Internet. Cyberpandemia. Cyberpandemic

Wstęp

Wstęp

Terminem „cyberpandemia" określamy podobieństwa między cyberatakami a pandemią, nie tylko COVID-19, destrukcyjne dla ludzi i gospodarki skutki ich globalnego, błyskawicznego rozpowszechniania. Masowe i nagłe przechodzenie z zawirusowanej przestrzeni realnej do cyberprzestrzeni upowszechniło świadomość szans związanych z transformacja cyfrową – zwłaszcza w ochronie zdrowia. Ujawniło też niedostateczne przygotowanie do bezpiecznego korzystania z cyberprzestrzeni, zaktywizowało cyberprzestępców i uczyniło zadaniem priorytetowym dla władz publicznych, przedsiębiorców i obywateli zwiększanie cyberbezpieczeństwa – potwierdzając aktualność teoretycznych konstatacji o waloryzacji deficytów, odczuwanych braków.

Przedmiotem analiz ekspertów, teoretyków i praktyków skupionych wokół Naukowego Centrum Prawno-Informatycznego, są w tym tomie kolejno: problemy cyberbezpieczeństwa w wymiarze międzynarodowym [część 1], militarnym i cywilnym [część 2], w sektorze publicznym [część 3] i prywatnym [część 4] oraz odrębnie cyberbezpieczeństwo w medycynie [część 5], a ponadto edukacja dla cyberbezpieczeństwa [część 6] oraz innowacyjność w czasie pandemii [część 7].

Powszechne zagrożenia życia i zdrowia oraz ograniczanie prywatności w przezwyciężaniu tych zagrożeń, kierują uwagę na kolizje dóbr i nowe aspekty wyważania zakresu ich ochrony, m.in. w ramach „cyfrowej solidarności" [*W. Wiewiórowski, Ł. Szoszkiewicz, A. Monarcha-Matlak*]. Odróżnianie interesu publicznego od prywatnych interesów osób fizycznych i prawnych jest przy tym znacznie bardziej skomplikowane niż przed dwudziestu laty, gdy ograniczenia praw i wolności człowieka uzasadniano zwiększaniem skuteczności walki z terroryzmem.

W ostatnich latach powstała rozbudowana, wielopoziomowa regulacja prawna niezbędna dla przeciwdziałania – transgranicznym w dużej części – cyberatakom. Do współdziałania w Europie przyczyniają się dyrektywa NIS,

której nową wersję proponuje obecnie Komisja Europejska oraz rozporządzenie ENISA, gdzie cyberbezpieczeństwo definiuje się jako działania (*activities*) niezbędne do ochrony sieci i „*information systems*", użytkowników takich systemów oraz innych osób przed cyberzagrożeniami: wszelkimi potencjalnymi okolicznościami, zdarzeniami lub działaniami, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informacyjnych, użytkowników takich systemów oraz innych osób. Istotne jest także finansowe wspieranie działań w tym zakresie z unijnych funduszy, o czym pisze *J. Romanowska*.

Specyfika aktywności w cyberprzestrzeni wiąże się z jej globalnym zasięgiem oraz łatwością wywołania dużych strat przy zastosowaniu niewielkich środków i zachowaniu anonimowości. Wielkoskalowym zagrożeniem są cyberoperacje podmiotów instytucjonalnych lub sponsorowanych przez nieprzyjazne struktury państwowe lub militarne, toteż potrzebna jest reorientacja z działań reaktywnych na rozpoznanie adwersarzy przez proaktywne „polowanie na zagrożenia" [*K. Molenda*]. Przykład cyberataku, którego ofiarą stała się w 2020 r. Europejska Agencja Leków pokazuje, jak istotna dla prawnomiędzynarodowej odpowiedzialności jest dynamiczna wykładnia zasad przypisania działań w cyberprzestrzeni określonemu państwu [*P. Roguski*].

Lawinowy wzrost cyberprzestępczości wiąże się z nowymi formami i metodami cyberataków, a także ze wzmożeniem transakcji w darknecie. Podczas pandemii, dla ochrony użytkowników Internetu przed atakami phishingowymi, zdecydowano się na utworzenie tzw. listy ostrzeżeń. Jest ona oparta na formie prawnej porozumienia i ma tymczasowy charakter. Równolegle procedowane są zmiany prawa powszechnie obowiązującego, których wagę potwierdzają modele prognostyczne [*J. Kosiński, A. Gryszczyńska, K.J. Jakubski*].

Przezwyciężanie aktualnych zagrożeń, zarówno związanych z cyberoperacjami, jak i aktywnością cyberprzestępców wymaga modyfikacji strategii i nowych regulacji, w których formułowaniu warto stosować metodę prawnoporównawczą [*D.K. Kipker, D. E. Scholz, M. Badowski, G. Magri, K. Rzęsiewicz*].

