystkie komputery w domenie (subdomenie) **nic.cz** są komputerami pod zarządem stowarzyszenia CZ.NIC. Nazwy głównych domen (ze względu na geografię) są ściśle podzielone.
Polčák stwierdza między innymi, że "nazwa domeny może być formą **wirtualnej rzeczywistości.** Jest to rekord w bazach danych DNS. **Jeśli władze domeny zdecydują się na usunięcie nazwy domeny, ta wirtualna rzeczywistość przestaje istnieć.** Nie ma znaczenia, czy nazwa domeny to np. www.tondovy_stranky.cz czy www.google.com.

[35] IETF - Grupa zadaniowa ds. inżynierii internetowej. Więcej informacji można znaleźć na stronie: https://www.ietf.org/

[36] Jest to zawsze osoba fizyczna lub prawna, która ma swoją siedzibę lub stałe miejsce zamieszkania. Dlatego prawo ma do nich zastosowanie tak samo jak do wszystkich innych podmiotów. W niektórych krajach (np. w **Chinach**) organem definiującym jest samo państwo.

[37] Lessig określa **standard definicyjny mianem kodu**.

[38] Por. LESSIG, Lawrence. *Code v. 2. s.* 6 Dostępny w wersji pełnej (angielski) [online]. [cyt. 13.3.2008]. Dostępny pod adresem: http://pdf.codev2.cc/Lessig-Codev2.pdf

dostawców usług internetowych bezpośrednio lub pośrednio wpływa na to, co się uda, a co nie uda w cyberprzestrzeni. Jeśli wystarczająco duża grupa użytkowników zdecyduje się na aktywne zaprzestanie korzystania z jednej z usług świadczonych przez dostawcę usług internetowych, usługa ta będzie zmuszona do zmiany swojego "zachowania" w oparciu o zapotrzebowanie użytkowników lub, w najgorszym przypadku, przestanie istnieć. Można się zastanawiać, jak duża grupa osób musiałaby przestać korzystać np. z usług Google, Microsoftu, Facebooka itd., aby nie było to dla tych firm marginalne, ale to właśnie w cyberprzestrzeni użytkownicy mają możliwość bezpośredniego wpływania na funkcjonowanie lub niefunkcjonowanie poszczególnych usług poprzez swoje aktywne działanie lub powstrzymywanie się od działania.

Można zatem wyciągnąć następujące wnioski:

- **Cyberprzestrzeń jest tworzona z woli organów definiujących.**
- **Wszyscy dostawcy usług społeczeństwa informacyjnego są organami definiującymi.**
- **Każdy usługodawca, tak jak każdy inny podmiot prawny, ponosi odpowiedzialność prawną za swoje działania.**

Celowo wspomniano tu o kwestii odpowiedzialności dostawców usług społeczeństwa informacyjnego (ISP) na mocy ustawy o niektórych usługach społeczeństwa informacyjnego, ponieważ jest ona bezpośrednio związana z problematyką cyberprzestępczości, odpowiedzialności użytkowników oraz identyfikacji i udostępniania informacji istotnych dla postępowania karnego. *"Zgodnie z ogólną zasadą, jeżeli informacja jest niezgodna z prawem, a dostawca usług internetowych nie miał wiedzy o jej stworzeniu lub przekazaniu, jest on zwolniony z odpowiedzialności na mocy ustawy*". [39]

Oprócz wyżej wymienionej ustawy, pojęcie usługodawcy zostało zdefiniowane na przykład w Konwencji o cyberprzestępczości, a konkretnie w art. 1 lit. c), który stanowi, że usługodawcą jest:

- każdy podmiot publiczny lub prywatny, który **umożliwia użytkownikom swoich usług komunikację za pośrednictwem systemu komputerowego,** oraz
- wszelkie inne podmioty, które **przetwarzają lub przechowują dane komputerowe na potrzeby takiej usługi komunikacyjnej lub użytkowników takiej usługi.**

3.1 Regulacje dotyczące dostawców usług internetowych w Republice Czeskiej

Podstawową normą prawną charakteryzującą działalność dostawców usług internetowych w Republice Czeskiej jest ustawa nr 480/2004 Dz.U. o niektórych usługach społeczeństwa informacyjnego[40] . Niniejsza ustawa stanowi wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego.[41]

Czeska ustawa o niektórych usługach społeczeństwa informacyjnego uznaje następujących trzech usługodawców, stwierdzając, że usługodawcą jest każda osoba fizyczna lub prawna, która świadczy którąkolwiek z następujących usług społeczeństwa informacyjnego: [42]

1. Zwykła przepustka lub dostawca dostępu.

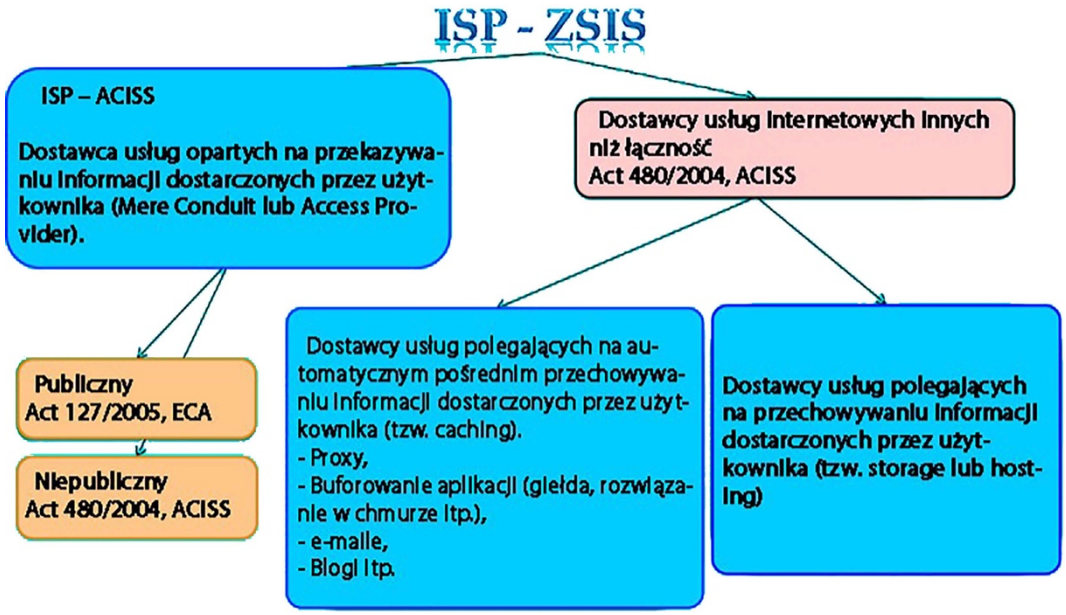
---

[39] POLČÁK, Radim. *Prawo w Internecie. Spam i odpowiedzialność dostawcy usług internetowych.* Brno: Computer Press, 2007, s. 55.
[40] zwana dalej ustawą o niektórych usługach społeczeństwa informacyjnego lub CISA
[41] Dostępny w Internecie: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535&qid=1624364501265
[42] Zob. § 2 lit. d) umowy ISA.

2. **Dostawcy usług polegających na automatycznym przechowywaniu informacji dostarczonych przez użytkownika** (tzw. cache).
3. **Usługodawcy świadczący usługi polegające na przechowywaniu informacji dostarczonych przez użytkownika** (tzw. przechowywanie lub hosting).

Żadna osoba nie jest wyłączona z powyższej definicji (np. nie musi to być osoba działająca na podstawie innego przepisu prawnego) jednak, jeśli dostawca podlega innym specjalnym przepisom (patrz np. jeden z dostawców usług przyłączeniowych), musi również ich przestrzegać.

Graficznie można przedstawić tych dostawców (oraz powiązanie poszczególnych przepisów prawnych) w następujący sposób:



Odbiorcą usługi społeczeństwa informacyjnego jest użytkownik, którym może być każda osoba fizyczna lub prawna, która korzysta z usługi społeczeństwa informacyjnego, w szczególności w celu znalezienia informacji lub uzyskania do niej dostępu.[43]

Zgodnie z ustawą o niektórych usługach społeczeństwa informacyjnego**, usługa społeczeństwa informacyjnego** oznacza *"każdą usługę świadczoną drogą elektroniczną na indywidualne żądanie użytkownika złożone drogą elektroniczną, zwykle świadczoną odpłatnie". Usługa jest świadczona drogą elektroniczną, jeżeli jest przesyłana za pośrednictwem sieci łączności elektronicznej i pobierana przez użytkownika z elektronicznego urządzenia do przechowywania danych."* [44]

Definicja w ustawodawstwie czeskim opiera się bezpośrednio na dyrektywie Parlamentu Europejskiego i Rady (UE) 2015/1535 (art. 1 lit. b)), która stanowi, że usługa to *"każda usługa społeczeństwa informacyjnego, tj. każda usługa świadczona, co do zasady, **za wynagrodzeniem, na odległość, drogą elektroniczną** i **na indywidualne żądanie usługobiorcy**".*

Z tej definicji wyłaniają się cztery podstawowe cechy usługi:

- jest przekazywana drogą elektroniczną,
- jest udostępniana na indywidualne życzenie użytkownika,
- jest zwykle udostępniana odpłatnie,

[43] Zob. § 2 lit. e) umowy ISA.
[44] § 2 lit. a) umowy ISA

- jest świadczona zdalnie.

Pojęcie świadczenia drogą **elektroniczną** zostało określone w dyrektywie Parlamentu Europejskiego i Rady (UE) 2015/1535 w art. 1 lit. b) ppkt (ii), który definiuje je jako usługę, która jest wysyłana z miejsca pochodzenia i odbierana w miejscu przeznaczenia za pomocą sprzętu do elektronicznego przetwarzania (w tym kompresji cyfrowej) i przechowywania danych. Usługa jako całość jest wysyłana, nadawana lub odbierana za pomocą środków przewodowych, radiowych, optycznych lub innych środków elektromagnetycznych. W rozporządzeniu czeskim zastosowano wykaz przykładowy, zgodnie z którym pojęcie to obejmuje w szczególności sieci łączności elektronicznej, urządzenia łączności elektronicznej, automatyczne systemy wybierania numerów i systemy łączności, końcowe urządzenia telekomunikacyjne i pocztę elektroniczną. [45]

Indywidualny wniosek użytkownika oznacza, że musi to być aktywne działanie ze strony użytkownika. Husovec stwierdza, że dzieje się tak na przykład wtedy, gdy użytkownik sam wpisuje adres w polu przeglądarki (IE, Firefox, Chrome itd.), formułując w ten sposób żądanie otwarcia odpowiedniej strony, lub pisze wiadomość SMS. Według Husoveca typowym przykładem usługi, która jest świadczona bez indywidualnego wniosku, jest na przykład transmisja telewizyjna.[46]

Najbardziej problematycznym kryterium definicji usługi społeczeństwa informacyjnego jest to, że jest ona **świadczona odpłatnie**. Również w tej kwestii rozporządzenie czeskie powiela regulacje międzynarodowe i zawiera zapis *"zwykle za wynagrodzeniem".* W środowisku Internetu lub innych sieci komputerowych istnieje wiele usług, które są świadczone "bezpłatnie". Husovec całkiem słusznie twierdzi, że pojęcie wynagrodzenia może być rozumiane jako obejmujące cały szereg rzeczy innych niż tylko świadczenia pieniężne.[47] Może to być świadczenie niepieniężne, w ramach którego dostawca usług internetowych uzyskuje informacje o użytkownikach w postaci danych osobowych, technicznych i innych, czasu korzystania z usługi, ofert reklamowania innych produktów użytkownikowi itp. Jednak zdaniem Husoveca warunek ten należy interpretować szerzej, w sensie prowadzenia działalności *potencjalnie gospodarczej.*[48]

Ze względu na fakt, że pod pojęciem "wynagrodzenie" można rozumieć różne opcje (np. podziękowanie, odwiedzenie strony internetowej lub linku, korzyści finansowe lub inne), a także ze względu na brzmienie ustawy o niektórych usługach społeczeństwa informacyjnego (zob. "*ogólnie* o wynagrodzeniu″), można stwierdzić, że działalność podmiotu świadczącego usługi społeczeństwa informacyjnego może być również prowadzona nieodpłatnie.

Termin **odległość** został zdefiniowany w dyrektywie Parlamentu Europejskiego i Rady (UE) 2015/1535 jako usługa, która jest świadczona bez jednoczesnej obecności stron.[49]

W swojej monografii Husovec podaje przykłady, które pokazują, co można uznać za usługę społeczeństwa informacyjnego. Zgodnie z dyrektywą 2000/31/WE Parlamentu Europejskiego i Rady terminem tym należy objąć szeroki zakres działań, które mają miejsce w świecie online. Mogą one obejmować sprzedaż towarów przez Internet, usługi zapewniające dostęp do informacji przez Internet, komunikację handlową lub usługi zapewniające narzędzia do wyszukiwania, dostępu i pobierania danych, usługi zapewniające przesyłanie informacji przez sieć komunikacyjną itp.

[45] Zob. § 2 lit. c) umowy ISA.
[46] Więcej informacji na ten temat można znaleźć w publikacji HUSOVEC, Martin. *Odpowiedzialność w Internecie w świetle prawa czeskiego i słowackiego*. Praga: CZ.NIC, 2014, s. 100.
[47] Tamże, zob. s. 98.
[48] Tamże, s. 99.
[49] Zob. art. 1 lit. b) ppkt (i) niniejszej dyrektywy.

"*Orzecznictwo TSUE uznało już, bezpośrednio lub pośrednio, na przykład AdWords (usługę reklamową wyszukiwarki Google)*[50] *, internetową usługę ubezpieczeń komunikacyjnych*[51] *, internetową sprzedaż soczewek kontaktowych*[52] *, łączenie się z Internetem*[53] *, rezerwację hotelu za pośrednictwem poczty elektronicznej*[54] *, rezerwację biura podróży za pośrednictwem poczty elektronicznej*[55] *, serwis aukcyjny eBay*[56] *oraz tradycyjne wyszukiwanie Google".* [57]

3.1.1 Dostawcy usług w zakresie przekazywania informacji dostarczonych przez użytkownika (zwykły kanał lub dostawca dostępu)

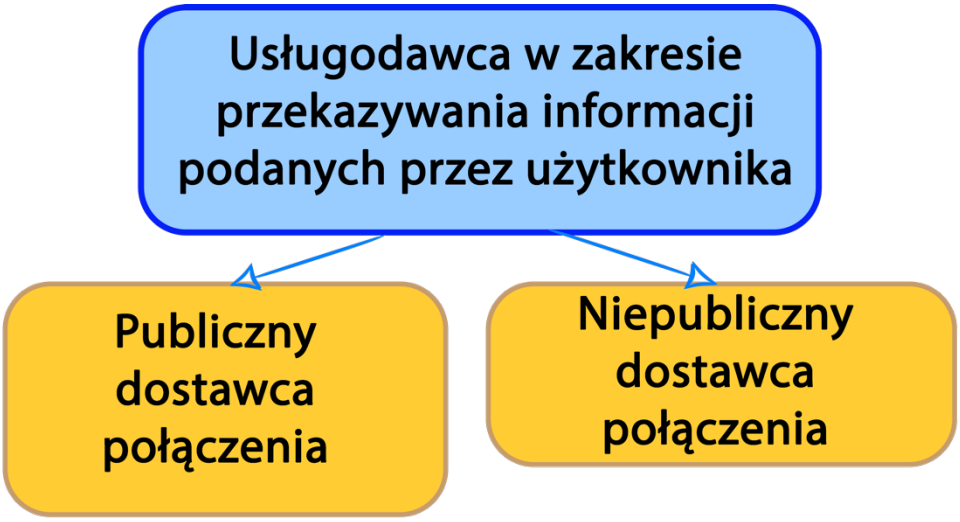
Z punktu widzenia ustawy o niektórych usługach społeczeństwa informacyjnego takim usługodawcą może być każda osoba fizyczna lub prawna, która jest w stanie świadczyć innym podmiotom (osobom fizycznym lub prawnym) usługi polegające na przesyłaniu informacji (dostarczonych przez użytkownika) za pośrednictwem sieci łączności elektronicznej lub na pośredniczeniu w dostępie do sieci łączności elektronicznej w celu przesyłania informacji.

Takim dostawcą będą nie tylko osoby prowadzące działalność polegającą na podłączaniu innych osób do sieci komputerowych lub Internetu (zazwyczaj są to osoby wpisane do *rejestru przedsiębiorców łączności elektronicznej na podstawie zezwolenia ogólnego*)[58] , ale każda osoba dostarczająca lub ułatwiająca przesyłanie informacji za pośrednictwem sieci łączności elektronicznej. W związku z tym można sobie wyobrazić, że osoba, która ustanawia i udostępnia innym osobom na przykład połączenie WiFi w restauracji, budynku mieszkalnym, gospodarstwie domowym itp. będzie również dostawcą połączenia w rozumieniu niniejszej ustawy. W tej kategorii znajdą się również np. szkoły (zazwyczaj uczelnie zapewniające swoim studentom i nauczycielom łączność w ramach swojej sieci lub z Internetem). Jednak usługą polegającą na przekazywaniu informacji jest również np. Skype, ICQ itp. Bardzo upraszczając, można określić tych dostawców jako **dostawców usług łączności.**

Jednak pod względem określania indywidualnych praw i obowiązków dostawców usług przyłączeniowych należy ich podzielić na dwie grupy: dostawców **publicznych i niepublicznych.** Obie grupy dostawców połączeń objęte są Ustawą o niektórych usługach społeczeństwa informacyjnego, ale publiczni dostawcy połączeń objęci są również Ustawą o łączności elektronicznej, która określa dodatkowe prawa i obowiązki tych dostawców. W ustaleniu, czy dany usługodawca należy do którejś z tych grup, pomaga wspomniany wyżej *Rejestr Przedsiębiorców Komunikacji Elektronicznej na podstawie zezwolenia ogólnego,* prowadzony przez Czeski Urząd Telekomunikacyjny.

---

[50] Decyzja *Google France* C-236/08 do C-238/08.
[51] Decyzja *Bundesverband* C-298/07.
[52] Decyzja *Ker-Optika* C-108/09.
[53] Decyzja *Promusicae* C-275/06 i *Tele 2*. C-557/07
[54] Decyzja *Alpenhof* C-144/09.
[55] Decyzja *Pammer* C-585/08.
[56] *L'Oreal przeciwko Ebay,* decyzja 324/09.
[57] HUSOVEC, Martin. *Odpowiedzialność w Internecie w świetle prawa czeskiego i słowackiego*. Praga: CZ.NIC, 2014. ISBN: 978-80-90-904248-8-3, s. 101-102.
[58] Baza danych przedsiębiorstw łączności elektronicznej posiadających ogólne zezwolenie jest dostępna w Internecie: https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni



3.1.1.1 Prawa i obowiązki dostawcy usług związane z przekazywaniem informacji dostarczonych przez użytkownika zgodnie z ZSIS

W przypadku dostawcy połączenia ustawa o niektórych usługach społeczeństwa informacyjnego ogranicza w możliwie największym stopniu odpowiedzialność tego podmiotu za przekazywane informacje. Szczególne wymagania i warunki obowiązują jednak operatorów świadczących usługi łączności elektronicznej. Warunki te zostały określone w ustawie o łączności elektronicznej. Artykuł 12 dyrektywy 2000/31/WE umożliwia państwom członkowskim nakazanie dostawcy zaprzestania świadczenia usług, za pośrednictwem których przekazywane są informacje bezprawnie naruszające prawa innych osób. Możliwość ta jest jednym ze sposobów zapobiegania naruszeniom prawa. Nakaz zaprzestania świadczenia usług jest zazwyczaj wydawany przez sąd.

Dostawca **połączenia może ponosić odpowiedzialność za treść informacji tylko wtedy,** gdy:

- inicjuje samą transmisję,
- wybiera użytkownika przesyłanych informacji **lub**
- wybiera lub modyfikuje treść przesyłanych informacji. [59]

Zgodnie z art. 6 ISA, **dostawca połączenia nie jest zobowiązany do** monitorowania treści przekazywanych informacji ani do aktywnego badania nielegalności przekazywanych informacji. Dostawca nie może ponosić odpowiedzialności za jakość informacji (której nie można mu przypisać), nawet jeśli jest świadomy nielegalności przekazywanych informacji.[60]

3.1.1.2 Prawa i obowiązki usługodawcy związane z przekazywaniem informacji dostarczonych przez użytkownika zgodnie z ustawą nr 127/2005.

Dostawców łączy publicznych reguluje również ustawa nr 127/2005 o łączności elektronicznej[61]. Niniejsza ustawa definiuje pewne pojęcia, które są używane poniżej. Dla celów niniejszej monografii są to:

[59] Te trzy możliwości powodują, że dostawca połączenia jest de facto odpowiedzialny tylko wtedy, gdy to on sam aktywnie przesyła lub w inny sposób manipuluje przesyłanymi informacjami.
[60] Por. art. 12 dyrektywy 2000/31/WE oraz art. 3 ust. 1 i 2 ustawy nr 480/2004 Dz.
[61] zwana dalej ZoEK

- **Usługi łączności elektronicznej** [§ 2(n) ustawy ZoEK[62]]. Zgodnie z paragrafem 2(n) ZoEK, termin ten oznacza usługę, która jest zwykle świadczona za wynagrodzeniem i polega (całkowicie lub głównie) na przesyłaniu sygnałów za pośrednictwem sieci łączności elektronicznej. Usługa ta nie obejmuje usług oferowania treści za pośrednictwem sieci i usług łączności elektronicznej ani sprawowania kontroli redakcyjnej nad treściami przesyłanymi za pośrednictwem sieci i świadczonymi w ramach usług łączności elektronicznej. Ponadto usługi społeczeństwa informacyjnego, które nie polegają w całości lub głównie na przesyłaniu sygnałów za pośrednictwem sieci łączności elektronicznej, nie są takimi usługami.
- **Publicznie dostępna usługa łączności elektronicznej** (§ 2(o) ZoEK). Usługa ta jest usługą komunikacji elektronicznej, z której korzystania nikt nie jest z góry wykluczony.

  Brak wyłączenia oznacza możliwość zawarcia umowy z przedsiębiorstwem świadczącym publicznie dostępne usługi łączności elektronicznej. Istotne jest, aby ta usługa była otwarta dla szerokiego grona osób, z których żadna nie jest z góry wykluczona. Przeciwieństwem takiej usługi może być np. przynależność do różnych stowarzyszeń, izb lub np. status ucznia szkoły.
- **Przedsiębiorstwo,** które udostępnia lub jest upoważnione do udostępniania publicznej sieci łączności lub urządzeń towarzyszących, jest określane w niniejszej ustawie mianem **operatora** (§ 2 lit. e) ZoEK).
- **Abonentem** [§ 2 (a) ZoEK] jest każdy, kto zawarł umowę z przedsiębiorstwem świadczącym publicznie dostępne usługi łączności elektronicznej o świadczenie takich usług. **Użytkownikiem** [§ 2(n) ZoEK] jest każdy, kto korzysta z publicznie dostępnych usług łączności elektronicznej lub żąda ich świadczenia.

Ustawa o łączności elektronicznej wprowadziła, na podstawie Dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. *w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności* **oraz** *zmieniającej dyrektywę 2002/58/WE*[63] , obowiązek prewencyjnego zatrzymywania **danych o ruchu i lokalizacji**[64] dotyczących wykonywanej łączności elektronicznej. Obowiązek ten dotyczy wyłącznie przedsiębiorstw, które udostępniają lub są upoważnione do udostępniania publicznej sieci łączności lub urządzeń towarzyszących.

Celem dyrektywy w sprawie zatrzymywania danych było **ujednolicenie przepisów państw członkowskich dotyczących obowiązku dostawców publicznie dostępnych usług łączności elektronicznej lub publicznych sieci łączności do** zatrzymywania danych o ruchu i lokalizacji, tak aby można je było udostępniać właściwym organom państw członkowskich w celu **zapobiegania poważnym przestępstwom, takim jak terroryzm i przestępczość zorganizowana, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania.**

---

[62] zwana dalej ZoEK

[63] Zwana dalej dyrektywą w sprawie **zatrzymywania danych.** Termin "zatrzymywanie danych" oznacza ogólne przechowywanie danych o ruchu i lokalizacji przez dostawców połączeń (w Republice Czeskiej przez dostawców na mocy ustawy o łączności elektronicznej).

[64] Zob. § 97 (4) ZoEK.

Dane operacyjne i lokalizacyjne to w szczególności dane pozwalające **na śledzenie i identyfikację źródła i adresata komunikacji, a** także **dane pozwalające na określenie daty, godziny, sposobu i czasu trwania komunikacji**.

Zakres danych operacyjnych i dotyczących lokalizacji, formę i sposób ich przekazywania organom uprawnionym do ich wykorzystywania zgodnie ze specjalnym przepisem prawnym (zob. § 97 ust. 3 ZoEK) oraz sposób ich usuwania określają przepisy wykonawcze. Rozporządzeniem wykonawczym jest **dekret nr 357/2012 Coll. w sprawie przechowywania, przekazywania i usuwania danych o ruchu i lokalizacji.**

Zakres dyrektywy został określony w obszarze danych operacyjnych i lokalizacyjnych dotyczących osób prawnych i fizycznych oraz powiązanych danych niezbędnych do identyfikacji abonenta lub zarejestrowanego użytkownika.

Dyrektywa ta nie miała zastosowania do treści komunikatów elektronicznych ani do informacji wymaganych podczas korzystania z sieci łączności elektronicznej.

Na mocy dyrektywy **państwa członkowskie były zobowiązane do zapewnienia, by dane telekomunikacyjne były zatrzymywane przez co najmniej sześć miesięcy i maksymalnie dwa lata od daty połączenia.** Dyrektywa została w różnej formie transponowana do prawa państw członkowskich UE. Jednak od samego początku istnienia dyrektywy dochodziło do sprzecznych opinii na jej temat. Respondenci twierdzili, że dyrektywa w nieproporcjonalny sposób ingeruje w podstawowe prawa i wolności człowieka, w szczególności poprzez faktyczne nakazanie powszechnego gromadzenia informacji o poszczególnych użytkownikach. Twierdzono ponadto, że dyrektywa (w tak ogólnej formie) nie będzie w stanie przejść testu proporcjonalności.

Test proporcjonalności jest standardowym narzędziem prawnym stosowanym zarówno przez sądy międzynarodowe, jak i sądy konstytucyjne (krajowe), gdy ocenie podlega konflikt między przepisem porządku prawnego, mającym na celu ochronę konstytucyjnie gwarantowanego prawa lub interesu publicznego, a innym podstawowym prawem lub wolnością. Test proporcjonalności obejmuje trzy kryteria oceny dopuszczalności interwencji:

1. **Zasada adekwatności** (przydatności do celu), zgodnie z którą dany **środek musi być w stanie osiągnąć zamierzony cel, którym** jest ochrona innego prawa podstawowego lub dobra publicznego.
2. **Zasada konieczności***, zgodnie z* którą **dozwolone jest użycie tylko takiego środka, który jest najłagodniejszy do osiągnięcia zamierzonego celu** (ingerencji w podstawowe prawa i wolności), **spośród kilku możliwych.**
3. **Zasada proporcjonalności** (w węższym znaczeniu), zgodnie z którą **szkoda wyrządzona prawu podstawowemu nie może być nieproporcjonalna w stosunku do zamierzonego celu, tzn.** środki ograniczające podstawowe prawa i wolności człowieka nie mogą - w przypadku konfliktu między prawem podstawowym lub wolnością a interesem publicznym - przewyższać pozytywnych skutków interesu publicznego takich środków.

Dyrektywa w sprawie zatrzymywania danych lub jej krajowa transpozycja były przedmiotem sporów konstytucyjnych w kilku krajach UE, zwłaszcza w sądach konstytucyjnych Rumunii (2009), Niemiec (2010) i Czech (2011). Skupię się na orzeczeniach sądów w Niemczech i Republice Czeskiej.

Federalny Trybunał Konstytucyjny Niemiec, który zajmował się konfliktem między wolnością a bezpieczeństwem (na podstawie dyrektywy w sprawie zatrzymywania danych) i orzekł na korzyść wolności jednostki. W dniu 2 marca 2010 r. sąd orzekł, że masowe zatrzymywanie danych o połączeniach telefonicznych i transmisji danych jest w Niemczech niezgodne z konstytucją.

Sąd odpowiedział na skargę zbiorową 35 000 obywateli, którzy domagali się uchylenia ustawy z 2008 roku, nakazującej firmom telekomunikacyjnym archiwizowanie przez sześć miesięcy zapisów rozmów telefonicznych i wiadomości e-mail na użytek organów śledczych. Federalny Trybunał Konstytucyjny uznał zaskarżone przepisy za niezgodne z konstytucją. Stwierdził ponadto, że choć obowiązek zatrzymywania danych w określonym zakresie nie jest od początku całkowicie niezgodny z konstytucją, to brakuje regulacji ustawowej odpowiadającej zasadzie proporcjonalności. Zdaniem Trybunału, zaskarżone przepisy nie spełniały konstytucyjnych wymogów bezpieczeństwa danych, cel wykorzystania danych (oraz przejrzystość wykorzystania danych) nie był jasno określony, a ochrona prawna nie była zapewniona w wystarczającym stopniu.

Trybunał stwierdził, że *"korzystanie przez obywateli z podstawowych praw i wolności (w tym przypadku z tajemnicy wiadomości przekazywanych za pomocą środków komunikacji elektronicznej) nie może być całkowicie monitorowane, dokumentowane i rejestrowane przez państwo; należy to do konstytucyjnej i prawnej tożsamości Republiki Federalnej Niemiec, którą Republika musi starać się zachować w kontekście europejskim i międzynarodowym".*[65]

W Republice Czeskiej dyrektywa w sprawie zatrzymywania danych została wdrożona przed jej wejściem w życie w UE (Dyrektywa została wdrożona w UE 15 marca 2007 r., a wymóg transpozycji został spełniony do 15 września 2007 r.). W Republice Czeskiej został on wprowadzony do § 97/3 ZOEK, z mocą obowiązującą od 1 maja 2005 r. Również w Czechach została złożona skarga konstytucyjna przez stowarzyszenie Iuricum Remedium, popierane przez grupę 51 posłów. Skarga ta została złożona w Trybunale Konstytucyjnym w marcu 2010 roku. W 2011 roku Trybunał Konstytucyjny wydał orzeczenie i w pełni uwzględnił wniosek o całkowite uchylenie odpowiednich fragmentów ustawy o łączności elektronicznej (mianowicie art. 97 ust. 3 i 4) oraz dekretu wykonawczego nr 485/2005 Coll. w sprawie zakresu danych o ruchu i lokalizacji, a także o uchylenie przepisów kodeksu postępowania karnego.[66] Trybunał wyraził swoją opinię w następujący sposób: *"Trybunał Konstytucyjny stwierdza, że zaskarżone przepisy naruszają granice konstytucyjne, ponieważ nie spełniają wymogów wynikających z zasady państwa prawnego i pozostają w sprzeczności z wymogami ograniczenia podstawowego prawa do prywatności w postaci prawa do samostanowienia informacyjnego w rozumieniu art. 10 ust. 3 i art. 13 Karty, które wynikają z zasady proporcjonalności."*

Ustawodawcy w Republice Czeskiej zareagowali na zastrzeżenia Trybunału Konstytucyjnego Republiki Czeskiej i przyjęto **nowe przepisy,** które nadal zezwalają na powszechne zatrzymywanie danych o ruchu i lokalizacji w Republice Czeskiej, ponieważ **są zgodne z wcześniej** wspomnianym **testem proporcjonalności, w** szczególności dzięki wyraźnemu określeniu zakresu podmiotów (uprawnionych do żądania danych o ruchu i lokalizacji) oraz celu, w jakim można żądać tych danych.

Jednocześnie podjęto środki mające na celu zobowiązanie przedsiębiorstw na mocy ustawy o łączności elektronicznej do przyjęcia zasad zapewniających, że dane o ruchu i lokalizacji mają taką samą jakość i podlegają takiemu samemu zabezpieczeniu i ochronie przed nieuprawnionym dostępem, zmianą, zniszczeniem, utratą lub kradzieżą albo innym nieuprawnionym przetwarzaniem lub wykorzystaniem, jak dane zgodnie z art. 88 ustawy o WE. [67]

Określono również **maksymalny okres przechowywania tych danych, który obecnie wynosi 6 miesięcy.** Po upływie tego okresu osoba prawna lub fizyczna przechowująca dane o ruchu i lokalizacji jest zobowiązana do ich zniszczenia, chyba że zostały one przekazane organom uprawnionym do ich wykorzystania na podstawie specjalnych przepisów prawnych lub jeśli prawo nie stanowi inaczej (§ 90 ZoEK). Ponadto wprowadzono **obowiązek zapewnienia, że treść wiadomości nie jest**

---

[65] *Niemiecki Federalny Trybunał Konstytucyjny odrzuca ustawę o retencji danych* [online]. [cyt. 16.7.2016]. Dostępny pod adresem: https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/
Por. dalej np:
Krajowe wyzwania prawne wobec dyrektywy w sprawie zatrzymywania danych. [online]. [cyt. 16.7.2016]. Dostępny pod adresem: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html
Zatrzymywanie danych w obecnej formie jest niezgodne z konstytucją. [online]. [cyt. 16.7.2016]. Dostępny pod adresem: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690
Niemiecki Bundestag uchwala nowe prawo o retencji danych. [online]. [cyt. 16.7.2016]. Dostępny pod adresem: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/

[66] Zob. orzeczenie Trybunału Konstytucyjnego Pl. ÚS ÚS 41/11 z 22 marca 2011 r. *Gromadzenie i wykorzystywanie danych o ruchu i lokalizacji w ruchu telekomunikacyjnym [*online]. [cyt. 24 sierpnia 2016]. Dostępny pod adresem: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=69635&pos=1&cnt=4&typ=result

[67] Więcej szczegółów w § 88a ZOEK

zatrzymywana podczas przechowywania danych o ruchu i lokalizacji oraz że takie przechowywane dane nie są przekazywane dalej (§ 97 ust. 3 ZoEK).

Jednocześnie zasada subsydiarności została podkreślona w Kodeksie postępowania karnego (zob. Sekcja 88 i 88a, Ust. No. 141/1961 o postępowaniu przed sądem karnym: "*jeżeli zamierzony cel nie może być osiągnięty w inny sposób lub jeżeli jego osiągnięcie byłoby znacznie trudniejsze*"). Gwarancja minimalnej ingerencji w podstawowe prawa człowieka w tych przypadkach jest zapewniona między innymi przez fakt, że nakaz udostępnienia danych o ruchu i lokalizacji jest wydawany przez sędziego na wniosek prokuratora.

Kto jest uprawniony do żądania udostępnienia danych operacyjnych i lokalizacyjnych w Republice Czeskiej i na jakich warunkach? Zgodnie z § 97 ust. 3 ustawy ZoEK osoba prawna lub fizyczna posiadająca dane o ruchu i lokalizacji jest zobowiązana do niezwłocznego ich udostępnienia na żądanie:

a) **organów ścigania** do celów i na warunkach określonych w przepisach szczególnych[68] ,

b) **Policji Republiki Czeskiej w** celu rozpoczęcia **poszukiwań konkretnej osoby poszukiwanej lub zaginionej**, **ustalenia tożsamości osoby o nieznanej tożsamości lub tożsamości znalezionych zwłok, zapobiegania lub wykrywania konkretnych zagrożeń w dziedzinie terroryzmu lub prowadzenia dochodzenia w sprawie osoby chronionej** oraz zgodnie z warunkami określonymi w specjalnym przepisie prawnym[69] ,

c) **Służbie Informacji Bezpieczeństwa w** celach i na warunkach określonych w przepisach szczególnych[70] ,

d) **Wywiadowi wojskowemu** do celów i na warunkach określonych w specjalnych przepisach[71],

e) **Czeskiemu Bankowi Narodowemu w** celach i na warunkach określonych w specjalnej regulacji prawnej[61)72] .

Następnie, w ramach Unii Europejskiej, TSUE (w dniu 8 kwietnia 2014 r.), w nawiązaniu do wcześniejszej opinii[73] rzecznika generalnego Pedro Cruz Villalón, wydał wyrok[74] **unieważniający odpowiednią dyrektywę w sprawie zatrzymywania danych (2006/24/WE).**

> *"Dzisiejszym wyrokiem Trybunał Sprawiedliwości stwierdza, że dyrektywa jest nieważna".*
>
> *"Ponieważ Trybunał Sprawiedliwości nie ograniczył skutków wyroku w czasie, stwierdzenie nieważności obowiązuje od dnia wejścia w życie dyrektywy".*

---

[68] Ustawa nr 141/1961 Zb. o postępowaniu karnym (Kodeks postępowania karnego), z późniejszymi zmianami.

[69] Ustawa nr 273/2008 Dz.U. o policji Republiki Czeskiej, z późniejszymi zmianami.
Ustawa nr 137/2001 Zb. o szczególnej ochronie świadków i innych osób w związku z postępowaniem karnym oraz o zmianach w ustawie nr 99/1963 Zb., Kodeks postępowania cywilnego, z późniejszymi zmianami.

[70] § 6 do 8 ustawy nr 154/1994 Sb. o Służbie Informacji Bezpieczeństwa, z późniejszymi zmianami.

[71] § Sekcje 9 i 10 ustawy nr 289/2005 Coll. o wywiadzie wojskowym.

[72] Ustawa nr 15/1998 Sb. o nadzorze nad rynkiem kapitałowym oraz o zmianach i uzupełnieniach innych ustaw, z późniejszymi zmianami.

[73] Opinia rzecznika generalnego Pedra Cruza Villalóna. Sprawy C-293/12 i C-594/12 [online]. [cyt. 15.7.2016]. Dostępny pod adresem: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

[74] Trybunał Sprawiedliwości Unii Europejskiej. Komunikat prasowy nr 54/14, 8 kwietnia 2014 r. **Wyrok w sprawach połączonych C-293/12 i C-594/12 [**online]. [cyt. 15.7.2016]. Dostępny pod adresem: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf

W szczególności TSUE skrytykował fakt, że "*prawodawca UE, przyjmując dyrektywę w sprawie zatrzymywania danych o ruchu, przekroczył granice wyznaczone przez wymóg przestrzegania zasady proporcjonalności".*

Decyzja o utrzymaniu lub uchyleniu istniejących przepisów dotyczących zatrzymywania danych o ruchu i lokalizacji w państwach członkowskich UE należy wyłącznie do zainteresowanych organów krajowych, a sama Unia nie zamierza zalecać ani udzielać żadnych wskazówek co do sposobu postępowania. [75]

Jak poradzić sobie z powszechnym przechowywaniem danych o ruchu i lokalizacji? Osobiście uważam, że w cyberprzestrzeni nie ma innej możliwości rekonstrukcji zdarzeń, które miały miejsce w przeszłości, niż poprzez przechowywanie danych o ruchu i lokalizacji. W rzeczywistości cyberprzestrzeń i technologie informacyjno-komunikacyjne, które pozwalają na bardzo szybkie zmiany topologii sieci, usług itp. oraz technologie umożliwiające uzyskanie kilku różnych tożsamości w ciągu kilku sekund, nie dopuszczają żadnej innej możliwości.

