Cyberbezpieczeństwo a ochrona danych osobowych

Maria Piątek

06.05.2021

Artykuł w skrócie:

– W dobie pandemii koronawirusa wzrosła ilość ataków cybernetycznych, których przedmiotem bywają dane osobowe.
– Problemem cyberbezpieczeństwa niejednokrotnie jest człowiek, który „wpuszcza" szkodliwy program infekujący komputer lub sprzęt mobilny, co często wynika z braku odpowiedniego przeszkolenia z zakresu zagrożeń cybernetycznych.
– W Stanach Zjednoczonych od kilku lat widoczny jest proces stopniowej regulacji ochrony danych osobowych na poziomie prawa stanowego, co może przyczynić się do uchwalenia aktu na poziomie federalnym.

Wstęp

W dobie pandemii koronawirusa wzrosła liczba ataków cybernetycznych. Powodem jest wzrost aktywności cyfrowych i digitalizacja procesów, które wcześniej wymagały fizycznej obecności człowieka w konkretnym miejscu – np. w urzędzie. W pierwszym kwartale 2020 roku eksperci z Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) zarejestrowali 6893 zgłoszeń, a liczba przeanalizowanych incydentów wynosiła 2507[1]. W drugim kwartale zarejestrowano 9689 zgłoszeń, natomiast liczba przeanalizowanych incydentów była równa 2723[2]. Dla porównania w całym 2019 roku zarejestrowano 6484 incydenty, co wówczas stanowiło rekordową liczbę[3]. W czasie wzmożonej przestępczości cybernetycznej przedmiotem ataków bywają dane osobowe. Z tego powodu coraz częściej słychać głosy o konieczności zapewnienia im prawnej ochrony.

Cyberbezpieczeństwo i dane osobowe

Cyberprzestrzeń jest jednym z najważniejszych obszarów bezpieczeństwa w XXI wieku.

[1] *NASK*, „Dane CERT Polska za pierwszy kwartał 2020 roku pokazują, że w okresie pandemii liczba zagrożeń wzrasta".
<https://www.nask.pl/pl/aktualnosci/3835,Dane-CERT-Polska-za-pierwszy-kwartal-2020-roku-pokazuja-ze-w-okresie-pandemii-li.html>
[2] *NASK*, „Co pokazują dane CERT Polska za drugi kwartał"
<https://www.nask.pl/pl/aktualnosci/3888,Co-pokazuja-dane-CERT-Polska-za-drugi-kwartal-2020-roku.html>
[3] *NASK*. 2019"Krajobraz Bezpieczeństwa Polskiego Internetu Raport Roczny 2019 Z Działalności CERT Polska". 2019.
<https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.>

Warto zwrócić uwagę na swoiste cechy, które ją wyróżniają:

– ponadnarodowy charakter;

– brak ograniczeń czasowych;

– większa anonimowość sprawców przestępstw;

– niski koszt użytkowania, pozwalający na nieograniczony dostęp do sieci[4].

Powyższe właściwości wpływają na zwiększenie przestępczości. W związku z tym cyberataki stały się zjawiskiem nieuchronnym i coraz częstszym. Ofiarami padają firmy, urzędy państwowe oraz osoby fizyczne.

W cyberprzestrzeni są gromadzone i przetwarzane dane na ogromną skalę. Każda aktywność w sieci jest rejestrowana przez systemy, co implikuje fakt, że korzystając codziennie z internetu, pozostawiamy po sobie ślad w postaci naszych danych osobowych. Wzmożony rozwój digitaliazji sprawia, że serwisy rządowe i korporacyjne, czy mnożące się portale społecznościowe są w posiadaniu danych dotyczących zarówno kariery zawodowej jak i życia prywatnego obywateli.

Jednym z praw człowieka gwarantowanych i chronionych na poziomie zarówno Konstytucji jak i traktatów oraz Karty Praw Podstawowych Unii Europejskiej jest prawo do prywatności. Jest ono dobrem osobistym, które obejmuje to wszystko, „co ze względu na uzasadnione odosobnienie się jednostki od społeczeństwa służy jej do rozwoju fizycznej i psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej”[5]. Choć przyjęta w polskim piśmiennictwie definicja zdaje się być mało konkretna i na jej podstawie trudno precyzyjnie określić, czym dokładnie jest prawo do prywatności, można bez wątpienia stwierdzić, iż w jej zakresie mieści się prawo do ochrony danych osobowych, które Rozporządzenie o ochronie danych osobowych (RODO) definiuje jako „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”[6]. Do takich informacji

[4] Stępień, Agnieszka. 2018. „Bezpieczeństwo zintegrowane współczesnej Polski” s. 57 <http://piz.san.edu.pl/docs/e-XIX-2-3.pdf>

[5] Kopff, Andrzej.1982. „Ochrona sfery życia prywatnego w świetle doktryny i orzecznictwa”, Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace Prawnicze, nr 100 (1982): 37.