Badania różnych problemów skuteczności prawa wskazują też na potrzebę odrębnego ich rozpatrywania w odniesieniu do sektora publicznego [*M. Ganczar, E. Marzec, T. Przybylski, A. Fijałkowska*] i prywatnego [*A. Mednis, D. Fuchs, D. Benduch, P. Hajduk*], choć można też zauważyć uniwersalne uwarunkowania techniczne i technologiczne [*B. Szafrański, M. Sakowska-Baryła*, *J. Kostrzewa*]. Z drugiej strony, ochrona zdrowia, a w szczególności informatyka medyczna, jest obszarem specyficznych rozwiązań, w których aspekty publicznoprawne i prywatnoprawne są niekiedy trudne do rozdzielenia [*M. Michalski, M. Świerczyński, Z. Więckowski, S. Sikorski, M. Florczak, K. Czaplicki, K. Świtała, K. Wojsyk*].

Wymuszona pandemią izolacja zweryfikowała istniejący potencjał zdalnej edukacji. Nowe władcze instrumenty administracyjnoprawne uczyniły pomocnicze wcześniej narzędzia informatyczne głównymi lub jedynymi, zmieniając też uwarunkowania efektywności kształcenia. Ujawniły się przy tym luki wiedzy i umiejętności prawno-informatycznych, m.in. w zakresie ochrony autorskoprawnej, cyberhigieny i ochrony danych osobowych. Dążenie do przezwyciężania ich dotkliwych konsekwencji znajduje wyraz w procesach legislacyjnych i w stosowaniu prawa, a także w próbach wypracowania dobrych praktyk zdalnego nauczania, nie tylko w warunkach pandemii [*K. Grzybczyk, N. Kohtamäki, A. Syryt, B. Zbarachewicz, K. Radomiński, W. Święcicki*, *P. Drobek*].

Pandemia mobilizowała do innowacyjności. Efekty dostępności danych cyfrowych, wykorzystania sztucznej inteligencji czy biotechnologii [*J. Cytowski, B. Fischer, E. Fabian*] budziły szerokie zainteresowanie, zwiększając znaczenie informacyjne mediów, choć stawały się niestety także pożywką dla dezinformacji.

Problemy rozwoju społeczeństwa informacyjnego, skoncentrowanego na zmniejszaniu niepewności, w tym potrzeby ochrony wolności, własności i bezpieczeństwa w Internecie, badane są w ramach Naukowego Centrum Prawno-Informatycznego już od dziesięciu lat. Wśród członków tej naukowej sieci są pracownicy naukowi: Akademii Marynarki Wojennej, Katolickiego Uniwersytetu Lubelskiego, Politechniki Warszawskiej, Uniwersytetu Ekonomicznego w Katowicach, Uniwersytetu Gdańskiego, Uniwersytetu Jagiellońskiego, Uniwersytetu Kardynała Stefana Wyszyńskiego, Uniwersytetu Mikołaja Kopernika, Uniwersytetu Pedagogicznego w Krakowie, Uniwersytetu Szczecińskiego, Uniwersytetu Śląskiego, Uniwersytetu Warszawskiego oraz Wojskowej Akademii Technicznej – w tym już dwudziestu profesorów. Są też eksperci-praktycy z sektora publicznego i prywatnego. Członkiem wspierającym NCPI jest Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, w którego misję wpisują się projekty badawcze i rozwojowe stowarzyszenia, współfinansowane m.in. przez Narodowe Centrum Badań i Rozwoju.

Debaty organizowane przez NCPI we współpracy z innymi podmiotami publicznymi, które zgromadziły w ciągu ostatniej dekady około 10 tys. uczestników, pozwalają – przez wykorzystanie metod heurystycznych – weryfikować wyniki indywidualnych ustaleń w interdyscyplinarnym kontekście, uwzględnianym w przygotowaniach do publikacji.

Kolejne tomy monografii serii „Internet", projektowane według konceptu „strategii natychmiastowej" i tak też – dzięki wydawcy Natalii Adamczyk z Wydawnictwa C.H.Beck – realizowane, dają czytelnikom możność refleksji nad szansami i pułapkami pojawiających się na horyzoncie globalnych „top trendów" technologicznych.

W roku 2021 skupiamy uwagę na globalnych „grach i graczach", nie wykluczając zainteresowania wobec *local games*. Zapraszamy do udziału w badaniach i debatach dotyczących: grywalizacji [nie tylko w video grach i e-sporcie], własności intelektualnej, nieuczciwej konkurencji i władztwa podatkowego w Internecie[1].

[1] Zob. *G. Szpor* (red.), Internet. Ochrona wolności, własności i bezpieczeństwa, Warszawa 2011; *G. Szpor*, *W.R. Wiewiórowski* (red.), Internet. Prawno-informatyczne problemy sieci, portali i e-usług, Warszawa 2012; *G. Szpor* (red.), Internet. Cloud computing. Przetwarzanie w chmurach, Warszawa 2013; *G. Szpor* (red.), Internet. Publiczne bazy danych i big data, Warszawa 2014; *G. Szpor* (red.), Internet rzeczy. Bezpieczeństwo w Smart city, Warszawa 2015; *G. Szpor*, *A. Gryszczyńska* (red.), Internet. Strategie bezpieczeństwa, Warszawa 2017; *G. Szpor, K. Czaplicki* (red.), Internet. Informacja przestrzenna, Warszawa 2018; *G. Szpor, K. Czaplicki* (red.), Internet. Przetwarzanie danych osobowych, Warszawa 2019; *G. Szpor, K. Czaplicki* (red.), Internet. Analityka danych, Warszawa 2019.