Zdaję sobie sprawę, że powszechne zatrzymywanie danych o ruchu i lokalizacji narusza moje podstawowe prawa i wolności, ale akceptując koncepcję umowy społecznej i rezygnując z części moich praw i wolności na rzecz organu (w tym przypadku państwa), który ma zapewnić ochronę moich praw, właściwie nie mam wyboru. Uważam, że jeśli chcemy skutecznie prowadzić dochodzenia i ścigać cyberprzestępczość, cyberataki i inne negatywne zjawiska zachodzące w cyberprzestrzeni, nie możemy się obyć bez tego narzędzia. Pytanie, którym powinniśmy się zająć, nie powinno brzmieć: *"Jak ograniczyć gromadzenie danych i danych o osobach w cyberprzestrzeni (ponieważ dzieje się to na zupełnie innych poziomach), a tym samym ograniczyć możliwości państwa w zakresie przeciwdziałania negatywnym zjawiskom w cyberprzestrzeni? "*Pytania, które są całkowicie uzasadnione i którymi należy się zająć, brzmią: "*Jak ustalić zasady, kto powinien mieć dostęp do tych danych i na jakich warunkach, co się dzieje z tymi danymi, do jakich celów można je wykorzystać itd.".*

Osobiście uważam, że takie dane powinny być przechowywane nie tylko przez publicznych dostawców usług internetowych, ale przez wszystkich dostawców usług internetowych, którzy świadczą usługi. Mam kilka powodów, dla których tak twierdzę.

Po pierwsze, uważam, że usługi inne niż te, które polegają na zapewnieniu łączności, stanowią i będą stanowić większość usług w cyberprzestrzeni. W ten sposób użytkownik przestaje się interesować tym, kto i jak go łączy, a interesuje się przede wszystkim usługami, które mogą mieć na przykład formę wirtualnych połączeń z różnymi środowiskami wirtualnymi. Dlatego ważne będzie nie samo fizyczne połączenie, ale wzajemne powiązanie usług.

Drugim powodem jest fakt, że obecnie dostawcy tych usług w przeważającej mierze przechowują nie tylko dane operacyjne i dane dotyczące lokalizacji, ale także cały szereg innych danych, na których przechowywanie pozwalają im użytkownicy na podstawie warunków umowy zawartej między dostawcą usług internetowych a użytkownikiem końcowym.

Ostatnim powodem jest ochrona własna dostawcy usług internetowych przed użytkownikami. Dostawca usług musi przestrzegać prawa i w jego najlepszym interesie jest zatrzymywanie danych, które mogą go zwolnić z odpowiedzialności za np. szkody lub inne krzywdy.

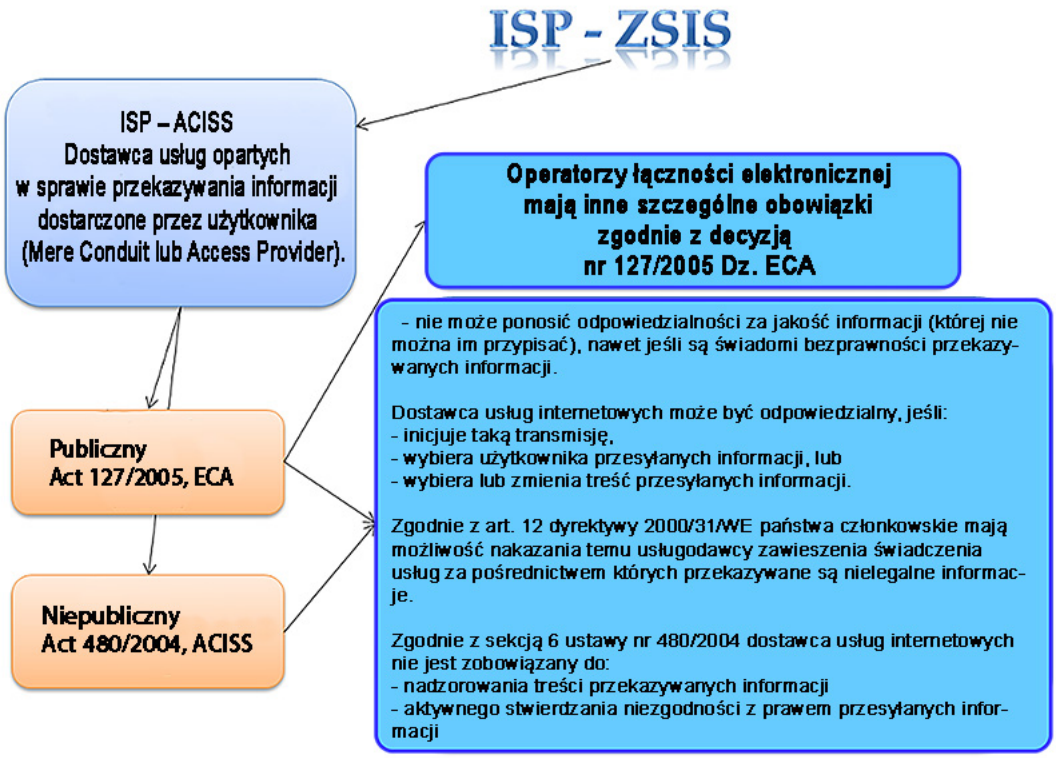
Rzecznik generalny[76] wypowiedział się ostatnio na temat zatrzymywania danych o ruchu i lokalizacji, stwierdzając, że zatrzymywanie danych jest w wielu przypadkach jedynym skutecznym narzędziem

---

[75] PETERKA, Jiří. *UE nie wymaga już od nas przechowywania danych o ruchu i lokalizacji. Ale nadal to robimy.* [online]. [cyt. 2015-11-10]. Dostępny pod adresem: http://www.earchiv.cz/b14/b0428001.php3

[76] Opinia rzecznika generalnego SAUGMANDSGAARDA ØE z dnia 19.7.2016 r. W sprawach połączonych C-203/15 i C-698/15 [online]. [cyt. 10.8.2016]. Dostępny pod adresem:

przeciwdziałania zagrożeniom dla bezpieczeństwa i poważnym przestępstwom. Jednocześnie sformułował wymogi dotyczące proporcjonalnego wdrożenia tej zasady w systemach prawnych państw członkowskich.



Graficzne przedstawienie rozmieszczenia dostawców usług przyłączeniowych oraz niektórych ich praw i obowiązków

3.1.2 Dostawcy usług polegających na automatycznym buforowaniu informacji dostarczanych przez użytkownika (tzw. caching).

Buforowanie polega na przesyłaniu informacji, podczas którego są one automatycznie tymczasowo przechowywane. Następnie informacje te są przekazywane usługobiorcy na jego prośbę.

"Buforowanie jest zasadniczo specjalną adaptacją zwykłego przekaźnika, ponieważ obejmuje również przesyłanie przejściowych informacji przechowywanych między magazynami. Jedyna różnica, w której buforowanie może wykraczać poza zakres szeroko rozumianej zwykłej usługi polega na tym, że przechowywanie podczas transmisji odbywa się przez "okres dłuższy niż rozsądnie konieczny do transmisji".[77]

Husovec bardzo zwięźle opisuje również usługi buforowania na przykładzie serwera proxy lub buforowania przeglądarki, które przyspieszają ładowanie stron internetowych. Odbiorcą usługi jest właściciel strony internetowej czasopisma (tzw. główny odbiorca), którego obrazy są przechowywane przez dostawcę usługi buforowania na komputerze znajdującym się bliżej geograficznie (np. w Europie), dzięki czemu nie musi on stale korzystać z komputera, na którym przechowywana jest oryginalna strona internetowa (np. w Afryce), co przyspiesza ogólne ładowanie strony (w Europie). Użytkownik, który odwiedza stronę internetową i jest kolejnym odbiorcą usługi (tzw. odbiorca

http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

[77] zob. HUSOVEC, Martin. *Odpowiedzialność w Internecie w świetle prawa czeskiego i słowackiego*. Praga: CZ.NIC, 2014, s. 133.

wtórny), otrzymuje w ten sposób obraz ze swojego komputera na podstawie indywidualnego żądania skierowanego do dostawcy usługi buforowania i nie jest zmuszony do "podróży" do pierwotnego komputera. [78]

Dostawcy usług buforowania nie są zwolnieni z odpowiedzialności za jakość informacji, jeśli z ich strony dojdzie do naruszenia standardowych lub uzgodnionych warunków technicznych dotyczących buforowania.[79]

Dostawca usługi buforowania ponosi odpowiedzialność na mocy sekcji 4 ISA, jeśli:

a) zmienia treść informacji,

b) nie spełnia warunków dostępu do informacji,

c) nie jest zgodna z zasadami aktualizacji informacji, które są ogólnie przyjęte i stosowane w danej branży,

d) wykracza poza dozwolone użycie technologii ogólnie przyjętej i stosowanej w danej branży w celu uzyskania informacji o danych użytkowych, lub

e) nie podejmuje natychmiastowych działań w celu usunięcia lub uniemożliwienia dostępu do przechowywanych przez siebie informacji, gdy dowie się, że informacje zostały usunięte lub uniemożliwione z sieci w początkowym punkcie transmisji lub gdy sąd nakazał usunięcie lub uniemożliwienie dostępu do informacji.

Dostawca usługi buforowania nie jest zobowiązany do aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną treść informacji ani do nadzorowania treści przekazywanych lub przechowywanych przez niego informacji.

3.1.3 Usługodawcy świadczący usługi polegające na przechowywaniu informacji dostarczonych przez Użytkownika (tzw. storage lub hosting)

Udostępnianie pamięci masowej lub hostingu oznacza udostępnianie pamięci masowej (miejsca) użytkownikowi w celu umieszczenia w niej danych. Przechowywanie informacji lub danych, w przeciwieństwie do zwykłego buforowania, jest nie tylko tymczasowe. Usługi hostingowe mogą obejmować:

a) Hosting WWW (Active 24, Ignum, Zoner itp.)

b) Pamięć masową w chmurze umożliwiającą przechowywanie dowolnych plików i danych (Dropbox, iCloud, Microsoft OneDrive, ownCloud itp.)

c) Przechowywanie plików (Rapidshare, DropBox itp.)

d) Przechowywanie filmów wideo (YouTube itp.)

e) Przechowywanie plików audio (iTunes itp.)

f) Internetowe serwisy aukcyjne (eBay itp.)

g) Blogi, fora, czaty itp.

h) Sieci społecznościowe (Facebook, Twitter itp.).

---

[78] Tamże, s. 133.

[79] Por. art. 13 dyrektywy 2000/31/WE oraz rozdział 4 rozporządzenia w sprawie ISA.
Por. POLČÁK, Radim. *Prawo w Internecie. Spam i odpowiedzialność dostawcy usług internetowych.* Brno: Computer Press, 2007, s. 58.

Powyższa lista nie jest wyczerpująca, w ramach hostingu można świadczyć szereg innych usług.

W przypadku dostawców usług hostingowych najbardziej złożona jest sytuacja związana z ich potencjalną odpowiedzialnością prawną.[80] Również w tym przypadku opiera się to na postanowieniach dyrektywy 2000/31/WE, której zalecenia ustawodawca czeski włączył do rozdziału 5 ustawy ISA. W przepisie tym występuje warunek co najmniej nieświadomego zaniedbania[81] usługodawcy w związku z nielegalną zawartością przechowywanych u niego informacji. **Ustawodawca nie nakłada** jednak **na dostawców obowiązku aktywnego wyszukiwania nielegalnych informacji wśród użytkowników serwisu**[82] (ponieważ w wielu przypadkach stanowiłoby to faktyczną ingerencję w podstawowe prawa i wolności gwarantowane przez Kartę - np. art. 13) ani nadzorowania treści przekazywanych lub przechowywanych informacji.

Podmiot świadczący usługi hostingowe ponosi odpowiedzialność zgodnie z art. 5 ust. 1 ISA, jeżeli:

a) ***mógł on wiedzieć, biorąc pod uwagę przedmiot swojej działalności oraz okoliczności i charakter sprawy, że treść przechowywanych informacji lub działania użytkownika są niezgodne z prawem,*** *lub*

b) ***jeżeli dowiedział się o bezprawnym charakterze treści przechowywanych informacji lub o bezprawnym postępowaniu użytkownika*** *i nie podjął niezwłocznie wszelkich kroków, jakich można od niego wymagać w celu usunięcia lub udostępnienia takich informacji*.

Dostawca usług hostingowych jest zawsze odpowiedzialny za treść przechowywanych informacji, jeśli wywierają one decydujący wpływ na działania użytkownika, bezpośrednio lub pośrednio.[83]

Na potrzeby niniejszej monografii wybrano tylko niektóre aspekty odnoszące się do dostawców usług społeczeństwa informacyjnego, zwłaszcza w odniesieniu do przydatności informacji w wykrywaniu i ściganiu cyberprzestępstw i cyberataków.

3.2 Regulacje dotyczące dostawców usług internetowych w Polsce

W Polsce reguluje to ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. Nr 144, poz. 1204), która znacznie ogranicza przypadki, w których dostawca usług internetowych może zostać pociągnięty do odpowiedzialności:
Art. 12. 1. Usługodawca świadczący usługi drogą elektroniczną, w tym polegające na transmisji danych przekazywanych przez usługobiorcę w sieci telekomunikacyjnej lub zapewnieniu dostępu do sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne, nie ponosi odpowiedzialności za treść tych danych, jeżeli:
1) nie jest inicjatorem transferu danych;
2) nie wybiera odbiorcy transferu danych;
3) nie wybiera ani nie modyfikuje informacji zawartych w wiadomości.
2. Wyłączenie odpowiedzialności, o którym mowa w ust. 1, obejmuje również automatyczne i krótkotrwałe pośrednie przechowywanie przekazywanych danych, jeżeli czynność ta służy wyłącznie do przekazania danych, a dane nie są przechowywane dłużej niż jest to zwykle konieczne do ich przekazania.
Art. 13. 1. Osoba, która przekazuje dane i zapewnia automatyczne i krótkoterminowe pośrednie przechowywanie tych danych w celu przyspieszenia ponownego dostępu do nich na podstawie art. 1 na wniosek innego podmiotu:
1) nie modyfikuje danych;

[80] Por. art. 14 dyrektywy 2000/31/WE i sekcja 5 porozumienia ISA.
[81] Por. art. 16 ust. 1 lit. b) TZK.
[82] Por. art. 15 dyrektywy 2000/31/WE oraz rozdział 6 rozporządzenia w sprawie ISA.
[83] § 5 ust. 2 ISA

2) wykorzystuje techniki informatyczne uznane i zwykle stosowane w tego typu działalności, które określają parametry techniczne dostępu do danych i ich aktualizacji, oraz
3) nie koliduje z wykorzystaniem technik informatycznych uznanych i zwykle stosowanych w tego typu działalności w zakresie gromadzenia informacji o wykorzystaniu zebranych danych.
2. Osoba, która na warunkach określonych w ust. 1 niezwłocznie usunie dane lub uniemożliwi dostęp do przechowywanych danych, gdy otrzyma wiadomość, że dane zostały usunięte z pierwotnego źródła transmisji lub dostęp do nich został uniemożliwiony, lub gdy sąd lub inny właściwy organ nakazał usunięcie danych lub uniemożliwienie dostępu do nich. Art. 14. 1. Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę, nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych.
2. Usługodawca, który otrzymał urzędowe zawiadomienie o bezprawnym charakterze przechowywanych danych przekazanych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie odpowiada wobec tego usługobiorcy za szkody powstałe w wyniku uniemożliwienia dostępu do tych danych.
3. Usługodawca, który uzyskał wiarygodną informację o bezprawnym charakterze przechowywanych danych przekazanych przez usługobiorcę i uniemożliwił dostęp do tych danych, nie odpowiada wobec tego usługobiorcy za szkodę wynikłą z uniemożliwienia dostępu do tych danych, jeżeli niezwłocznie powiadomił usługobiorcę o zamiarze uniemożliwienia dostępu do nich.
4. Przepisów ust. 1-3 nie stosuje się, jeżeli usługodawca przejął kontrolę nad usługobiorcą w rozumieniu przepisów o ochronie konkurencji i konsumentów.
Artykuł 15. Podmiot, który świadczy usługi, o których mowa w art. 12-14, nie jest obowiązany do sprawdzania przekazywanych, przechowywanych lub udostępnianych przez niego danych, o których mowa w art. 1. 12-14

3.4 Możliwości odpowiedzialności prawnej użytkownika za działania w cyberprzestrzeni

Wielu użytkowników systemów informacyjnych i komunikacyjnych nie zdaje sobie sprawy z potencjalnej odpowiedzialności za niewłaściwe korzystanie z tych technologii.[84] Systemy informacyjne i komunikacyjne są rzeczami, a ci, którzy z nich korzystają, są zobowiązani do postępowania w **taki sposób, aby uniknąć nieuzasadnionej szkody dla wolności, życia, zdrowia lub mienia innych osób.**[85]

Jeśli **krzywdziciel wyrządzi szkodę poszkodowanemu, naruszając umyślnie dobre obyczaje, jest zobowiązany do jej naprawienia;** jeśli jednak skorzysta ze swojego prawa, krzywdziciel jest zobowiązany do naprawienia szkody tylko wtedy, gdy jego głównym celem było wyrządzenie szkody drugiemu człowiekowi.[86]

Z tego dictum kodeksu cywilnego wynika więc wyraźnie zarówno obowiązek właściwego zarządzania systemami teleinformatycznymi, jak i obowiązek zapobiegania szkodom, które mogłyby powstać w

[84] W tej części tekstu wykorzystano tezy, które zostały częściowo opublikowane w artykule: Odpowiedzialność za własne urządzenie oraz przechowywane w nim dane i aplikacje. W: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14).* [B.m.], c2014, s. 321 - 324. recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.
[85] § 2900 KK
[86] § 2909 i nast. kk

wyniku ich działalności (w tym korzystania z technologii teleinformatycznych w środowisku internetowym).

Wielu zwykłych użytkowników lekceważy ochronę i bezpieczeństwo zasobów TIK, którymi dysponują, czy to przez zaniedbanie, czy celowo.

Określenie rodzaju winy w postępowaniu użytkownika końcowego ma decydujące znaczenie dla ewentualnej odpowiedzialności cywilnej lub karnej. Stwierdzenie to można udowodnić na przykładzie trzech przykładów z praktyki.

Użytkownik komputera osobistego korzystał z nielegalnej kopii systemu operacyjnego Windows 7 i celowo nie aktualizował systemu. Użytkownik świadomie instalował na komputerze programy, które umożliwiały osobom trzecim manipulowanie komputerem bez jego dalszej współpracy.

Celem opisanego powyżej działania użytkownika było zwolnienie się z ewentualnej odpowiedzialności karnej za atak przeprowadzony przez inną osobę przy użyciu tak przygotowanego komputera (np. komputer ten celowo wchodzi w skład botnetu).

W praktyce można spotkać napastników, którzy opierają swoją obronę na fakcie, że nie byli osobą, która przeprowadziła konkretny atak za pośrednictwem danego komputera.

Moim zdaniem, nie jest możliwe powołanie się na to, że dana osoba nie jest bezpośrednim napastnikiem i nie spowodowała swoim działaniem konkretnego ataku, a raczej nie jest możliwe całkowite zaakceptowanie tego twierdzenia.

Z perspektywy prawa karnego można by rozważyć przynajmniej zastosowanie instytucji współudziału i zasady pomocnictwa[87] , ponieważ zachowanie osoby, która umożliwiła lub ułatwiła innej osobie popełnienie przestępstwa (w szczególności **przez dostarczenie środków**, **usunięcie przeszkód,** zwabienie ofiary na miejsce przestępstwa, pilnowanie przestępstwa, doradzanie, zachęcanie lub obiecywanie pomocy po popełnieniu przestępstwa), można objąć przepisami dotyczącymi pomocnictwa.[88] Środki w tym przypadku obejmowałyby udostępnienie systemu komputerowego lub jego części w celu popełnienia przestępstwa umyślnego.

Jeśli udowodniony zostanie wyższy poziom bezpośredniego udziału użytkownika w bezprawnym działaniu innej osoby, użytkownik taki może zostać uznany za współwinnego[89] przestępstwa. Czynnikiem decydującym byłby stopień świadomości wykorzystania danego komputera do czynu zabronionego oraz świadomość, że działanie to może naruszyć lub zagrozić interesom chronionym przez prawo karne.[90]

Z punktu widzenia prawa cywilnego działania takiego użytkownika mogłyby być objęte art. 2909 kodeksu cywilnego lub można by zastosować art. 2915 kodeksu cywilnego, który reguluje przypadek, gdy szkoda jest wyrządzona przez kilka osób. Przepis ten stanowi, że: *"jeżeli kilka osób jest zobowiązanych do odszkodowania, są one zobowiązane solidarnie do naprawienia szkody; jeżeli jedna z osób jest zobowiązana na podstawie innego prawa do odszkodowania tylko do pewnej wysokości, jest ona zobowiązana solidarnie z innymi osobami do naprawienia szkody w tym zakresie".* ***Dotyczy to również sytuacji, gdy kilka osób popełniło odrębne czyny bezprawne, z których każdy mógł spowodować szkodliwe następstwa z prawdopodobieństwem bliskim pewności, i gdy nie można***

[87] Jest to zasada uzależnienia odpowiedzialności karnej i karalności uczestnika (zob. art. 24 kodeksu karnego) od odpowiedzialności karnej i karalności głównego sprawcy (zob. art. 22 kodeksu karnego), pod warunkiem że główny sprawca co najmniej usiłował popełnić przestępstwo, w którym uczestniczył uczestnik.
[88] Pod warunkiem uzyskania zgody uczestnika i głównego sprawcy. Patrz § 24 ust. 1 lit. c) TZK
[89] Patrz § 23 TZK
[90] Patrz paragraf 15 ust. 1 lit. b) TZK

ustalić, która osoba spowodowała szkodę. "*Moim zdaniem* drugie zdanie sekcji 2915(1) KK można bardzo dobrze zastosować do opisanego powyżej przypadku.

Użytkownik komputera osobistego korzystał z nielegalnej kopii systemu operacyjnego Windows 7 i celowo nie aktualizował systemu. Zainstalował on na swoim komputerze szereg gier i innych aplikacji, które naruszały prawa autorskie, w szczególności poprzez obchodzenie lub tłumienie elementów ochrony praw autorskich oraz poprzez wykorzystanie keygenów lub cracków[91] *, które zawierały złośliwe oprogramowanie pochodzące od innych atakujących. Użytkownik nie był świadomy, że jego komputer jest używany przez innych użytkowników.*

W praktyce jest to najczęstszy przypadek nadużycia komputera bez wiedzy jego uprawnionego użytkownika, nawet jeśli ten ostatni swoim bezprawnym zachowaniem (w szczególności naruszeniem praw autorskich) lub zwykłą nieznajomością techniki komputerowej spowodował sytuację, w której jego komputer jest nadużywany do atakowania osób trzecich.

Z punktu widzenia prawa karnego instytucja współuczestnictwa i zasada pomocnictwa nie mogą być zastosowane w tym przypadku, ponieważ zachowanie osoby, która umożliwiła lub ułatwiła popełnienie przestępstwa przez inną osobę, nie było umyślne, a zatem nie miało na celu udzielenia pomocy głównemu sprawcy przestępstwa.

Z punktu widzenia zawinienia do użytkownika zaatakowanego w ten sposób komputera można by zastosować przepisy dotyczące zaniedbania bez wiedzy, ponieważ sprawca nie wiedział, że jego działania mogą spowodować naruszenie lub narażenie na niebezpieczeństwo dobra chronionego prawem karnym, chociaż powinien i mógł o tym wiedzieć, biorąc pod uwagę okoliczności i jego sytuację osobistą.[92]

Ponieważ Kodeks karny nie zawiera przestępstwa zaniedbania z paragrafu 230 Kodeksu karnego: *nieuprawniony dostęp do systemu komputerowego i nośnika informacji*, w tym konkretnym przypadku nie będzie możliwe skorzystanie z instytucji prawa karnego.

Z punktu widzenia prawa cywilnego zachowanie takiego użytkownika można by objąć paragrafem 2912(1) kodeksu cywilnego: *"Jeżeli sprawca nie postępuje tak, jak można by tego oczekiwać od osoby o przeciętnym charakterze w życiu prywatnym, uważa się, że dopuścił się zaniedbania".* W tym kontekście należy przypomnieć, że osoba, która wyrządziła szkodę (szkodnik), jest zobowiązana do jej naprawienia, niezależnie od swojej winy, w przypadkach wyraźnie przewidzianych przez prawo.[93]

Użytkownik odpowiednio "dbał" o swój komputer (ma legalne oprogramowanie, aktualizuje je na bieżąco itp.) i rozsądnie go zabezpieczył (stosuje ochronę i kontrolę antywirusową, antyspamową i antymalware), a mimo to komputer ten został zaatakowany z zewnątrz (np. włączony do botnetu), a następnie użyty do ataku na inny.

Uważam, że w tym przypadku, z punktu widzenia zawinienia, nawet przepisy dotyczące zaniedbania bez wiedzy nie mogłyby być zastosowane wobec użytkownika zaatakowanego w ten sposób komputera. Wobec aktywnej postawy użytkownika nie wchodzi również w rachubę zastosowanie paragrafu 232 Kodeksu karnego: *Uszkodzenie zapisu w systemie komputerowym i na nośniku informacji oraz nieumyślna ingerencja w sprzęt komputerowy,* ponieważ przepis ten wymaga rażącego

[91] Obejmują one ingerencję w programy przez inne osoby w celu ich zmodyfikowania dla łatwiejszego wykonania (keygens), osłabienia ochrony programu, aby uniemożliwić jego kopiowanie lub wykonanie na wcześniej określonych warunkach (cracks), oraz dalsze przerabianie tych programów w celu późniejszego wykorzystania lub rozpowszechniania wśród innych osób.
[92] Patrz § 16 ust. 1 lit. b) TZK
[93] Patrz § 2895 kk

niedbalstwa.[94]

Moim zdaniem, z punktu widzenia prawa cywilnego, zachowanie takiego użytkownika nie może być objęte wspomnianą wyżej sekcją 2912(1) KK, ponieważ w tym przypadku użytkownik działał tak, jak można było od niego wymagać. Należy to jednak rozumieć szerzej, ponieważ jeśli użytkownik dowie się, że jego zasoby teleinformatyczne są wykorzystywane do bezprawnego atakowania innych osób, ma obowiązek bez zbędnej zwłoki zgłosić ten fakt osobie, której może to zaszkodzić[95] , i ostrzec ją o możliwych konsekwencjach. Jeżeli poszkodowany wywiąże się z obowiązku powiadomienia, nie przysługuje mu prawo do odszkodowania za szkodę, której można było zapobiec po powiadomieniu.[96]

W konkretnym przypadku zawsze będą miały znaczenie wszystkie okoliczności sprawy i tylko sąd jest uprawniony do określenia obowiązku wypłaty odszkodowania.

Z drugiej strony, jeśli użytkownik nie "dba" o komputer (tj. nie zabezpiecza go, nie przeprowadza konserwacji itp.), a następnie jest on niewłaściwie wykorzystywany, realne jest, że sąd w postępowaniu o naprawienie szkody nałoży na takiego użytkownika obowiązek częściowego lub całkowitego (np. wykorzystana zostanie moc obliczeniowa jednego centrum danych) naprawienia szkody wyrządzonej poszkodowanemu przez komputer użytkownika.

---

[94] Patrz paragraf 16(2) kodeksu karnego: *"Przestępstwo karne jest popełnione przez rażące niedbalstwo, jeśli stosunek sprawcy do wymogu należytej staranności wskazuje na oczywistą lekkomyślność sprawcy wobec interesów chronionych przez prawo karne".*

[95] Pytanie brzmi, czy taką osobę można realistycznie zidentyfikować w danym momencie (momencie ataku).

[96] Zob. § 2092 kk

PODSUMOWANIE ROZDZIAŁU

- Organy definiujące uczestniczą w tworzeniu prawa w Internecie, w ograniczaniu lub rozszerzaniu jego działalności, poprzez tworzenie norm definicyjnych.
- Standardy definiowania są tworzone i wdrażane przez podmioty uprawnione do definiowania środowiska sieci informacyjnej. Są one de facto normami *sui generis,* które definiują sieci informacyjne jako takie. Występują one w warstwach, które są od siebie zależne. *"Standardy definiujące są tworzone przez operatorów telekomunikacyjnych, przez producentów oprogramowania biurowego, ale także np. przez twórców lub operatorów gier online, przez każdego, kto otwiera bloga lub ma skrzynkę pocztową (standardem definiującym tworzonym przez użytkownika tej skrzynki jest np. filtr, który automatycznie wykonuje określoną operację na skrzynce)".*
- Autorytety definiujące są twórcami norm definicyjnych; są podmiotami, które tworzą reguły systemu logicznego, w którym funkcjonuje dany autorytet. Jak wspomniano wcześniej, ICANN zajmuje uprzywilejowaną pozycję wśród tych organów, ponieważ jest organizacją odpowiedzialną za przydzielanie, administrowanie i ustalanie zasad funkcjonowania systemu nazw domen. Innym organem definiującym jest na przykład IETF. Mimo że organy definiujące mogą wydawać się nieograniczonymi administratorami cyberprzestrzeni, nadal podlegają prawu danego państwa.
- Internet istnieje właśnie dzięki autorytetom definicyjnym. Składa się z nich. Żadna operacja nie odbywa się bez udziału (wykonania lub pośredniczenia w wykonaniu operacji) organu definiującego.
- Cyberprzestrzeń jest tworzona z woli władz definiujących.
- Wszyscy dostawcy usług społeczeństwa informacyjnego są organami definiującymi.
- Każdy usługodawca, tak jak każdy inny podmiot prawny, ponosi odpowiedzialność prawną za swoje działania.
- Termin dostawca usług internetowych został również zdefiniowany w konwencji o cyberprzestępczości, a konkretnie w art. 1 lit. c), który stanowi, że dostawca usług to:
    - każdy podmiot publiczny lub prywatny, który umożliwia użytkownikom swoich usług komunikację za pośrednictwem systemu komputerowego, oraz
    - wszelkie inne podmioty, które przetwarzają lub przechowują dane komputerowe na potrzeby takiej usługi komunikacyjnej lub użytkowników takiej usługi.
- Czeska ustawa o niektórych usługach społeczeństwa informacyjnego uznaje następujących trzech usługodawców, stwierdzając, że usługodawcą jest każda osoba fizyczna lub prawna, która świadczy którąkolwiek z następujących usług społeczeństwa informacyjnego: [97]
    - Zwykła przepustka lub dostawca dostępu.
    - Dostawcy usług polegających na automatycznym przechowywaniu informacji dostarczonych przez użytkownika (tzw. cache).
    - Usługodawcy świadczący usługi polegające na przechowywaniu informacji dostarczonych przez użytkownika (tzw. przechowywanie lub hosting).

[97] Zob. § 2 lit. d) umowy ISA.

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

- DOSTAWCA USŁUG INTERNETOWYCH
- Organ definiujący
- Norma definicyjna
- Zwykły przewód lub dostawca dostępu
- Dostawca usług kasowych
- Dostawca usług hostingowych
- Przechowywanie danych

PYTANIA KONTROLNE

- Zdefiniuj pojęcie dostawcy usług internetowych.
- Jak podzieleni są dostawcy usług internetowych? Według jakich kryteriów?
- Jakie obowiązki mają dostawcy usług internetowych?
- Co to jest norma definicyjna?
- Kto jest organem definiującym i jaka jest jego rola?
- Co to jest retencja danych?

4. Cyberbezpieczeństwo i jego regulacje prawne

Wysiłki zmierzające do rozwiązania problemu cyberbezpieczeństwa można zaobserwować de facto od początku stosowania technologii informacyjno-komunikacyjnych. Stopniowo przyjmowano zalecenia, standardy i normy techniczne w tej dziedzinie, które zwykle określały minimalne wymagania gwarantujące pewien poziom bezpieczeństwa.

Istnieje wiele powodów, dla których warto przyjąć i wdrożyć zasady bezpieczeństwa cybernetycznego. Najczęstsze z nich to na przykład negatywne skutki ekonomiczne w przypadku udanego ataku cybernetycznego, podczas którego skradzione zostaną dane wrażliwe. Udany atak cybernetyczny może również zagrozić własnym operacjom i funkcjonowaniu organizacji, ponieważ dostęp do systemów komputerowych lub danych może być ograniczony np. przez oprogramowanie typu ransomware. Innym powodem wprowadzenia cyberbezpieczeństwa może być także utrata wiarygodności zaatakowanej organizacji itp.

Ostatnim, ale nie mniej ważnym powodem wdrażania bezpieczeństwa cybernetycznego jest przestrzeganie przepisów prawnych oraz wynikających z nich praw i obowiązków. Dla wielu podmiotów ten powód legislacyjny wynika z ustawy o bezpieczeństwie cybernetycznym, ale błędem jest zakładanie, że jest to jedyna norma prawna odnosząca się do kwestii bezpieczeństwa cybernetycznego.

Szczególnie w ostatnich latach nastąpił znaczny wzrost liczby aktów prawnych, głównie międzynarodowych, które koncentrują się na działaniach podmiotów (osób fizycznych, prawnych, państw i innych organizacji) w cyberprzestrzeni.

Dziedzina bezpieczeństwa cybernetycznego bardzo różni się od innych obszarów, w których standardowe zasady bezpieczeństwa są stosowane w świecie rzeczywistym. Różnica ta polega przede wszystkim na możliwości dynamicznego rozwoju i natychmiastowej zmiany cyberataków i zagrożeń (większość zagrożeń w świecie rzeczywistym pozostaje względnie stała), co może stwarzać pewne problemy w odniesieniu do prawodawstwa. Regulacja prawna w tej dziedzinie musi być z jednej strony na tyle ogólna, aby umożliwić skuteczną reakcję na częściowo negatywne zjawiska w cyberprzestrzeni bez konieczności szczegółowego ich określania, z drugiej zaś nie może być zbyt ogólnikowa, aby nie naruszać praw i uzasadnionych interesów osób fizycznych w stopniu większym niż jest to absolutnie konieczne.

Przed przystąpieniem do analizy obowiązujących i skutecznych przepisów prawnych w dziedzinie cyberbezpieczeństwa należy zauważyć, że nie tylko w Unii Europejskiej istnieje wyraźne dążenie do wdrożenia bardziej skutecznych instrumentów prawnych, które poprawiłyby jakość bezpieczeństwa cybernetycznego i umożliwiły odpowiednie reagowanie na zagrożenia i ataki cybernetyczne. Stopniowo usuwane są niespójności i braki w normach prawnych państw członkowskich UE i innych krajów, które zdecydowały się aktywnie uczestniczyć w rozwoju cyberbezpieczeństwa.

"Metody ochrony danych i systemów informatycznych są obecnie przedmiotem wielu badań naukowych, ale sama techniczna ochrona tych systemów i danych bez podstawy prawnej może okazać się nieskuteczna ze względu na niejasne określenie, jak daleko może sięgać taka ochrona. *W tym kontekście w pełni widoczna jest niespójność prawa krajowego z prawem innych krajów. Rozwój technologii komputerowych i informatycznych, który decyduje o międzynarodowym charakterze cyberprzestępczości, sprawia, że skuteczna ochrona systemów komputerowych i danych jest nie do pomyślenia bez międzynarodowych lub ponadnarodowych ram prawnych, nie tylko między państwami członkowskimi UE, ale w skali globalnej."*[98]

[98] KOLOUCH, Jan i Petr VOLEVECKÝ. *Ochrona prawnokarna przed cyberprzestępczością.* Praga: Akademia Policyjna Republiki Czeskiej w Pradze, 2013, s. 65.

W tym rozdziale skoncentrujemy się na ramach prawnych dotyczących bezpieczeństwa cybernetycznego w UE i krajach partnerskich programu Erasmus+.

4.1 Dokumenty UE/WE wykorzystywane do harmonizacji przepisów dotyczących bezpieczeństwa cybernetycznego

Systemy i usługi sieciowe i informacyjne odgrywają istotną rolę w społeczeństwie. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i społecznej, a w szczególności dla funkcjonowania rynku wewnętrznego.

Skala, częstotliwość i skutki incydentów bezpieczeństwa są coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Systemy te mogą również stać się celem celowych szkodliwych działań mających na celu uszkodzenie lub przerwanie działania systemów. Takie incydenty mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników i wyrządzać poważne szkody gospodarce Unii.

Systemy sieciowe i informacyjne, a przede wszystkim Internet, odgrywają zasadniczą rolę w ułatwianiu transgranicznego przepływu towarów, usług i osób. Ze względu na ten ponadnarodowy charakter, istotne zakłócenia tych systemów, zamierzone lub niezamierzone, niezależnie od miejsca ich wystąpienia, mogą mieć wpływ na poszczególne państwa członkowskie i Unię jako całość. Bezpieczeństwo sieci i systemów informatycznych ma zatem zasadnicze znaczenie dla sprawnego funkcjonowania rynku wewnętrznego.

W oparciu o znaczne postępy poczynione w ramach europejskiego forum państw członkowskich w zakresie wspierania dyskusji i wymiany dobrych praktyk politycznych, w tym opracowania zasad europejskiej współpracy w sytuacjach kryzysów cybernetycznych, należy powołać grupę współpracy złożoną z przedstawicieli państw członkowskich, Komisji oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji ("ENISA"), której zadaniem będzie wspieranie i ułatwianie strategicznej współpracy między państwami członkowskimi w zakresie bezpieczeństwa sieci i systemów informatycznych. Aby grupa ta była skuteczna i obejmowała wszystkich, konieczne jest, by wszystkie państwa członkowskie dysponowały minimalnymi zdolnościami i strategią zapewniającą wysoki poziom bezpieczeństwa sieci i systemów informatycznych na swoim terytorium. Ponadto wymogi dotyczące bezpieczeństwa i powiadamiania powinny mieć zastosowanie do operatorów usług podstawowych i dostawców usług cyfrowych, aby promować kulturę zarządzania ryzykiem i zapewnić zgłaszanie najpoważniejszych incydentów.[99]
W szczególności, ze względu na specyfikę nieograniczoności cyberprzestrzeni i potrzebę skutecznej współpracy międzynarodowej, UE stara się zbliżyć do siebie przepisy poszczególnych państw członkowskich, tak aby można było skutecznie rozwiązywać problemy związane z bezpieczeństwem cybernetycznym.