[6] Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 Z Dnia 27 Kwietnia 2016 R. W Sprawie Ochrony Osób Fizycznych W Związku Z Przetwarzaniem Danych Osobowych I W Sprawie Swobodnego Przepływu Takich Danych Oraz Uchylenia Dyrektywy 95/46/WE (Ogólne Rozporządzenie O Ochronie Danych). 2016.

można zaliczyć m.in. imię, nazwisko, miejsce zamieszkania czy internetowy identyfikator użytkownika.

Rozwój systemów nowych technologii niesie za sobą ogromne korzyści, ale również i zagrożenia. Dzisiejsze rozwiązania umożliwiają systemom analizowanie oraz wyciąganie wniosków z dostarczonych im danych. Z pewnością szybki proces przetwarzania pozwala uzyskać odpowiedź na zadane pytania. Ułatwia to określenie i przewidywanie pewnych zachowań społecznych. Jednakże fakt przetwarzania ich w skomplikowany sposób budzi pytanie o należytą ochronę prywatności, demokracji i wolności słowa.

Wzmożenie przetwarzania danych osobowych w internecie – nasilone w szczególności w ostatnim roku w wyniku pandemii – implikuje mocniejszy nacisk na ochronę cyberprzestrzeni. Niebezpieczeństwo istnieje na różnych poziomach. Od najmniejszych jednostek, którymi są osoby fizyczne, poprzez niewielkie przedsiębiorstwa, urzędy, po ogromne firmy i całe państwa. Do typowych form cyberataków należy zaliczyć m.in. wirusy, phishing, vishing, spyware, malware czy trojany. W 2019 roku phishing stanowił ok. 54 % wszystkich zarejestrowanych przez CERT Polska ataków[7].

Sposób dokonywania ataków na przestrzeni ostatnich kilku lat zmienił się. **Cyberprzestępcy nie tylko żądają okupu za odszyfrowanie danych, ale w coraz większym stopniu również za ich nieujawnienie. Ich działanie jest spowodowane – w pewnym sensie – przepisami wynikającymi z RODO.** Mianowicie rozporządzenie reguluje kwestie zasad dotyczących przetwarzania danych osobowych i sankcjonuje ich naruszenie, nakładając karę w wysokości do 20 000 000 EUR lub 4% wartości rocznego światowego obrotu przedsiębiorstwa. W myśl legislatora tak wysoka kara ma zmotywować przedsiębiorców do inwestowania w odpowiednią infrastrukturę, zapewniającą właściwą ochronę danych. Jednakże w rzeczywistości może sprawić, że przedsiębiorcy w obawie przed karą administracyjną za niezachowanie bezpieczeństwa danych zapłacą okup przestępcom.

Problemem związanym z obroną przed cyberatakami jest czynnik ludzki. Zazwyczaj to właśnie pracownik, będący swoistą pierwszą linią obrony, popełnia błąd i „wpuszcza" złośliwe oprogramowanie. Między innymi z tego właśnie powodu phishing – polegający na wysyłaniu np. stargetowanych e-maili, które mają zachęcić odbiorcę do kliknięcia w link

[7] *NASK*. 2019"Krajobraz Bezpieczeństwa Polskiego Internetu Raport Roczny 2019 Z Działalności CERT Polska". 2019. <https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.>

przekierowujący do fałszywej strony – plasuje się tak wysoko pod względem popularności wśród cyberprzestępców. **Podmioty przechowujące oraz przetwarzające dane osobowe powinny w szczególności kłaść nacisk na szkolenia pracowników.**

Efekty braku należytej procedury bezpieczeństwa oraz odpowiedniej edukacji pracowników widać na przykładzie ataku z początku lutego, którego ofiarą stał się Urząd Marszałkowski w Krakowie. Atakujący użyli oprogramowania szyfrującego pliki, co doprowadziło do utraty dostępu do danych osobowych oraz zażądali okupu za ich odblokowanie.