Rozporządzenia, dyrektywy, decyzje ramowe i inne dokumenty UE/WE są głównymi środkami zbliżania prawa poszczególnych państw UE. Z punktu widzenia bezpieczeństwa cybernetycznego najważniejsze są następujące dokumenty:

Prawo pierwotne UE

- Karta Praw Podstawowych Unii Europejskiej

Dyrektywa Parlamentu Europejskiego i Rady

- 91/250/EWG w sprawie ochrony prawnej programów komputerowych

[99] https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

- 98/34/WE ustanawiająca procedurę udzielania informacji w zakresie norm i przepisów technicznych, zmieniona dyrektywą 98/48/WE
- 1999/5/WE w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności
- 2000/31/WE w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego, w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)
- 2002/19/WE w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz wzajemnych połączeń (dyrektywa o dostępie)
- 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (dyrektywa o zezwoleniach), zmieniona dyrektywą 2009/140/WE
- 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa), zmieniona dyrektywą 2009/140/WE
- 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej)
- 2002/58/WE w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej
- 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności
- 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony
- 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW
- 2013/11/UE w sprawie alternatywnych metod rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) nr 2006/2004 i dyrektywy 2009/22/WE (dyrektywa w sprawie alternatywnych metod rozstrzygania sporów konsumenckich)
- 2013/40/UE w sprawie ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW
- 2015/1535 w sprawie procedury udzielania informacji w zakresie przepisów technicznych i przepisów dotyczących usług społeczeństwa informacyjnego
- 2015/2366 w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 2002/65/WE, 2009/110/WE i 2013/36/UE oraz rozporządzenie (UE) nr 1093/2010 i uchylająca dyrektywę 2007/64/WE ("zmieniona dyrektywa w sprawie usług płatniczych")
- 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych, w sprawie swobodnego przepływu takich danych oraz uchylenia decyzji ramowej Rady 2008/977/WSiSW
- **2016/1148 w sprawie środków mających na celu zapewnienie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii (NIS)**

Rozporządzenie Parlamentu Europejskiego i Rady

- 460/2004/WE ustanawiająca Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, zmieniona rozporządzeniem (WE) nr 1007/2008
- 1077/2011/WE ustanawiająca europejską agencję do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości
- 526/2013 w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (**ENISA**) i uchylające rozporządzenie (WE) nr 460/2004 Tekst mający znaczenie dla EOG
- 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (**eIDAS**[100])
- 679/2016 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych i o swobodnym przepływie takich danych oraz uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych - **GDPR**)

Decyzja Rady

- 92/242/EWG w sprawie bezpieczeństwa systemów informacyjnych
- 2005/222/WSiSW w sprawie ataków na systemy informatyczne
- 2011/292/UE w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE

Inne dokumenty

- Konwencja Rady Europy nr 185 o cyberprzestępczości
- Protokół dodatkowy nr 189 Rady Europy do Konwencji o cyberprzestępczości
- Konwencja Rady Europy nr 196 o zapobieganiu terroryzmowi
- Rozporządzenie wykonawcze Komisji (UE) 2018/151 ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, które mają być uwzględniane przez dostawców usług cyfrowych w zarządzaniu zagrożeniami dla bezpieczeństwa, na które narażone są sieci i systemy informatyczne, oraz parametrów oceny, czy skutki incydentu są znaczące

Normy międzynarodowe

- ISMS serii ISO/IEC 27000
- w Republice Czeskiej ČSN ISO/IEC 27001:2014

Obecnie najważniejszym dokumentem Unii Europejskiej odnoszącym się do cyberbezpieczeństwa jest DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 z dnia 6 lipca 2016 r. dotycząca środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w całej Unii.[101]

Dyrektywa ta jest obecnie poddawana przeglądowi, a dyrektywa NIS2 jest w trakcie przygotowywania. Pierwszy ogólnounijny akt prawny dotyczący cyberbezpieczeństwa, dyrektywa NIS, wszedł w życie w 2016 r. i pomógł osiągnąć wyższy i bardziej wyrównany poziom

[100] Zwany dalej **eIDAS**
[101] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=CS

bezpieczeństwa sieci i systemów informatycznych w całej UE. W związku z bezprecedensową cyfryzacją w ostatnich latach nadszedł czas, aby go odświeżyć.

Zmiany w zrewidowanej dyrektywie zostały jasno przedstawione w dokumencie Komisji Europejskiej[102] :

[102] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72155

4.2 Przepisy dotyczące bezpieczeństwa cybernetycznego w Republice Czeskiej

Kwestia bezpieczeństwa cybernetycznego została po raz pierwszy podjęta przez państwo w sposób systematyczny w **2000 roku.**

W 2010 r**.** przyjęto uchwałę rządu nr 205 dotyczącą **kwestii bezpieczeństwa cybernetycznego w Republice Czeskiej.**[103] Na mocy tej uchwały Ministerstwo Spraw Wewnętrznych Republiki Czeskiej

[103] *UCHWAŁA RZĄDU REPUBLIKI CZESKIEJ z dnia 15 marca 2010 r. nr 205 w sprawie rozwiązania kwestii bezpieczeństwa cybernetycznego w Republice Czeskiej.* [online]. Dostępny pod adresem: https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ

zostało wyznaczone na centralny punkt kontaktowy do spraw bezpieczeństwa cybernetycznego i organ krajowy w tej dziedzinie. Minister Spraw Wewnętrznych otrzymał ponadto polecenie, aby:

1. koordynować działania innych instytucji państwowych w dziedzinie bezpieczeństwa cybernetycznego,
2. Koordynować reprezentowania Republiki Czeskiej w kwestiach bezpieczeństwa cybernetycznego na forach międzynarodowych, w tym udział organów państwowych w działaniach odpowiednich organizacji międzynarodowych,
3. Przedłożyć rządowi do zatwierdzenia statut Międzyresortowej Rady Koordynacyjnej ds. Cyberbezpieczeństwa do dnia 30 kwietnia 2010 r,
4. przedłożyć rządowi strategię bezpieczeństwa cybernetycznego do 15 grudnia 2010 r,
5. uruchomić rządowy CSIRT (Computer Security Incident Response Team) nie później niż 31 grudnia 2010 r.

W dniu **19 października 2011 r.** rząd Republiki Czeskiej przyjął uchwałę nr 781 ustanawiającą Biuro Bezpieczeństwa Narodowego jako punkt centralny ds. bezpieczeństwa cybernetycznego i organ krajowy w tej dziedzinie.[104] Jednocześnie rząd Republiki Czeskiej powołał **Radę ds. Bezpieczeństwa Cybernetycznego**[105] i zatwierdził utworzenie **Narodowego Centrum Bezpieczeństwa Cybernetycznego** (w ramach NSA).

W **2011 roku** przyjęto **Strategię bezpieczeństwa cybernetycznego Republiki Czeskiej na lata 2011-2015**[106] oraz **plan działania dla tej strategii.** Jednak ze względu na przeniesienie odpowiedzialności z Ministerstwa Spraw Wewnętrznych do NSA, strategia ta jest częściej określana jako: **Strategia bezpieczeństwa cybernetycznego Republiki Czeskiej na lata 2012-2015.**[107]

W strategii określono następujące cele strategiczne i działania:

- tworzenie ram prawnych,
- budowa Narodowego Centrum Cyberbezpieczeństwa i rządowego zespołu CERT,
- ochrona krytycznych infrastruktur informacyjnych,
- wzmocnienie bezpieczeństwa cybernetycznego systemów teleinformatycznych administracji publicznej,
- zwiększenie skuteczności walki z cyberprzestępczością,
- koordynowanie działań na rzecz zapewnienia bezpieczeństwa cybernetycznego w Europie,
- wykorzystując wiarygodne i godne zaufania technologie informacyjne,
- podnoszenie świadomości w zakresie bezpieczeństwa cybernetycznego,
- reagowanie na ataki cybernetyczne.

---

[104] *UCHWAŁA RZĄDU REPUBLIKI CZESKIEJ z dnia 19 października 2011 r. nr 781 ustanawiająca Biuro Bezpieczeństwa Narodowego jako agencję wiodącą w zakresie bezpieczeństwa cybernetycznego oraz organ krajowy w tej dziedzinie.* [online]. Dostępny pod adresem: https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E

[105] Rada jest organem doradczym Prezesa Rady Ministrów w zakresie bezpieczeństwa cybernetycznego.

[106] *Strategia bezpieczeństwa cybernetycznego Republiki Czeskiej na lata 2011-2015* [online]. Dostępny pod adresem: https://www.databaze-strategie.cz/cz/cr/strategie/strategie-pro-oblast-kyberneticke-bezpecnosti-cr-2011-2015?typ=struktura

[107] *Strategia bezpieczeństwa cybernetycznego Republiki Czeskiej na lata 2012-2015* [online]. Dostępny pod adresem: https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf

W dniu 28 czerwca 2013 r. NSA przedłożył rządowi Republiki Czeskiej projekt ustawy o cyberbezpieczeństwie. Kolejny proces legislacyjny został przeprowadzony bez istotnych uwag i **ustawa nr 181/2014 Coll. , o cyberbezpieczeństwie i o zmianach w powiązanych ustawach** (ustawa o cyberbezpieczeństwie) weszła w życie 29 sierpnia 2014 r. z mocą obowiązującą od **1 stycznia 2015 r.**

Wraz z ustawą opracowano również przepisy wykonawcze, a mianowicie:

- Dekret nr 316/2014 w sprawie środków bezpieczeństwa, incydentów związanych z bezpieczeństwem cybernetycznym, środków reaktywnych oraz w sprawie ustanowienia formalności dotyczących zgłoszeń w dziedzinie bezpieczeństwa **cybernetycznego** (**dekret w sprawie bezpieczeństwa cybernetycznego**);
- Dekret nr 317/2014 **określający istotne systemy informacyjne i kryteria ich definiowania**;
- Dekret nr 315/2014, zmiana dekretu rządowego nr 432/2010 Dz.U. **w sprawie kryteriów wyznaczania elementu infrastruktury krytycznej**.

Wszystkie rozporządzenia wykonawcze weszły w życie w tym samym czasie, co ustawa o bezpieczeństwie cybernetycznym.

W sierpniu 2015 r. został wybrany operator Krajowego Zespołu CERT na podstawie wymagań określonych w ZoKB. Operator ten stał się stowarzyszeniem CZ.NIC.[108] W dniu 18 grudnia 2015 r. podpisano Porozumienie publicznoprawne w sprawie zapewnienia działalności Narodowego CERT oraz współpracy w zakresie cyberbezpieczeństwa.[109] Umowa ta została zawarta na czas nieokreślony.

Od czasu wejścia w życie w 2015 r. ustawa o bezpieczeństwie cybernetycznym została poddana dwóm istotnym zmianom.

Pierwsza zmiana została wprowadzona ustawą nr 104/2017 Coll.,[110] z mocą obowiązującą od 1 lipca 2017 r. oraz ustawą nr 205/2017 Coll. z mocą obowiązującą od 1 sierpnia 2017 r. Zmiana ta rozszerzyła zakres osób zobowiązanych objętych ZoKB o operatorów systemów informatycznych oraz wprowadziła dalsze zmiany w zakresie niektórych sankcji.

Druga, bardziej znacząca zmiana została wprowadzona ustawą nr 205/2017 Coll.,[111] z mocą obowiązującą od 1 sierpnia 2017 r. Nowelizacja ta wdrożyła do ZOKB **dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków zapewniających wysoki wspólny poziom bezpieczeństwa sieci i systemów informatycznych w Unii (NIS),** a także powołała **Krajowy Organ ds. Bezpieczeństwa Cybernetycznego i Informatycznego (NACIS)**, który przejął prawa i obowiązki KWB w zakresie cyberbezpieczeństwa, w tym ochrony informacji niejawnych w zakresie systemów teleinformatycznych oraz ochrony kryptograficznej. NUCIB jest centralnym organem administracyjnym w wyżej wymienionych obszarach.

Obecnie kwestia bezpieczeństwa cybernetycznego jest szczegółowo uregulowana w ustawie o bezpieczeństwie cybernetycznym, ale częściowe aspekty ochrony Republiki Czeskiej przed

---

[108] Zob. https://www.nic.cz/page/351/.
[109] Zob. [online]. Dostępny pod adresem: https://www.nic.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf
[110] Ustawa nr 104/2017 Dz. U., zmieniająca ustawę nr 365/2000 Dz. U., **o systemach informacyjnych administracji publicznej** i o zmianach w innych ustawach, z późniejszymi zmianami, ustawa nr 181/2014 Dz. U., o bezpieczeństwie cybernetycznym i o zmianach w powiązanych ustawach (ustawa o bezpieczeństwie cybernetycznym) oraz niektóre inne ustawy. [online]. Dostępny pod adresem: https://www.zakonyprolidi.cz/cs/2017-104
[111] Ustawa nr 205/2017 Coll., zmieniająca ustawę nr 181/2014 Coll., o cyberbezpieczeństwie i o zmianach w powiązanych ustawach (ustawa o cyberbezpieczeństwie), zmienioną ustawą nr 104/2017 Coll., oraz niektóre inne ustawy. [online]. Dostępny pod adresem: https://www.zakonyprolidi.cz/cs/2017-205

cyberatakami można znaleźć także w innych aktach prawnych. Z punktu widzenia cyberbezpieczeństwa najważniejsze są następujące dokumenty:

Prawa konstytucyjne

- Ustawa konstytucyjna nr 1/1993 Sb., Konstytucja Republiki Czeskiej, z późniejszymi zmianami
- Ustawa konstytucyjna nr 2/1993 Dz. U., Karta Podstawowych Praw i Wolności, z późniejszymi zmianami[112]
- Ustawa konstytucyjna nr 110/1998 Dz.U., o bezpieczeństwie Republiki Czeskiej

Przepisy

- Ustawa nr 106/1999 Sb. o wolnym dostępie do informacji, z późniejszymi zmianami
- Ustawa nr 101/2000 Dz. U. o ochronie danych osobowych i o zmianach niektórych ustaw, z późniejszymi zmianami[113]
- Ustawa nr 121/2000 Dz.U. o prawie autorskim, prawach pokrewnych prawu autorskiemu oraz o zmianach niektórych ustaw (ustawa o prawie autorskim), z późniejszymi zmianami
- Ustawa nr 240/2000 Dz. U. o zarządzaniu kryzysowym i zmianach niektórych ustaw (Ustawa o kryzysie), z późniejszymi zmianami
- Ustawa nr 365/2000 Sb. o systemach informacyjnych administracji publicznej, z późniejszymi zmianami
- Ustawa nr 480/2004 Sb. o niektórych usługach społeczeństwa informacyjnego i o zmianach niektórych ustaw (ustawa o niektórych usługach społeczeństwa informacyjnego), z późniejszymi zmianami [114]
- Ustawa nr 127/2005 Coll. o łączności elektronicznej, z późniejszymi zmianami [115]
- Ustawa nr 412/2005 Dz.U. o ochronie informacji niejawnych i poświadczeniach bezpieczeństwa, z późniejszymi zmianami [116]
- Ustawa nr 69/2006 Zb. o wprowadzaniu sankcji międzynarodowych, z późniejszymi zmianami
- Ustawa nr 300/2008 Dz.U., o aktach elektronicznych i dozwolonej konwersji dokumentów, z późniejszymi zmianami
- Ustawa nr 40/2009 Dz.U., Kodeks karny, z późniejszymi zmianami [117]
- Ustawa nr 111/2009 Dz. U. o rejestrach podstawowych, z późniejszymi zmianami
- Ustawa nr 418/2011 Zb. o odpowiedzialności karnej osób prawnych i postępowaniu wobec nich
- Ustawa nr 89/2012 Dz.U., Kodeks cywilny

---

[112] zwana dalej Kartą Podstawowych Praw i Wolności lub **Kartą**.
[113] W związku z wejściem w życie GDPR ustawa ta zostanie zmieniona i ma zostać zastąpiona ustawą o przetwarzaniu danych osobowych. Więcej szczegółów można znaleźć np. w [online]. Dostępny pod adresem: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5
[114] zwana dalej ustawą o niektórych usługach społeczeństwa informacyjnego lub **ISA**.
[115] zwana dalej **ZoEK**
[116] zwana dalej **ZoOUI**
[117] Zwany dalej Kodeksem karnym lub **TCC**.

- **Ustawa nr 181/2014 Dz.U. o bezpieczeństwie cybernetycznym i o zmianach w ustawach powiązanych (ustawa o bezpieczeństwie cybernetycznym)**
- Ustawa nr 297/2016 Dz.U. o usługach zaufania dla transakcji elektronicznych

Przepisy wykonawcze

- Rozporządzenie rządu nr 522/2005 Dz.U. ustanawiające wykazy informacji niejawnych, z późniejszymi zmianami
- Rozporządzenie nr 523/2005 Dz.U. w sprawie bezpieczeństwa systemów informacyjno-komunikacyjnych i innego sprzętu elektronicznego, w którym przetwarzane są informacje niejawne, oraz w sprawie certyfikacji komór osłonowych, z późniejszymi zmianami
- Rozporządzenie nr 529/2006 Dz.U. w sprawie wymagań dotyczących struktury i zawartości koncepcji informacyjnej i dokumentacji operacyjnej oraz wymagań dotyczących bezpieczeństwa i zarządzania jakością systemów informacyjnych administracji publicznej (rozporządzenie w sprawie długoterminowego zarządzania systemami informacyjnymi administracji publicznej)
- **Rozporządzenie rządu nr 432/2010 Dz.U. w sprawie kryteriów wyznaczania elementów infrastruktury krytycznej**
- Dekret 357/2012 Coll. w sprawie przechowywania, przekazywania i usuwania danych operacyjnych i lokalizacyjnych
- **Dekret nr 317/2014 Dz.U. w sprawie ważnych systemów informacyjnych i kryteriów ich określania**
- **Dekret nr 437/2017 Dz.U. w sprawie kryteriów określania operatora usługi podstawowej**
- **Dekret nr 82/2018 Dz.U.** w sprawie środków bezpieczeństwa, incydentów związanych z bezpieczeństwem cybernetycznym, środków reaktywnych, wymogów archiwizacji w dziedzinie bezpieczeństwa cybernetycznego i usuwania danych (**dekret w** sprawie bezpieczeństwa **cybernetycznego**)

4.3 Przepisy prawne dotyczące bezpieczeństwa cybernetycznego w Polsce

Biorąc pod uwagę polskie uwarunkowania prawne w zakresie przestępczości komputerowej, należy stwierdzić, że praktycznie wszystkie przestępstwa ujęte w rozdziale XXXIII Kodeksu karnego mogą być popełnione przy użyciu komputera. Wówczas staną się one przestępstwami komputerowymi. W niektórych przypadkach użycie komputera stanowi okoliczność zaostrzającą odpowiedzialność karną, np. art. 268 § 2 i 3 k.k., natomiast w innych sytuacjach sprawca, popełniający przestępstwo z użyciem komputera, będzie traktowany tak samo jak sprawca działający w inny sposób, np. art. 265 k.k., art. 266 k.k. Obecnie, w ramach wspomnianego rozdziału Kodeksu karnego, ustawodawca penalizuje takie zachowania jak:

- bezprawny dostęp do informacji lub systemu informatycznego oraz do informacji z nimi związanych (art. 267 Kodeksu karnego)

- działania polegające na niszczeniu, uszkadzaniu, usuwaniu, zastępowaniu istotnych informacji lub podobnych czynnościach (art. 268 Kodeksu karnego),

- działania polegające na niszczeniu, uszkadzaniu, usuwaniu, zmienianiu lub utrudnianiu dostępu do danych informatycznych albo na istotnym zakłócaniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania takich danych (art. 268a Kodeksu karnego),

- czyny polegające na tzw. sabotażu informatycznym (art. 269 Kodeksu karnego), zwanym również dywersją informatyczną,

- czyny polegające na znacznym zakłóceniu działania systemu komputerowego lub sieci teleinformatycznej (art. 269a kodeksu karnego)

- czynów polegających na bezprawnym wytwarzaniu (lub podobnych działaniach) urządzeń lub programów komputerowych przystosowanych do popełniania określonych przestępstw, haseł komputerowych, kodów dostępu lub innych danych (art. 269b kodeksu karnego).

Oprócz wyżej wymienionego rozdziału ustawodawca uregulował odrębnie przestępstwo oszustwa komputerowego (art. 287 k.k.), kradzieży programu komputerowego (art. 278 § 2 k.k.) oraz posługiwania się programem komputerowym (art. 293 k.k.). Wszystkie przestępstwa zawarte w rozdziale XXXIII należą do kategorii przestępstw pospolitych, z wyjątkiem art. 269 Kodeksu karnego, art. 269a Kodeksu karnego i art. 269b Kodeksu karnego. Mają one charakter aplikacyjny.

Rozwiązania przyjęte w rozdziale XXXIII Kodeksu karnego są konsekwencją podpisania przez Polskę w dniu 23 listopada 2001 r. Konwencji nr 185 Rady Europy o cyberprzestępczości oraz Decyzji Ramowej Rady 2005/222/WSiSW w sprawie ataków na systemy informatyczne.

Artykuł 267 Kodeksu karnego stanowi prawnokarną ochronę prywatności użytkowników Internetu. W art. 267 § 1 Kodeksu karnego penalizowane są działania mające na celu uzyskanie nielegalnego dostępu do informacji nieprzeznaczonych dla sprawcy. Z punktu widzenia karalności zachowania sprawcy nie ma znaczenia, gdzie informacje są przechowywane - na dysku twardym czy na zewnętrznym serwerze w sieci. Oznacza to, że przepis ten chroni szeroko rozumiane prawo podmiotowe do dysponowania informacją. Zachowanie sprawcy przestępstwa określonego w art. 267 § 1 Kodeksu karnego może polegać na otwarciu zamkniętego listu, podłączeniu się do sieci telekomunikacyjnej lub przełamaniu albo obejściu zabezpieczeń elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń. Treść przepisu wskazuje, że ustawodawca penalizuje działania wskazane w części dyspozytywnej, niezależnie od tego, czy sprawca zapoznał się z treścią informacji. Oznacza to, że znamiona przestępstwa z art. 267 k.k. wypełni również osoba, która uzyska dostęp do informacji dla niej nieprzeznaczonej, nawet w sytuacji, gdy nie zamierzała zapoznać się z jej treścią. Prywatność użytkowników Internetu może być również naruszana poprzez łamanie lub omijanie istniejących zabezpieczeń, a tym samym włamywanie się do komputera ofiary. Szerokie określenie w art. 267 § 1 Kodeksu karnego rodzajów zabezpieczeń, których złamanie lub ominięcie jest karalne, oznacza, że zabezpieczenie pliku hasłem będzie spełniało warunki informacji zabezpieczonej.

Działania sprawcy zmierzające do uzyskania dostępu do całości lub części systemu informatycznego stanowią przestępstwo z art. 267 § 2 k.k. Odnosząc się do strony podmiotowej czynu, należy zwrócić uwagę na użyte przez ustawodawcę pojęcie "sieć telekomunikacyjna", które nie zostało zdefiniowane w Kodeksie karnym. Konieczne wydaje się zatem odwołanie do art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, który definiuje sieć telekomunikacyjną jako systemy transmisyjne oraz urządzenia przełączające lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju. Z analizy powyższej definicji wynika, że siecią telekomunikacyjną może być zarówno istniejąca infrastruktura kablowa, jak i sieć bezprzewodowa.

Pojęcie systemu informatycznego nie zostało również zdefiniowane w Kodeksie karnym, jego definicję zawiera art. 7 pkt 2a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, który stanowi, że "systemem informatycznym jest zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, służących do przetwarzania danych". Termin ten pojawia się również w art. 1 lit. 2005/222/WSiSW z 24 lutego 2005 r., w którym określono,

że system informatyczny to każde urządzenie lub grupa połączonych lub powiązanych ze sobą urządzeń, z których co najmniej jedno dokonuje automatycznego przetwarzania danych komputerowych zgodnie z oprogramowaniem, a także danych przechowywanych, przetwarzanych, wyszukiwanych lub dostarczanych przez nie do celów ich działania, użytkowania, ochrony lub konserwacji. Inna definicja systemu informatycznego zawarta jest w Konwencji Rady Europy nr 185 o cyberprzestępczości. Zgodnie z art. 1 lit. i Konwencji, system informatyczny to dowolne urządzenie lub grupa połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych. Ze względu na fakt, że pojęcie systemu informatycznego odgrywa istotną rolę w określaniu odpowiedzialności za cyberprzestępczość, w literaturze przedmiotu system informatyczny opisuje się jako zbiór współpracujących ze sobą elementów sprzętowych i programowych, które służą do wprowadzania, przetwarzania i odczytywania informacji. System informatyczny nie obejmuje zatem urządzeń do transmisji danych.

Warto zauważyć, że ustawodawca w art. 267 § 2 k.k. nie określił sposobu działania sprawcy, a jedynie jego skutek. Zgodnie z powyższym, każde zachowanie polegające na nieuprawnionym dostępie do systemu informatycznego jest karane, niezależnie od tego, czy doszło do naruszenia bezpieczeństwa komputera lub systemu.

W art. 267 § 3 Kodeksu karnego ustawodawca sankcjonuje inny czyn zabroniony, polegający na zainstalowaniu lub używaniu urządzenia podsłuchowego, wizualnego lub innego urządzenia lub oprogramowania w celu uzyskania informacji, do których nie jest się uprawnionym. Warunkiem odpowiedzialności na podstawie tego przepisu nie jest uzyskanie informacji, wystarczy, że sprawca podejmie określone działania. Działania te muszą być jednak podejmowane w określonym celu, tj. w celu uzyskania informacji, do których sprawca nie jest uprawniony.

W art. 267 § 4 Kodeksu karnego ustawodawca penalizuje ujawnienie innej osobie informacji uzyskanych w sposób określony w § 1-3.

Kolejny art. 268 Kodeksu karnego sankcjonuje zachowanie sprawcy zmierzające do naruszenia integralności danych informatycznych. Zgodnie z zapisami ustawy, naruszenie to może polegać na zniszczeniu, uszkodzeniu, usunięciu lub zmianie zapisu istotnych informacji.

W art. 268 § 2 k.k. ustawodawca uwzględnił sytuację, gdy czyn sprawcy dotyczy zapisu na informatycznym nośniku danych, np. na dysku twardym lub płycie CD. Zwraca się uwagę, że przedmiotem ochrony art. 268 k.k. jest dostępność informacji, a celem działania sprawcy jest uniemożliwienie lub znaczne utrudnienie osobie uprawnionej dostępu do odpowiedniej informacji. Konieczność wystąpienia skutku w postaci udaremnienia lub znacznego utrudnienia dostępu do informacji oznacza, że przestępstwo polegające na niszczeniu, uszkadzaniu, usuwaniu, zastępowaniu istotnych informacji lub podobnych działaniach należy do kategorii przestępstw skutkowych. Taka kwalifikacja jest zgodna z utrwalonym w literaturze przedmiotu poglądem. Ustawodawca w art. 268 Kodeksu karnego posługuje się pojęciem "informacji istotnej", nie wskazując cech, jakie musi posiadać informacja, aby była istotna w rozumieniu tego przepisu. Dlatego też ocena charakteru danej informacji musi być dokonywana indywidualnie dla każdego przypadku na podstawie zarówno obiektywnych, jak i subiektywnych kryteriów.

Przedmiot ochrony art. 268a k.k., w odróżnieniu od art. 268 k.k., został określony szeroko i jest nim bezpieczeństwo i dostępność danych informatycznych, które nie muszą spełniać cech istotności. Znamiona przestępstwa z art. 268a Kodeksu karnego to niszczenie, uszkadzanie, usuwanie, zmienianie lub utrudnianie dostępu do danych informatycznych. Penalizowane w art. 268a Kodeksu karnego zachowanie może również polegać na znacznym zakłóceniu lub uniemożliwieniu automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych. Drugi zestaw zabronionych zachowań musi mieć znaczenie, które powinno być związane ze stopniem zakłócenia lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania

danych informatycznych, a nie z zakresem danych zmodyfikowanych przez sprawcę. O ważności działań podejmowanych przez sprawcę mówimy wtedy, gdy działania te charakteryzują się odpowiednio wysokim stopniem intensywności. Przedmiotem ochrony art. 268a Kodeksu karnego jest bezpieczeństwo informacji przechowywanych, przesyłanych i przetwarzanych w systemach opartych na danych informatycznych.

Na gruncie polskiego systemu prawnego pojęcie "dane informatyczne" nie zostało zdefiniowane, a odgrywa ono istotną rolę. Dlatego konieczne jest odwołanie się do prawa międzynarodowego - zgodnie z treścią art. 1 lit. b Konwencji nr 185 Rady Europy o cyberprzestępczości. Zgodnie z cytowanym przepisem termin ten oznacza "wszelkie przedstawienie faktów, informacji lub pojęć w formie nadającej się do przetwarzania w systemie komputerowym, w tym odpowiedni program powodujący wykonanie funkcji przez system informatyczny".

Definicja danych informatycznych zawarta jest również w art. 1 lit. b decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne i oznacza "wszelkie przedstawienie faktów, informacji lub idei w formie odpowiedniej do przetwarzania w systemie informatycznym, w tym program odpowiedni do spowodowania wykonania funkcji przez system".

Przedstawione definicje wskazują, że dane informatyczne to wszelkie dane będące nośnikiem informacji, a także programy komputerowe wykorzystywane zarówno przez indywidualnie określone osoby, jak i wykorzystywane w sieciach teleinformatycznych przez nieokreśloną liczbę osób.

W art. 269 Kodeksu karnego ustawodawca penalizuje zachowanie polegające na tzw. sabotażu informatycznym. Istotą tego przestępstwa jest niszczenie, uszkadzanie, usuwanie lub zmienianie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, a także zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania tych danych.

W art. 269 § 2 k.k. ustawodawca wskazał, że przestępstwo sabotażu może polegać na zniszczeniu lub wymianie informatycznego nośnika danych albo na zniszczeniu lub uszkodzeniu urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych. Jak wynika z treści omawianego przepisu, przedmiotem ochrony są dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządu terytorialnego oraz systemu automatycznego przetwarzania, gromadzenia lub przekazywania tych informacji. Sabotaż informatyczny jest uznawany za typ kwalifikowany w odniesieniu do przestępstw z art. 268 § 2 k.k., art. 268a k.k. i 269a k.k. Cechą kwalifikującą jest tu rodzaj chronionych danych, tj. danych o szczególnym znaczeniu dla wartości wymienionych w art. 269 Kodeksu karnego. Ustawodawca podzielił penalizowane zachowania sprawcy na dwie grupy. Pierwsze z nich to działania mające na celu niszczenie, uszkadzanie, usuwanie lub zmienianie danych komputerowych o szczególnym znaczeniu dla wartości chronionych przez rozporządzenie. Przedmiotem ochrony tej części przepisu jest integralność danych należących do określonej kategorii. Druga grupa cech to działania polegające na zakłócaniu lub uniemożliwianiu automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. W tym przypadku przedmiotem ochrony jest dostępność danych określonych w wyżej wymienionym przepisie.

W art. 269 § 2 kk ustawodawca, chroniąc dobra określone w § 1, usankcjonował działania sprawcy polegające na niszczeniu lub wymianie informatycznego nośnika danych albo niszczeniu lub uszkadzaniu urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania

danych informatycznych. Działania te mogą polegać na fizycznym niszczeniu, uszkadzaniu, wymianie np. dysków twardych, a także na utrudnianiu lub uniemożliwianiu ich przetwarzania poprzez np. uszkadzanie urządzeń sieciowych. Ze względu na materialny charakter przestępstwa sabotażu informatycznego, dla przypisania sprawcy czynu z art. 269 k.k. konieczne jest wystąpienie konkretnego skutku w postaci zniszczenia lub uszkodzenia określonych danych komputerowych albo zakłócenia lub uniemożliwienia ich automatycznego przetwarzania lub przekazywania.

Innym przepisem regulującym odpowiedzialność karną za cyberprzestępstwa jest art. 269a polskiego Kodeksu karnego. Istotą tego przepisu jest ochrona bezpieczeństwa operacyjnego systemu komputerowego lub sieci teleinformatycznej. W literaturze przedmiotu pojęcie systemu komputerowego utożsamiane jest z pojęciem systemu informacyjnego. Odpowiedzialności karnej na podstawie tego przepisu podlega osoba, która bez uprawnienia w istotny sposób zakłóca działanie systemu komputerowego lub sieci teleinformatycznej poprzez przekazywanie, niszczenie, usuwanie, uszkadzanie, utrudnianie dostępu lub zmianę danych informatycznych. Sposoby działania penalizowane przez ustawę zostały enumeratywnie wymienione w przepisie i co do zasady nie powinny budzić wątpliwości interpretacyjnych. Wyjątkiem jest termin "transmisja", który nie został zdefiniowany przez ustawodawcę. W literaturze termin ten oznacza przenoszenie informacji z jednego miejsca w systemie komputerowym do innego, np. z pamięci operacyjnej na dysk, z dysku na drukarkę, z jednego komputera w sieci do innego komputera sieciowego. Sankcjonowane przekazywanie danych informatycznych na odległość ma się odbywać w formie zakodowanej, a nie na nośnikach zewnętrznych, np. na płytach CD.

Artykuł 269b Kodeksu karnego sankcjonuje wytwarzanie, nabywanie, sprzedaż lub udostępnianie innym osobom urządzeń lub programów komputerowych przystosowanych do popełniania wymienionych przestępstw. Warto zauważyć, że do znamion tego przestępstwa należy szereg czynności przygotowawczych, które mogą być związane z popełnieniem przestępstw wskazanych w części dyspozytywnej przepisu. Penalizacja obejmuje działania polegające na tworzeniu i przystosowaniu urządzeń lub programów do popełniania przestępstw z art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 lub § 2 w zw. z § 1, art. 269 § 2 lub art. 269a, ich udostępnianiu i uzyskiwaniu, a także łamaniu haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej. Przedmiotem ochrony jest bezpieczeństwo informacji przetwarzanych elektronicznie we wszystkich aspektach, tj. poufności, integralności i dostępności danych i systemów informatycznych. Mimo że ustawodawca używa liczby mnogiej w odniesieniu do sankcjonowanych działań, karalne z mocy prawa będzie pojedyncze zachowanie, np. sprzedaż tylko jednego programu. Taki pogląd jest ugruntowany zarówno w doktrynie, jak i w orzecznictwie.

W art. 287 Kodeksu karnego ustawodawca uregulował przestępstwo oszustwa komputerowego. To przestępstwo jest ujęte w Rozdziale XXXV "Przestępstwa przeciwko mieniu". Przedmiotem ochrony tego artykułu są dane informatyczne wraz z zawartymi w nich informacjami. Dane te mogą być przechowywane zarówno w pamięci komputera, jak i na dysku CD lub serwerze. Karalne zachowanie sprawcy polega na wpływaniu bez upoważnienia na automatyczne przetwarzanie, gromadzenie lub przekazywanie informacji albo na zmianę, usunięcie lub wprowadzenie nowego zapisu na danych informatycznych. Opisane zachowanie sprawcy musi mieć na celu osiągnięcie korzyści majątkowej lub wyrządzenie szkody innej osobie. W literaturze przedmiotu wskazuje się, że działanie sprawcy mające na celu wywarcie wpływu na automatyczne przetwarzanie, gromadzenie lub przekazywanie informacji przybiera postać bezprawnej ingerencji podmiotu zewnętrznego w przebieg automatycznych procesów, co powoduje, że po ustaniu wpływu sprawcy ich przebieg, w szczególności przetwarzanie, gromadzenie lub przekazywanie, będzie inny niż gdyby nie doszło do działania sprawcy. Oszustwo komputerowe jest przestępstwem. Oznacza to, że przestępstwo z art. 287 § 1 k.k. jest dokonywane w momencie wprowadzania zmian lub innej

ingerencji w urządzenie lub system gromadzenia, przetwarzania lub przekazywania informacji za pomocą techniki komputerowej, opisanych w tym przepisie. Konieczność wyrządzenia szkody nie jest jedną z jej cech charakterystycznych.

W art. 287 § 2 Kodeksu karnego ustawodawca określił typ uprzywilejowany ze względu na przypadek mniejszej wagi. Przestępstwo z art. 287 Kodeksu karnego ma z reguły charakter publicznoskargowy. Natomiast w przypadku, gdy zostało ono popełnione na szkodę osoby najbliższej, powoduje, zgodnie z postanowieniami § 3, zmianę trybu ścigania na wnioskowy.

Powyższa analiza przepisów regulujących odpowiedzialność karną za cyberprzestępstwa wskazuje, że podstawowym przedmiotem ochrony kryminalizacji przestępstw komputerowych jest tradycyjna wolność i prywatność jednostki, choć postrzegana z perspektywy komputera. Ochronie podlegają jednak również dane gromadzone w systemach, a także same systemy i ich integralność, których naruszenie może mieć często bardzo poważne konsekwencje społeczne. Jednocześnie należy wspomnieć, że prawnokarna regulacja cyberprzestępczości napotka dwa podstawowe problemy. Pierwsza z nich jest związana z zasadą jurysdykcji. Przestępstwa komputerowe popełniane w Internecie bardzo często mają charakter transgraniczny, a czasem nawet terytorialny, w tym sensie, że często popełniane są w oderwaniu od terytorium danej jurysdykcji. Drugim problemem jest bardzo szybki rozwój nowych form cyberprzestępczości, za którym ustawodawcy zazwyczaj nie nadążają.

Niemniej jednak, biorąc pod uwagę przedstawione aspekty prawnokarne, powaga zagrożenia, jakie niesie ze sobą cyberprzestępczość oraz potrzeba odpowiedniej reakcji na nie, w szczególności poprzez regulacje z zakresu prawa karnego, nie może budzić żadnych wątpliwości.

5. System zarządzania bezpieczeństwem informacji (ISMS, SZBI)

5.1 Ramy ISMS

System zarządzania bezpieczeństwem informacji[118] (**ISMS**) **to zbiór zasad mających na** celu utrzymanie poufności, integralności i dostępności informacji poprzez zastosowanie procesu zarządzania ryzykiem oraz zapewnienie zainteresowanych stron, że ryzyko jest odpowiednio zarządzane. [119]

W ramach ISMS chronione są aktywa, zarządza się ryzykiem związanym z bezpieczeństwem informacji i monitoruje się już wdrożone środki.

System zarządzania bezpieczeństwem informacji oznacza tę część systemu zarządzania, która opiera się na podejściu do systemu teleinformatycznego opartym na analizie ryzyka. Ta część systemu zarządzania określa, w jaki sposób bezpieczeństwo informacji i danych jest ustanawiane, wdrażane, obsługiwane, monitorowane, przeglądane, utrzymywane i doskonalone.

Już z powyższej definicji jasno wynika, że **ISMS jest częścią procesów i ogólnego systemu zarządzania organizacją** oraz **jest zintegrowany z tymi systemami**.

ISMS może być stosowany do organizacji jako całości, jak również do elementu organizacyjnego w organizacji lub do specjalnie wyznaczonego systemu informacyjno-komunikacyjnego lub jego części.

"ISMS może być wdrożony i stosowany zarówno w organizacji zatrudniającej dziesięciu pracowników, jak i w dużym holdingu, który może zatrudniać tysiące osób. Mówiąc wprost, istnieje tylko jeden ISMS, i to taki, który został opisany w normie ISO/IEC 27001. Jednak interpretacja i wdrażanie poszczególnych zaleceń może się znacznie różnić w zależności od skali systemu, liczby użytkowników, sposobu przetwarzania danych, ich wartości, a przede wszystkim realnych zagrożeń

[118] Zwany dalej **ISMS**
[119] Por. Wprowadzenie do ISO/IEC 27001

bezpieczeństwa itp. Strategia ISMS nie jest zwykle opisywana tak szczegółowo w małych i średnich firmach, jak ma to miejsce w dużych, zwłaszcza międzynarodowych organizacjach.

ISMS ma zastosowanie nie tylko do przedsiębiorstw przemysłowych i organizacji prywatnych - ISMS dotyczy wszystkich organizacji, w tym instytucji publicznych i organów rządowych. Dowodem na to jest istnienie wielu krajowych uchwał rządowych i resortowych zalecających i/lub wymagających wdrożenia ISMS w organizacjach kontrolowanych przez państwo i mających siedzibę w państwie. "[120]

Szereg norm ISMS ma na celu pomóc organizacjom wszystkich typów i rozmiarów we wdrożeniu i obsłudze ISMS. Składa się on z następujących norm międzynarodowych o wspólnym tytule *Technika informatyczna - Techniki bezpieczeństwa*[121] (wymienionych poniżej w kolejności numerycznej):

- ISO/IEC 27000 — *Systemy zarządzania bezpieczeństwem informacji - przegląd i słowniczek*
- **ISO/IEC 27001** — ***Systemy zarządzania bezpieczeństwem informacji - wymagania***
- ISO/IEC 27002 — *Zestaw procedur dotyczących środków bezpieczeństwa informacji*
- ISO/IEC 27003 — *Wytyczne dotyczące wdrażania systemu zarządzania bezpieczeństwem informacji*
- ISO/IEC 27004 — *Zarządzanie bezpieczeństwem informacji - pomiar*
- ISO/IEC 27005 — *Zarządzanie ryzykiem w zakresie bezpieczeństwa informacji*
- ISO/IEC 27006 — *Wymagania dla jednostek audytujących i certyfikujących systemy zarządzania bezpieczeństwem informacji*
- ISO/IEC 27007 — *Wytyczne dotyczące audytowania systemów zarządzania bezpieczeństwem informacji*
- ISO/IEC TR 27008 — *Wytyczne dla audytorów środków bezpieczeństwa informacji*
- ISO/IEC 27009 — *Specyficzne dla branży zastosowanie normy ISO/IEC 27001 - Wymagania*
- ISO/IEC 27010 — *Zarządzanie bezpieczeństwem informacji w komunikacji międzysektorowej i międzyorganizacyjnej*
- ISO/IEC 27011 — *Wytyczne dotyczące zarządzania bezpieczeństwem informacji dla organizacji telekomunikacyjnych oparte na normie ISO/IEC 27002*
- ISO/IEC 27013 — *Wytyczne dotyczące zintegrowanego wdrażania norm ISO/IEC 27001 i ISO/IEC 20000-1*
- ISO/IEC 27014 — *Zarządzanie i kierowanie bezpieczeństwem informacji*

---

[120] POŽÁR, Josef i Luděk NOVÁK. *Podręcznik pracy kierownika ds. bezpieczeństwa.* Praga: POŽÁR, Josef i Luděk NOVÁK. *System zarządzania bezpieczeństwem informacji.* [online]. [cyt. 6 lipca 2018]. Dostępny pod adresem: https://www.cybersecurity.cz/data/srib.pdf s. 1

[121] Wspólny tytuł "Technika informatyczna - *techniki bezpieczeństwa*" wskazuje, że niniejsze normy międzynarodowe zostały opracowane przez ISO/IEC JTC 1 *Technika informatyczna,* Podkomisja SC 27 *Techniki bezpieczeństwa IT*

- ISO/IEC TR 27015 *Wytyczne dotyczące zarządzania bezpieczeństwem informacji w sektorze usług finansowych*
- ISO/IEC TR 27016 *Zarządzanie bezpieczeństwem informacji - Ekonomika organizacji*
- ISO/IEC 27017 *Zestaw praktyk dotyczących środków bezpieczeństwa informacji dla usług w chmurze w oparciu o ISO/IEC 27002*
- ISO/IEC 27018 *Zestaw procedur ochrony informacji umożliwiających identyfikację osób (PII) w chmurach publicznych działających jako podmioty przetwarzające PII*
- ISO/IEC 27019 *Wytyczne dotyczące zarządzania bezpieczeństwem informacji oparte na normie ISO/IEC 27002 dla systemów kontroli procesów specyficznych dla sektora energetycznego*

Poniżej wymieniono normy międzynarodowe, które nie są wymienione pod tym wspólnym tytułem, ale są również częścią serii norm ISMS:

- ISO 27799 *Informatyka w ochronie zdrowia - Systemy zarządzania bezpieczeństwem informacji w ochronie zdrowia zgodne z normą ISO/IEC 27002*[122]

Rozwiązanie ISMS wymaga systemowego i kompleksowego podejścia, uwzględniającego zasady i elementy w całym cyklu życia bezpieczeństwa cybernetycznego. System zarządzania ISMS opiera się na cyklu Deminga, czyli **cyklu PDCA** (Plan-Do-Check-Act; Planuj-Wykonaj-Sprawdź-Działaj).

Cykl PDCA to jedna z podstawowych zasad zarządzania, polegająca na stopniowej poprawie jakości procesów, usług, danych, produktów itp. poprzez ciągłe powtarzanie czterech podstawowych czynności: planuj-wykonaj-sprawdź-działaj.

Obecnie istnieje wiele wariantów cyklu PDCA[123] , a jedną z odpowiednich modyfikacji tego cyklu, która ma zastosowanie również w dziedzinie bezpieczeństwa cybernetycznego, jest wariant **OPDCA**, który rozszerza oryginalny model poprzez dodanie fazy **Obserwacji przed** fazą Planowania.

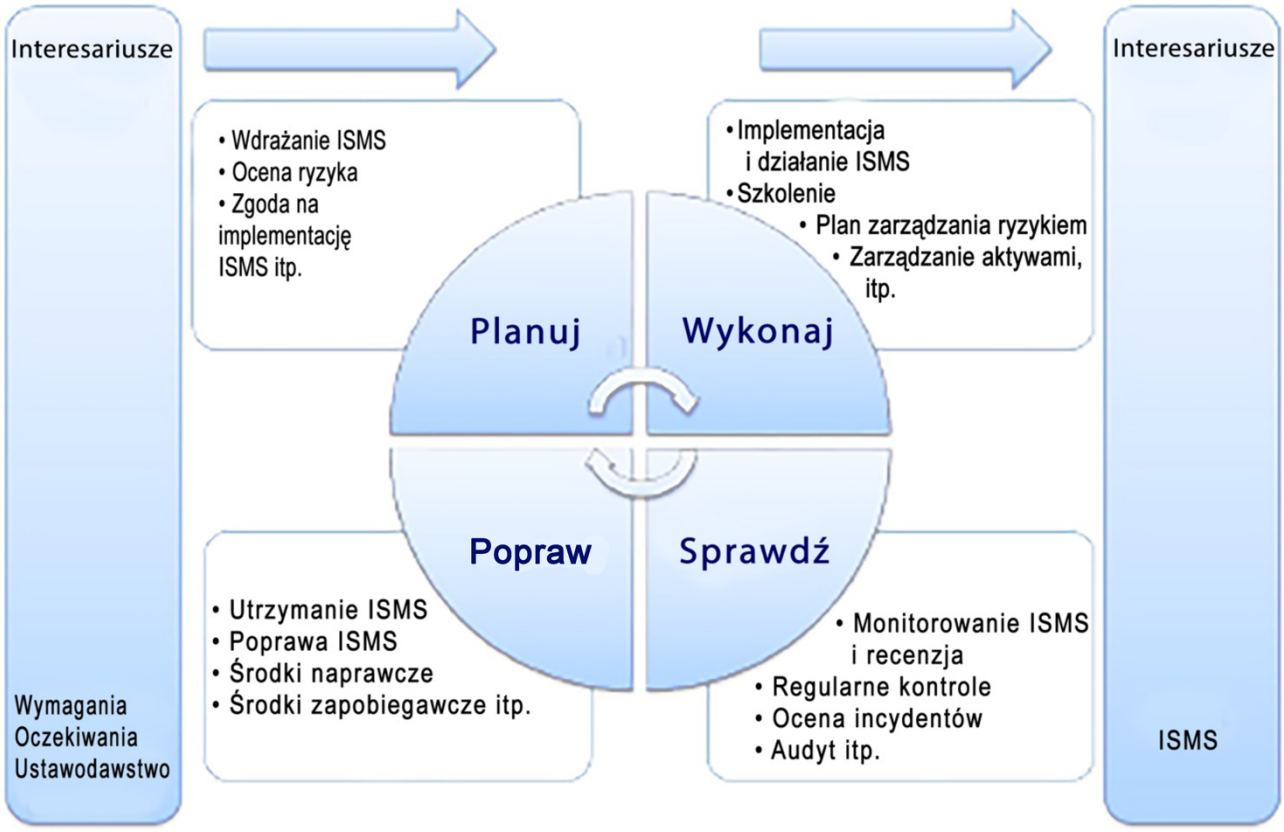
Cykl PDCA lub niektóre jego modyfikacje mogą być stosowane do wszystkich procesów ISMS. W najprostszy sposób model ten można przedstawić jako niekończące się koło:

[122] Przegląd norm znajduje się w EN ISO/IEC 27000 (369790) - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Przegląd i glosariusz

[123] ROSER, Christoph. *Wiele smaków PDCA* [online]. [cytowany 2018-07-06]. Dostępny pod adresem: https://www.allaboutlean.com/pdca-variants/

Obraz: Model PDCA[124]

Model PDCA został również przedstawiony w normie ISO/IEC 27001:2005 i ilustruje, w jaki sposób system ISMS przyjmuje wymagania dotyczące bezpieczeństwa informacji i oczekiwania interesariuszy jako dane wejściowe, a następnie wykorzystuje niezbędne działania i procesy w celu uzyskania wyników w zakresie bezpieczeństwa informacji, które spełniają te wymagania i oczekiwania.



Rysunek: Model PDCA zastosowany do procesów ISMS[125]

---

[124] *Cykl PDCA.* [online]. [cytowany 2018-07-06]. Dostępny pod adresem: https://www.creativesafetysupply.com/glossary/pdca-cycle/

[125] Zmodyfikowany i uzupełniony model PDCA. Oryginalny model został wprowadzony w normie ISO/IEC 27001:2005 str. 7

Plan (ustanowienie ISMS)	Ustanowienie polityki, celów, procesów i procedur ISMS związanych z zarządzaniem ryzykiem i poprawą bezpieczeństwa informacji w celu osiągnięcia wyników zgodnych z ogólną polityką i celami organizacji.
Do (wdrożenie i eksploatacja ISMS)	Wdrożenie i stosowanie polityk, środków, procesów i procedur ISMS.
Kontrola (monitorowanie i przegląd ISMS)	Ocenianie, tam gdzie to możliwe, i mierzenie wydajności procesu w odniesieniu do polityki ISMS, celów i praktycznych doświadczeń oraz zgłaszanie wyników kierownictwu organizacji do przeglądu.
Jednej (utrzymywanie i doskonalenie ISMS)	Podejmowanie działań korygujących i zapobiegawczych w oparciu o wyniki audytu wewnętrznego ISMS oraz przeglądu systemu zarządzania przez kierownictwo w celu osiągnięcia ciągłego doskonalenia ISMS.

Norma ISO/IEC 27001 promuje przyjęcie podejścia procesowego do **ustanawiania**, **wdrażania, obsługi**, **monitorowania**, **utrzymywania** i **doskonalenia ISMS organizacji.** W szczególności nacisk kładzie się na:

- zrozumienie wymagań organizacji w zakresie bezpieczeństwa informacji oraz potrzeby ustanowienia polityki i celów w zakresie bezpieczeństwa informacji,
- wdrażanie i stosowanie środków zarządzania bezpieczeństwem informacji w kontekście zarządzania ogólnym ryzykiem związanym z działalnością organizacji,
- monitorowanie i przegląd wyników i skuteczności ISMS,
- Ciągłe doskonalenie oparte na obiektywnych pomiarach.

"W przypadku ISMS w organizacji należy jasno opisać organizację zarządzania, obowiązki w zakresie bezpieczeństwa informacji na wszystkich szczeblach zarządzania, organy zawodowe oraz role w systemie bezpieczeństwa informacji.

Bezpieczeństwo informacji musi być odzwierciedlone w strukturze organizacyjnej organizacji, tak aby obejmowało działania i współpracę kierownictwa, osób odpowiedzialnych za systemy aplikacji, usługi operacyjne, użytkowników końcowych oraz osób odpowiedzialnych za poszczególne działania. Bezpieczeństwo informacji wymaga ścisłej współpracy między wszystkimi tymi grupami personelu oraz zapewnienia szkoleń z zakresu bezpieczeństwa informacji, tak aby oprócz osób odpowiedzialnych za bezpieczeństwo informacji i innych elementów bezpieczeństwa w organizacji, także personel zarządzający informacjami oraz wszyscy użytkownicy technologii informacyjnych posiadali podstawową wiedzę na temat bezpieczeństwa informacji."[126]

W związku z powyższym możliwe jest zdefiniowanie standardowych celów ISMS w organizacji:

- zapewnienie bezpieczeństwa systemów i usług teleinformatycznych,
- zapewnienie ciągłości działania systemów i usług teleinformatycznych,
- ochrona danych i informacji,
- ochrona innych aktywów,

[126] POŽÁR, Josef i Luděk NOVÁK. *Podręcznik pracy kierownika ds. bezpieczeństwa.* Praga: POŽÁR, Josef i Luděk NOVÁK. *System Zarządzania Bezpieczeństwem Informacji.* [online]. [cyt. 6 lipca 2018]. Dostępny pod adresem: https://www.cybersecurity.cz/data/srib.pdf s. 2

- radzenie sobie z zagrożeniami, zdarzeniami i incydentami, w tym zapobieganie im,
- poprawa bezpieczeństwa systemów i usług informacyjno-komunikacyjnych,
- Podnoszenie ogólnej świadomości użytkowników w zakresie bezpieczeństwa i zagrożeń bezpieczeństwa (edukacja),
- dzielenie się doświadczeniami z innymi podmiotami.

Wdrożenie ISMS w organizacji **nie może** jednak **zapewnić pełnego bezpieczeństwa** jej **aktywów.** Jednak wdrożenie ISMS może znacznie zmniejszyć ryzyko ingerencji w zasoby do akceptowalnego poziomu. Cały system jest tylko tak silny, jak jego najsłabsze ogniwo. W tym przypadku najsłabszym ogniwem, a zarazem największym zagrożeniem dla bezpieczeństwa informacji, jest człowiek.

5.2 Zarządzanie ryzykiem

Zgodnie z art. 7 NIS każde państwo członkowskie ma przyjąć krajową strategię bezpieczeństwa sieci i systemów informatycznych, określającą cele strategiczne oraz odpowiednie środki polityczne i regulacyjne w celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych. W szczególności przedmiotem krajowej strategii bezpieczeństwa sieci i systemów informatycznych są następujące cele i działania:

a) cele i priorytety krajowej strategii bezpieczeństwa sieci i systemów informacyjnych;

b) ramy zarządzania służące realizacji celów i priorytetów krajowej strategii bezpieczeństwa sieci i systemów informatycznych, w tym rolę i obowiązki organów rządowych i innych właściwych podmiotów;

c) ustanowienie środków gotowości, reagowania i odbudowy, w tym współpracy publiczno-prywatnej;

d) określanie programów edukacyjnych, informacyjnych i szkoleniowych związanych z krajową strategią bezpieczeństwa sieci i systemów informatycznych;

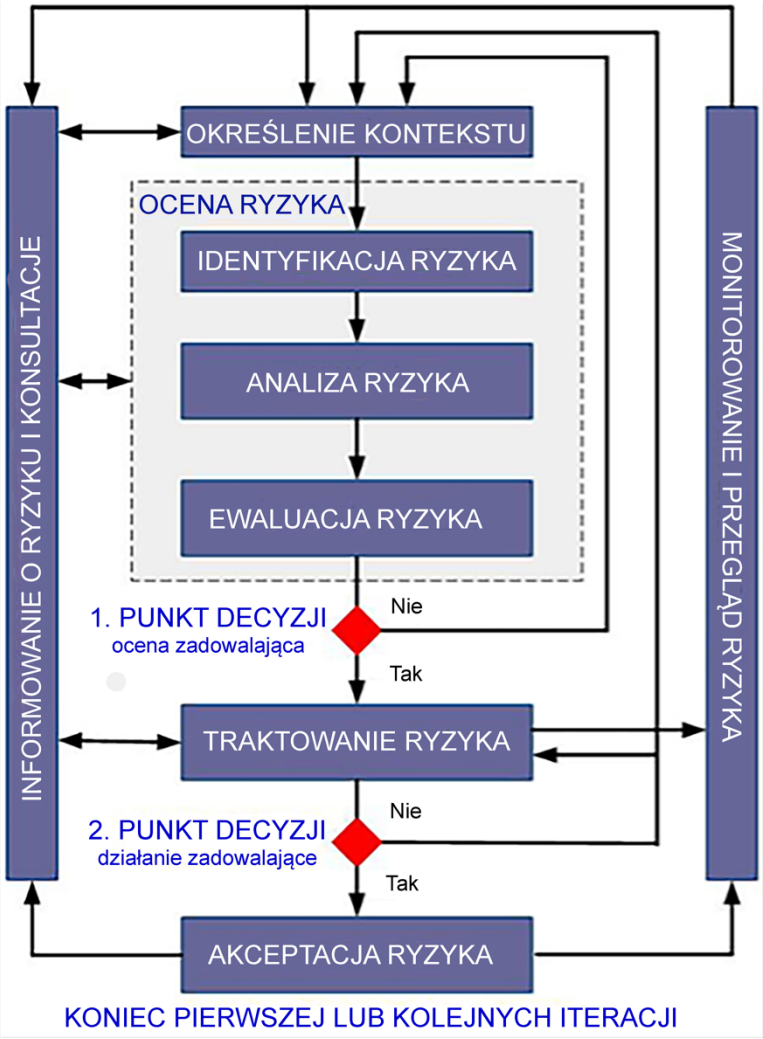
e) określanie planów badań i rozwoju związanych z narodową strategią bezpieczeństwa sieci i systemów informatycznych;

f) plan oceny ryzyka w celu identyfikacji zagrożeń;

g) wykaz różnych podmiotów zaangażowanych we wdrażanie krajowej strategii bezpieczeństwa sieci i systemów informatycznych.

Zgodnie z czeskim ustawodawstwem **ocena ryzyka** oznacza **ogólny proces identyfikacji, analizy i oceny ryzyka.**

Proces oceny ryzyka jest omówiony na przykład w normie ISO/IEC 27005, gdzie przedstawiono ten proces.



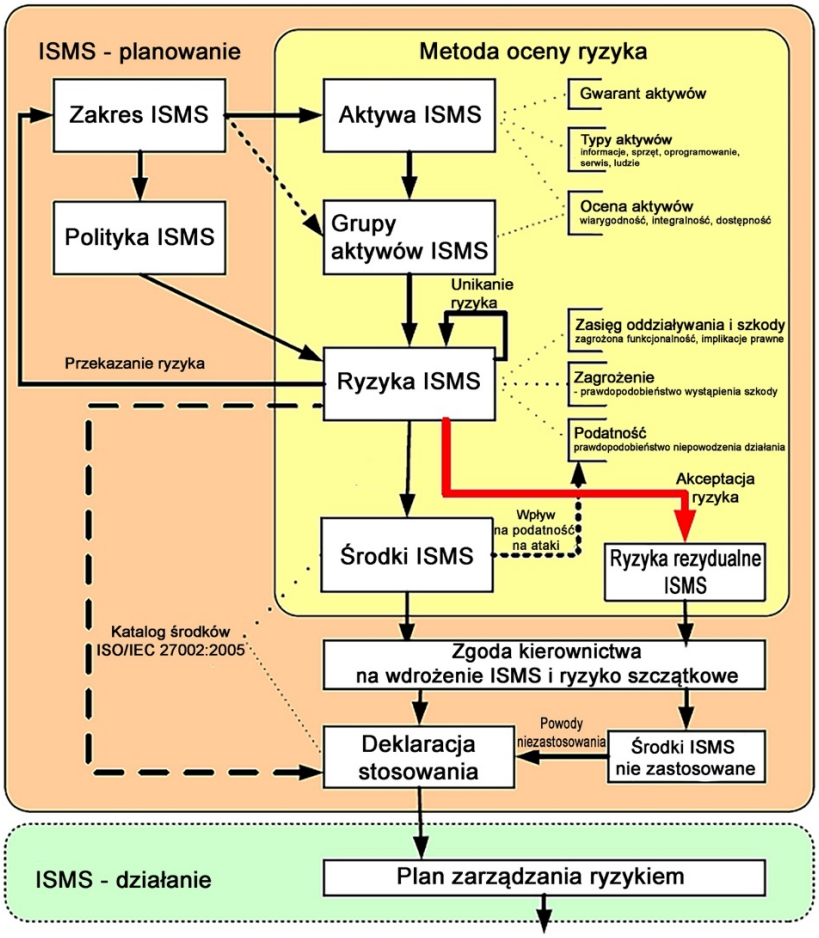
Rysunek: Demonstracja oceny ryzyka w ISMS[127]

Nawet w procesie oceny ryzyka należy przestrzegać modelu PDCA, ale dostosować go do oceny ryzyka.[128]

Proces ISMS	**Proces oceny ryzyka ISMS**
Planuj	Tworzenie kontekstu Oszacowanie ryzyka Opracowywanie planu zarządzania ryzykiem Akceptacja ryzyka
Wykonaj	Wdrażanie planu zarządzania ryzykiem
Sprawdź	Ciągłe monitorowanie i przegląd ryzyka
Popraw	Utrzymanie i doskonalenie procesu oceny ryzyka i zarządzania nim Proces kontroli

[127] ISO/IEC 27005 s. 8
[128] ISO/IEC 27005 s. 9

Jeśli chodzi o faktyczne zarządzanie ryzykiem, proces ten można przedstawić graficznie w następujący sposób:



Obraz: Zarządzanie ryzykiem w procesie ISMS[129]

Wartość ryzyka jest najczęściej wyrażana jako funkcja wpływu, zagrożenia i podatności. Na przykład do faktycznej oceny ryzyka można wykorzystać następującą funkcję:

Ryzyko = wpływ * zagrożenie * podatność

Jeśli dłużnik stosuje metodę oceny ryzyka, w której nie ma rozróżnienia na ocenę zagrożenia i podatności na zagrożenia, skale oceny zagrożenia i podatności na zagrożenia mogą być połączone. Połączenie skal nie powinno prowadzić do utraty możliwości rozróżniania poziomów zagrożenia i podatności. W tym celu można na przykład użyć komentarza, aby jasno wyrazić zarówno poziom zagrożenia, jak i poziom podatności. Podobne podejście należy przyjąć w przypadku, gdy osoba zobowiązana stosuje inną liczbę poziomów do oceny oddziaływań, zagrożeń, podatności na zagrożenia i ryzyka.[130]

W załączniku 3 do VoKB wymieniono również skale stosowane do oceny zagrożeń, podatności i ryzyka.

---

[129] POŽÁR, Josef i Luděk NOVÁK. *Podręcznik pracy kierownika ds. bezpieczeństwa.* Praga: POŽÁR, Josef i Luděk NOVÁK. *System zarządzania bezpieczeństwem informacji.* [online]. [cyt. 6 lipca 2018]. Dostępny pod adresem: https://www.cybersecurity.cz/data/srib.pdf s. 5

[130] Patrz załącznik 3(5) do VoKB

Poziom	Opis
Niski	Zagrożenie nie istnieje lub jest mało prawdopodobne. Przewiduje się, że zagrożenie **nie będzie się** pojawiać **częściej niż raz na 5 lat.**
Średnii	Jest mało prawdopodobne, aby zagrożenie było prawdopodobne. Oczekuje się, że zagrożenie zostanie zrealizowane w okresie od **1 do 5 lat**.
Wysoki	Zagrożenie jest prawdopodobne lub bardzo prawdopodobne. Oczekuje się, że zagrożenie zostanie zrealizowane w okresie od **1 miesiąca do 1 roku**.
Krytyczny	Zagrożenie jest bardzo prawdopodobne do mniej lub bardziej pewnego. Oczekuje się, że zagrożenie będzie występować **częściej niż raz w miesiącu.**

Rysunek: Skala oceny zagrożenia

Poziom	Opis
Niski	**Luka nie istnieje lub jej** wykorzystanie **jest mało prawdopodobne**. Stosowane są środki bezpieczeństwa umożliwiające wczesne wykrywanie potencjalnych słabych punktów lub prób ich wykorzystania.
Średnii	**Wykorzystanie tej luki jest mało prawdopodobne**. Stosowane są środki bezpieczeństwa, których skuteczność jest regularnie sprawdzana. Zdolność środków bezpieczeństwa do wykrywania potencjalnych słabych punktów lub prób ich pokonania w odpowiednim czasie jest ograniczona. Nie są znane żadne udane próby pokonania środków bezpieczeństwa.
Wysoki	**Wykorzystanie tej** luki **jest bardzo prawdopodobne.** Istnieją środki bezpieczeństwa, ale ich skuteczność nie obejmuje wszystkich niezbędnych aspektów i nie jest regularnie monitorowana. Znane są częściowe udane próby pokonania zabezpieczeń.
Krytyczny	**Wykorzystanie tej luki jest bardzo prawdopodobne,** ale **mniej lub bardziej pewne.** Środki bezpieczeństwa nie są wdrażane lub ich skuteczność jest poważnie ograniczona. Skuteczność środków bezpieczeństwa nie jest sprawdzana. Znane są udane próby pokonania środków bezpieczeństwa.

Rysunek: Skala oceny podatności na zagrożenia

Poziom	Opis
Niski	**Ryzyko jest** uważane za **dopuszczalne**.
Średnii	**Ryzyko można zmniejszyć za pomocą mniej wymagających środków** lub, w przypadku bardziej wymagających środków, ryzyko jest dopuszczalne.
Wysoki	**Ryzyko jest nieakceptowalne w dłuższej perspektywie** i należy podjąć systematyczne działania w celu jego wyeliminowania.
Krytyczny	**Ryzyko jest niedopuszczalne** i należy niezwłocznie podjąć kroki w celu jego wyeliminowania.

Rysunek: Skala oceny ryzyka

5.3 Polityka bezpieczeństwa

Polityka bezpieczeństwa oznacza **zbiór zasad i reguł określających sposób zapewnienia ochrony aktywów.**

Standard polityki bezpieczeństwa stanowi, że wyznaczone podmioty w odniesieniu do systemu zarządzania bezpieczeństwem informacji są zobowiązane do:

a) **ustanowienie polityki bezpieczeństwa** i **prowadzenie dokumentacji bezpieczeństwa** obejmującej następujące obszary polityki:[131]

- system zarządzania bezpieczeństwem informacji,
- zarządzanie aktywami,
- bezpieczeństwo organizacyjne,
- zarządzanie dostawcami,
- bezpieczeństwo zasobów ludzkich,
- zarządzanie ruchem i komunikacją,
- kontrola dostępu,
- bezpieczne zachowanie użytkowników,
- tworzenie kopii zapasowych i odzyskiwanie danych oraz przechowywanie długoterminowe,
- bezpieczne przesyłanie i wymiana informacji,
- zarządzanie podatnością na zagrożenia techniczne,
- bezpieczne korzystanie z urządzeń mobilnych,
- pozyskiwanie, rozwój i utrzymanie,
- ochrona danych osobowych,
- bezpieczeństwo fizyczne,
- bezpieczeństwo sieci komunikacyjnych,
- ochrona przed złośliwym kodem,
- wdrażanie i używanie narzędzia do wykrywania zdarzeń związanych z bezpieczeństwem cybernetycznym,
- bezpieczne korzystanie z ochrony kryptograficznej,
- zarządzanie zmianą,
- zarządzanie incydentami związanymi z bezpieczeństwem cybernetycznym,
- zarządzanie ciągłością działania.

Określa ona również **zawartość dokumentacji bezpieczeństwa**, która musi zawierać:

- raport z audytu bezpieczeństwa cybernetycznego,
- sprawozdanie z przeglądu systemu zarządzania bezpieczeństwem informacji,

[131] Szczegółowe informacje zawiera Załącznik 5 VoKB

- metodologię identyfikacji i oceny aktywów oraz oceny ryzyka,
- sprawozdanie z oceny aktywów i ryzyka,
- oświadczenie o stosowalności,
- plan zarządzania ryzykiem,
- Plan rozwoju świadomości bezpieczeństwa,
- zapis zmian,
- zgłoszone dane kontaktowe,
- przegląd ogólnie obowiązujących przepisów prawa, regulaminów wewnętrznych i innych zasad oraz zobowiązań umownych,
- inna zalecana dokumentacja (np. topologia infrastruktury, przegląd urządzeń sieciowych).

b) **regularny przegląd polityki bezpieczeństwa** i **dokumentacji bezpieczeństwa,**

c) Należy zapewnić aktualność polityki bezpieczeństwa i dokumentacji dotyczącej bezpieczeństwa.

Polityka bezpieczeństwa i dokumentacja bezpieczeństwa muszą być:

- dostępne w formie papierowej lub elektronicznej,
- przekazywane w obrębie osoby zobowiązanej,
- w rozsądny sposób dostępne dla zainteresowanych stron,
- kontrolowane,
- chronione pod względem poufności, integralności i dostępności,
- przechowywane w taki sposób, aby informacje w nich zawarte były kompletne, czytelne, łatwe do zidentyfikowania i łatwe do wyszukania.

5.4 Bezpieczeństwo organizacyjne

Definicja bezpieczeństwa organizacyjnego, a w szczególności zakotwiczenie bezpieczeństwa cybernetycznego lub teleinformatycznego w już funkcjonujących strukturach organizacji, ma bardzo istotne znaczenie dla potencjalnego zarządzania zagrożeniami lub atakami cybernetycznymi.

Kwestia bezpieczeństwa powinna być rozpatrywana na poziomie operacyjnym, taktycznym i strategicznym w organizacji z perspektywy jej kierownictwa.

Z punktu widzenia bezpieczeństwa ważne jest, aby jednostka (dział) zajmująca się bezpieczeństwem cybernetycznym była oddzielona od jednostki (działu), która zapewnia funkcjonowanie technologii informacyjno-komunikacyjnych.[132]

Przykład: autor spotkał się z administratorem sieci, który został zobowiązany przez pracodawcę do objęcia stanowiska kierownika ds. bezpieczeństwa. W praktyce oznaczałoby to, że administrator opracowywałby wytyczne, których należałoby przestrzegać, a także samodzielnie sprawdzałby je i egzekwował. Absurdalność tej sytuacji jest widoczna na pierwszy rzut oka.

[132] Por. *Role związane z bezpieczeństwem i ich integracja w organizacji.* [online]. [cited 2018 Aug 21]. Dostępny pod adresem: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 3

Bezpieczeństwo organizacyjne z założenia polega na tym, że wyznaczone podmioty stosują system zarządzania bezpieczeństwem informacji:

- **zapewnić, aby polityka bezpieczeństwa i cele ISMS były ustalone** w sposób zgodny z kierunkiem strategicznym osoby zobowiązanej,
- **zapewnić włączenie ISMS** do procesów osoby zobowiązanej,
- **zapewnić dostępność zasobów** potrzebnych do funkcjonowania **ISMS**,
- **informowanie personelu o znaczeniu ISMS** oraz o tym, jak ważne jest osiągnięcie zgodności z jego wymaganiami ze wszystkimi zainteresowanymi stronami,
- **zapewnić wsparcie w** osiąganiu zamierzonych wyników **ISMS**,
- **kierowanie** i wspieranie **personelu w rozwijaniu skuteczności ISMS**,
- **promować ciągłe doskonalenie ISMS**,
- **wspieranie osób pełniących** funkcje **związane z bezpieczeństwem w** promowaniu bezpieczeństwa cybernetycznego w obszarach, za które są odpowiedzialne,
- **zapewnić ustanowienie zasad wyznaczania administratorów** i **osób, które będą pełnić funkcje związane z bezpieczeństwem**,

  Role bezpieczeństwa to:

  - **Kierownik ds.** bezpieczeństwa cybernetycznego,
  - **Architekt** ds. bezpieczeństwa cybernetycznego,
  - **poręczyciel majątkowy**,
  - **Audytor** bezpieczeństwa cybernetycznego.
- **zapewnić zachowanie poufności** administratorów i osób pełniących role związane z bezpieczeństwem,
- **zapewnić osobom pełniącym role w zakresie ochrony odpowiednie uprawnienia** i zasoby, w tym środki budżetowe, do pełnienia swoich ról i wykonywania związanych z nimi zadań,
- **zapewnienie testowania planów ciągłości działania, odzyskiwania danych i procesów związanych z zarządzaniem incydentami związanymi z bezpieczeństwem cybernetycznym**.

Aby przypisać i wyświetlić (w tabeli) obowiązki poszczególnych osób (role bezpieczeństwa wg VoKB) w organizacji, należy zastosować **macierz odpowiedzialności RACI (matryca RACI)**. RACI to akronim złożony z początkowych liter słów:

R - Odpowiedzialny	kto jest odpowiedzialny za wykonanie zadania (czynności)
A - Odpowiedzialność (lub zatwierdzający)	kto jest odpowiedzialny za całe zadanie lub za zapewnienie, że proces jest realizowany zgodnie z wcześniej ustalonymi zasadami
C - konsultowany	który może udzielać cennych rad lub konsultacji w zakresie zadania, ale nie bierze odpowiedzialności za wykonanie procesu
I - poinformowany	kto ma być informowany o postępach w realizacji zadania lub decyzjach dotyczących zadania

Zasadą jest, że tylko jedna osoba ponosi ogólną odpowiedzialność (A - Accountability) za dane zadanie; liczba zaangażowanych osób (R - Responsibility) powinna być odpowiednia do zadania. Metoda RACI jest prostą formą modelu kompetencji.[133]

Procesy:	**Rola:**	**Komitet KB**	**Kierownik KB**	**Architekt KB**	**Audytor KB**	**Gwarant aktywów**
Ogólne zarządzanie i rozwój KB		**A**	**R**	**R**		**C**
System zarządzania bezpieczeństwem informacji		**A**	**R**	**C**		**C**
Projektowanie środków bezpieczeństwa		**C**	**A**	**R**		**C**
Wdrażanie środków bezpieczeństwa		**C**	**A**	**R**		**C**
Zapewnienie rozwoju, wykorzystania i bezpieczeństwa aktywów			**A**	**C**		**R**
KB Audyt		**I**	**C**	**C**	**A/R**	**C**

Rysunek: matryca RACI[134]

5.5 Zarządzanie aktywami

Aktywa to wszystko, co ma wartość dla danej osoby, organizacji lub państwa.

Z punktu widzenia prawa cywilnego majątek może być rzeczą **materialną** (budynek, system komputerowy, sieć, energia, towary itp.) lub **niematerialną** (informacje, wiedza, dane, programy itp.).

Zasobem może być jednak również **właściwość** (np. dostępność i funkcjonalność systemu i danych itp.) lub **reputacja** itp. Z punktu widzenia bezpieczeństwa cybernetycznego zasobem są również **ludzie** (użytkownicy, administratorzy itp.) oraz ich wiedza i doświadczenie.

Zasoby pomocnicze to zasoby techniczne, pracownicy i wykonawcy zaangażowani w eksploatację, rozwój, zarządzanie lub bezpieczeństwo systemu teleinformatycznego.

Podstawowym składnikiem **aktywów** jest informacja lub usługa przetwarzana lub dostarczana przez system teleinformatyczny.

"W ramach rozsądnego zarządzania bezpieczeństwem informacji ważne jest, aby mieć przegląd powiązań i zależności między aktywami głównymi i pomocniczymi".[135]

W ramach zarządzania aktywami jednostki są zobowiązane do:

- **ustanowienie metodologii identyfikacji aktywów**,

[133] Więcej informacji na ten temat można znaleźć np. w *Macierzy Odpowiedzialności RACI.* [online]. [cited 2018 Aug 21]. Dostępne pod adresem: https://managementmania.com/cs/matice-odpovednosti-raci lub *Role bezpieczeństwa i ich integracja w organizacji.* [online]. [cited 2018 Aug 21]. Dostępny pod adresem: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 6

[134] Macierz RACI w opisie podstawowych procesów związanych z rolami bezpieczeństwa. Relacje między poszczególnymi rolami i procesami bezpieczeństwa mogą się różnić w zależności od organizacji. *Role związane z bezpieczeństwem i ich integracja w organizacji.* [online]. [cited 2018 Aug 21]. Dostępny pod adresem: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 7.

[135] MAISNER, Martin i Barbora VLACHOVÁ. *Ustawa o cyberbezpieczeństwie. Komentarz.* Praga: Wolters Kluwer, 2015. s. 85

- ustanowienie metodologii **wyceny aktywów**,
- **identyfikację i ewidencję aktywów**,
- **zidentyfikować** i zarejestrować **poręczycieli aktywów**,
- **oceniać i rejestrować aktywa podstawowe** pod względem poufności, integralności i dostępności oraz klasyfikować je na różnych poziomach aktywów,
- **Identyfikowanie i rejestrowanie powiązań między aktywami podstawowymi i pomocniczymi** oraz ocena skutków zależności między aktywami podstawowymi i pomocniczymi,
- **ocenić zasoby wspierające i uwzględnić** współzależności między zasobami głównymi i wspierającymi,
- określić i **wdrożyć zasady ochrony** niezbędne do zabezpieczenia **każdego poziomu aktywów**,
- ustalenie dopuszczalnych sposobów korzystania z aktywów oraz zasad postępowania z aktywami, z uwzględnieniem poziomu aktywów, w tym zasad bezpiecznego elektronicznego udostępniania i fizycznego przekazywania aktywów,
- określenie sposobu likwidacji danych, danych operacyjnych, informacji i ich kopii lub likwidacji technicznych nośników danych, z uwzględnieniem poziomu aktywów.

Oceniając znaczenie aktywów podstawowych, należy wziąć pod uwagę:

- zakres i znaczenie danych osobowych, specjalnych kategorii danych osobowych lub tajemnic handlowych,
- zakres obowiązków prawnych lub innych zobowiązań,
- zakres zakłóceń w zarządzaniu wewnętrznym i działaniach kontrolnych,
- szkody dla interesów publicznych, handlowych lub gospodarczych oraz ewentualne straty finansowe,
- wpływ na świadczenie podstawowych usług,
- zakres zakłóceń w normalnej działalności,
- ma wpływ na zachowanie reputacji lub ochronę wartości firmy,
- wpływ na bezpieczeństwo i zdrowie ludzi,
- wpływ na stosunki międzynarodowe,
- wpływ na użytkowników systemu informacyjno-komunikacyjnego.

5.6 Bezpieczeństwo zasobów ludzkich

Podmioty są również zobowiązane do dbania o bezpieczeństwo zasobów ludzkich jako jednego z aktywów w ramach ISMS. Jak wspomniano wcześniej, człowiek jest zwykle najsłabszym ogniwem w systemie bezpieczeństwa cybernetycznego. W szczególności podmioty te są zobowiązane do:

- **Ustanowienia planu rozwoju świadomości bezpieczeństwa w** celu zapewnienia odpowiednich szkoleń i poprawy świadomości bezpieczeństwa,

  Plan ten obejmuje formę, treść i zakres:

    - Szkolenie użytkowników, administratorów, osób pełniących role związane z bezpieczeństwem oraz wykonawców w zakresie ich obowiązków i polityki bezpieczeństwa,
    - niezbędne teoretyczne i praktyczne szkolenie użytkowników, administratorów i osób pełniących role związane z bezpieczeństwem.
- **wskazania osób odpowiedzialnych** za realizację poszczególnych działań wymienionych w planie,
- **zapewnienia**, **aby** użytkownicy, administratorzy, osoby pełniące role związane z bezpieczeństwem oraz wykonawcy **byli informowani o** swoich obowiązkach i polityce bezpieczeństwa poprzez szkolenia wstępne i regularne,
- **zapewnienia regularnych szkoleń dla osób pełniących funkcje związane z bezpieczeństwem**,
- zapewnienia **regularnych szkoleń** i weryfikacji świadomości bezpieczeństwa **pracowników** zgodnie z ich opisem stanowiska pracy,
- zapewnienia, że **użytkownicy**, administratorzy i osoby pełniące role związane z bezpieczeństwem **są monitorowani pod kątem zgodności z polityką bezpieczeństwa**,
- w przypadku zakończenia stosunku umownego z administratorami i osobami pełniącymi role związane z bezpieczeństwem **zapewnienia przekazania obowiązków**,
- **ocenienia skuteczności planu rozwoju świadomości** bezpieczeństwa, przeprowadzonych szkoleń i innych działań związanych z podnoszeniem świadomości bezpieczeństwa,
- **określenia zasad i procedur postępowania** w **przypadku naruszenia ustalonych zasad bezpieczeństwa** przez użytkowników, administratorów i osoby pełniące role związane z bezpieczeństwem.