Innym głośnym przypadkiem wycieku ogromnej ilości danych osobowych był podwójny wyciek z Politechniki Warszawskiej w 2020 roku. Wyciek był bardzo poważny, gdyż zawierał dane dotyczące nazwisk, numerów dowodów osobistych i PESEL oraz numerów rekrutacyjnych. Dodatkowo, co również warto zaznaczyć, do ataków doszło w ciągu dwóch miesięcy. Podczas pierwszego z nich ucierpiało ok. 5 tys. studentów i pracowników.

Ostanim przykładem poważnego naruszenia ochrony danych osobowych, który warto przywołać, to wyciek danych ponad 50 tys. sędziów, prokuratorów, aplikantów, asesorów oraz urzędników, które miała w swoich zasobach Krajowa Szkoła Sądownictwa i Prokuratury w Krakowie (KSSiP)[8]. Informacje, które ujawnili przestępcy dotyczyły m.in. numerów telefonów, adresów zamieszkania, numerów ICQ. W następstwie zdarzenia, pracownicy wymiaru sprawiedliwości zaczęli być zastraszani. Na ten problem warto spojrzeć szerzej – mianowicie KSSiP jest instytucją nadzorowaną przez Ministra Sprawiedliwości, która posiada dane wszystkich sędziów oraz prokuratorów, będących funkcjonariuszami publicznymi. Sytuacja, w której dane osób sprawujących władzę sądowniczą w państwie oraz jedynej instytucji zajmującej się ich szkoleniem znajdują się w niepowołanych rękach, mogłaby doprowadzić do dalekosiężnych negatywnych konsekwencji w funkcjonowaniu całego państwa.

Aspekt międzynarodowy

Jak zostało już wspomniane, jednym z praw podstawowych gwarantowanych i chronionych na mocy traktatów UE jest właśnie prawo do prywatności oraz ochrony danych osobowych. Unia

[8] tvn24, 2020. „Już ponad 400 prokuratorów i sędziów otrzymało groźby po wielkim wycieku danych osobowych” <https://tvn24.pl/polska/wyciek-danych-z-krajowej-szkoly-sadownictwa-i-prokuratury-ponad-400-prokuratorow-i-sedziow-otrzymalo-grozby-4937550>

od kilka lat podejmuje działania zmierzające do zostania liderem w zakresie bezpiecznej transformacji cyfrowej, w ramach której zapewniona będzie ochrona danych osobowych. Warto zauważyć, że żaden inny podmiot międzynarodowy nie uregulował i nie nadał tak wysokiej ochrony prawu do prywatności. Budowanie gospodarki cyfrowej ma opierać się na:

– unijnych wartościach i zasadach podstawowych;

– ochronie praw podstawowych, w tym prawa do prywatności oraz danych osobowych;
– prawie do bezpiecznego internetu, zapewniającego nieograniczony przepływ informacji;
– demokratycznym i wydajnym zarządzaniu polityką bezpieczeństwa cybernetycznego, które angażuje różne grupy społeczne;
– wspólnej odpowiedzialności za zapewnienie bezpieczeństwa[9]

Unia Europejska zauważa problem jaki stanowi cyberprzestępczość, dlatego utworzono wyspecjalizowane Europejskie Centrum ds. Walki z Cyberprzestępczością, które działa w ramach Europolu. W ramach cyberprzestępczości wyróżnia się niedozwolone zachowania polegające na:

– przejęciu kontroli nad urządzeniami osobistymi za pomocą złośliwego oprogramowania;

– kradzieży lub narażeniu na naruszenie danych osobowych i własności intelektualnej w celu dokonania oszustwa internetowego;

– rozpowszechnianiu nielegalnych treści poprzez użycie internetu (podkreślając znaczenie mediów społecznościowych);

– korzystanie z darknetu do sprzedaży nielegalnych towarów lub usług hakerskich[10].