Istnieje obowiązek prowadzenia rejestru powyższych szkoleń, zawierającego temat szkolenia oraz listę osób, które odbyły szkolenie.

Przykład: ponieważ standardowe szkolenia, które są obowiązkowe tylko dla użytkowników, nie okazują się zbyt skuteczne, niektóre organizacje uciekają się do metod sprawdzających faktyczne zrozumienie informacji przedstawionych na szkoleniu. Może to być np. wysyłanie wiadomości phishingowych do użytkowników po sesji szkoleniowej poświęconej temu zagadnieniu. Następnie organizacja monitoruje, ilu użytkowników odpowiedziało na atak przez pomyłkę. Należy jednak zauważyć, że takie testy muszą być dobrze przemyślane i nie powinno się w ich planowaniu pomijać doradztwa prawnego, aby ocenić, czy zastosowany test nie będzie np. nadmiernym naruszeniem prywatności pracownika.

5.7 Zarządzanie ciągłością działania

Zarządzanie ciągłością działania (**BCM**) to proces identyfikowania kluczowych elementów (systemów i procesów) w organizacji, a następnie ustanawiania procesów i procedur zapewniających ciągłość działania lub odtworzenie tych elementów na wcześniej określonym poziomie, na którym można nadal wykonywać podstawowe zadania organizacji.

W przypadku zarządzania ciągłością działania należy przeprowadzić ocenę ryzyka i analizę istniejących systemów i usług teleinformatycznych, a na podstawie uzyskanych danych określić:

- **minimalny poziom usług możliwy do** zaakceptowania w zakresie użytkowania, obsługi i zarządzania systemem teleinformatycznym,

- **czas** przywracania minimalnego poziomu usług systemu teleinformatycznego po wystąpieniu incydentu zagrażającego bezpieczeństwu cybernetycznemu,
- **punkt odzyskiwania danych** jako okres czasu, w którym należy odzyskać dane po incydencie lub awarii związanej z bezpieczeństwem cybernetycznym.

Osoba zobowiązana powinna ponadto w ramach zarządzania ciągłością działania:

- **określa prawa i obowiązki** administratorów oraz osób pełniących role związane z bezpieczeństwem,
- wykorzystując ocenę ryzyka i analizę wpływu, oceniać i **dokumentować potencjalny wpływ incydentów** związanych z **bezpieczeństwem cybernetycznym oraz oceniać potencjalne ryzyko** związane z zagrożeniami dla ciągłości działania,
- **ustalenie polityki zarządzania ciągłością działania**,
- **opracowywanie, aktualizowanie i regularne testowanie planów ciągłości działania i planów awaryjnych** związanych z funkcjonowaniem systemu teleinformatycznego i związanych z nim usług,
- **wdraża środki mające** na **celu zwiększenie odporności systemu teleinformatycznego** na incydenty związane z bezpieczeństwem cybernetycznym i ograniczeniami dostępności.

5.8 Środki techniczne

Środki techniczne, wraz ze środkami organizacyjnymi, stanowią podstawowe elementy środków bezpieczeństwa. Podczas gdy środki organizacyjne koncentrują się przede wszystkim na ustalaniu zasad i polityki w organizacji, środki techniczne dotyczą przede wszystkim zasad tworzenia systemów i usług informacyjno-komunikacyjnych.

W ramach każdego działania technicznego przedstawione zostaną ewentualne narzędzia open source mające zastosowanie do danego działania.

5.8.1 Bezpieczeństwo fizyczne

Bezpieczeństwo fizyczne koncentruje się przede wszystkim na ochronie zasobów technicznych jednostki. W odniesieniu do bezpieczeństwa fizycznego Maisner stwierdza, że *"celem tego środka jest przede wszystkim uniemożliwienie osobom nieupoważnionym dostępu do poszczególnych elementów infrastruktury, serwerowni, miejsc pracy administratorów systemu itp. Celem jest zapobieganie kradzieży aktywów bezpośrednio i pośrednio związanych z systemem informatycznym lub zapobieganie uszkodzeniom sprzętu materialnego i niematerialnego oraz wyposażenia pomieszczeń. Ponadto stara się zapobiegać wyciekom informacji i danych".*[136]

Osoba zobowiązana jest w ramach bezpieczeństwa fizycznego:

- **zapobiegać uszkodzeniu**, kradzieży lub niewłaściwemu wykorzystaniu aktywów albo przerwaniu świadczenia usług systemu teleinformatycznego,
- ustanowić **fizyczną granicę bezpieczeństwa** ograniczającą obszar, na którym przechowywane i przetwarzane są informacje oraz znajdują się zasoby techniczne systemu teleinformatycznego,

[136] MAISNER, Martin i Barbora VLACHOVÁ. *Ustawa o cyberbezpieczeństwie. Komentarz.* Praga: Wolters Kluwer, 2015.

- **stosować środki ochrony** fizycznej **na** granicy fizycznej:
    - **aby zapobiec nieautoryzowanemu dostępowi,**
    - **aby zapobiec uszkodzeniom i ingerencjom osób niepowołanych,**
    - **aby zapewnić ochronę na poziomie obiektu i wewnątrz obiektów.**

Termin **obwód bezpieczeństwa** fizycznego określa wyznaczony obszar lub granice tego obszaru. Przestrzenią tą może być na przykład zbiór obiektów, sam obiekt lub jego część.

Budynek oznacza obiekt budowlany lub inną zamkniętą przestrzeń. **Granica obiektu oznacza przegrodę** budowlaną, barierę fizyczną (ogrodzenie) lub inną widocznie określoną granicę obszaru. **Obszar zabezpieczony** oznacza strukturalnie lub w inny widoczny sposób wydzieloną przestrzeń w obrębie obiektu.

Środkami bezpieczeństwa fizycznego mogą być:

- **urządzenia do barier mechanicznych** (np. zamki, drzwi, kraty, folie, szkło i inne elementy konstrukcyjne i budowlane związane z bezpieczeństwem, sejfy gabinetowe, drzwi skarbców i sejfy komorowe,
- **system kontroli dostępu do zabezpieczonego obszaru** [alarmowe i elektroniczne systemy bezpieczeństwa, czujki (ruchu, zbicia szyby itp.) określające warunki wejścia: element identyfikacyjny, PIN, dane biometryczne (lub ich kombinacja)],
- **elektryczne urządzenia sygnalizacyjne bezpieczeństwa** (systemy alarmowe i awaryjne - panele sterowania **elektrycznymi urządzeniami sygnalizacyjnymi bezpieczeństwa**, czujki **elektrycznych urządzeń sygnalizacyjnych** bezpieczeństwa, czujki wstrząsowe, systemy detekcji obwodowej, systemy awaryjne itp,)
- **specjalne systemy telewizyjne (systemy kamer,** systemy nadzoru CCTV itp.),
- **elektryczny system alarmu pożarowego** (podłączenie do centrali alarmu pożarowego lub do centrali alarmu pożarowego),
- **środki ograniczające skutki pożarów i klęsk żywiołowych** (systemy alarmowe, czujniki dymu, systemy tryskaczowe itp.),
- **sprzęt zapewniający ochronę przed awarią zasilania** (źródła rezerwowe - UPS, generatory diesla itp.).

Możliwe jest także wdrożenie np:

- **urządzenia chroniącego przed pasywnym i aktywnym podsłuchem.**[137]

Obszary, do których dostęp powinien być ograniczony lub uregulowany z punktu widzenia bezpieczeństwa systemów teleinformatycznych, to w szczególności **serwerownie** (podstawowe,

[137] Ściany, drzwi, podłogi i sufity muszą zapewniać odpowiednią izolację akustyczną przed pasywnym i aktywnym podsłuchem, a okna, otwory wentylacyjne i klimatyzacyjne muszą być zabezpieczone za pomocą środków technicznych. Obszar ten powinien być zabezpieczony przed echem spoza obszaru spotkań. W obszarze tym nie wolno umieszczać żadnych mebli ani sprzętu, chyba że zostały one sprawdzone pod kątem braku możliwości nieuprawnionego korzystania z technicznych środków pozyskiwania informacji w obszarze spotkań. Należy zarejestrować meble i wyposażenie znajdujące się na danym obszarze (w tym typ, numer seryjny i inwentarzowy, jeśli dotyczy), łącznie z historią przemieszczeń. Nie jest pożądane umieszczanie w tym obszarze urządzeń telefonicznych. Jeżeli ich instalacja jest absolutnie konieczna, należy je wyposażyć w odłącznik lub ręcznie odłączyć przed spotkaniem. Na teren obiektu nie wolno wnosić telefonów komórkowych, urządzeń nagrywających, urządzeń nadawczych, sprzętu do testowania, mierzenia i diagnostyki oraz innych urządzeń elektronicznych (nie dotyczy to urządzeń wykorzystywanych w ramach inspekcji przeprowadzanej za wiedzą osoby odpowiedzialnej lub jej przedstawiciela). Dla danego obszaru należy opracować zasady rejestracji i przemieszczania się osób i sprzętu.

zapasowe), **obszary z elementami sieci (**routery, przełączniki itp.), **obszary przechowywania danych** (szafy na dokumenty, pamięci NAS itp.), **pomieszczenia administratorów teleinformatycznych** itp.

Przykład: bezpieczeństwo fizyczne jest jednym z obszarów, w których zazwyczaj dochodzi do naruszeń zasad organizacyjnych i w których konieczne jest przeprowadzanie okresowych audytów. Podczas gdy większość pozostałych czynności w organizacji jest wykonywana przez administratorów, zarządzanie dostępem fizycznym jest często powierzane, na przykład ze względu na oszczędności, mniej wykwalifikowanym pracownikom, którzy mogą nie mieć takiej samej świadomości rzeczywistych problemów związanych z bezpieczeństwem.

Autor spotkał się z kilkoma sytuacjami, w których po pewnym czasie osoba odpowiedzialna za fizyczną kontrolę dostępu, choć nie miała wystarczających uprawnień do udzielenia pozwolenia, zaczęła przyznawać uprawnienia do dostępu osobom, które nie powinny mieć dostępu do danych obszarów (np. serwerowni), na przykład tylko dlatego, że przełożony poprosił o dostęp do obszaru chronionego.

Narzędzia typu open source mogą być również wykorzystywane do zapewniania bezpieczeństwa fizycznego. W szczególności będzie to przypadek *"wdrożenia centralnych konsoli bezpieczeństwa, w tym systemów nadzoru CCTV". Do tego celu można wykorzystać narzędzia przeznaczone do monitorowania elementów sieci (**Icinga, Nagios** itp.), uzupełnione o interfejsy dla odpowiednich czujników, połączone z programami do przesyłania i przechwytywania sygnałów wideo z kamer bezpieczeństwa."*[138]

5.8.2 Narzędzia do ochrony integralności sieci komunikacyjnych

Niektórzy administratorzy są zobowiązani:

- **zapewnić segmentację sieci** komunikacyjnej,
- zapewnić kontrolę komunikacji w obrębie sieci komunikacyjnej i na obwodzie sieci komunikacyjnej (tzn. **kontrolować bezpieczny dostęp między siecią wewnętrzną i zewnętrzną**),
- **stosować kryptografię** w **celu zapewnienia poufności i integralności danych podczas zdalnego dostępu**, zdalnego **zarządzania lub dostępu do sieci** komunikacyjnej z wykorzystaniem **technologii bezprzewodowych** (np. użycia kryptografii by zapewnić połączenie sieci teleinformatycznej VPN z **siecią** Wi-Fi itp,)
- **aktywnie blokować niechcianą komunikację** (np. filtry spamu itp.),
- zapewnić segmentację sieci i zarządzać komunikacją między segmentami sieci z użyciem narzędzi zapewniających ochronę integralności sieci komunikacyjnej.

*"Narzędzie do ochrony integralności sieci komunikacyjnych jest tu rozumiane jako **odpowiednio zaprojektowana topologia sieci**, w tym zastosowanie elementów sieciowych, które umożliwiają wymaganą segmentację sieci i filtrowanie ruchu między poszczególnymi elementami. Urządzenia stosowane do spełnienia tych wymagań to przełączniki Ethernet, routery i zapory sieciowe. Jeśli segmentacja sieci nie może być zapewniona przez sieci VLAN na zarządzalnym przełączniku, może być zapewniona przez kilka mniejszych, niezarządzalnych przełączników, z których każdy realizuje pojedynczą fizyczną sieć LAN.*

[138] KODET, Jaroslav. *Cyberprzestrzeganie prawa: Wykorzystaj w pełni narzędzia open source.* [online]. [cytowany 2018-04-25]. Dostępny pod adresem: https://**www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf**

W przypadku segmentacji niektórych sieci możliwe jest także zastosowanie np. routerów Turris (https://www.turris.cz/cs/), które gwarantują wysoki poziom bezpieczeństwa (dzięki oprogramowaniu sprzętowemu, które zostało zaprojektowane z myślą o maksymalnym bezpieczeństwie) oraz niskie zużycie energii.

***Routery programowe/ zapory sieciowe**: www.ipcop.org/ ; https://www.ipfire.org/*

***Przełącznik** Ethernet dla środowisk zwirtualizowanych: http://www.openvswitch.org/".*[139]

5.8.3 Narzędzie do weryfikacji tożsamości użytkownika

W ramach bezpieczeństwa fizycznego niektórzy administratorzy są zobowiązani do korzystania z narzędzia do zarządzania tożsamością użytkowników, administratorów i aplikacji systemu teleinformatycznego oraz do weryfikowania ich tożsamości.

Narzędzie to jest obecnie de facto częścią wszystkich powszechnie używanych systemów operacyjnych (Linux, iOS, Windows). Jak podaje VoKB, narzędzie to ma zapewnić:

- **weryfikację tożsamości osoby** (przed rozpoczęciem działań w systemie teleinformatycznym),
- **kontrolę liczby** możliwych nieudanych **prób logowania**,
- **odporność** przechowywanych lub przesyłanych **danych** uwierzytelniających **na kradzież i niewłaściwe wykorzystanie,**
- **przechowywanie** danych uwierzytelniających w formie odpornej na ataki offline,
- **ponowne uwierzytelnianie tożsamości** po określonym czasie bezczynności,
- **zachowanie poufności danych uwierzytelniających** podczas przywracania dostępu,
- **scentralizowane zarządzanie tożsamością**.

Osoba zobowiązana wykorzystuje następujące elementy do weryfikacji tożsamości użytkowników, administratorów i aplikacji:

1. **mechanizm uwierzytelniania,** który nie **opiera się wyłącznie** na użyciu identyfikatora konta i hasła, ale na **uwierzytelnianiu wieloczynnikowym z** użyciem **co najmniej dwóch różnych typów czynników,**
2. narzędzie do weryfikacji tożsamości użytkowników, administratorów i aplikacji, wykorzystujące **uwierzytelnianie za** pomocą **klucza kryptograficznego** i gwarantujące podobny poziom bezpieczeństwa[140] ,
3. Narzędzie do **uwierzytelniania** użytkowników, administratorów i aplikacji, które do **uwierzytelniania** wykorzystuje **identyfikator konta i hasło.**[141]

Jeśli do uwierzytelniania używane są konto i hasło, muszą być spełnione następujące warunki:

- minimalna długość hasła:
    - **12 znaków dla użytkowników** i
    - **17 znaków dla administratorów i aplikacji.**

---

[139] KODET, Jaroslav. *Cyberprzestrzeganie prawa: Wykorzystaj w pełni narzędzia open source.* [online]. [cytowany 2018-04-25]. Dostępny pod adresem: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[140] Zakładając, że użytkownik nie spełnił jeszcze warunków pierwszego z preferowanych mechanizmów uwierzytelniania.

[141] Zakładając, że użytkownik nie spełnił jeszcze warunków pierwszego lub drugiego z preferowanych mechanizmów uwierzytelniania

- **możliwość wprowadzenia hasła składającego się z co najmniej 64 znaków,**
- możliwość stosowania w **haśle dużych i małych liter, cyfr i znaków specjalnych,**
- **możliwość zmiany hasła**, z zachowaniem co najmniej **30-minutowych odstępów między zmianami** hasła**,**
- **niezezwalanie użytkownikom i administratorom na:**
    - **wybranie najczęściej używanego hasła,**
    - **tworzenie haseł na podstawie** wielu powtarzających się znaków, nazwy logowania, adresu e-mail, nazwy systemu itp,
    - ponowne wykorzystanie wcześniej używanych haseł **z pamięcią co najmniej 12 poprzednich haseł**.
- **obowiązkowa zmiany hasła** w **odstępach nie dłuższych niż 18 miesięcy**, z wyjątkiem kont używanych do odzyskiwania danych po awarii,
- **wymuszenie natychmiastowej zmianę domyślnego hasła po pierwszym użyciu,**
- **natychmiastowe** unieważnienie **hasła użytego do przywrócenia dostępu po jego pierwszym użyciu lub po upływie maksymalnie 60 minut od jego utworzenia,**
- **uwzględnienie zasad tworzenia bezpiecznych haseł w planie zwiększania świadomości bezpieczeństwa**.

Przykład: podczas szkolenia użytkowników zaleca się korzystanie z praktycznych przykładów. Na przykład narzędzia CEWL lub CUPP. Oba te rozwiązania można znaleźć na przykład w dystrybucji Linuksa Kali. Narzędzie CEWL może utworzyć słownik do ataku słownikowego dostosowany do konkretnej organizacji na podstawie zawartości jej strony internetowej. Narzędzie CUPP może wówczas utworzyć słownik dostosowany do potrzeb konkretnego użytkownika. Te praktyczne demonstracje są, jak wynika z doświadczeń autorów, bardzo przydatne dla użytkowników, ponieważ mogą oni praktycznie przekonać się, że ich wcześniej używane hasło składające się na przykład z daty urodzenia i imienia rodzinnego psa może zostać wygenerowane, jeśli atakujący posiada wystarczające informacje na ich temat.

"W zakresie praktycznego uwierzytelniania tożsamości użytkowników społeczność open source oferuje wiele programów zgodnych z ich komercyjnymi odpowiednikami. Należą do nich:

FreeRADIUS - http://freeradius.org/ /RADIUS

OpenLDAP - http://www.openldap.org/ /Microsoft AD, Oracle Internet Directory

Kerberos - https://www.gnu.org/software/shishi/

OpenDiameter - https://sourceforge.net/projects/diameter/

Wszystkie te narzędzia zapewniają możliwość egzekwowania określonej złożoności hasła oraz innych atrybutów wymaganych przez ZoKB, albo samodzielnie poprzez login.conf, *albo przy użyciu zewnętrznych mechanizmów, takich jak cracklib i słowniki popularnych "haseł".*[142]

[142] KODET, Jaroslav. *Cyberprzestrzeganie prawa: Wykorzystaj w pełni narzędzia open source.* [online]. [cytowany 2018-04-25]. Dostępny pod adresem: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

5.8.4 Narzędzie kontroli uprawnień dostępu

Niektórzy administratorzy są zobowiązani do stosowania scentralizowanego narzędzia kontroli dostępu w ramach bezpieczeństwa fizycznego.

Termin "**zezwolenie" oznacza** prawo dostępu do zasobu (zazwyczaj systemu informatycznego lub komunikacyjnego, aplikacji itp.) W praktyce jest to narzędzie do "zarządzania użytkownikami i grupami" oraz narzędzie do ustawiania uprawnień do plików i katalogów. Narzędzia te są zastrzeżoną częścią wszystkich standardowych systemów operacyjnych.

Scentralizowane narzędzie do zarządzania uprawnieniami dostępu, zapewniające zarządzanie uprawnieniami:

- w celu uzyskania dostępu do poszczególnych zasobów systemu teleinformatycznego; oraz
- do odczytu danych, zapisu danych i zmiany uprawnień.

Wskazane jest zastosowanie narzędzi do scentralizowanego zarządzania uprawnieniami dostępu, które będą **komunikować się z centralnym serwerem AAA** (Authentication, Authorization, Accounting).

Przykład: podczas projektowania oprogramowania należy pamiętać o zarządzaniu uprawnieniami dostępu. Autor zna aplikację, która miała bardzo ogólne uprawnienia i w zasadzie posiadała tylko role administratora i użytkownika. Administrator został upoważniony do dodawania innych użytkowników i administratorów, a użytkownik został upoważniony do wykonywania innych czynności. Aplikacja ta zawierała jednak ważne informacje o klientach organizacji. Ponieważ aplikacja ta nie pozwalała na żadną granulację uprawnień, wszyscy użytkownicy, niezależnie od ich rzeczywistych potrzeb, byli uprawnieni do dostępu do dowolnej części informacji o kliencie. Sytuacja ta doprowadziła w końcu do wycieku danych dotyczących konkretnego klienta.

5.8.5 Narzędzie do ochrony przed złośliwym kodem

Niektórzy administratorzy wprowadzają ochronę przed złośliwym kodem jako część systemu bezpieczeństwa fizycznego mającego:

- **zapewnić** (biorąc pod uwagę znaczenie aktywów) **stosowanie narzędzia do ciągłej automatycznej ochrony**
    - stacje końcowe,
    - urządzenia mobilne,
    - serwery,
    - przechowywanie danych i wymienne nośniki pamięci,
    - sieci komunikacyjnej i elementów sieci komunikacyjnej,
    - podobne urządzenia.
- **monitorować i kontrolować korzystanie z urządzeń wymiennych i nośników danych,**
- **kontrolować automatyczne uruchamianie zawartości** urządzeń wymiennych i nośników danych,
- **kontrolować uprawnienia do wykonywania kodu,**
- **przeprowadzać regularne i skuteczne aktualizacje** narzędzia **do** ochrony przed złośliwym kodem.

*"**Ochrona przed złośliwym oprogramowaniem rozpowszechnianym za pośrednictwem poczty elektronicznej.** Rozwiązaniem typu open source zapewniającym ochronę przed złośliwym oprogramowaniem jest projekt ASSP (AntiSpam SMTP Proxy, https://sourceforge.net/projects/assp/), który umożliwia złożoną konfigurację zachowania serwera proxy za pomocą interfejsu WWW.*

***Ochrona przed złośliwym oprogramowaniem rozpowszechnianym za pośrednictwem Internetu.** Dobrym rozwiązaniem jest na przykład projekt HTTP AntiVirus Proxy (http://www.havp.org/) lub www.cacheguard.com. Również w tym przypadku należy zapewnić odpowiednią ochronę stacji roboczych punktów końcowych, ponieważ zaszyfrowany ruch nie może być skanowany w czasie rzeczywistym w trybie "man-in-the-middle".*

Blokowanie jego ruchu sieciowego, zarówno na poziomie infrastruktury danych, jak i na poziomie "osobistych zapór ogniowych" stacji końcowych. Zasady komunikacji sieciowej powinny być ustawione w sposób "paranoidalny", tzn. zezwalać tylko na ruch niezbędny do działania legalnego oprogramowania, nie zezwalać na wszystko inne. Jednak środki po stronie serwera, serwera proxy lub elementów infrastruktury sieciowej w żadnym wypadku nie zastępują w pełni ochrony przed złośliwym oprogramowaniem na stacjach roboczych punktów końcowych, zwłaszcza że nie zawsze są one w stanie przechwycić ruch szyfrowany, który jest odszyfrowywany dopiero w programie klienckim. "[143]

5.8.6 Narzędzie do wykrywania zdarzeń związanych z bezpieczeństwem cybernetycznym

W ramach bezpieczeństwa fizycznego niektórzy administratorzy są zobowiązani do wdrożenia w sieci komunikacyjnej, której częścią jest system teleinformatyczny, narzędzia do wykrywania zdarzeń związanych z bezpieczeństwem cybernetycznym w celu zapewnienia:

- **weryfikacji i kontroli przesyłanych danych w sieciach komunikacyjnych** i pomiędzy nimi,
- **weryfikacji i kontroli przesyłanych danych na granicy** sieci komunikacyjnej; oraz
- **blokowania niechcianej komunikacji**.

"Do wykrywania zdarzeń związanych z bezpieczeństwem cybernetycznym można wykorzystać dane wyjściowe wielu narzędzi programowych, takich jak Logwatch (https://sourceforge.net/projects/logwatch/files/), Epylog (https://fedoraproject.org/wiki/Infrastructure/Fedorahosted-retirement), systemy wykrywania włamań, takie jak OpenVAS (http://openvas.org/), Suricata (https://suricata-ids.org/), Snort (https://www.snort.org/) czy Samhain (la-samhna.de/Samoin). "[144]

5.8.7 Narzędzie do zbierania i oceny zdarzeń związanych z bezpieczeństwem cybernetycznym

W ramach bezpieczeństwa fizycznego niektórzy administratorzy są zobowiązani do stosowania **narzędzia do gromadzenia i ciągłej oceny zdarzeń związanych z bezpieczeństwem cybernetycznym,** aby umożliwić

- **gromadzenie i ocenę zdarzeń**,

---

[143] KODET, Jaroslav. *Cyberprzestrzeganie prawa: Wykorzystaj w pełni narzędzia open source.* [online]. [cytowany 2018-04-25]. Dostępny pod adresem: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[144] KODET, Jaroslav. *Cyberprzestrzeganie prawa: Wykorzystaj w pełni narzędzia open source.* [online]. [cytowany 2018-04-25]. Dostępny pod adresem: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

- **wyszukiwanie i grupowanie powiązanych rekordów,**
- **przekazywanie wyznaczonym** osobom **odpowiedzialnym za bezpieczeństwo informacji** o wykrytych zdarzeniach związanych z bezpieczeństwem cybernetycznym,
- **ocenianie zdarzeń związanych z bezpieczeństwem cybernetycznym w** celu identyfikacji incydentów związanych z bezpieczeństwem cybernetycznym, w tym wczesne ostrzeganie wyznaczonych osób odpowiedzialnych za bezpieczeństwo,
- ograniczanie przypadków nieprawidłowej oceny zdarzeń poprzez regularne aktualizowanie ustawień reguł dla:
    - ocena zdarzeń związanych z bezpieczeństwem cybernetycznym,
    - wczesne ostrzeżenie,
- wykorzystanie informacji uzyskanych przez narzędzie do gromadzenia i oceny zdarzeń związanych z bezpieczeństwem cybernetycznym w celu optymalnego ustawienia środków bezpieczeństwa systemu teleinformatycznego.

Narzędzia służące do gromadzenia i oceny zdarzeń związanych z bezpieczeństwem cybernetycznym określa się mianem **SIEM** (Security Incident and Event Management).

W ramach rozwiązania SIEM typu open source można wykorzystać na przykład OSSIM/USM (https://www.alienvault.com/products/usm-anywhere/try-it-now), OSSEC (www.ossec.net/) lub Logalyze (www.logalyze.com).[145]

5.8.8 Bezpieczeństwo aplikacji

W przypadku bezpieczeństwa aplikacji uwagę zwraca się na aplikacje wykorzystywane w systemach informatycznych (w ramach systemu komputerowego, urządzenia mobilnego lub jako aplikacja internetowa). Bezpieczeństwo aplikacji zapewnia się m.in. poprzez testy penetracyjne aplikacji lub zapory aplikacji.

W ramach bezpieczeństwa fizycznego niektórzy administratorzy są zobowiązani do przeprowadzania **testów penetracyjnych** systemu teleinformatycznego, koncentrując się na krytycznych zasobach, tj:

- **przed** ich **uruchomieniem oraz**
- **w związku z istotną zmianą**.

Osoba zobowiązana musi również **zapewnić stałą ochronę wniosków**, **informacji i transakcji przed:**

- niedozwolonym działaniem,
- przeciwdziałaniem podjętym działaniom.

"Do zapór aplikacji należą na przykład moduły bezpieczeństwa webservera (www.modsecurity.org) lub OWASP Web Application Firewall. Komercyjne narzędzia do testowania bezpieczeństwa aplikacji to między innymi Nessus (www.tenable.com/products/nessusvulnerability-scanner). Jego otwartą alternatywą jest projekt Open-VAS (www.openvas.org/)."[146]

---

[145] KODET, Jaroslav. *Cyberprzestrzeganie prawa: Wykorzystaj w pełni narzędzia open source.* [online]. [cytowany 2018-04-25]. Dostępny pod adresem: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[146] Ibid

5.8.9 Zasoby kryptograficzne

Kryptografia (szyfrowanie) to dziedzina nauki zajmująca się przekształcaniem zrozumiałych informacji w formę, która jest niezrozumiała dla odbiorcy, chyba że posiada on klucze, które mogą być użyte do odszyfrowania informacji.

W związku z przekazywaniem znacznej ilości danych i informacji do systemów teleinformatycznych należy zwrócić większą uwagę na możliwości szyfrowania (utajniania treści) przesyłanych danych.

Od niektórych administratorów wymaga się, aby w ramach bezpieczeństwa fizycznego chronili zasoby systemu teleinformatycznego:

- wykorzystywali obecnie sprawdzone algorytmy kryptograficzne i klucze kryptograficzne,
- stosowali system zarządzania kluczami i certyfikatami, który:
    - zapewnia generowanie, dystrybucję, przechowywanie, modyfikowanie, ograniczanie ważności, unieważnianie certyfikatów oraz usuwanie kluczy,
    - umożliwi kontrolę i audyt.
- promowali bezpieczne posługiwanie się zasobami kryptograficznymi,
- uwzględniali zalecenia dotyczące środków kryptograficznych wydane przez Urząd (NUCIB), opublikowane na jego stronie internetowej.

*"Biblioteki OpenSSL (*openssl.org*) są wykorzystywane do zapewnienia wystarczająco solidnego szyfrowania ruchu sieciowego, ale konieczne jest zapewnienie, że są one aktualne i odpowiednio skonfigurowane, aby spełnić wymagania tego dekretu. Konieczne jest monitorowanie bieżących raportów o lukach w zabezpieczeniach i niezwłoczne uaktualnianie niezgodnych wersji bibliotek do wariantów bez znanych luk. W tym zakresie można polecić projekt bettercrypto (https://bettercrypto.org/), który ma pomóc administratorom w jak najlepszym zabezpieczeniu usług i kryptografii, z których korzystają. "*[147]

5.8.10 Narzędzie do zapewniania poziomu dostępności informacji

W ramach bezpieczeństwa fizycznego niektórzy administratorzy są zobowiązani do wdrożenia środków zapewniających odpowiedni poziom dostępności:

- **dostępność systemu informacji i komunikacji**,
- **odporność systemu teleinformatycznego** na incydenty związane z bezpieczeństwem cybernetycznym, które mogłyby ograniczyć jego dostępność,
- **dostępność krytycznych zasobów technicznych** systemu teleinformatycznego,
- **nadmiarowość zasobów** niezbędnych do zapewnienia dostępności systemu teleinformatycznego.

Wdrożenie narzędzia służącego do zapewnienia poziomu dostępności informacji prowadzi do realizacji wartości organizacyjnej: zarządzania ciągłością działania (**BCM**).

"Aby osiągnąć wymagany poziom dostępności, można wykorzystać technologie klastrowe i chmurowe opracowane jako open source (KVM, OpenStack) lub oprogramowanie do tworzenia kopii

[147] KODET, Jaroslav. *Cyberprzestrzeganie prawa: Wykorzystaj w pełni narzędzia open source.* **[online]. [cytowany 2018-04-25]. Dostępny pod adresem:** https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

zapasowych/odtwarzania (https://sourceforge.net/projects/bacula/), które zapewnia dostępność zastępczego zasobu w określonym czasie. "[148]

[148] Ibid

PODSUMOWANIE ROZDZIAŁU

- Istnieje wiele powodów, dla których warto przyjąć i wdrożyć zasady bezpieczeństwa cybernetycznego. Najczęstsze z nich to na przykład negatywne skutki ekonomiczne w przypadku udanego ataku cybernetycznego, podczas którego skradzione zostaną dane wrażliwe. Udany atak cybernetyczny może również zagrozić własnym operacjom i funkcjonowaniu organizacji, ponieważ dostęp do systemów komputerowych lub danych może być ograniczony np. przez oprogramowanie typu ransomware. Innym powodem wdrożenia bezpieczeństwa cybernetycznego może być również utrata wiarygodności zagrożonej organizacji.
- Obecnie najważniejszym dokumentem Unii Europejskiej odnoszącym się do kwestii cyberbezpieczeństwa jest DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 z dnia 6 lipca 2016 r. dotycząca środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w całej Unii.
- System zarządzania bezpieczeństwem informacji (ISMS) to zbiór zasad mających na celu ochronę poufności, integralności i dostępności informacji poprzez zastosowanie procesu zarządzania ryzykiem oraz zapewnienie zainteresowanych stron, że ryzyko jest odpowiednio zarządzane.
- Rozwiązanie ISMS wymaga systemowego i kompleksowego podejścia, uwzględniającego zasady i elementy w całym cyklu życia bezpieczeństwa cybernetycznego. System zarządzania ISMS opiera się na cyklu Deminga, czyli cyklu PDCA (Plan-Do-Check-Act; Planuj-Wykonaj-Sprawdź-Działaj).
- Cykl PDCA to jedna z podstawowych zasad zarządzania, polegająca na stopniowej poprawie jakości procesów, usług, danych, produktów itp. poprzez ciągłe powtarzanie czterech podstawowych czynności: planuj-wykonaj-sprawdź-działaj.
- Wartość ryzyka jest najczęściej wyrażana jako funkcja wpływu, zagrożenia i podatności. Na przykład do rzeczywistej oceny ryzyka można wykorzystać następującą funkcję:
    - Ryzyko = wpływ * zagrożenie * podatność
- Polityka bezpieczeństwa oznacza zbiór zasad i reguł określających sposób zapewnienia ochrony aktywów.
- Zdefiniowanie bezpieczeństwa organizacyjnego, a w szczególności zakotwiczenie bezpieczeństwa cybernetycznego lub bezpieczeństwa technologii informacyjno-komunikacyjnych w już funkcjonujących strukturach organizacji, ma bardzo istotne znaczenie dla potencjalnego zarządzania zagrożeniami lub atakami cybernetycznymi.
- Aktywa to wszystko, co ma wartość dla danej osoby, organizacji lub państwa.
- Zasoby pomocnicze to zasoby techniczne, pracownicy i wykonawcy zaangażowani w eksploatację, rozwój, zarządzanie lub bezpieczeństwo systemu teleinformatycznego.
- Podstawowym składnikiem aktywów jest informacja lub usługa przetwarzana lub dostarczana przez system teleinformatyczny.
- Zarządzanie ciągłością działania (BCM) to proces identyfikowania kluczowych elementów (systemów i procesów) w organizacji, a następnie ustanawiania procesów i procedur zapewniających ciągłość działania lub odtworzenie tych elementów na wcześniej określonym poziomie, na którym można nadal wykonywać podstawowe zadania organizacji.

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

- Dyrektywa NIS
- ISMS
- PDCA
- Zagrożenie
- Ryzyko
- Impact
- Podatność na zagrożenia
- Polityka bezpieczeństwa
- Aktywa
- Bezpieczeństwo fizyczne
- Zarządzanie ciągłością działania

PYTANIA KONTROLNE

- Zdefiniuj ISMS.
- Co to jest cykl PDCA i jak się go stosuje?
- Jakie elementy można zaliczyć do bezpieczeństwa fizycznego?
- Co to jest zarządzanie ciągłością działania?
- Zdefiniuj pojęcie zagrożenia.
- Zdefiniuj pojęcie ryzyka.
- Zdefiniuj pojęcie wpływu.
- Zdefiniuj pojęcie podatności na zagrożenia.
- Zdefiniuj pojęcie aktywów.
- Jakie aktywa rozpoznajemy i co to jest aktywum?

6. Ochrona danych osobowych w cyberprzestrzeni

W pierwszej kolejności chciałbym się skupić na ochronie osoby fizycznej, a konkretnie na ochronie wizerunku i prywatności jednostki. Prywatność jest jednym z podstawowych praw człowieka zapisanych w Powszechnej Deklaracji Praw Człowieka z 1948 r.[149] .

6.1 Wchodzenie w prawa i obowiązki wynikające z określonych przepisów prawnych

Jesteśmy głęboko przekonani, że **nie należy oddzielnie traktować kwestii bezpieczeństwa cybernetycznego i innych obszarów** (np. ochrony danych osobowych, danych związanych z łącznością elektroniczną i innych podobnych danych).

Powodem tego przekonania jest rosnąca integracja i współzależność różnych kategorii danych z systemami komputerowymi i działającymi na nich aplikacjami. Te wzajemne połączenia i digitalizacja danych analogowych będą się w przyszłości tylko nasilać.

Z tego powodu zasadne wydaje się zajęcie się kwestią bezpieczeństwa w sposób kompleksowy, a nie tylko w kontekście praw i obowiązków wynikających z ustawy o cyberbezpieczeństwie czy innych przepisów.

Celem organizacji lub osoby fizycznej powinno być wprowadzenie zasad, procesów, procedur i środków bezpieczeństwa, które spełniają wymogi NIS, a także, na przykład, GDRP, ePrivacy, eIDAS itp. Taki proces umożliwi stworzenie **zintegrowanego** systemu **bezpieczeństwa.**[150]

---

[149] Dostępny w Internecie: http://www.osn.cz/wp-content/uploads/2015/03/vseobecna-deklarace-lidskych-prav.pdf
W Powszechnej Deklaracji Praw Człowieka prawa te są zapisane przede wszystkim w artykułach 12 i 18.
Artykuł 12: *"Nikt nie **może być narażony na samowolną ingerencję w swoje życie prywatne**, rodzinne, domowe lub **korespondencję,** ani też na zamachy na jego honor lub reputację. **Każdy ma prawo do ochrony prawnej przed taką ingerencją lub zamachami**".* "
Artykuł 18: *"Każdy człowiek ma prawo do wolności myśli, sumienia i wyznania; prawo to obejmuje swobodę zmiany religii lub przekonań oraz swobodę głoszenia swej religii lub przekonań, indywidualnie lub wspólnie z innymi, publicznie lub prywatnie, poprzez nauczanie, praktykowanie, uprawianie kultu i przestrzeganie obyczajów".*

[150] Więcej szczegółów można znaleźć np. w GREENFIELD, David. *Bezpieczeństwo zintegrowane: czy nadszedł jego czas?* [online]. [cyt. 1 marca 2018]. Dostępny pod adresem: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/

Obraz: Przykład zintegrowanego rozwiązania w zakresie bezpieczeństwa[151]

6.2 GDPR

Ogólne rozporządzenie o ochronie danych (UE) 2016/679[152] jest jednym z głównych międzynarodowych dokumentów prawnych bezpośrednio związanych z kwestią cyberbezpieczeństwa, choć nie jest ono skierowane przede wszystkim do sektora ICT.