W 2007 roku Estonia padła ofiarą dużego ataku cybernetycznego typu DDoS, czyli rozproszonej odmowy dostępu, polegającej na blokadzie serwera lub całej infrastruktury. **W efekcie zdarzenia społeczeństwo utraciło dostęp do bankowości i poczty e-mail oraz zostały zablokowane strony rządu i Zgromadzenia Państwowego.** Estońskie Ministerstwo Obrony określiło, że celem ataku było podważenie funkcjonowania publicznych i prywatnych

[9] Wspólny Komunikat Do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego I Komitetu Regionów - Strategia Bezpieczeństwa Cybernetycznego Unii Europejskiej: Otwarta, Bezpieczna I Chroniona Cyberprzestrzeń (JOIN(2013) 1 Final Z 7.2.2013). 2013.
[10] Rada Europejska, Rada Unii Europejskiej. „Cyberbezpieczeństwo: Jak UE Radzi Sobie Z Cyberzagrożeniami” <https://www.consilium.europa.eu/pl/policies/cybersecurity/.>

systemów informacyjnych. Ówczesne wydarzenia są na tyle istotne, iż stanowiły pierwszy w historii zmasowany cyberatak przeciwko państwu. Estonia już wtedy była krajem bardzo rozwiniętym cyfrowo, co dobitniej pokazuje jak konieczne są odpowiednie zabezpieczenia infrastruktury cyberprzestrzeni.

RODO reguluje kwestie przekazywania danych osobowych z państw Europejskiego Obszaru Gospodarczego (EOG) państwom trzecim oraz organizacjom międzynarodowym. Warunkiem przekazania jest fakt uznania przez Komisję Europejską danego podmiotu za zapewniający im odpowiednią ochronę, takie przekazanie nie wymaga specjalnego pozwolenia. Na chwilę obecną KE uznała 12 państw za dające odpowiedni stopień ochrony[11].

Z racji niespełniania europejskich wymogów dotyczących ochrony danych osobowych przez Stany Zjednoczone, ale jednocześnie mając na uwadze silne powiązania między UE a USA, w 2016 roku została wydana decyzja Komisji ustanawiająca Program Tarczy Prywatności UE–USA *Privacy Shield*. Umożliwiała ona przekazywanie danych osobowych przedsiębiorcom z USA, którzy przystąpili do tego programu, pod warunkiem że przetwarzali je zgodnie z przepisami. Jeżeli jakiś podmiot uchybiał zasadom i wymogom, wówczas Komisja Europejska miała kompetencję do wykreślenia takiego przedsiębiorstwa z listy.

Funkcjonowanie Tarczy Prywatności trwało zaledwie cztery lata, gdyż w ubiegłym roku Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wydał orzeczenie, w którym stwierdził nieważność umowy. Decyzja TSUE wynikała m.in. z odmienności rozumienia wartości ochrony danych osobowych. Dla UE jest to jedno z podstawowych praw, które może być ograniczone tylko na zasadzie proporcjonalności, czyli wtedy kiedy zakres i forma działania Unii nie wykraczają poza to, co jest konieczne do osiągnięcia celów Traktatów[12]. **Natomiast sposób uregulowania tego problemu w prawie amerykańskim nie jest równoważny z unijnym. Amerykańskie normy prawne nie zapewniają wystarczającej ochrony przed ingerencją władz publicznych w dostęp przekazanych danych osobowych**[13].

[11] Komisja Europejska. „Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection.” <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents>

[12] Traktat o Unii Europejskiej

[13] Shoper.pl "Koniec Tarczy Prywatności UE-USA, co to oznacza dla twojego sklepu?” <https://www.shoper.pl/blog/koniec-tarczy-prywatnosci-ue-usa-co-to-oznacza-dla-twojego-sklepu/>

Mimo różnic w podejściu co do ochrony danych osobowych między USA a Europą, należy zauważyć wielość różnych inicjatyw legislacyjnych za oceanem. Poszczególne stany, od kilku lat pracują nad aktami regulującymi daną problematykę. Co prawda, wiele działań ugrzęzło na poziomie burzliwych dyskusji w organach ustawodawczych, ale są i takie, w efekcie których udało się wypracować ustawę. W szczególności warto zwrócić uwagę w tym aspekcie na dwie regulacje ze stanów Kalifornia oraz Wirginia.