> ***"GDPR ≠ IT + oprogramowanie.***
>
> *Nowe rozporządzenie o ochronie danych liczy 778 wierszy, a tylko 26 z nich jest bezpośrednio związanych z bezpieczeństwem informatycznym. Czy masz pojęcie, co zawierają pozostałe "*
>
> Mgr. Eva Škorničková[153]

To właśnie GDPR i realizacja obowiązków wynikających z tej regulacji pokazują, że wskazane jest kompleksowe podejście do kwestii bezpieczeństwa, a nie sztuczne wyodrębnianie obowiązków wynikających z różnych norm prawnych (w tym przypadku ustawy o cyberbezpieczeństwie i GDPR).

Celem niniejszej publikacji nie jest przedstawienie odrębnej i kompleksowej analizy GDPR. W tym miejscu zdefiniowane zostaną jedynie częściowe pojęcia oraz prawa i obowiązki wynikające z GDPR i pokrywające się z bezpieczeństwem cybernetycznym.

GDPR to **ogólne ramy prawne dotyczące ochrony danych osobowych,** obowiązujące w całej UE, a w niektórych przypadkach także poza nią. Główne cele GDPR to zapewnienie kompleksowej ochrony praw osób, których dane dotyczą, przed nieuprawnionym przetwarzaniem ich danych i

---

[151] *Zintegrowana ochrona multidyscyplinarna.* [online]. [cyt. 2018 luty 17]. Dostępny pod adresem: https://www2.deloitte.com/cz/cs/pages/risk/solutions/integrovana-multidisciplinarni-bezpecnost.html

[152] [online]. Dostępny pod adresem: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&qid=1488972453767&from=CS

[153] ŠKORNIČKOVÁ, Eva. *Prosty test.* [online]. [cyt. 10. 11. 2017]. Dostępny pod adresem: *https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*

danych osobowych, osiągnięcie równowagi między uzasadnionymi interesami administratorów, podmiotów przetwarzających i osób, których dane dotyczą, stworzenie systemu jednolitego egzekwowania przepisów i jednolitego mechanizmu sankcji w tej dziedzinie itp.

Gromadzenie i udostępnianie danych osobowych znacznie się nasiliło dzięki technologiom informacyjno-komunikacyjnym i związanym z nimi usługom. Technologie informacyjno-komunikacyjne pozwalają zarówno firmom prywatnym, jak i organom publicznym w niespotykanym dotąd zakresie wykorzystywać dane osobowe do prowadzenia swojej działalności. Z drugiej strony, można też zaobserwować masowe, dobrowolne ujawnianie danych osobowych przez zainteresowane osoby fizyczne.

Technologie informacyjno-komunikacyjne znacząco zmieniły gospodarkę i życie społeczne, dlatego powinny ułatwiać swobodny przepływ danych osobowych w Unii Europejskiej oraz przekazywanie ich do krajów trzecich i organizacji międzynarodowych. Równocześnie jednak technologie te i związane z nimi procesy powinny zapewniać wysoki poziom ochrony danych osobowych. [154]

Powyższe rozważania prowadzą jednak do **interesującego paradoksu**, który polega na następujących kwestiach:

- **Osoby fizyczne same i dobrowolnie ujawniają coraz większą ilość danych** (zdjęć, nagrań wideo itp.) na **swój temat,** zazwyczaj korzystając z usług społeczeństwa informacyjnego w celu rozpowszechniania tych danych, które opierają się na umowach EULA[155] lub SLA[156] między użytkownikiem a dostawcą usług,
- **Większość danych osobowych jest publikowana na portalach społecznościowych**, które ze swej natury oczekują takiej publikacji i określają w warunkach umownych zasady traktowania takich danych,
- **Osoby fizyczne, korzystając z wielu usług społeczeństwa informacyjnego, zakładają i często oczekują interakcji między tymi technologiami a swoją cyberosobowością**[157] ,
- Społeczność międzynarodowa, państwo i same **osoby fizyczne wymagają większego bezpieczeństwa danych osobowych i uniemożliwienia dostępu do nich innym** (zwykle nieuprawnionym) **podmiotom, przy jednoczesnym zachowaniu pierwszych trzech punktów tego paradoksu.**

---

[154] Por. motyw 6 GDPR

[155] **EULA** (End Users Licence Agreement) to nazwa warunków, które umożliwiają korzystanie z usług danego dostawcy usług. EULA to umowa, która jest zazwyczaj jednostronnie określana przez dostawcę usług. Użytkownik nie jest jednak w żaden sposób ograniczony w swoich prawach, ponieważ może zrezygnować z takich jednostronnie określonych warunków umowy. W przypadku zgody na korzystanie z takich usług można ogólnie stwierdzić, że zastosowanie mają przede wszystkim normy prawa prywatnego.
Pytanie brzmi, czy użytkownik jest rzeczywiście świadomy warunków umowy, na które się zgodził, kiedy stają się one dla niego wiążące i jaką ewentualną (prawną) ingerencję w jego podstawowe prawa i wolności człowieka stanowi taka zgoda. Innym nieuniknionym faktem jest to, że usługi świadczone w ten sposób mogą naruszać prawa i uzasadnione interesy (np. bezpieczeństwo IT, poufność danych itp.) osób trzecich (np. pracodawców itp.), które nie wyraziły wyraźnej zgody na korzystanie z danej usługi.
Smutnym faktem jest to, że bardzo niewielki odsetek użytkowników jest skłonny czytać warunki korzystania z usług.

[156] **SLA (**Service-Level Agreement) to umowa wynegocjowana między dostawcą usług a ich użytkownikiem.

[157] **Interakcję tę można zaobserwować podczas korzystania z usług pozycjonowania i geolokalizacji** (np. Google Maps, Waze, Lista Map itp.), ponieważ osoba zakłada, że system komputerowy będzie w stanie ją zlokalizować i wskazać najlepszą trasę. Podobnie interakcja ta jest oczekiwana np. **w usługach umożliwiających sprzedaż i zakup towarów** (np. Letgo - zobacz polecane ogłoszenia na podstawie geolokalizacji lub już zakupionych towarów), **usługach restauracyjnych i noclegowych** (np. Tripadvisor, Booking.com, Airbnb itp.) itp.

Konsekwencja tego paradoksu jest oczywista. W związku z tym dostawcy usług społeczeństwa informacyjnego[158] muszą poświęcić więcej wysiłku na zabezpieczenie poszczególnych usług, które świadczą na rzecz użytkownika końcowego, na wyższy poziom bezpieczeństwa danych dotyczących użytkownika, na modyfikację istniejących warunków umownych oraz na wprowadzenie innych wymogów wynikających z GDPR.

6.2.1 Lokalny zakres GDPR

Można by pomyśleć, że sposobem na uniknięcie GDPR jest przeniesienie się poza jego zasięg, tj. poza UE. GDPR ma jednak zastosowanie, gdy:

- **siedziba administratora lub podmiotu przetwarzającego znajduje się w UE**, niezależnie od tego, czy przetwarzanie odbywa się w UE,
- **administratorzy danych lub podmioty przetwarzające nie mają siedziby w UE, ale**
  - towary lub usługi są oferowane osobom, których dane dotyczą, w UE (niezależnie od wynagrodzenia),
  - monitorowane jest zachowanie osób, których dane dotyczą, na terenie UE.[159]

Dzięki takiemu zdefiniowaniu lokalnego zakresu GDPR ma zasięg eksterytorialny i de facto będzie miało zastosowanie do wszystkich usług społeczeństwa informacyjnego, do których można uzyskać dostęp z terytorium geograficznego UE lub które monitorują zachowanie osób, których dane dotyczą, na terytorium UE.

6.2.2 Dane osobowe

Zgodnie z art. 4 ust. 1 GDPR, dane osobowe to ***"wszelkie informacje** o **zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej"**. Możliwa do zidentyfikowania osoba fizyczna to osoba fizyczna, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator sieciowy lub jeden bądź kilka szczególnych elementów fizycznej, fizjologicznej, genetycznej, psychicznej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby fizycznej. "*

Zgodnie z przepisami GDRP dane **osobowe** to **wszelkie informacje** (np. wizualne, pisemne, ustne, cyfrowe, genetyczne, medyczne itp.), które **są powiązane** (treść - np. imię i nazwisko, adres, stanowisko, adres e-mail itp.[160] Z tego punktu widzenia oraz zgodnie z interpretacją przedstawioną w motywach 30, 34, 35 i 38 GDPR[161] , za dane osobowe należy uznać następujące elementy:

- imię i nazwisko,
- **numer identyfikacyjny**,
- numer urodzenia,
- **dane o lokalizacji (geo-)**,

---

[158] Więcej szczegółów w: KOLOUCH, Jan. *Cyberprzestępczość.* Praga: CZ.NIC, 2016, s. 78 i nast. oraz s. 109 i nast.

[159] Zob. art. 3 GDPR - zakres lokalny

[160] Zgodnie z art. 4 ust. 1 GDPR osoba, **której dotyczą dane**, **to** zidentyfikowana lub możliwa do zidentyfikowania **osoba fizyczna. Obiekt może zostać zidentyfikowany:**

- **Racja,**
- **pośrednio (np. wybór przez przeznaczenie itp.).**

[161] Motywy to przepisy poprzedzające właściwy tekst GDPR i w niektórych przypadkach stanowią interpretację lub w pewnym stopniu uzasadnienie właściwego tekstu rozporządzenia.

- wiek i data urodzenia,
- płeć,
- stan osobowy,
- obywatelstwo,
- **identyfikatory sieci,**
  - **Adres IP**,
  - **identyfikatory plików cookie**,
  - identyfikatory o częstotliwości radiowej itp.,
- **fotografie**,
- **elementy** tożsamości fizycznej, fizjologicznej, genetycznej, psychologicznej, ekonomicznej, **kulturowej lub społecznej,**
- adres osobisty lub służbowy,
- numer telefonu osobistego lub służbowego,
- **prywatną lub służbową pocztę elektroniczną**,
- **dane identyfikacyjne uwierzytelniania**,
- numery identyfikacyjne nadane przez państwo.

Dane osobowe zapisane pogrubioną czcionką dotyczą zazwyczaj technologii informacyjno-komunikacyjnych oraz aplikacji wykorzystujących te technologie. Rozszerzenie zakresu danych, które można uznać za dane osobowe, ma istotne implikacje dla bezpieczeństwa cybernetycznego i ochrony danych zarządzanych przez organizację.

Jeśli skupimy się na **identyfikatorach sieciowych i danych uwierzytelniających, okaże się, że szereg danych, które umożliwiają podstawowe funkcjonowanie systemu komputerowego w sieci**, **może być i prawdopodobnie będzie uznawanych za dane osobowe.**

Pytanie - czy adres IP to dane osobowe?

Oprócz GDPR w tej kwestii należy wziąć pod uwagę orzecznictwo Trybunału Sprawiedliwości UE, który wydał wyrok m.in. w sprawie **Patrick Breyer** przeciwko **Republice Federalnej Niemiec.** [162]

Patrick Bayer zwrócił się do sądów niemieckich o zaprzestanie przechowywania jego adresów IP, które zostały uzyskane podczas jego "wizyt" na kilku publicznie dostępnych stronach internetowych niemieckich władz federalnych. Z punktu widzenia operatorów odnośnych stron internetowych było to klasyczne logowanie usług oferowanych przez dostawcę usług internetowych.[163]

Sądy niemieckie zawiesiły postępowanie i zwróciły się do Trybunału Sprawiedliwości UE z pytaniem prejudycjalnym, ponieważ w tej sprawie nie ma jednolitej wykładni prawa UE.

W szczególności chodzi o to, czy kryterium *"obiektywne"* lub "*względne" jest wymagane, by dane były* danymi osobowymi, a zatem by można było zidentyfikować konkretną osobę.

---

[162] Więcej informacji na ten temat można znaleźć na stronie: [online]. Dostępny pod adresem: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=1403270

[163] Na temat faktycznego pojęcia dostawcy usług internetowych oraz praw i obowiązków poszczególnych dostawców usług internetowych zob. np. KOLOUCH, Jan. *Cyberprzestępczość.* Praga: CZ.NIC, 2016, s. 78 i nast. oraz s. 109 i nast.

"Obiektywne" kryterium oznacza, że dane takie jak **adresy IP mogą być uznane za dane osobowe** przetwarzane przez dostawcę usług innych niż połączenie (np. operatora strony internetowej), nawet jeśli **tylko strona trzecia** (zazwyczaj dostawca usług internetowych połączenia) byłaby w **stanie zidentyfikować konkretnego użytkownika.**

Kryterium "względności" oznacza, że **adresy IP mogą być uznane za dane osobowe przez dostawcę usług internetowych**, ponieważ umożliwiają mu dokładną identyfikację użytkownika, ale **nie przez dostawcę usług, który w rzeczywistości dysponuje tylko danymi dotyczącymi adresów IP i nie zna nazwiska odwiedzającego.**

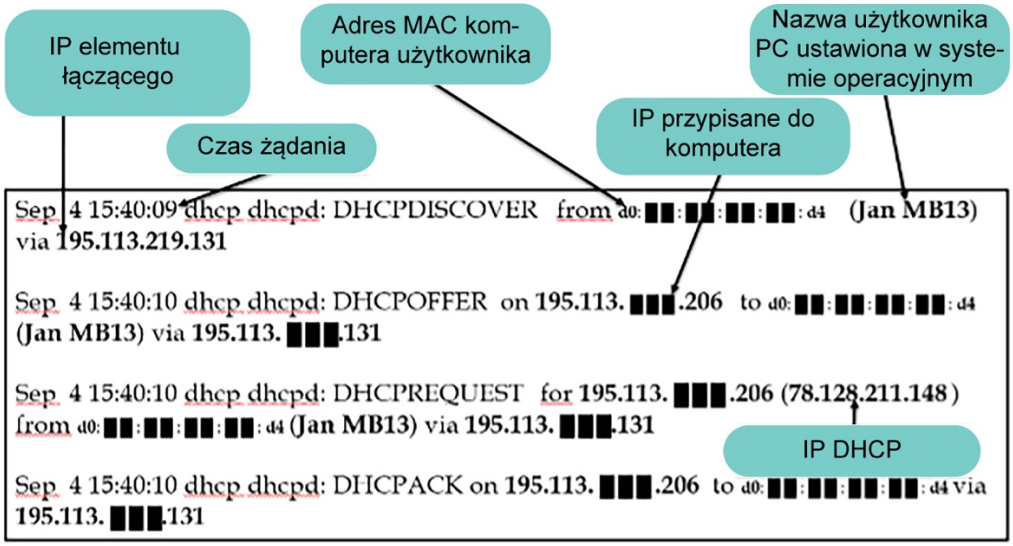
TSUE orzekł, że **bezsporne jest, iż dynamiczny adres IP nie stanowi informacji o "zidentyfikowanej osobie"**, ponieważ **adres ten nie ujawnia bezpośrednio tożsamości osoby fizycznej będącej właścicielem** komputera, z którego odwiedzono stronę internetową, **ani tożsamości żadnej innej osoby, która mogła korzystać z tego komputera**.

Z drugiej jednak strony Trybunał Sprawiedliwości (druga izba) uznał również (a następnie orzekł), że **dynamiczny adres** protokołu internetowego przechowywany przez **dostawcę internetowych usług medialnych w związku z dostępem danej osoby do strony internetowej udostępnionej** publicznie przez tego **dostawcę stanowi** dla tego dostawcy **dane osobowe w rozumieniu** art. 2 ust. 1 lit. a) Traktatu WE. (a) dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, pod warunkiem **że dostawca dysponuje środkami prawnymi umożliwiającymi identyfikację osoby, której dane dotyczą, na podstawie dodatkowych informacji posiadanych przez dostawcę połączenia internetowego tej osoby.**

Dynamiczny adres IP może w pewnych okolicznościach stanowić dane osobowe, zgodnie z tym wyrokiem z dnia 19 października 2016 r.

Wpływ faktu, że **adres IP oraz inne identyfikatory sieciowe mogą być danymi osobowymi, pokazujemy na** dwóch przykładach.

Poniższy rysunek przedstawia komunikację między komputerem PC a poszczególnymi elementami sieci (AP, serwer DHCP) oraz późniejsze podłączenie komputera PC do sieci.

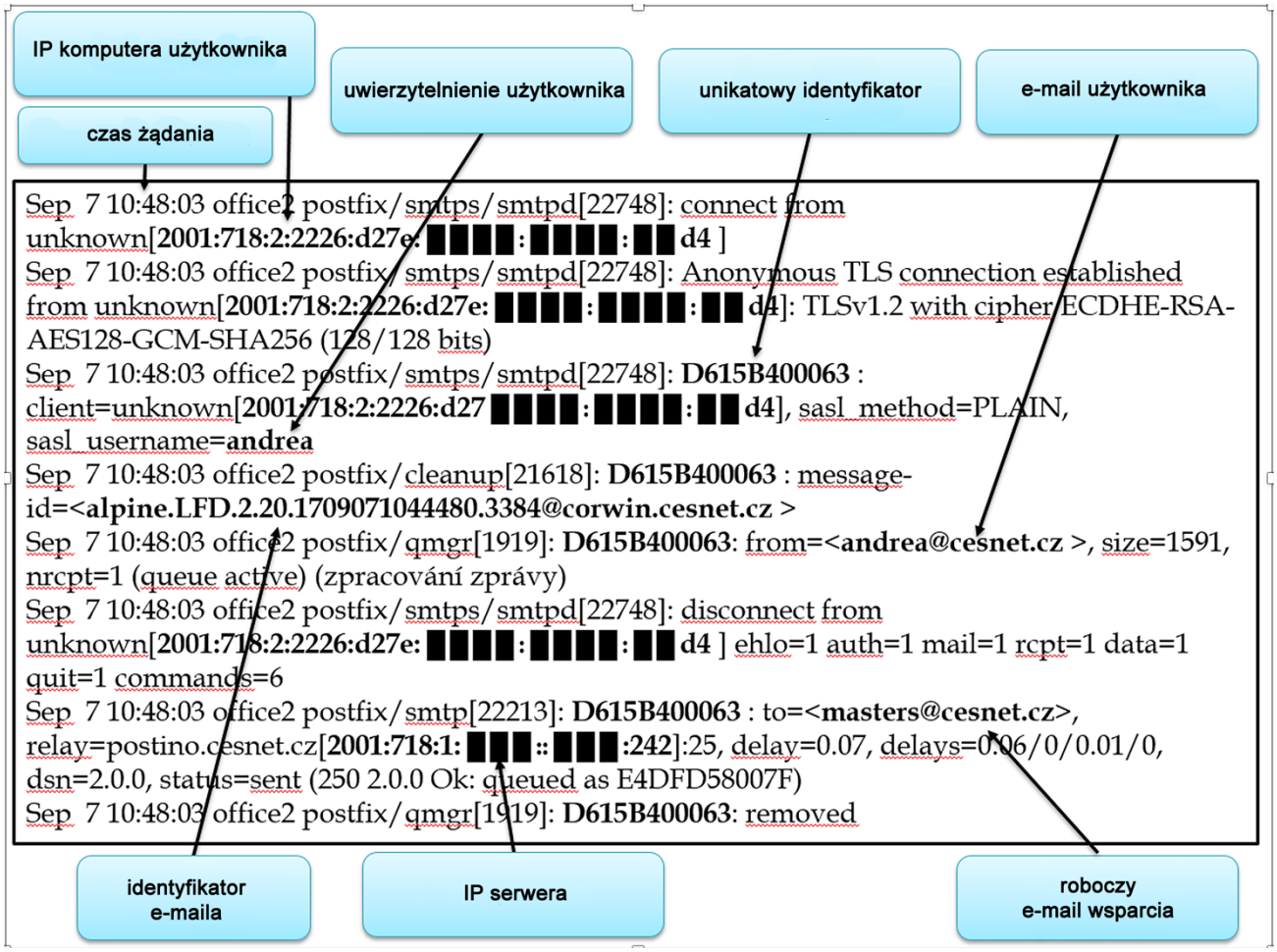


Obraz:DHCP

Jeśli konsekwentnie skupimy się na **danych** (informacjach), które są **związane z osobą, której** dane dotyczą, **i które umożliwiają jej identyfikację,** to w tym przypadku danymi osobowymi nie będą tylko adres IP elementu łączącego i adres IP serwera DHCP.

Teoretycznie czas żądania również stanowi dane osobowe, ponieważ jest to ślad, który można wykorzystać do identyfikacji osoby fizycznej, zwłaszcza w połączeniu z unikalnymi identyfikatorami i innymi informacjami gromadzonymi przez serwery.[164] Jest to również bardzo ważna informacja, ponieważ bez dokładnego czasu nie można określić, komu (jakiemu systemowi komputerowemu) został przydzielony dany adres IP.

Innym przykładem ilustrującym zakres przetwarzania danych, które można uznać za dane osobowe, jest przetwarzanie danych osobowych podczas wysyłania wiadomości e-mail za pomocą protokołu SMTP.



Obraz:SMTP

I znów, jeśli konsekwentnie skupiamy się na **danych** (informacjach), **które są związane z osobą, której** dane dotyczą, **i które umożliwiają jej identyfikację,** to w tym przypadku danymi osobowymi nie będzie tylko adres IP serwera.

E-mail służbowy może ponownie stanowić dane osobowe, jeżeli zostaną z nim powiązane dodatkowe identyfikatory umożliwiające identyfikację osoby fizycznej.

Kluczowe pytanie brzmi, **czy w** kontekście wszystkich procesów zachodzących w systemach komputerowych (elementach TIK) zarządzanych przez dany podmiot (osobę fizyczną lub prawną)

[164] Więcej szczegółów można znaleźć w motywie 30 GDPR

jesteśmy w stanie odróżnić sytuację, w której dane są przekazywane wyłącznie między systemami komputerowymi, bez związku z jakąkolwiek osobą fizyczną, od sytuacji, w której osoba fizyczna jako podmiot danych w rozumieniu GDPR jest już zaangażowana w te procesy.

Uważamy, że - poza szczególnymi wyjątkami - nie będziemy w stanie wyizolować procesów, które zachodzą bez udziału człowieka. Na podstawie tego stwierdzenia wymogi GDPR należy stosować do wszystkich procesów, w których przetwarzane są informacje związane z osobą, której dane dotyczą, i umożliwiające jej identyfikację. Jednocześnie konieczne będzie podjęcie odpowiednich środków bezpieczeństwa w celu właściwej ochrony zarówno systemu transmisji, systemów komputerowych i aplikacji przetwarzających takie informacje, jak i samych informacji (lub danych).

Oprócz powyższych danych osobowych, GDPR definiuje specjalne kategorie danych osobowych, które obejmują dane dotyczące:

- pochodzenie rasowe lub etniczne,
- religia,
- poglądy polityczne,
- członkostwo w związkach zawodowych lub innych organizacjach,
- orientacja seksualna,
- popełnianie wykroczeń (przestępstw/wykroczeń itp.) i bycie za nie ukaranym,
- dane genetyczne (DNA i RNA),
- dane biometryczne,
- dane dotyczące zdrowia.

6.2.3 Przetwarzanie danych osobowych

Zgodnie z art. 4 ust. 2 GDRP przetwarzanie danych osobowych oznacza **każdą operację lub** zestaw operacji wykonywanych przy **pomocy procesów zautomatyzowanych lub bez ich pomocy,** takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptacja lub modyfikacja, pobieranie, konsultowanie, wykorzystywanie, ujawnianie przez transmisję, rozpowszechnianie lub jakiekolwiek inne ujawnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Ochrona osób, których dane dotyczą, ma zastosowanie do przetwarzania danych osobowych, jeśli dane te są przechowywane w rejestrze lub mają być do niego wprowadzone.[165]

Jednak pojęcie **przetwarzania w rozumieniu** GDPR **nie może być rozumiane jako jakiekolwiek przetwarzanie danych osobowych. Przetwarzanie danych osobowych należy uznać za bardziej zaawansowaną działalność, którą administrator danych prowadzi z danymi osobowymi w określonym celu i z pewnej perspektywy robi to systematycznie.** [166]

Z przetwarzania danych osobowych na mocy GDPR wyłączone są między innymi **czynności wykonywane przez osobę fizyczną w czysto osobistym charakterze lub czynności wykonywane wyłącznie w domu, a więc bez związku z działalnością zawodową lub handlową.** [167]

---

[165] Zob. motyw 15 GDPR.
[166] Więcej szczegółów można znaleźć w dokumencie *GDPR Essential Guide.* [online]. [cited 2018 Aug 7]. Dostępny pod adresem: *https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938*
[167] Zob. motyw 15 GDPR.

W art. 5 ust. 1 lit. a) GDPR określono zasady przetwarzania danych osobowych. Zgodnie z GDPR zasady te obejmują:

- **zgodność z prawem, rzetelność, przejrzystość** [art. 5 ust. 1 lit. a) GDPR] - administrator danych jest zobowiązany:
    - poinformować osobę, której dane dotyczą, o trwającej operacji przetwarzania i jej celach,
    - informować osobę, której dane dotyczą, o profilowaniu i jego konsekwencjach,
    - poinformować osobę, której dane dotyczą, jeśli dane osobowe są od niej pobierane, czy jest ona zobowiązana do przekazania tych danych oraz o konsekwencjach ich nieprzekazania,
    - **wykazać istnienie co najmniej jednej podstawy prawnej do przetwarzania danych osobowych**,
    - **udokumentować:**
        - co, jak i dlaczego się przetwarza,
        - zgodę i powód prawny,
        - czas potrzebny na przetworzenie,
        - **zastosowane zabezpieczenia i środki ostrożności**.
- **ograniczenie celu** [art. 5 ust. 1 lit. b) GDPR] - dane osobowe muszą być gromadzone w określonych, jednoznacznych i legalnych celach i nie mogą być dalej przetwarzane w sposób niezgodny z tymi celami,
- **minimalizację danych** [art. 5 ust. 1 lit. c) GDPR] - dane osobowe muszą być adekwatne i istotne w stosunku do celu, w jakim są przetwarzane,
- **dokładność** [art. 5 ust. 1 lit. d) GDPR] - dane osobowe muszą być dokładne i w razie potrzeby aktualizowane; należy podjąć wszelkie uzasadnione kroki w celu niezwłocznego usunięcia lub poprawienia danych osobowych, które są niedokładne, z uwzględnieniem celów, dla których są przetwarzane,
- **ograniczenie przechowywania** [art. 5 ust. 1 lit. e) GDPR] - dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, wyłącznie przez okres niezbędny do celów, w których są przetwarzane,
- **integralność i poufność** [art. 5 ust. 1 lit. f) GDPR] - dane osobowe muszą być **przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę za pomocą odpowiednich środków technicznych lub organizacyjnych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub uszkodzeniem technicznego i organizacyjnego bezpieczeństwa danych osobowych**.

6.2.4 Bezpieczeństwo danych osobowych

Jednym z obszarów wyraźnie uwzględnionych w GDPR jest **bezpieczeństwo przetwarzania danych osobowych**.

Artykuł 32 GDPR stanowi, że **administrator** (lub podmiot przetwarzający, w zależności od przypadku) **musi,** uwzględniając stan wiedzy **technicznej,** koszt wdrażania, charakter, zakres,

kontekst i cele przetwarzania, a także różne prawdopodobne i różnie poważne zagrożenia dla praw i wolności osób fizycznych, **podjąć odpowiednie środki techniczne** i **organizacyjne, aby zapewnić poziom bezpieczeństwa stosowny do danego ryzyka,** w tym, w stosownych przypadkach:

- **pseudonimizację i szyfrowanie danych osobowych,**
- **zdolność do zapewnienia ciągłej poufności, integralności, dostępności i odporności systemów i usług przetwarzania,**
- **zdolność do przywrócenia dostępności i dostępu do danych osobowych w odpowiednim czasie w przypadku incydentów fizycznych lub technicznych,**
- **proces regularnego testowania, oceny i ewaluacji skuteczności środków technicznych i organizacyjnych stosowanych w celu zapewnienia bezpieczeństwa przetwarzania danych.**

*"**Oceniając odpowiedni poziom bezpieczeństwa, należy wziąć** pod **uwagę w szczególności ryzyko związane** z przetwarzaniem, zwłaszcza przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób. "*[168]

Określenie ryzyka opiera się w szczególności na kategorii danych osobowych, których może dotyczyć naruszenie, charakterze naruszenia oraz liczbie osób, których dane dotyczą. Większe ryzyko stanowią bardziej "wrażliwe" dane osobowe (zob. np. specjalne kategorie danych osobowych), większy zbiór danych osobowych lub dane, które mogą wyrządzić szkodę osobie, której dane dotyczą, lub naruszyć jej prawa.

Zgodnie z art. 32 ust. 4 GDPR administrator i podmiot przetwarzający podejmują środki w celu zapewnienia, by każda osoba fizyczna działająca w imieniu administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała te dane osobowe wyłącznie na polecenie administratora, chyba że przetwarzanie jest już wymagane przez prawo Unii lub państwa członkowskiego.

6.2.5 Ocena wpływu na ochronę danych (DPIA)

Ocena skutków **dla** ochrony danych **(DPIA)** to narzędzie, które należy stosować, gdy określony rodzaj **przetwarzania, w szczególności przy wykorzystaniu nowych technologii, może spowodować wysokie ryzyko dla praw i wolności osób fizycznych,** z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania. Jest to narzędzie, które może pomóc administratorom w identyfikacji potencjalnego ryzyka związanego z przetwarzaniem danych osobowych oraz we wprowadzeniu odpowiednich środków.

Ocena skutków dla ochrony danych musi być przeprowadzona w następujących przypadkach:

- **systematyczna i szeroko zakrojona ocena aspektów osobowych dotyczących osób fizycznych,** oparta na **zautomatyzowanym przetwarzaniu, w tym profilowaniu,** na podstawie której podejmowane są decyzje wywołujące skutki prawne w odniesieniu do osób fizycznych lub mające podobnie znaczący wpływ na osoby fizyczne,
- **przetwarzanie szczególnych kategorii danych osobowych** (danych biometrycznych lub danych dotyczących wyroków skazujących i przestępstw oraz związanych z nimi środków bezpieczeństwa),
- szeroko zakrojone, systematyczne monitorowanie przestrzeni publicznie dostępnych,

[168] Artykuł 32 ust. 2 GDPR

- **wszelkie inne operacje, w przypadku których właściwy organ nadzorczy uzna, że przetwarzanie może stanowić wysokie ryzyko dla praw i wolności osób, których dane dotyczą.**

Treść oceny skutków dla ochrony danych powinna obejmować:

- opis planowanych operacji przetwarzania,
- ocena konieczności i proporcjonalności operacji w odniesieniu do ich celu (**test** proporcjonalności**)**,
- **ocenę zagrożeń dla praw i wolności uczestników**,
- **środki planowane w celu przeciwdziałania tym zagrożeniom, w tym zabezpieczenia, środki bezpieczeństwa itp.**

Samo GDPR zawiera również inne kategorie (np. pseudonimizacja, wymagania dotyczące usuwania lub przenoszenia danych osobowych itp.), które mogą odnosić się do czynności wykonywanych w ramach systemów informacyjno-komunikacyjnych i które wymagają odpowiedniego poziomu bezpieczeństwa i ochrony.

Niezbędne jest określenie wpływu GDPR na organizację, jej poszczególne części i procesy. De facto chodzi o przeprowadzenie audytu tego, gdzie dane osobowe są przetwarzane w związku z GDPR wszędzie w organizacji lub przez osobę fizyczną. Następnie procedura polega na modyfikacji lub tworzeniu zasad i procesów (w razie potrzeby) zarówno wewnątrz organizacji, jak i w odniesieniu do osoby, której dane dotyczą. Wszystkie te działania powinny być prowadzone z poszanowaniem podstawowych zasad bezpieczeństwa.

Podobnie jak w przypadku wdrażania zasad bezpieczeństwa w ogóle, przy wdrażaniu GDPR lub innych dokumentów i zaleceń należy pamiętać, że nie ma jednej zasady, modelu, narzędzia, rozwiązania czy procedury, która miałaby zastosowanie w każdej organizacji i w każdej sytuacji.

Należy przyjąć i wdrożyć własne rozwiązanie zgodne z GDPR.

Konieczne jest indywidualizowanie.

PODSUMOWANIE ROZDZIAŁU

- GDPR to ogólne ramy prawne dotyczące ochrony danych osobowych, obowiązujące w całej UE, a w niektórych przypadkach także poza nią. Główne cele GDPR to zapewnienie kompleksowej ochrony praw osób, których dane dotyczą, przed nieuprawnionym przetwarzaniem ich danych i danych osobowych, osiągnięcie równowagi między uzasadnionymi interesami administratorów, podmiotów przetwarzających i osób, których dane dotyczą, stworzenie systemu jednolitego egzekwowania przepisów i jednolitego mechanizmu sankcji w tej dziedzinie itp.
- GDPR ma jednak zastosowanie, gdy:
    - siedziba administratora lub podmiotu przetwarzającego znajduje się w UE, niezależnie od tego, czy przetwarzanie odbywa się w UE,
    - administratorzy danych lub podmioty przetwarzające nie mają siedziby w UE, ale
        - towary lub usługi są oferowane osobom, których dane dotyczą, w UE (niezależnie od wynagrodzenia),
        - monitorowane jest zachowanie osób, których dane dotyczą, na terenie UE.
- Zgodnie z art. 4 ust. 1 GDPR, dane osobowe to *"wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej". Możliwa do zidentyfikowania osoba fizyczna to osoba fizyczna, której tożsamość można ustalić bezpośrednio lub pośrednio, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator sieciowy lub jeden bądź kilka szczególnych elementów fizycznej, fizjologicznej, genetycznej, psychicznej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby fizycznej."*
- Zgodnie z art. 4 ust. 2 GDRP przetwarzanie danych osobowych oznacza każdą operację lub zestaw operacji wykonywanych przy pomocy procesów zautomatyzowanych lub bez ich pomocy, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptacja lub modyfikacja, pobieranie, konsultowanie, wykorzystywanie, ujawnianie przez transmisję, rozpowszechnianie lub jakiekolwiek inne ujawnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
- Biorąc pod uwagę stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania, a także różne prawdopodobne i różnie poważne zagrożenia dla praw i wolności osób fizycznych, administrator (lub podmiot przetwarzający, w zależności od przypadku) musi podjąć odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiedni do danego ryzyka, w tym, w stosownych przypadkach:
    - pseudonimizacja i szyfrowanie danych osobowych,
    - zdolność do zapewnienia ciągłej poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
    - zdolność do przywrócenia dostępności i dostępu do danych osobowych w odpowiednim czasie w przypadku incydentów fizycznych lub technicznych,
    - proces regularnego testowania, oceny i ewaluacji skuteczności środków technicznych i organizacyjnych stosowanych w celu zapewnienia bezpieczeństwa przetwarzania danych.

- Ocena skutków dla ochrony danych (DPIA) to narzędzie, które należy stosować, gdy określony rodzaj przetwarzania, w szczególności przy wykorzystaniu nowych technologii, może spowodować wysokie ryzyko dla praw i wolności osób fizycznych, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania. Jest to narzędzie, które może pomóc administratorom w identyfikacji potencjalnego ryzyka związanego z przetwarzaniem danych osobowych oraz we wprowadzeniu odpowiednich środków.

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

- GDPR
- Dane osobowe
- Administrator danych osobowych
- Przetwarzanie danych osobowych
- Ocena skutków ochrony danych

PYTANIA KONTROLNE

- Jaki jest lokalny zakres zastosowania GDPR?
- Co to są dane osobowe?
- Czy adres IP to dane osobowe?
- Jakie obowiązki ma administrator danych?
- Co należy rozumieć przez przetwarzanie danych osobowych?
- Co oznacza ocena skutków w zakresie ochrony danych?

7. Prywatność i bezpieczeństwo w ICT, ochrona danych w cyberprzestrzeni

Żyjąc w epoce cyfrowej, mam wrażenie, że moje działania są anonimowe lub ukryte przed wzrokiem innych użytkowników,[169] . Moim zdaniem to naiwne. Wraz z nadejściem ery cyfrowej pojawiają się nie tylko jej pozytywne, ale i negatywne aspekty.[170] Jednym z takich negatywnych zjawisk jest fakt, że coraz mniej interesuje nas to, jak działają usługi świadczone w cyberprzestrzeni.

Nasz świat, który coraz częściej rozumiemy jako "świat informacji" lub "świat Internetu", jest silnie związany z technologiami informacyjnymi i komunikacyjnymi, które w bardzo znaczący sposób ingerują w życie jednostki. Technologie te ułatwiają dostęp do informacji oraz upraszczają lub przyspieszają komunikację między użytkownikami itp. Z drugiej jednak strony należy zdawać sobie sprawę, że każda publikacja naszych prywatnych informacji w Internecie stanowi ryzyko, które może zostać wykorzystane przez każdego, kto znajduje się w cyberprzestrzeni.

Wszystkie aplikacje, niezależnie od systemu komputerowego, na którym są używane, serwisy internetowe[171] , a zwłaszcza portale społecznościowe,[172] gromadzą znaczną ilość informacji o swoich użytkownikach, które w większości przypadków nie są im potrzebne do funkcjonowania, ale które z jednej strony pozwalają danemu dostawcy usług internetowych świadczyć usługi "za darmo", a z drugiej - "ukierunkowywać" lub modyfikować oferowane przez niego usługi. Informacje, które w normalnych warunkach nie są niezbędne do bezpośredniego korzystania z poszczególnych usług, obejmują na przykład informacje o charakterze **osobistym** (imię, nazwisko, adres e-mail, numer telefonu, miejsce zamieszkania itp.), informacje **wrażliwe** (np. informacje o używanym systemie operacyjnym komputera, wersje poszczególnych aplikacji, pliki cookie itp.), **dane dotyczące lokalizacji** (współrzędne GPS, informacje o WiFi, GPRS itp.), dane operacyjne itp. [173]

Informacje te można wykorzystać na różne sposoby. Usługodawca może wykorzystać te informacje do oferowania np. dodatkowych usług lub reklam opartych na wymaganiach, zainteresowaniach lub hobby użytkowników. Dzięki temu policja może śledzić codzienne czynności osoby, która na przykład zaginęła lub została porwana, a tym samym przyspieszyć jej poszukiwania. Jednocześnie jednak informacje te mogą być bardzo łatwo wykorzystane przez sprawców przestępstw do nawiązania kontaktu z ofiarą lub do zaplanowania samego przestępstwa.