W dniu 2 marca 2021 roku Virginia Consumer Data Protection Act (VCDPA) została podpisana przez gubernatora stanu Ralpha Northama. Dokument ten jest na tyle istotny na tle innych aktów regulujących, gdyż jest drugim – po dokumencie podpisanym w Kalifornii – tak szeroko i kompleksowo normującym kwestię ochrony danych osobowych[14]. Gwarantuje ona konsumentom (zdefiniowanym jako osoby fizyczne zamieszkujące Wirginię, działające indywidualnie, których działania nie są związane z działalnością gospodarczą lub zawodową) możliwość dostępu, poprawiania oraz usuwania danych osobowych. Zobowiązuje firmy do zwrócenia się o bezpośrednią zgodę konsumenta w zakresie gromadzenia i wykorzystywania jego danych wrażliwych, do których akt zalicza m.in. rasę, orientację seksualną, zdrowie i status imigranta. Ponadto tylko prokurator generalny Wirginii będzie miał prawo do pozywania firm, które nie przestrzegają przepisów ustawy[15].

Z początkiem 2023 roku ma wejść w życie California Privacy Rights Act (CPRA), będąca „poprawioną" wersją California Consumer Privacy Act (CCPA), która natomiast weszła w życie 1 stycznia 2020 roku. Celem dokumentu jest rozszerzenie ochrony prywatności osób mieszkających w Kalifornii. CPRA wprowadza przepisy podobne do norm RODO, w tym np. kategorię danych wrażliwych oraz rozszerza zakres aktywności objętych obowiązkiem uzyskania zgody konsumenta. Należy podkreślić, że powyższe akty dotyczące ochrony danych osobowych są przejawem prawa stanowego. **Coraz więcej stanów podejmuje aktywności legislacyjne, co może skutkować powstaniem między nimi dużych rozbieżności prawnych. Amerykańskie firmy oraz organizacje branżowe coraz częściej zwracają uwagę na konieczność stworzenia federalnych regulacji.** Prawdopodobnie do tego ruchu władz federalnych może niedługo dojść.

[14] Kornbacher, Devika. Falcon, Briana. 2021 „Virginia Is For Lovers . . . Of Data Privacy - UPDATED March 2021"
<https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3509049/>
[15] Senate Bill No.1392 2 Amendment in the nature of substitute
<https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1+pdf>

	VCDPA	CCPA, as amended by the CPRA	GDPR
Right to opt-out of sale	✓	✓	✗
Opt-in or opt-out for processing of sensitive information	Opt-in	Opt-out	Opt-in
Statutory cure period for violations	✓	✓	✗
Right to appeal denials of requests	✓	✗	✗
Express obligations regarding de-identified data	✓	✗	✗
Requirement to perform data protection impact assessments	✓	✓	✓
Private right of action	✗	✓	✓
Governmental enforcement entities	Attorney General	CPPA, Attorney General	DPAs
Penalties	Up to $7,500 per violation	Up to $2,500 per violation and up to $7,500 per intentional violation or violation involving minors	Up to €10 million, or 2% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of less severe violations. Up to €20 million, or 4% of worldwide annual revenue from the preceding financial year, whichever amount is higher, in the case of more serious violations.
Operative date	January 1, 2023	January 1, 2023	May 25, 2018

źródło: Kornbacher, Devika. Falcon, Briana. 2021 „Virginia Is For Lovers Of Data Privacy - UPDATED March 2021" <https://www.jdsupra.com/legalnews/virginia-is-for-lovers-of-data-privacy-3509049/>

Wspomniane powyżej rozbieżności legislacyjne między poszczególnymi stanami mogą doprowadzić do chaosu prawnego. Jak zauważa Alan Chapell, prezes firmy *Chapell and Associates* „Jedyną rzeczą, która może wywierać presję polityczną [na federalne ustawodawstwo dotyczące prywatności], jest więcej pojedynczych stanów wymyślających szalone drakońskie przepisy"[16].

Amerykańscy politycy w dużej mierze są ze sobą zgodni w kontekście ustanowienia prawa federalnego. Jednakże, są między nimi istotne różnice. Demokraci chcieliby dać osobom fizycznym uprawnienie do pozywania firm, które naruszają ich prawo, podczas gdy republikanie chcą przyznać tę kompetencję prokuratorowi generalnemu.

Kolejnym powodem zwiększającym szansę na stworzenie jednolitych przepisów jest problem Chin. **Ochronę prywatności obywateli Stanów Zjednoczonych należy rozpatrywać jako element bezpieczeństwa narodowego.** Rozrost chińskich firm na rynku amerykańskim, przy jednoczesnym rozwoju technologicznym i wdrażaniu nowych rozwiązań w funkcjonowanie

[16] Kaye, Kate. 2021. „Cheat sheet: What to expect in state and federal privacy regulation in 2021" <https://digiday.com/media/cheatsheet-what-to-expect-in-state-and-federal-privacy-regulation-in-2021/>

gospodarki, implikuje fakt ułatwionego dostępu do ogromnych zasobów danych przez stronę chińską. Brak odpowiednich standardów zabezpieczeń umożliwia wykorzystanie ich w sposób sprzeczny z zasadami gospodarki, bezpieczeństwem narodowym, oraz wartościami demokratycznymi takimi jak np. prawa człowieka.

Wspomniany rozwój nowych technologii, w tym głównie rozwój sztucznej inteligencji, wpływa na prawdopodobieństwo dokonania ataku cybernetycznego. Należy pamiętać, że technologie znajdują zastosowanie zarówno w kwestiach cywilnych jak i militarnych. Algorytmy podejmujące czynności działają na podstawie pobranych z otoczenia danych – w tym również danych osobowych. W sytuacji, gdy digitalizacja następuje tak szybko, a czego skutkiem jest wzrost cyberataków, państwa powinny podejmować kroki w celu – w miarę możliwości – jak najlepszego zabezpieczenia danych. Przykładem cyberprzestępstwa, kiedy ofiarą stała się amerykańska firma, była kradzież danych z Equifax (firma ratingowa). Od maja do końca lipca 2017, czyli momentu wykrycia, chińscy hakerzy wykradli dane osobowe ponad 147 milionów obywateli USA. Wskutek tego zdarzenia, Stany oskarżyły czterech chińskich oficerów wojskowych, jednakże Chiny zaprzeczają zarzutom. W akcie oskarżenia prokurator generalny określił włamanie „jednym z największych naruszeń danych w historii”[17].

Podsumowanie

Bez wątpienia jednym z ważniejszych wyzwań, z którym dzisiejsze społeczeństwa i podmioty międzynarodowe muszą się zmierzyć to cyberbezpieczeństwo. Każdego dnia ludzkość produkuje mniej więcej ok. 1,145 tryliona megabajtów danych[18]. Wśród różnorodnych danych, które przetwarza sieć, znajdują się również te najbardziej związane z osobą fizyczną – dane osobowe. Wiele podmiotów podjęło działania w celu uregulowania i zabezpieczenia ich przed niepożądaną, a wręcz bezprawną aktywnością. Wśród nich jest m.in. Unia Europejska ze swoim rozporządzeniem o ochronie danych osobowych oraz niektóre stany USA. W Stanach Zjednoczonych widoczne są zakusy, by ujednolić prawo na poziomie federalnym, jednakże z pewnością na efekt tych starań będzie trzeba jeszcze poczekać.

[17] Corera, Gordon. 2020. „Equifax: US charges four Chinese military officers over huge hack” <https://www.bbc.com/news/world-us-canada-51449778>
[18] Bulao, Jacquelyn. 2021. „How Much Data Is Created Every Day in 2020?” <https://techjury.net/blog/how-much-data-is-created-every-day/#gref>

W czasach pandemii Covid-19 ogromny procent ludzi zmieniło tryb pracy z tradycyjnej na zdalną. W efekcie braku odpowiedniego przygotowania zdarzają się przypadki, kiedy pracownik dokonuje czynności służbowych na prywatnym komputerze. Taka sytuacja zwiększa prawdopodobieństwo wykradzenia danych. Brak świadomości pracowników wynika z małej ilości lub niskiej jakości prowadzonych szkoleń. Cyberataków będzie coraz więcej, tym bardziej potrzebna jest wzmożona aktywność w zakresie uświadamiania społeczeństwa jak się zachowywać i jak się uchronić przed niebezpiecznym działaniem.

O AUTORCE

Maria Piątek. Absolwentka studiów licencjackich na kierunku europeistyka w Centrum Europejskim UW oraz studentka III roku prawa na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Zainteresowania badawcze to procesy integracyjne i dezintegracyjne w Europie, dyplomacja, rozwój technologiczny oraz geopolityka.

JEŻELI DOCENIASZ NASZĄ PRACĘ, DOŁĄCZ DO GRONA NASZYCH DARCZYŃCÓW!

Z otrzymanych funduszy sfinansujemy powstanie kolejnych publikacji.

Możliwość wsparcia to bezpośrednia wpłata na konto Instytutu Nowej Europy: 95 2530 0008 2090 1053 7214 0001 tytułem: „darowizna na cele statutowe”.