Podając te dane (nawet mimowolnie lub nieświadomie), użytkownik serwisu umożliwia innym uzyskanie ważnych informacji o swoim życiu (np. informacji o swoim zachowaniu w ciągu dnia,

---

[169] Pod pojęciem użytkownika rozumiem wszystkie podmioty, które mają wpływ na wydarzenia w cyberprzestrzeni. Do tej grupy należy zaliczyć przede wszystkim **dostawców** usług **internetowych.** Nie wszyscy dostawcy usług internetowych podlegają jednak jurysdykcji prawa czeskiego (czy to ze względu na geolokalizację, czy też dlatego, że ich działalność nie jest regulowana przez prawo). Innymi "użytkownikami" będą niewątpliwie **LEA** (Law Enforcement Agencies - organy ścigania, którym normy prawne poszczególnych państw pozwalają na jedną z najbardziej intensywnych ingerencji w podstawowe prawa i wolności człowieka), **zespoły CERT/CSIRT, administratorzy działów IT, użytkownicy końcowi itp.**

[170] Na przykład cyberprzestępczość, uzależnienia i demencja cyfrowa. Więcej szczegółów w: SPITZER, Manfred. *Demencja cyfrowa.* Brno: Gospodarz, 2014 r. ISBN 978-80-7294-872-7

[171] *Poprawa bezpieczeństwa, ochrona prywatności i tworzenie prostych narzędzi, które dają użytkownikowi kontrolę i możliwość wyboru, są dla nas bardzo ważne.* [online]. [cyt. 2014-04-04]. Dostępny pod adresem: https://www.google.cz/intl/cs/policies/?fg=1

[172] Zob. *Deklaracja Praw i Obowiązków.* [online]. [cyt. 4.4.2014]. Dostępny pod adresem: https://www.facebook.com/legal/terms

[173] **Jednak niektóre systemy uwierzytelniania wymagają tych dodatkowych informacji do działania.**

miejscach, które odwiedza, zajęciach i osobach, z którymi się kontaktuje).[174] W tym momencie **my sami stajemy się informacją lub towarem, którym ktoś inny może handlować**.

Różne dane statystyczne dostępne na stronie[175] wskazują, że całkowita liczba ludności wynosi obecnie około 7 359 244 000 osób. Z tej liczby około 3,6 miliarda osób to aktywni użytkownicy Internetu, a ponad 2,1 miliarda osób to aktywni użytkownicy sieci społecznościowych. Ponad 3,6 mld użytkowników posiada urządzenia mobilne, a ponad 1,7 mld użytkowników korzysta z sieci społecznościowych za pośrednictwem tych urządzeń. Facebook jest liderem wśród portali społecznościowych z ponad 1,59 mld użytkowników: [176]

W tym rozdziale postaram się zwrócić uwagę na możliwe zagrożenia bezpieczeństwa, które przyzwyczailiśmy się de facto akceptować lub nie akceptować, a w przypadku których większość osób lub organizacji jest całkowicie nieświadoma potencjalnego niebezpieczeństwa.

7.1 Ślad cyfrowy

Zagrożenia te, a raczej ryzyka, bardzo często dotyczą pozostawiania śladów cyfrowych w cyberprzestrzeni. Ślady cyfrowe, w zależności od tego, czy użytkownik może na nie wpływać, czy nie, można ogólnie **podzielić na ślady**, **na które można wpływać, i ślady, na które nie można wpływać.**

Dzielenie ścieżek cyfrowych:

- **Ślad cyfrowy pozostaje nienaruszony**
  - informacje z systemu komputerowego;
  - połączenie z sieciami komputerowymi, zwłaszcza z Internetem;
  - wykorzystanie świadczonych usług itp.
- **Cyfrowy ślad ma wpływ na**
  - świadome korzystanie z usług;
  - dobrowolne ujawnianie informacji
    - blogi, fora
    - sieci społecznościowe,
    - e-mail,

---

[174] KOLOUCH, Jan, Michal DVOŘÁK, Tomáš NAJMAN i Terezie JANÍKOVÁ. niebezpieczne zachowania na Facebooku. W. *Aplikacje mobilne.* Sieci społeczne: University of West Bohemia in Pilsen, 2014, s. 39-47. ISBN 978-80-261-0362-2 s. 40

[175] Więcej informacji na ten temat można znaleźć np:
Światowi użytkownicy Internetu i dane o ludności z 2015 r. [online]. [cyt. 2015-08-09]. Dostępny pod adresem: http://www.internetworldstats.com/stats.htm
Digital, Social & Mobile Worldwide in 2015 [online]. [cyt. 2015-08-09]. Dostępny pod adresem: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/
Największe sieci społecznościowe na świecie? Facebook może i jest numerem jeden, ale... [online]. [cyt. 10.8.2015]. Dostępny pod adresem: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/
Current World Population [online]. [cyt. 2015-08-10]. Dostępny pod adresem: http://www.worldometers.info/world-population/

[176] *Wiodące sieci społecznościowe na świecie według stanu na kwiecień 2016 r., uszeregowane według liczby aktywnych użytkowników (w milionach)* [online]. [cit.10.8.2015]. Dostępny pod adresem: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

- magazyny danych,
- usługi w chmurze itp.

W dalszej części artykułu omówię niektóre aspekty poszczególnych śladów cyfrowych i zawartych w nich informacji. Celem jest zwrócenie uwagi użytkownika na to, że jego działania w środowisku TIK nie są tak anonimowe, jak mogłoby się wydawać.

W świecie technologii informacyjno-komunikacyjnych obowiązuje jedna zasada: gdy **cokolwiek przesyłasz, transmitujesz, pośredniczysz, umieszczasz w cyberprzestrzeni, pozostaje tam "na zawsze". Zawsze będzie istniała** kopia (utworzona dzięki funkcjonalności systemu komputerowego lub przechowywana przez innego użytkownika) danych użytkownika. Nawet jeśli użytkownik usunie te dane, nie dojdzie do ich faktycznego, trwałego i nieodwracalnego usunięcia. Dlatego warto zwracać uwagę na swój cyfrowy ślad oraz informacje i dane, które pozostawiamy w cyberprzestrzeni.

7.1.1 Ślad cyfrowy pozostaje nienaruszony

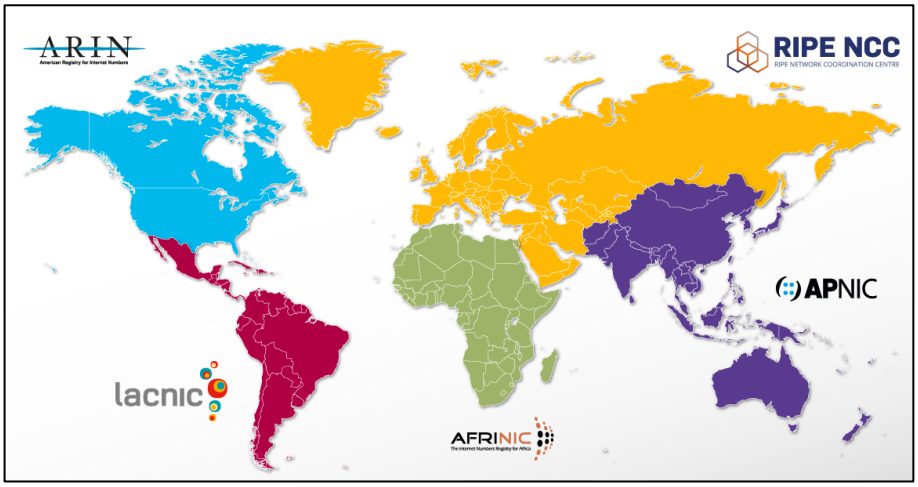
Ślady nieinfluencyjne są najczęściej tworzone przez interakcję jednego systemu komputerowego z innym systemem komputerowym lub przez funkcjonalność systemu komputerowego (i związanego z nim oprogramowania). Przykłady takich śladów obejmują informacje z systemu operacyjnego (np. komunikaty o błędach systemu Windows lub informacje systemowe) lub inne informacje i dane, które są przechowywane w oparciu o funkcjonalność systemu bez konieczności ich przesyłania (np. system komputerowy nigdy nie był podłączony do żadnej sieci lub innego systemu komputerowego).[177] Nie do końca słuszne byłoby bezkompromisowe stwierdzenie, że na te ślady nie można wpływać. Jeżeli użytkownik posiada wystarczające umiejętności, może zmodyfikować, zamaskować lub zlikwidować wiele "nieinfiltrowanych" śladów cyfrowych (np. po prostu używając trybu anonimowego w przeglądarce internetowej w celu wyłączenia plików cookie). Jednak ruch użytkownika w Internecie może być śledzony na różne sposoby.

Adres IP

Podłączenie systemu komputerowego do Internetu jest typowym przykładem stosunkowo nieuciążliwego śladu. Adres IP lub adres MAC, który jest przekazywany wraz z innymi informacjami do dostawcy usług internetowych. Adres IP nie jest domyślnie anonimowy i jest używany przez system komputerowy jako jeden z jego identyfikatorów podczas komunikacji z innymi systemami komputerowymi. Adresy IP są przydzielane hierarchicznie, przy czym dominującą rolę odgrywa **ICANN, która** podzieliła świat rzeczywisty na regiony zarządzane przez **Regionalne Rejestry** Internetowe (**RIR**). Rejestratorzy ci otrzymali od ICANN zakres adresów IP, które przydzielają adresom LIR w swoim regionie. Rejestratorzy regionalni są podzieleni na pięć następujących jednostek terytorialnych

1. Obszar "euroazjatycki" - RIPE NCC: https://www.ripe.net/
2. Region "Azja i Pacyfik" - APNIC: https://www.apnic.net/
3. Region "Ameryka Północna" - ARIN: https://www.arin.net/
4. Region "Ameryka Południowa" - LACNIC: http://www.lacnic.net/
5. Region "afrykański" - AFRINIC: http://www.afrinic.net/

[177] Lub, w większości, informacje, które są rejestrowane i archiwizowane na temat aktywności użytkownika w miejscach, do których użytkownik nie ma dostępu i nad którymi nie ma kontroli [np. użytkownik nie jest w stanie usunąć dzienników pokazujących jego aktywność (np. uzyskiwanie dostępu, wysyłanie wiadomości e-mail itp.) na serwerze pocztowym]. Na własnym komputerze użytkownik może wpływać na przechowywane dane i informacje. Ma on prawo do usuwania (np. historii, e-maili itp.), edytowania itp.



Rysunek - Światowy podział między RIR

Regionalni rejestratorzy witryny[178] prowadzą na swoich stronach internetowych usługę *Whois, która* jest nazwą bazy danych zawierającej informacje o posiadaczach adresów IP. Te bazy danych zawierają szereg informacji, które można wykorzystać do zidentyfikowania np. zakresu używanych publicznych adresów IP, danych kontaktowych, kontaktu w sprawie nadużyć[179] , hierarchicznego macierzystego dostawcy usług internetowych itp. Często możliwe jest wykorzystanie tych ogólnodostępnych baz danych w celu zidentyfikowania "właściciela" (operatora, dostawcy) danego adresu IP. [180]

```
Responsible organisation: Policejni akademie CR v Praze
Abuse contact info: abuse@polac.cz

inetnum:          195.113.149.160 - 195.113.149.175
organisation:     ORG-PACV1-RIPE
org-name:         Policejni akademie CR v Praze
org-type:         OTHER
address:          Policejni akademie CR v Praze
address:          Lhotecka 559/7
address:          P. O. Box 54
address:          Praha 4
address:          143 01
address:          The Czech Republic
phone:            +420 974 828 551
e-mail:           polac@polac.cz
abuse-mailbox:    abuse@polac.cz

route:            195.113.0.0/16
descr:            CESNET-TCZ
origin:           AS2852
mnt-by:           AS2852-MNT
remarks:          Please report abuse -> abuse@cesnet.cz
created:          1970-01-01T00:00:00Z
last-modified:    2006-06-26T14:36:38Z
source:           RIPE
```

Rysunek - Wyodrębnianie informacji z bazy danych RIR

Rejestratorzy regionalni następnie rozdzielają przydzielone zakresy IP między lokalnych **rejestratorów** internetowych (**LIR**). Lokalnym rejestratorem jest zazwyczaj dostawca usług internetowych (w Republice Czeskiej jest to dostawca usług społeczeństwa informacyjnego, a konkretnie dostawca łącza, publiczny lub niepubliczny). Rejestrator ten może następnie udostępnić swój zakres adresów IP na przykład części swojej organizacji lub innym podmiotom.

Skrócony wybór z bazy danych RIR wskazuje LIR (w tym przypadku stowarzyszenie CESNET, z. s. p. o., korzystające z zakresu adresów IP: 195.113.0.0/16) oraz organizację, której CESNET przydzielił część adresów publicznych [Akademia Policyjna Republiki Czeskiej z zakresem adresów IP 195.113.149.160 - 195.113.149.175. Akademia Policyjna może następnie ponownie rozdzielić te adresy między inne części organizacji (np. wydziały, laboratoria lub inne zarządzane przez nią podsieci)]. Na podstawie adresu IP i dokładnego czasu można zidentyfikować

[178] *Regionalne rejestry internetowe.* [online]. [cyt. 4.8.2015]. Dostępny pod adresem: https://*www.nro.net/about-the-nro/regional-internet-registries*

[179] Jest to osoba kontaktowa, do której użytkownik może się zwrócić w przypadku wyrządzenia mu szkody przez dany adres IP lub zakres adresów (np. cyberatak w postaci spamu, phishingu itp.). Jest to kontakt znajdujący się najbliżej źródła ataku.

[180] Nie są to jednak jedyne bazy danych. Istnieje wiele serwisów, które oferują te same informacje. Na przykład istnieją inne bazy danych: http://whois.domaintools.com/; https://www.whois.net/; http://www.nic.cz/whois/; https://whois.smartweb.cz/ itd.

konkretny system komputerowy w oparciu o hierarchiczny przydział adresów. Informacje o połączeniu końcowego systemu komputerowego (źródłowego) z docelowym systemem komputerowym (np. podłączenie komputera do Internetu i wyświetlenie żądanej strony WWW) są przechowywane przez każdego dostawcę usług internetowych na całej trasie między źródłem a miejscem docelowym.

Dzięki ścisłym zasadom określającym zarządzanie adresami IP oraz publicznie dostępnym bazom danych RIR zawierającym informacje o posiadaczach poszczególnych bloków adresowych można szybko ustalić, do jakiej sieci należy dany adres IP i kto jest jego operatorem. Operator danej sieci może ustalić, kto (lub jaki system komputerowy) korzystał z danego adresu IP w określonym czasie, rejestrując informacje o ruchu sieciowym. Identyfikacja ta stanowi bardzo ważne źródło informacji podczas postępowania z incydentami bezpieczeństwa (cyberatakami) oraz podczas poszukiwania ich źródła (inicjatora).

e-mail

Poczta elektroniczna jako jedna z najczęściej używanych usług w środowisku internetowym, z pewnością nie jest usługą anonimową. Wiadomość wysyłana ze źródła do miejsca docelowego (odbiorcy) zazwyczaj zawiera różne informacje, które pozwalają zidentyfikować zarówno dostawcę usługi (poczty elektronicznej), jak i dostawcę połączenia z urządzeniem, z którego wysłano wiadomość. Informacje te nie są wyświetlane w treści wiadomości (tj. w tekście wysyłanym do konkretnej osoby), lecz w kodzie źródłowym (nagłówku) wiadomości. Z tego kodu źródłowego można dowiedzieć się na przykład o ścieżce przez serwery, faktycznym nadawcy, nazwie komputera źródłowego, nazwie komputera, czasie wysłania wiadomości (wraz ze strefą czasową), używanym systemie operacyjnym, kliencie poczty itp. Poniżej znajduje się przykład nagłówka przesłanej dalej wiadomości[181] z potencjalnie interesującymi informacjami, które zostały wyróżnione.

[181] wiadomość e-mail została przekazana z adresu: jan.kolouch@fit.cvut.cz na adres e-mail: kyber.test@seznam.cz

```
From - Wed Aug 19 15:14:52 2015
X-Account-Key: account1
X-UIDL: 7
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Received: from relay.fit.cvut.cz (relay.fit.cvut.cz [147.32.232.237])
    by email-smtpd5.ko.seznam.cz (Seznam SMTPD 1.3.4) with ESMTP;
    Wed, 19 Aug 2015 15:14:16 +0200 (CEST)
Received: from imap.fit.cvut.cz (imap.fit.cvut.cz [IPv6:2001:718:2:2901:0:0:0:238])
    by relay.fit.cvut.cz (8.15.2/8.15.2) with ESMTP id t7JDE1Mm072888
    for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
Received: from PCP[redacted] (cust-178.17.4.174.uvt.cz [178.17.4.174] (may be forged))
        (authenticated bits=0 as user ko[redacted])
        by imap.fit.cvut.cz (8.15.2/8.15.2) with ESMTPSA id t7JDE139012575
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NOT)
        for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
X-Authentication-Warning: imap.fit.cvut.cz: Host cust-178.17.4.174.uvt.cz [178.17.4
From: "JUdr. Jan Kolouch, Ph.D." <jan.kolouch@fit.cvut.cz>
To: <kyber.test@seznam.cz>
References: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
In-Reply-To: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
Subject: =?UTF-8?Q?FW:_Chci=2C_aby_partner_s_v=C3=A1mi_na_?=
    =?UTF-8?Q?tomto_projektu?=
Date: Wed, 19 Aug 2015 15:14:15 +0200
Message-ID: <006901d0da80$f3599db0$da0cd910$@fit.cvut.cz>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_006A_01D0DA91.B6E2BBD0"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AQDP5b3kQbONWI2VUUpIa1oprzeNE6AVNk1w
Content-Language: cs
X-FIT-MailScanner-ID: t7JDE1Mm072888
X-FIT-MailScanner: Found to be clean
X-FIT-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
    score=-0.381, required 7, autolearn=not spam, RP_MATCHES_RCVD -0.38)
X-FIT-MailScanner-From: jan.kolouch@fit.cvut.cz
X-FIT-MailScanner-Watermark: 1440594843.20583@MBoaO3F9jzMModBIjGdzYg
X-Spam-Status: No
```

Obraz - wyświetlanie informacji z nagłówka wiadomości e-mail

Przeglądarka internetowa

Przeglądarka internetowa to kolejna aplikacja, która domyślnie przekazuje informacje o użytkowniku i jego systemie komputerowym do systemu komputerowego (serwera) odwiedzanej witryny. Serwer ten następnie, w ramach zapytania od klienta, ustala np. referrer (czyli stronę, z której przyszedł użytkownik), używaną przeglądarkę internetową i system operacyjny (w tym dokładną wersję), pliki cookie, pliki flash cookie, historię, pamięć podręczną itp.

Oprócz adresu IP, to właśnie między innymi pliki cookie[182] pomagają stworzyć "odcisk palca" systemu komputerowego użytkownika (komputera, smartfona itp.). Ten odcisk palca umożliwia identyfikację konkretnego systemu komputerowego[183] , nawet jeśli użytkownik korzysta z innej przeglądarki internetowej, usuwa pliki cookie, loguje się z innego adresu IP itp.

Jedną z wielu obecnie stosowanych metod "fingerprintingu" jest canvas fingerprinting.[184] Canvas fingerprinting działa poprzez instruowanie przeglądarki internetowej użytkownika, aby "narysowała ukryty obraz", gdy odwiedzany jest serwer WWW. Ten obraz jest unikatowy dla danej przeglądarki internetowej i systemu komputerowego. Narysowany obraz jest następnie przekształcany w kod

[182] W protokole HTTP plik cookie oznacza niewielką ilość danych, która jest wysyłana przez odwiedzający serwer WWW (prościej: odwiedzaną stronę WWW) do przeglądarki internetowej, która następnie zapisuje ją na komputerze użytkownika. Dane te są następnie przesyłane z powrotem do serwera WWW za każdym razem, gdy odwiedzany jest ten sam serwer.

[183] Jeśli użytkownik chce dowiedzieć się więcej o tym, co przeglądarka internetowa ujawnia na temat jego aktywności, polecam następujące adresy URL: http://panopticlick.eff.org , http://browserspy.dk/, http://samy.pl/evercookie.

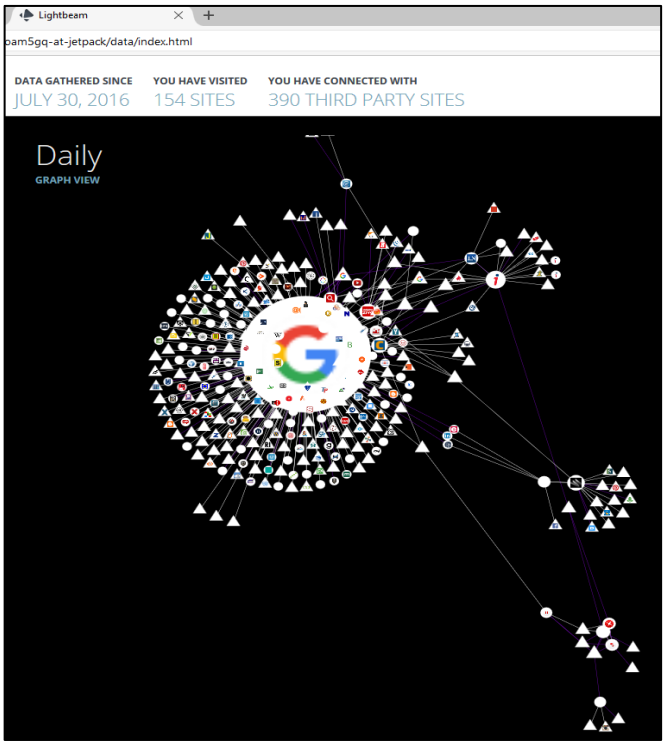
[184] ANGWIN, Julia. *Poznaj urządzenie śledzące online, które jest praktycznie niemożliwe do zablokowania.* [online]. [cyt. 10.6.2016]. Dostępny pod adresem: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

identyfikacyjny, który jest przechowywany na serwerze internetowym na wypadek, gdyby użytkownik odwiedził go ponownie. [185]

Obraz - demonstracja odcisków palców na płótnie

Oprócz fingerprintingu interesujące jest również śledzenie przekazywania informacji stronom trzecim (zarówno podmiotom, jak i usługom, które mogą wykorzystywać informacje o użytkowniku). Przekazywanie danych odbywa się zazwyczaj na podstawie warunków umowy z dostawcą usług internetowych. Na przykład każdy użytkownik końcowy może korzystać z aplikacji Light Beam[186] , która wyświetla wszystkie strony, z którymi użytkownik (często nieświadomie) wchodzi w interakcje w sieci (przekazywanie danych osobom trzecim). Przekazywanie informacji o użytkownikach osobom trzecim z pewnością nie jest czymś wyjątkowym; wręcz przeciwnie, w świecie cyfrowym jest to zjawisko powszechne i stanowi "warunek konieczny" funkcjonowania wielu dostawców usług internetowych.

1. Na pierwszym slajdzie przedstawiono działalność Firefoksa od 30 lipca 2016 r. do 4 sierpnia 2016 r. W tym czasie odwiedzono 154 strony i nawiązano połączenia z **390 witrynami osób trzecich.**

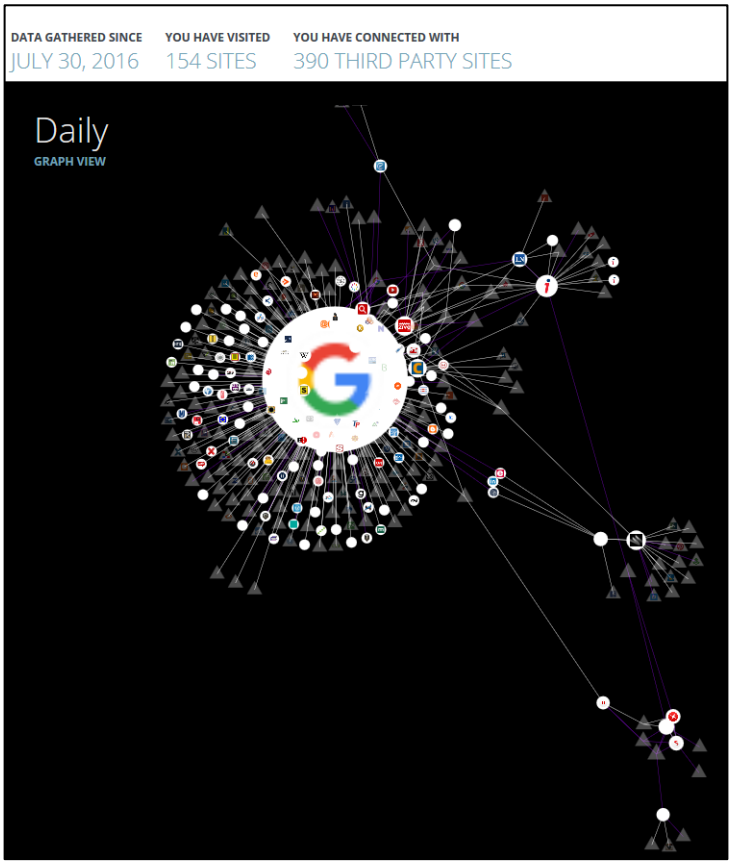


2. Drugi printscreen przedstawia tę samą mapę, ale odfiltrowuje witryny innych firm, które są przedstawione w postaci trójkątów.

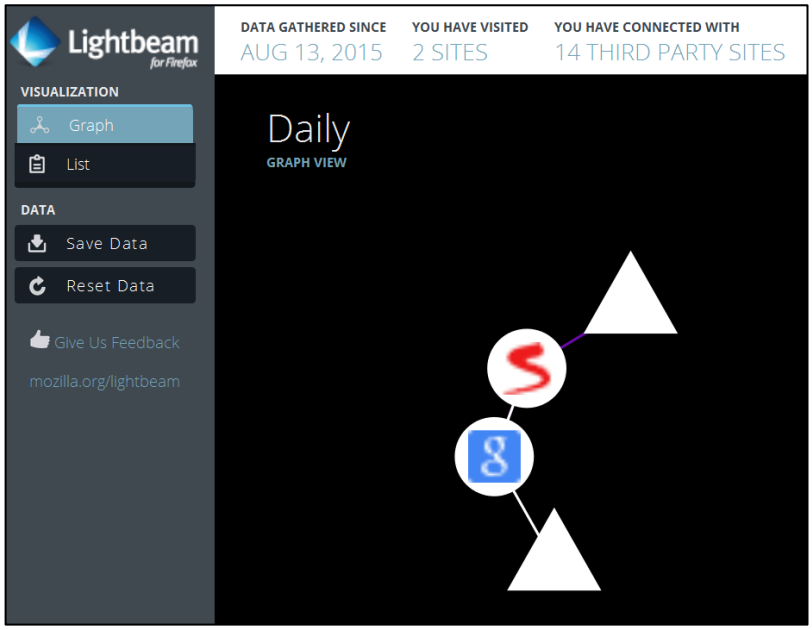
---

[185] Pokaz pobierania odcisków palców w Canavas. Możesz wypróbować test pokazujący odcisk palca przeglądarki w artykule ANGWIN, Julia. *Poznaj urządzenie śledzące online, które jest praktycznie niemożliwe do zablokowania.* [online]. [cyt. 10.6.2016]. Dostępny pod adresem: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

[186] Aplikacja umożliwia graficzne przedstawienie powiązań między poszczególnymi usługami oraz przekazywanie informacji stronom trzecim. Jest to dodatek do przeglądarki internetowej Firefox, dostępny pod adresem: https://www.mozilla.org/en-US/lightbeam/.



3. Ostatni printscreen przedstawia aplikację LightBeam po oczyszczeniu i wyświetleniu następujących stron: www.seznam.cz; www.google.com;



Inne zastosowania

W dalszej części tekstu skupię się częściowo na urządzeniach inteligentnych (smartfonach, tabletach itp.) oraz aplikacjach związanych z faktyczną działalnością "urządzeń inteligentnych". Celowo wybrałem te urządzenia, ponieważ są to systemy komputerowe, na których użytkownicy instalują prawdopodobnie największą liczbę programów (bardzo często niezweryfikowanych, jedynie polecanych przez "znajomego"). To właśnie te urządzenia, które - między innymi ze względu na

warunki umowne - mogą nie znajdować się pod pełną kontrolą użytkownika, administratora itp. stanowią zagrożenie bezpieczeństwa zarówno dla użytkownika końcowego, jak i dla firmy (organizacji).

Według wspomnianego wcześniej badania statystycznego[187] , w Internecie spędzamy średnio: 4,4 godziny. (dostęp przez komputer stacjonarny lub laptop itp.) oraz 2,7 godziny (dostęp przez urządzenie mobilne) dziennie. W przypadku komputera bezpieczeństwo urządzenia jest na ogół zapewnione, ale urządzenia przenośne (smartfon, tablet itp.) nie mają zazwyczaj ustalonych zasad dotyczących ewentualnej instalacji oprogramowania (z zaufanych lub niezaufanych źródeł) i często nie mają nawet podstawowej ochrony w postaci oprogramowania antywirusowego.[188]

To przede wszystkim użytkownik końcowy ma możliwość zainstalowania na urządzeniu z systemem Android oprogramowania, które będzie przesyłało (do innych podmiotów) i przechowywało informacje o jego działaniach, w tym przechowywało i przesyłało treść przesyłanych informacji. Usługa Sklep Play udostępniana przez firmę Google w ramach systemu operacyjnego Android pozwala każdemu programiście ustalić zasady dotyczące na przykład tego, co aplikacja ma zbierać i gdzie wysyłać dane.

Osobiście uważam, że nie jest błędem umożliwienie programistom i twórcom aplikacji uzyskania wystarczających informacji o ich aplikacjach, ich funkcjonalności itp. Jeśli uregulujemy gromadzenie tych informacji, to niewątpliwie uregulujemy i utrudnimy ewentualny postęp i dalszy rozwój tych i innych aplikacji. Z drugiej jednak strony istnieją atakujący, którzy - ponieważ Sklep Play nie uwierzytelnia i nie weryfikuje aplikacji - mogą oferować aplikacje zainfekowane złośliwym oprogramowaniem, które po zainstalowaniu w systemie komputerowym użytkownika końcowego mogą na przykład przejąć kontrolę nad jego smartfonem.

Określanie systemu komputerowego na podstawie informacji o jego składnikach

Jednym z unikalnych, ale zmiennych w pewnych okolicznościach, identyfikatorów systemu komputerowego jest adres MAC, który jest ściśle związany z kartą sieciową systemu komputerowego. Karta sieciowa nie jest jednak jedynym elementem sprzętowym, który jest w stanie przesłać niepowtarzalny identyfikator systemu komputerowego do innego systemu komputerowego.

---

[187] *Digital, Social & Mobile Worldwide in 2015* [online]. [cyt. 2015-08-09]. Dostępny pod adresem: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

[188] Należy zauważyć, że na przykład z raportu opublikowanego przez Kaspersky Lab wynika, że istnieje ponad 340 000 typów szkodliwego oprogramowania przeznaczonego głównie dla urządzeń mobilnych. Kaspersky Lab twierdzi ponadto, że 99% tego szkodliwego oprogramowania jest kierowane na urządzenia z systemem Android. Należy zauważyć, że takie ukierunkowanie jest całkowicie zrozumiałe, ponieważ zróżnicowanie urządzeń i wersji systemu operacyjnego Android jest znaczne (niektóre raporty podają, że system operacyjny Android jest wykorzystywany przez ponad 24 000 różnych urządzeń).
Więcej informacji na ten temat można znaleźć np:
Pierwsze mobilne szkodliwe oprogramowanie: jak Kaspersky Lab odkrył Cabir. [online]. [cyt. 1.8.2016]. Dostępny pod adresem: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
Wejdź na stronę: *Ciekawe statystyki dotyczące mobilnych strategii transformacji cyfrowej* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/
Fragmentacja systemu Android bije kolejne rekordy: 24 000 różnych urządzeń [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/

Naukowcy z Uniwersytetu Princeton odkryli, że system komputerowy można zidentyfikować na przykład na podstawie informacji o jego baterii, a przeglądarki internetowe są istotnym elementem przekazywania tych informacji. [189]

W praktyce stosuje się proces, który wykorzystuje możliwości języka HTML5. Standard ten obejmuje funkcję, która pozwala stronie internetowej (lub serwerowi WWW) określić stan baterii systemu komputerowego uzyskującego do niej dostęp (przekazywane są informacje o tym, ile baterii pozostało, jak długo potrwa rozładowanie lub naładowanie). W założeniu właścicieli serwerów WWW użytkownik, którego bateria jest na wyczerpaniu, będzie miał możliwość obejrzenia strony w wersji oszczędzającej energię. Dwa skrypty opisane przez badaczy z Uniwersytetu Princeton wykorzystują już dane dotyczące baterii, zbierając jednocześnie inne informacje - takie jak adres IP czy odciski palców. Takie kombinacje mogą już zapewnić bardzo dokładną identyfikację systemu komputerowego.[190]

7.1.2 Ślad cyfrowy, na który można wpływać

Ślad cyfrowy influencera to wszelkie informacje, które użytkownik dobrowolnie przekazuje innej osobie (fizycznej lub prawnej, a nawet np. dostawcy usług internetowych). Pod pojęciem przekazania należy rozumieć szereg czynności, które mogą polegać np. na wysłaniu wiadomości e-mail, umieszczeniu wpisu w dyskusji, na forum, opublikowaniu dowolnego materiału (zdjęcia, wideo, audio itp.) w sieciach społecznościowych itp. Obejmuje również rejestrację i korzystanie ze wszystkich możliwych usług w cyberprzestrzeni [np. systemów operacyjnych, poczty elektronicznej (w tym bezpłatnej), serwisów społecznościowych, serwisów randkowych, sieci P2P, czatów, blogów, BBS-ów, stron internetowych, usług w chmurze, przechowywania danych itp.]

Ślady cyfrowe, na które można wpływać, to ślady, nad którymi użytkownik może mieć względną kontrolę i to od niego zależy, jakie informacje o sobie zechce udostępnić innym. Należy jednak pamiętać o przedstawionej już przesłance: wszelkie dane lub informacje wprowadzone do cyberprzestrzeni pozostaną w niej.

Teoretycznie można by zdefiniować kategorię **śladów hipotetycznie wpływalnych,** co jest w pewnym sensie oksymoronem, jednak kategoria ta obejmuje pewne fakty, na które użytkownik teoretycznie może wpływać, tzn. jest w stanie wpływać, ale zazwyczaj tego nie robi, gdyż de facto znacznie ograniczyłoby to możliwości jego funkcjonowania w świecie cyfrowym. Ślady te mogą obejmować np. korzystanie z usług największych dostawców usług internetowych (Microsoft, Apple, Google, Facebook itp.), w przypadku których korzystanie z usług jest uzależnione od uzgodnienia warunków umownych (EULA), które pozwalają tym dostawcom uzyskać znaczną ilość informacji. Ponadto ślady te mogą obejmować ślady utworzone na przykład w wyniku korelacji śladów nieinfluencyjnych i wpływowych; informacje publikowane na nasz temat przez innych użytkowników; dane, które są odzwierciedlane; dane EXIF[191]

---

[189] Więcej informacji można znaleźć w materiałach ENGLEHARDT, Steven i Ardvin NARAYANAN. *Śledzenie w Internecie: Pomiar i analiza 1 miliona miejsc.* [online]. [cyt. 2016 Aug 5]. Dostępny pod adresem: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

[190] Więcej informacji na ten temat można znaleźć w artykule VOŽENÍLEK, David. *Nie pomoże smarowanie "sucharów", internet cię wyda i baterie.* [online]. [cyt. 4.8.2016]. Dostępny pod adresem: http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz

[191] EXIF - *wymienny format* plików *graficznych.* Jest to format metadanych umieszczanych w zdjęciach cyfrowych przez aparaty cyfrowe. Metadane te mogą na przykład

- Marka i model aparatu.
- Data i godzina wykonania zdjęcia.
- Pozycja GPS.
- Informacje o autorze (osobie, która zarejestrowała aparat).

7.2 Warunki Umowy (EULA)

W następnej części tego rozdziału postaram się opisać, jakie informacje o użytkownikach są domyślnie zbierane przez głównych dostawców usług internetowych.[192] Wybrałem firmę Google Inc., ponieważ uważam, że istnieje minimalna liczba użytkowników, którzy nigdy nie korzystali z żadnego z produktów tej firmy (np. systemu operacyjnego Android, wyszukiwarki na stronie www.google.com, poczty Gmail, przeglądarki Google Chrome itd.)[193] Moim celem nie jest w żaden sposób "atakowanie" firmy Google Inc. lub innych firm (w tym ich produktów). Celem jest przedstawienie możliwych zagrożeń bezpieczeństwa związanych z korzystaniem z niektórych świadczonych usług oraz akceptacja warunków (EULA - End Users License Agreement), którymi obwarowane jest korzystanie z tych usług.

Warunki umowne umożliwiające korzystanie z usług danego dostawcy usług są w istocie niczym innym jak jednostronnym określeniem praw i obowiązków przez dostawcę usług (ISP). Użytkownik nie jest jednak w żaden sposób ograniczony w swoich prawach, ponieważ może zrezygnować z takich jednostronnie określonych warunków umowy. W przypadku zgody na korzystanie z takich usług można ogólnie stwierdzić, że zastosowanie mają przede wszystkim normy prawa prywatnego.

Pytanie brzmi, czy użytkownik jest rzeczywiście świadomy warunków umowy, na które się zgodził, kiedy stają się one dla niego wiążące i jaką ewentualną (prawną) ingerencję w jego podstawowe prawa i wolności człowieka stanowi taka zgoda. Innym nieuniknionym faktem jest to, że usługi świadczone w ten sposób mogą naruszać prawa i uzasadnione interesy (np. bezpieczeństwo IT, poufność danych itp.) osób trzecich (np. pracodawców itp.), które nie wyraziły wyraźnej zgody na korzystanie z danej usługi.

Teoretycznie można stwierdzić, że prawie 3 miliardy użytkowników zawarło prywatną umowę z tą firmą w ciągu całego okresu jej istnienia.[194] Smutnym faktem jest to, że bardzo niewielki odsetek użytkowników jest skłonny czytać warunki korzystania z usług.[195]

Fragmenty warunków korzystania z usług Google Inc.[196]

Google wyraźnie stwierdza, że jeśli użytkownik zaczyna korzystać z jakichkolwiek usług Google, zgadza się na obowiązujące warunki. Wyraźnie określa również relacje między użytkownikiem a nią samą jako dostawcą usług, w przypadku gdy użytkownik jest zobowiązany do zaakceptowania dodatkowych zasad i warunków. Związek ten jest wyrażony w następujący sposób: "*Oferta naszych usług jest szeroka, a niektóre z nich mogą podlegać dodatkowym warunkom lub wymaganiom (w tym ograniczeniom wiekowym).* ***Dodatkowe zasady i warunki*** *będą udostępniane wraz z odpowiednimi usługami.* ***Jeśli użytkownik korzysta z tych usług, dodatkowe warunki stają się częścią ustaleń umownych między stronami."***

- Ustawienia aparatu.
- Podgląd obrazu również.

[192] W tej części tekstu wykorzystano tezy opublikowane w artykule: KOLOUCH, Jan. Pseudoanonimowość - zagrożenie dla bezpieczeństwa użytkowników Internetu. *DSM -data security management* [online]. 2015. vol. 19, issue 3, pp. 24-29 ISSN 1211-8737. Dostępny pod adresem: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/

[193] Należy zauważyć, że następujące firmy mają bardzo podobne warunki umowne (umożliwiające im przekazywanie informacji w porównywalnym zakresie): Microsoft, Apple, Facebook itp.

[194] Według artykułu SMITH, Craig. *Według liczb: 100 zadziwiających statystyk i faktów dotyczących wyszukiwarki Google* [online]. [cyt. 2016 Aug. 4]. Dostępny pod adresem: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/ Miesięcznie w wyszukiwarce Google dokonuje się 100 miliardów wyszukiwań.

[195] A według jednego z uczestników konferencji Security 2015, normalny człowiek poświęciłby około 10-20 lat swojego życia na przeczytanie wszystkich ciągle zmieniających się warunków.

[196] Zwana dalej Google. Wszystkie fragmenty Warunków korzystania z usługi zostały zaczerpnięte z: Warunki korzystania z https://policies.google.com/terms?hl=pl&gl=pl https://www.google.cz/intl/cs/policies/terms/regional.html

Na początku warunków Google stwierdza, że *"**Możemy sprawdzać zawartość witryny***[197] *, aby ustalić, czy **jest ona legalna i zgodna z naszymi zasadami,** a jeśli uznamy, że narusza ona nasze zasady lub prawo, możemy usunąć tę zawartość lub uniemożliwić jej wyświetlanie. Należy pamiętać, że **powyższe nie oznacza, że weryfikujemy treści.**"*

Z punktu widzenia bezpieczeństwa, moim zdaniem, sekcja dotycząca **ochrony danych i praw autorskich** stanowi istotną część Regulaminu.[198] W tej sekcji firma Google określa, jakie informacje gromadzi o użytkownikach i w jaki sposób je przetwarza. Z punktu widzenia bezpieczeństwa i "poczucia anonimowości" kluczowe znaczenie mają następujące informacje. Myślę, że deklaracja, iż poniższe informacje są gromadzone, *"abyśmy mogli świadczyć lepsze usługi wszystkim naszym użytkownikom - od określania prostych rzeczy, takich jak język, którym się posługujesz, po bardziej złożone, takie jak to, które reklamy będą dla Ciebie najbardziej użyteczne, jakie osoby są dla Ciebie najbardziej interesujące na stronie lub jakie filmy na YouTube możesz polubić",* jest być może godna pochwały, ale co najmniej rzuca się w oczy. Porównanie do wspomnianego wcześniej Raportu mniejszości w zakresie kierowania reklam jest aż nadto oczywiste. Co więcej, Manfred Spitzer i *Cyfrowa demencja* znów przychodzą mi na myśl, ponieważ po pewnym czasie to już nie ja decyduję o tym, co oglądam lub czego szukam (lub też mogę nie być i nie otrzymuję wszystkich istotnych odpowiedzi).

Google gromadzi informacje o użytkownikach zasadniczo na dwa sposoby:

1. **Informacje dostarczone przez użytkownika.** Zazwyczaj obejmuje to:
   - *imię i nazwisko, adres e-mail, numer telefonu lub kartę kredytową.*
2. **Informacje uzyskane podczas korzystania z usług Google.** Gromadzone są informacje o usługach, z których korzysta użytkownik, w tym o sposobie korzystania z nich (*"na przykład, gdy ogląda on film w serwisie YouTube, odwiedza witrynę internetową, która korzysta z naszych usług reklamowych, ogląda nasze reklamy i treści lub reaguje na nie*"). Jak podaje Google, obejmuje to:
   - ***Informacje o urządzeniu*** *(np. model sprzętu, wersja systemu operacyjnego, unikalne identyfikatory urządzenia*[199] *oraz informacje o sieci komórkowej, w tym numer telefonu).* Google może powiązać identyfikatory urządzenia lub numer telefonu użytkownika z jego kontem użytkownika Google
   - ***Informacje o protokole:***
     - *szczegółowe informacje o tym, jak użytkownik korzystał z Google,*
     - *Informacje o rejestrze połączeń (np. numer telefonu, identyfikator rozmówcy, numery przekierowania połączeń, godzina i data połączeń, czas trwania połączeń, szczegóły trasowania SMS-ów i typy połączeń),*

---

[197] Treść oznacza zawartość (dane), która nie należy do Google. Odpowiedzialność za treść spoczywa na podmiocie, który ją opublikował.

[198] W szczególności *Polityka prywatności* [online]. [cit.14.6.2016]. Dostępny pod adresem: https://www.google.cz/intl/cs/policies/privacy/

[199] Definicja Google. *Unikalny identyfikator urządzenia.* [online]. [cyt. 14.6.2016]. Dostępny pod adresem: https://www.google.cz/intl/cs/policies/privacy/key-terms/#toc-terms-unique-device-id
"*Unikalny identyfikator urządzenia (czasami nazywany uniwersalnym unikalnym identyfikatorem lub UUID) to ciąg znaków zakodowanych w urządzeniu przez producenta w celu jego jednoznacznej identyfikacji (na przykład numer IMEI telefonu komórkowego). Poszczególne identyfikatory urządzeń różnią się pod względem tego, czy są trwałe, czy użytkownicy mogą je resetować i w jaki sposób można uzyskać do nich dostęp. Dane urządzenie może zawierać kilka różnych niepowtarzalnych identyfikatorów. Unikalne identyfikatory urządzeń mogą być wykorzystywane do różnych celów, takich jak bezpieczeństwo, wykrywanie oszustw, synchronizacja usług, np. skrzynek* pocztowych*, lub przechowywanie ustawień użytkownika i wyświetlanie odpowiednich reklam. "*

- *Adres protokołu internetowego,*
- *informacje o zdarzeniach dotyczących urządzenia (np. awarie, aktywność systemu, ustawienia sprzętu, typ przeglądarki, język przeglądarki, data i godzina żądania lub odsyłający adres URL,*
- *pliki cookie, które mogą być unikatowymi identyfikatorami przeglądarki lub konta Google*.

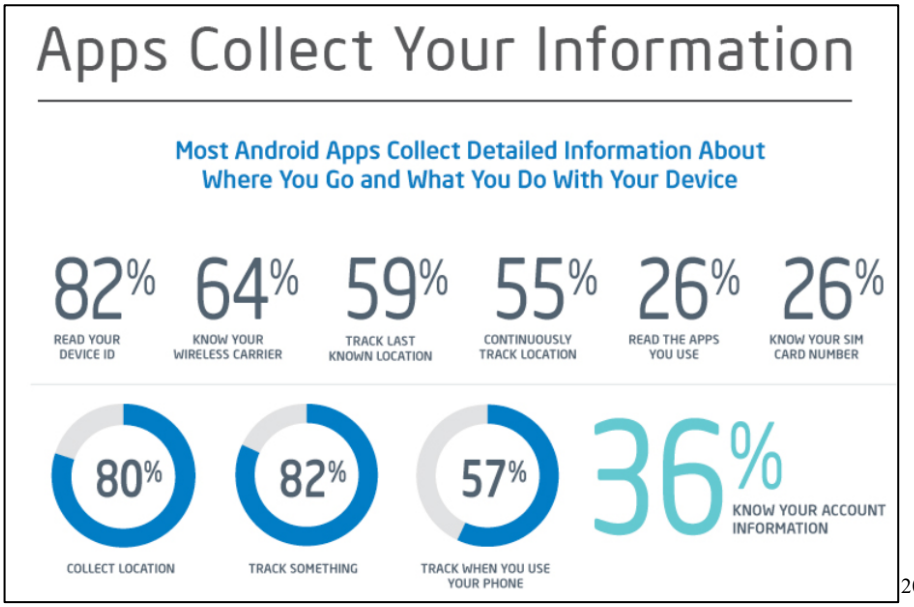
- ***Informacje o lokalizacji.*** Firma Google jest upoważniona do gromadzenia i przetwarzania informacji o aktualnej lokalizacji użytkowników. Do określania lokalizacji Google może używać różnych technologii, takich jak adres IP, GPS i inne czujniki, które mogą dostarczać Google informacji o znajdujących się w pobliżu urządzeniach, punktach dostępu do sieci Wi-Fi i nadajnikach sieci komórkowej.
- ***Unikatowe numery aplikacji.*** **Zazwyczaj jest to numer licencji i typ (wersja) danego zainstalowanego oprogramowania.** Regulamin nie oznacza, że unikatowe numery aplikacji są rejestrowane tylko w przypadku urządzeń, których głównym systemem operacyjnym jest Android. Można zatem stwierdzić, że jeśli korzysta się z usług Google, to informacje o unikatowych numerach aplikacji są zbierane również z innych systemów operacyjnych (iOS, Linux, Windows itd.).
- ***Magazyn lokalny.*** **Zgodnie z Warunkami korzystania z usługi Google może:** ***"****gromadzić i przechowywać informacje (w tym dane osobowe) w pamięci lokalnej na urządzeniu użytkownika"*. Ponownie można dojść do takiego samego wniosku, jak w przypadku unikalnych numerów aplikacji.

  Moim zdaniem problem polega również na tym, że nigdzie w ogólnych warunkach umowy nie jest dokładnie określone[200] , jaka lokalizacja, a zwłaszcza jakie zabezpieczenia będą wykorzystywane przez Google, a zatem teoretycznie możliwe jest korzystanie z pamięci masowej jako całości. Możliwe jest pobieranie informacji o plikach (np. ich nazw, lokalizacji oraz, ad absurdum, hasha, który następnie zostanie porównany np. z bazą danych innej usługi, w której przechowywane są dane - np. DropBox, OneDrive itp.)

  Moim zdaniem, zagrożeniem dla użytkownika jest także możliwość niewłaściwego wykorzystania tak przechowywanych danych przez napastnika. Informacje (zazwyczaj zapisywane w plikach cookie itp.) przechowywane w lokalnej pamięci masowej użytkownika mogą również stać się interesującym celem dla atakującego, ponieważ na ich podstawie można poznać np. wzorce zachowań użytkownika.
- ***Pliki cookie i podobne technologie. "****Gdy użytkownik odwiedza usługę Google, my* ***i nasi partnerzy*** *używamy różnych technologii do zbierania i przechowywania informacji. Może to obejmować m.in. wykorzystanie plików cookie lub podobnych technologii do identyfikacji przeglądarki lub urządzenia użytkownika. Technologie te* ***wykorzystujemy również do zbierania i przechowywania informacji podczas korzystania przez użytkownika z usług oferowanych przez nas naszym partnerom****, takich jak usługi reklamowe lub funkcje Google, które mogą pojawiać się w innych witrynach."*

Jakie informacje są zbierane przez aplikacje działające w systemie operacyjnym Android:

[200] Odpowiednio, zgodnie z wymaganą funkcją, będzie to głównie przechowywanie informacji i danych w folderze danej przeglądarki (webbrowser), ale zgodnie z warunkami umowy może to dotyczyć także innych aplikacji niż webbrowser.



[201]

Google ma ponadto prawo do wykorzystywania tych informacji na podstawie uzgodnionych warunków. Firma Google jest uprawniona między innymi do analizowania treści (w tym wiadomości e-mail) za pomocą zautomatyzowanych systemów. Jest również uprawniony do łączenia danych osobowych z jednej usługi z informacjami i danymi osobowymi z innej usługi (np. Google).

Obsługa tych informacji obejmuje ich udostępnianie, zarówno za zgodą użytkownika, jak i bez niej.[202] Warto przytoczyć dosłowne brzmienie warunków umownych zezwalających na **udostępnianie danych do celów przetwarzania zewnętrznego i z przyczyn prawnych:**

"Przekazujemy dane osobowe firmom stowarzyszonym lub innym zaufanym firmom lub osobom, które przetwarzają je dla nas zgodnie z naszymi instrukcjami i zgodnie z naszą polityką prywatności oraz innymi obowiązującymi środkami zachowania poufności i bezpieczeństwa.

"Udostępniamy dane osobowe firmom, organizacjom i osobom** spoza **firmy** Google, jeśli w **dobrej wierze jesteśmy przekonani, że dostęp do nich, ich wykorzystanie, zachowanie lub ujawnienie jest w uzasadnionym stopniu konieczne do osiągnięcia tego celu:

- *Zgodność z obowiązującym prawem, przepisami, procedurą prawną lub egzekwowalnymi wymogami rządowymi,*
- *egzekwowanie odpowiednich warunków umowy, w tym prowadzenie dochodzeń w sprawie ewentualnych naruszeń,*
- *wykrywać oszustwa, trudności techniczne lub problemy z bezpieczeństwem, zapobiegać im lub w inny sposób im przeciwdziałać,*
- *chronić przed naruszeniem praw, własności lub bezpieczeństwa firmy Google, jej użytkowników lub społeczeństwa w zakresie wymaganym lub dozwolonym przez prawo".*

Jednak z punktu widzenia bezpieczeństwa i utraty anonimowości za najbardziej problematyczny uważam następujący fragment Warunków korzystania z usługi, który dotyczy treści zamieszczanych przez użytkowników w usługach świadczonych przez Google:

---

[201] CAETANO, Lianne. *Czy Twoje aplikacje nadmiernie się dzielą? Raport o bezpieczeństwie mobilnym 2014 mówi wszystko.* [online]. [cyt. 2015-04-10]. Dostępny pod adresem: https://blogs.mcafee.com/consumer/mobile-security-report-2014/

[202] Na przykład z administratorami domen, do celów przetwarzania zewnętrznego lub z przyczyn prawnych.

*"Jeśli użytkownik przesyła**, przekazuje, przechowuje lub otrzymuje treści do Usług lub za ich pośrednictwem, udziela firmie Google** (oraz podmiotom, z którymi współpracuje Google) obowiązującej **na całym świecie licencji na używanie, hosting, przechowywanie, reprodukcję, modyfikowanie, tworzenie dzieł pochodnych** (takich jak dzieła będące wynikiem tłumaczenia, adaptacji lub mod**yfikacji mających na** celu lepsze działanie w Usługach)*[203] *, **komunikowanie, publikowanie, wykonywanie, publiczne wyświetlanie i rozpowszechnianie takich treści**.Adres ....License jest zachowany nawet po zaprzestaniu korzystania z Usług (np. w przypadku dodania wpisu biznesowego do Map Google). **Niektóre usługi umożliwiają użytkownikowi dostęp do treści przesłanych przez niego do serwisu lub ich usunięcie...."*

Osobiście uważam, że przynajmniej w tej części regulaminu przekroczona została wyimaginowana granica określająca adekwatność gromadzonych informacji o poszczególnych użytkownikach. Sekcja ta dotyczy de facto "legalnego wykorzystania" wszelkich treści, z którymi Google ma "styczność". Osobiście uważam, że to właśnie ingerencja w treść np. przekazywanych informacji powinna być ostatecznością, a nie rodzajem "oczywistego" postanowienia umownego.

[203] Zrozumiałe jest, że Google próbuje tłumaczyć utwory, strony internetowe lub inne treści, na przykład po to, aby użytkownik nieznający oryginalnego języka utworu mógł go przeczytać. Jednak ad absurdum, można sobie wyobrazić, że zostanie opublikowany Twój prywatny wiersz miłosny, który wysłałeś za pomocą jednej z usług Google'a, Twoje zdjęcie, Twój genialny pomysł na perpetuum mobile itp.

PODSUMOWANIE ROZDZIAŁU

- Wszystkie aplikacje, niezależnie od systemu komputerowego, na którym są używane, serwisy internetowe, a zwłaszcza portale społecznościowe, gromadzą znaczną ilość informacji o swoich użytkownikach, które w większości przypadków nie są im potrzebne do działania, ale które pozwalają danemu dostawcy usług internetowych świadczyć usługi "za darmo" oraz "ukierunkowywać" lub modyfikować oferowane przez niego usługi. Informacje, które w normalnych warunkach nie są niezbędne do bezpośredniego korzystania z poszczególnych usług, to na przykład informacje o charakterze osobistym (imię, nazwisko, adres e-mail, numer telefonu, miejsce zamieszkania itp.), informacje wrażliwe (np. informacje o używanym systemie operacyjnym komputera, wersje poszczególnych aplikacji, pliki cookie itp.), dane dotyczące lokalizacji (współrzędne GPS, informacje o WiFi, GPRS itp.), dane operacyjne itp.
- Ślady cyfrowe, w zależności od tego, czy użytkownik może na nie wpływać, czy nie, można ogólnie podzielić na ślady, na które można wpływać, i ślady, na które nie można wpływać.
- W świecie technologii informacyjno-komunikacyjnych obowiązuje jedna zasada: gdy cokolwiek przesyłasz, transmitujesz, pośredniczysz, umieszczasz w cyberprzestrzeni, pozostaje tam "na zawsze". Ślady niemożliwe do prześledzenia są najczęściej tworzone przez interakcję jednego systemu komputerowego z innym systemem komputerowym lub przez funkcjonalność systemu komputerowego (i związanego z nim oprogramowania). Przykłady takich śladów obejmują informacje z systemu operacyjnego (np. komunikaty o błędach systemu Windows lub informacje systemowe) lub inne informacje i dane, które są przechowywane w oparciu o funkcjonalność systemu bez konieczności ich przesyłania (np. system komputerowy nigdy nie był podłączony do żadnej sieci lub innego systemu komputerowego). Nie do końca słuszne byłoby bezkompromisowe stwierdzenie, że na te ślady nie można wpływać. Jeżeli użytkownik posiada wystarczające umiejętności, może zmodyfikować, zamaskować lub zlikwidować wiele "nieinfiltrowanych" śladów cyfrowych (np. po prostu używając trybu anonimowego w przeglądarce internetowej w celu wyłączenia plików cookie). Jednak ruch użytkownika w Internecie może być śledzony na różne sposoby.
- Ślad cyfrowy influencera to wszelkie informacje, które użytkownik dobrowolnie przekazuje innej osobie (osobie fizycznej lub prawnej, a nawet np. dostawcy usług internetowych). Pod pojęciem przekazania należy rozumieć szereg czynności, które mogą polegać np. na wysłaniu wiadomości e-mail, umieszczeniu postu na forum dyskusyjnym, opublikowaniu dowolnego materiału (zdjęcia, wideo, audio itp.) w sieciach społecznościowych itp. Obejmuje również rejestrację i korzystanie z wszelkich możliwych usług w cyberprzestrzeni [np. systemów operacyjnych, poczty elektronicznej (w tym bezpłatnej), portali społecznościowych, serwisów randkowych, sieci P2P, czatów, blogów, BBS-ów, stron internetowych, usług w chmurze, przechowywania danych itp.]

SŁOWA KLUCZOWE, KTÓRE WARTO ZAPAMIĘTAĆ

- Cyfrowy ślad
- Ślad cyfrowy pozostaje nienaruszony
- Cyfrowy ślad mający wpływ
- EULA

PYTANIA KONTROLNE

- Zdefiniuj pojęcie śladu cyfrowego.
- Czym różnią się od siebie ścieżki cyfrowe?
- Jakie są elementy, które składają się na nieskażony ślad cyfrowy?
- Kim jest LIR?
- Jakie informacje o użytkowniku zawiera adres IP?
- Co to jest umowa EULA?

Wnioski

Wraz z rozwojem technologii informacyjno-komunikacyjnych i rosnącą liczbą danych publikowanych przez samych użytkowników nieuchronnie pojawiają się wnioski o usunięcie danych, które nie są aktualne lub w jakiś sposób szkodzą samym użytkownikom.

Wizja, w której świat cyfrowy i jego użytkownicy staną się anonimowi, jest moim zdaniem utopią. Nawet różne możliwości anonimizacji w postaci sieci TOR[204] itp. nie zmienią tego stwierdzenia, ponieważ zawsze będzie istniała interakcja ze światem rzeczywistym i zawsze będą użytkownicy w świecie cyfrowym, którzy są zawodni i popełniają błędy w ukrywaniu informacji o swoich działaniach. Podobnie utopijne jest przekonanie, że technologia będzie niepomna. Dane o użytkownikach będą nadal gromadzone. Nastąpi dalsze techniczne dostosowanie tego, kto będzie, a kto nie będzie miał dostępu do tych danych.

Wzajemne powiązanie różnych oferowanych usług oraz możliwość przekazywania informacji o użytkownikach osobom trzecim, a także **Internet przedmiotów (IoT**) niewątpliwie przyczyniają się do "deanonimizacji" użytkowników**.**

Ciekawe rozwiązanie w zakresie "deanonimizacji" użytkowników opracowuje m.in. firma Facebook, która rozwija metodę **DeepFace**, polegającą na tworzeniu trójwymiarowego modelu twarzy na podstawie zdefiniowanych punktów początkowych na zdjęciu.[205] Dzięki tej metodzie można zidentyfikować nawet osoby, które nie mają konta na Facebooku i zostały jedynie oznaczone (zidentyfikowane) jako konkretne osoby. Metoda DeepFace została tu wymieniona celowo, ponieważ możliwość jej wykorzystania jest zapisana w regulaminie serwisu Facebook i pozwala, nawet jeśli użytkownik sobie tego nie życzy (np. nie zaznacza siebie celowo pod zdjęciem), na jego identyfikację.

Jeśli chodzi o **IoT,** wkraczanie nowych technologii i nasza "deanonimizacja" są jeszcze bardziej widoczne. Jako przykład podam "inteligentną telewizję"[206] , która po zainstalowaniu ponownie oferuje warunki umowy, a następnie natychmiast "pyta" o możliwość połączenia z Internetem. Bardziej szczegółowa analiza warunków może ujawnić na przykład, że telewizor jest uprawniony do udostępniania nagrań poufnych i osobistych rozmów lub czynności, które *użytkownik "przeprowadza" przed nim, pod warunkiem że* korzysta z funkcji sterowania głosem lub ruchem. W ramach warunków użytkownik jest również informowany o tym, że zarejestrowane dane są przekazywane producentowi i osobom trzecim. Jedynym sposobem zapobiegania przekazywaniu tych informacji jest wyłączenie funkcji rozpoznawania głosu lub ruchu. Pytanie brzmi, czy jest to rzeczywiście rozwiązanie. Osobiście uważam, że rozwiązaniem byłoby uniemożliwienie lub ograniczenie przekazywania danych albo wskazanie podmiotu, któremu byłbym skłonny udostępnić te dane osobowe.

Jeśli chodzi o prawo do bycia zapomnianym, mogę sobie wyobrazić hipotetyczną sytuację, w której użytkownik zwróciłby się do firmy, która wyprodukowała telewizor lub inny system komputerowy o podobnych warunkach umownych, o usunięcie nagrania rozmowy z dnia, na przykład, 1 marca 2016 r. Sąd zastosował w tym przypadku również prawo do bycia zapomnianym, ale powstaje pytanie, kto

---

[204] Niektóre przypadki naruszenia bezpieczeństwa sieci TOR:
FBI wykorzystuje lukę we Flashu do złamania zabezpieczeń sieci Tor. [online]. [cyt. 2016-07-23]. Dostępny pod adresem: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/
Informacja o bezpieczeństwie sieci Tor: Atak polegający na potwierdzaniu ruchu "relay early". [online]. [cyt. 2016-07-23]. Dostępny pod adresem: https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

[205] Na przykład: *Facebook wkrótce będzie w stanie zidentyfikować użytkownika na każdym zdjęciu.* [online]. [cyt. 2015-08-09]. Dostępny pod adresem: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

[206] Zob. też np. ČÍŽEK, Jakub. *Inteligentne telewizory nas monitorują. Pogódź się z tym.* [online]. [cyt. 9.8.2015]. Dostępny pod adresem: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx

faktycznie zagwarantuje użytkownikowi, że jego dane zostały usunięte z wszystkich magazynów danych.

Fragment z umowy EULA firmy Samsung:

> ***Należy pamiętać, że jeśli wypowiadane przez Ciebie słowa zawierają dane osobowe lub inne poufne informacje, znajdą się one wśród danych przechwyconych i przekazanych osobom trzecim w wyniku korzystania z funkcji rozpoznawania głosu.***

W Internecie nie ma anonimowości i z pewnością nie będzie jej w najbliższej przyszłości. Użytkownicy często, całkiem logicznie i słusznie, intensywnie walczą z ingerencją państwa w ich prywatność, ale z drugiej strony sami dobrowolnie i znacznie chętniej oferują tę prywatność wszystkim wokół (np. w sieciach społecznościowych, usługach w chmurze itp.).

Nie sądzę, by przepaść między światem rzeczywistym a cyfrowym była aż tak wielka, i może dlatego często nie rozumiem bezmyślnego zachowania użytkowników, jeśli chodzi o usługi oferowane przez dostawców usług internetowych. Tak, jako użytkownicy otrzymujemy usługę w ramach warunków umowy, którą zawieramy. Pytanie brzmi, czy ta umowa jest dobra i czy cena, jaką płacimy za tę usługę, jest rozsądna.

Osobiście mam pełną świadomość tego, że moja wolność, w tym pewien stopień "anonimowości" w Internecie, jest już utopią. Sądzę, że ta utopia w niedalekiej przyszłości, dzięki IoT i coraz ściślejszemu powiązaniu wszystkich "usług", zostanie doprowadzona niemal do sytuacji nie przypominającej tej z Raportu mniejszości. Z drugiej strony wierzę, a raczej chcę wierzyć, że nadal jestem wolny i mam prawo wyboru.

Prawo wyboru polega więc co najmniej na tym, że to ja decyduję, czy chcę korzystać z usług (usług) i na jakich warunkach. Uważam, że użytkownicy powinni stać się prawdziwym autorytetem w Internecie, przynajmniej w formie wyrażania swojej woli i prób wywalczenia swoich praw nawet wobec dostawcy usług, ponieważ w przypadku interwencji państwa w ich prywatność w wielu przypadkach im się to udaje.

Nawiasem mówiąc, aby ocenić, jak "agresywna" jest dana usługa lub jak bardzo ingeruje w prywatność użytkownika, można znaleźć np. Regulamin usługi, Nie czytałem: https://tosdr.org/. Jeśli nic innego (choć można tu zastosować analogię do "cyfrowej demencji"), to przynajmniej sprawdzenie podstawowych zasad i warunków na tej stronie może pomóc użytkownikom w zrozumieniu problemu.

Żyjemy w czasach, w których technologie informacyjne i komunikacyjne są nieodłącznie związane z każdym aspektem naszej egzystencji. Pewnym paradoksem jest to, że de facto nie mamy możliwości uniknięcia tego przenikania i interakcji z technologiami informacyjno-komunikacyjnymi, co jednocześnie czyni nas bardziej podatnymi na zagrożenia.

Dzięki technologiom informacyjno-komunikacyjnym i połączonym usługom tworzymy w świecie wirtualnym odbicie naszej tożsamości lub osobowości.

Nasze cyfrowe "ja" ma wszelkie predyspozycje, aby być "znacznie trwalsze" niż nasze ciało fizyczne. Informacje o naszej aktywności w cyberprzestrzeni, o naszej cyberosobowości, kontach i śladach cyfrowych będą żyły po naszej śmierci dzięki archiwizacji danych i informacji o nas.

W miarę jak rośnie ilość danych i informacji przechowywanych u poszczególnych dostawców usług internetowych, coraz częściej poruszane są kwestie ich skutecznego zabezpieczenia, przekazywania lub usuwania, nie tylko na podstawie umowy zawartej między dostawcą usług a użytkownikiem końcowym, ale także na podstawie nowo powstających przepisów.

Państwa, organizacje i osoby prywatne są coraz bardziej świadome, że informacje i dane stanowią znaczący potencjał, który jest coraz częściej atakowany w ramach ataków cybernetycznych, mających na celu kradzież, uszkodzenie, uniemożliwienie dostępu lub usunięcie danych.

Jeśli chcemy żyć we współczesnym społeczeństwie i korzystać z jego dobrodziejstw, nie można zrezygnować z technologii informacyjno-komunikacyjnych, a już na pewno nie ma sensu zaprzestać ich stosowania. Musimy zacząć uczyć się, jak korzystać z tych technologii i usług, jak unikać lub przynajmniej eliminować skutki cyberataków.

W cyberprzestrzeni, podobnie jak w świecie rzeczywistym, nie ma jednego systemu bezpieczeństwa i ochrony, który można by powszechnie stosować wobec wszystkich. Jeśli chcemy zająć się bezpieczeństwem, należy podejść do niego w sposób holistyczny i zindywidualizowany.

Lista wykorzystanych źródeł i innych zasobów

1. ANGWIN, Julia. *Poznaj urządzenie śledzące online, które jest praktycznie niemożliwe do zablokowania.* [online]. [cyt. 10.6.2016].
2. BARLOW, Perry John. *Deklaracja niepodległości cyberprzestrzeni.* [online]. [cyt. 23.9.2014]. Dostępny pod adresem: https://www.eff.org/cyberspace-independence.
3. CAETANO, Lianne. *Czy Twoje aplikacje nadmiernie się dzielą? Raport o bezpieczeństwie urządzeń mobilnych 2014 mówi wszystko.* [online]. [cytowany 2015-04-10]. Dostępny pod adresem: https://blogs.mcafee.com/consumer/mobile-security-report-2014/
4. ČÍŽEK, Jakub. *Inteligentne telewizory nas monitorują. Pogódź się z tym.* [online]. [cit.9.8.2015]. Dostępny pod adresem: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx
5. *CNN o seksie pedofilskim w Second Life.* [online]. [cyt. 18.6.2009]. Dostępny pod adresem: http://www.youtube.com/watch?v=AQM-SiiaipE
6. *Current World Population* [online]. [cyt. 2015-08-10]. Dostępny pod adresem: http://www.worldometers.info/world-population/
7. Wejdź na stronę: *Ciekawe statystyki dotyczące mobilnych strategii transformacji cyfrowej* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/
8. *Zatrzymywanie danych w obecnej formie jest niezgodne z konstytucją.* [online]. [cyt. 16.7.2016]. Dostępny pod adresem: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690
9. *Delokalizacja stosunków prawnych w Internecie* [online]. [cit.15.4.2012]. Dostępny pod adresem: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html
10. *Digital, Social & Mobile Worldwide in 2015* [online]. [cyt. 2015-08-09]. Dostępny pod adresem: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/
11. ENGLEHARDT, Steven i Ardvin NARAYANAN. *Śledzenie w Internecie: Pomiar i analiza 1 miliona miejsc.* [online]. [cyt. 2016 Aug 5]. Dostępny pod adresem: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf
12. *Facebook wkrótce będzie w stanie zidentyfikować użytkownika na każdym zdjęciu.* [online]. [cyt. 2015-08-09]. Dostępny pod adresem: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo
13. *FBI wykorzystuje lukę we Flashu do złamania zabezpieczeń sieci Tor.* [online]. [cyt. 2016-07-23]. Dostępny pod adresem: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/
14. *Pierwsza poprawka.* [online]. [cyt. 2016-07-10]. Dostępny pod adresem: https://www.law.cornell.edu/constitution/first_amendment.
15. *Niemiecki Bundestag uchwala nowe prawo o retencji danych.* [online]. [cyt. 16.7.2016]. Dostępny pod adresem: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/
16. GREENFIELD, David. *Bezpieczeństwo zintegrowane: czy nadszedł jego czas?* [online]. [cyt. 1 marca 2018]. Dostępny pod adresem: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/
17. HAINES, Lester. *Gracz internetowy dźgnięty nożem z powodu "skradzionego" cyberhasła.* [online]. [cyt. 3.10.2006]. Dostępny pod adresem: http://www.theregister.co.uk/2005/03/30/online_gaming_death/
18. http://news.bbc.co.uk/2/hi/technology/6638331.stm
19. http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html
20. HUSOVEC, Martin. *Odpowiedzialność w Internecie w świetle prawa czeskiego i słowackiego*. Praga: CZ.NIC, 2014. ISBN: 978-80-90-904248-8-3, s. 101-102.
21. *Cenzura Internetu* [online]. [cyt. 10.8.2016]. Dostępny pod adresem: http://www.deliveringdata.com/2010_10_01_archive.html
22. *Internetowa historia lat 80.* [online]. [cyt. 2016 Jun 7]. Dostępny pod adresem: http://www.computerhistory.org/internethistory/1980s/
23. *Internet, łączność i możliwy rozwój (Część 2 - Historia i rozwój Internetu).* [online]. [cyt. 2008-02-10]. Dostępny pod adresem: http://www.internetprovsechny.cz/clanek.php?cid=163
24. JOHNSON, David R. i David POST. *Powstanie prawa w cyberprzestrzeni.* [online]. [cyt. 10.7.2016]. Dostupné z: http://poseidon01.ssrn.com/delivery.php?ID=797101088103069021099122095084084095061040041017050027018013071117008115007025117112101013061121056036119084118089028085067043023001058093120 0

700840690850890120000191271200910781150901250171200300140001010950311090030940690691131141121102&EXT=pdf
25. KODET, Jaroslav. *Cyberprzestrzeganie prawa: Wykorzystaj w pełni narzędzia open source.* [online]. [cytowany 2018-04-25]. Dostępny pod adresem: https://**www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf**
26. KOLOUCH, Jan i Andrea KROPÁČOVÁ. Odpowiedzialność za własne urządzenie oraz przechowywane w nim dane i aplikacje. W: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14).* [B.m.], c2014, s. 321 - 324. recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.
27. KOLOUCH, Jan i Petr VOLEVECKÝ. *Ochrona prawnokarna przed cyberprzestępczością.* Praga: Akademia Policyjna Republiki Czeskiej w Pradze, 2013, s. 65.
28. KOLOUCH, Jan. *Cyberprzestępczość.* Praga: CZ.NIC, 2016, s. 78 i nast. oraz s. 109 i nast.
29. KOLOUCH, Jan. Pseudoanonimowość - zagrożenie dla bezpieczeństwa użytkowników Internetu. *DSM -data security management* [online]. 2015. vol. 19, issue 3, pp. 24-29 ISSN 1211-8737. Dostępny pod adresem: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/
30. *Wiodące sieci społecznościowe na świecie według stanu na kwiecień 2016 r., uszeregowane według liczby aktywnych użytkowników (w milionach)* [online]. [cit.10.8.2015]. Dostępny pod adresem: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
31. LESSIG, Lawrence. *Code v. 2. s.* 6 Dostępny w wersji pełnej (j. angielski) [online]. [cyt. 13.3.2008]. Dostępny pod adresem: http://pdf.codev2.cc/Lessig-Codev2.pdf
32. MAISNER, Martin i Barbora VLACHOVÁ. *Ustawa o cyberbezpieczeństwie. Komentarz.* Praga: Wolters Kluwer, 2015. s. 85
33. MATEJKA, Ján. *Internet jako przedmiot prawa: poszukiwanie równowagi między autonomią a prywatnością.* Praga: CZ.NIC, 2013. ISBN 978-80-904248-7-6 s. 25
34. *Krajowe wyzwania prawne wobec dyrektywy w sprawie zatrzymywania danych.* [online]. [cyt. 16.7.2016]. Dostępny pod adresem: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html
35. *Największe sieci społecznościowe na świecie? Facebook może i jest numerem jeden, ale...* [online]. [cyt. 10.8.2015]. Dostępny pod adresem: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/
36. *Cykl PDCA.* [online]. [cytowany 2018-07-06]. Dostępny pod adresem: https://www.creativesafetysupply.com/glossary/pdca-cycle/
37. PETERKA, Jiří. *UE nie wymaga już od nas przechowywania danych o ruchu i lokalizacji. Ale nadal to robimy.* [online]. [cyt. 2015-11-10]. Dostępny pod adresem: http://www.earchiv.cz/b14/b0428001.php3
38. POLČÁK, Radim. *Prawo w Internecie. Spam i odpowiedzialność dostawcy usług internetowych.* Brno: Computer Press, 2007, s. 7.
39. POŽÁR, Josef i Luděk NOVÁK. *Podręcznik pracy kierownika ds. bezpieczeństwa.* Praga: POŽÁR, Josef i Luděk NOVÁK. *System zarządzania bezpieczeństwem informacji.* [online]. [cyt. 6 lipca 2018]. Dostępny pod adresem: https://www.cybersecurity.cz/data/srib.pdf s. 1
40. REED, Chris. *Prawo internetowe*. Cambridge: Cambridge University Press, 2004, s. 218.
41. *Regionalne rejestry internetowe.* [online]. [cyt. 4.8.2015]. Dostępny pod adresem: https://*www.nro.net/about-the-nro/regional-internet-registries*
42. ROSER, Christoph. *Wiele smaków PDCA* [online]. [cytowany 2018-07-06]. Dostępny pod adresem: https://www.allaboutlean.com/pdca-variants/
43. ŠKORNIČKOVÁ, Eva. *Prosty test.* [online]. [cyt. 10. 11. 2017]. Dostępny pod adresem: *https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*
44. SMEJKAL, Vladimir. *Internet i §§* 2. aktualizacji. wyd. 2 i rozszerzone. Praga: Grada, 2001, s. 32.
45. SMITH, Craig. *Według liczb: 100 zadziwiających statystyk i faktów dotyczących wyszukiwarki Google* [online]. [cyt. 2016 Aug 4]. Dostępny pod adresem: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/
46. Trybunał Sprawiedliwości Unii Europejskiej. Komunikat prasowy nr 54/14, 8 kwietnia 2014 r. Wyrok w sprawach połączonych C-293/12 i C-594/12 [online]. [cyt. 15.7.2016]. Dostępny pod adresem: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf
47. SPITZER, Manfred. *Demencja cyfrowa.* Brno: Gospodarz, 2014 r. ISBN 978-80-7294-872-7
48. Opinia rzecznika generalnego Pedra Cruza Villalóna. Sprawy C-293/12 i C-594/12 [online]. [cyt. 15.7.2016]. Dostępny pod adresem: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954
49. Opinia rzecznika generalnego SAUGMANDSGAARDA ØE z dnia 19.7.2016 r. W sprawach połączonych C-203/15 i C-698/15 [online]. [cyt. 10.8.2016]. Dostępny pod adresem:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650
50. ŠTOČEK, Mediolan. *W duchu "Hitler przeciw Hitlerowi".* [online]. [cit.10.7.2016]. Dostępny pod adresem: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325
51. *Surface Web, Deep Web, Dark Web - na czym polega różnica.* [online]. [cyt. 2016-07-20]. Dostępny pod adresem: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference
52. *Ciemna sieć - wyjaśnienie.* [online]. [cyt. 2016-07-20]. Dostępny pod adresem: https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html
53. *Fragmentacja systemu Android bije kolejne rekordy: 24 000 różnych urządzeń* [online]. [cyt. 2016-07-15]. Dostępny pod adresem: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/
54. *Pierwsze mobilne szkodliwe oprogramowanie: jak Kaspersky Lab odkrył Cabir.* [online]. [cyt. 1.8.2016]. Dostępny pod adresem: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
55. THOMAS, Douglas. *Przestępczość na granicy elektronicznej.* W Cyberprzestępczość. Londyn: Routledge, 2003, s. 17 i nast.
56. *Informacja o bezpieczeństwie sieci Tor: Atak polegający na potwierdzaniu ruchu "relay early".* [online]. [cyt. 2016-07-23]. Dostępny pod adresem: https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack
57. TRADOC. Operacje w cyberprzestrzeni: Plan Zdolności Koncepcyjnych na lata 2016-2028 [online]. [cited 2018 Feb 18], pp. 8-9 Available from: www.fas.org/irp/doddir/army/pam525-7-8.pdf?
58. VOŽENÍLEK, David. *Nie pomoże smarowanie "sucharów", internet cię wyda i bateria.* [online]. [cyt. 4.8.2016]. Dostępny pod adresem: http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz
59. *Światowi użytkownicy Internetu i dane o ludności z 2015 r.* [online]. [cyt. 2015-08-09]. Dostępny pod adresem: http://www.internetworldstats.com/stats.htm
60. *Bardzo ważne jest dla nas zwiększanie bezpieczeństwa, ochrona prywatności i tworzenie prostych narzędzi, które dają użytkownikowi kontrolę i możliwość wyboru.* [online]. [cyt. 2014-04-04]. Dostępny pod adresem: https://www.google.cz/intl/cs/policies/?fg=1