USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Komentarz

redakcja naukowa
Grażyna Szpor
Agnieszka Gryszczyńska, Kamil Czaplicki

KOMENTARZE

Wolters Kluwer

USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Komentarz

redakcja naukowa
Grażyna Szpor
Agnieszka Gryszczyńska, Kamil Czaplicki

KOMENTARZE

Wolters Kluwer

WARSZAWA 2019

Stan prawny na 1 lutego 2019 r.

Wydawca
Izabella Małecka

Redaktor prowadzący
Paulina Staniszewska-Chudzik

Opracowanie redakcyjne
Joanna Ośka

Łamanie
Fotoedytor

Komentarze do poszczególnych artykułów napisali:

Kamil Czaplicki: wprowadzenie do ustawy pkt 1, art. 21–25
Piotr Drobek: art. 37–40
Agnieszka Gryszczyńska: wprowadzenie do ustawy pkt 1, art. 17–20, art. 45–50
Katarzyna Prusak-Górniak; art. 26–36, art. 41–44, art. 73–76
Krzysztof Silicki: art. 26–36, art. 41–44
Bolesław Szafrański: wstęp do rozdz. 3; art. 10 pkt 2–4, 6–7; art. 11 pkt 1–2, 4–5; art. 12 pkt 3–6; art. 13 pkt 1–2; art. 14 pkt 1–4, 7; art. 15 pkt 5–8
Grażyna Szpor: wprowadzenie do ustawy pkt 2–6, art. 1–4, art. 60–67, art. 68–72
Krzysztof Świtała: wstęp do rozdz. 3; art. 8–9; art. 10 pkt 1, 4–5; art. 11 pkt 3; art. 12 pkt 1–2; art. 13 pkt 3; art. 14 pkt 5–6; art. 15 pkt 1–4, 9; art. 16; art. 51–52
Martyna Wilbrandt Gotowicz: art. 5–7, art. 53–59, art. 77–94

ISBN 978-83-8160-442-0

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

Spis treści

Wykaz skrótów

dyrektywa NIS	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1)
Konstytucja RP	– Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. poz. 483 ze sprost. i zm.)
k.k.	– ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2018 r. poz. 1600 ze zm.)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2018 r. poz. 2096 ze zm.)
p.g.g.	– ustawa z 9.06.2011 r. – Prawo geologiczne i górnicze (Dz.U. z 2017 r. poz. 2126 ze zm.)
pr. bank.	– ustawa z 29.08.1997 r. – Prawo bankowe (Dz.U. z 2018 r. poz. 2187 ze zm.)
pr. energ.	– ustawa z 10.04.1997 r. – Prawo energetyczne (Dz.U. z 2018 r. poz. 755 ze zm.)
pr. lot.	– ustawa z 3.07.2002 r. – Prawo lotnicze (Dz.U z 2018 r. poz. 183 ze zm.)
p.p.s.a.	– ustawa z 30.8.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2018 r. poz. 1302 ze zm.)
pr. przeds.	– ustawa z 6.03.2018 r. – Prawo przedsiębiorców (Dz.U. poz. 646 ze zm.)

u.s.o.	– ustawa z 7.09.1991 r. o systemie oświaty (Dz.U. z 2018 r. poz. 1457 ze zm.)
pr. telekom.	– ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2018 r. poz. 1954 ze zm.)
rozporządzenie 2016/679, RODO	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1)
rozporządzenie eIDAS	– rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 257, s. 73)
rozporządzenie wykonawcze 2018/151	– rozporządzenie wykonawcze Komisji (UE) 2018/151 z 30.01.2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.Urz. UE L 26, s. 48)
TFUE	– Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 2016 r., s. 47)
u.ABW	– ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2018 r. poz. 2387 ze zm.)

u.d.a.r.	– ustawa z 4.09.1997 r. o działach administracji rządowej (Dz.U. z 2018 r. poz. 762 ze zm.)
u.d.i.p.	– ustawa z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2018 r. poz. 1330 ze zm.)
u.dz.a.	– ustawa z 20.06.2016 r. o działaniach antyterrorystycznych (Dz.U. z 2018 r. poz. 452 ze zm.)
u.f.p.	– ustawa z 27.08.2009 r. o finansach publicznych (Dz.U. z 2017 r. poz. 2077 ze zm.)
u.g.k.	– ustawa z 20.12.1996 r. o gospodarce komunalnej (Dz.U. z 2017 r. poz. 827 ze zm.)
u.i.d.p.z.p.	– ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 ze zm.)
u.k.a.r.	– ustawa z 15.07.2011 r. o kontroli w administracji rządowej (Dz.U. Nr 185, poz. 1092)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U poz. 1000 ze zm.)
u.o.i.f.	– ustawa z 29.07.2005 r. o obrocie instrumentami finansowymi (Dz.U. z 2018 r. poz. 2286 ze zm.)
u.p.z.p.	– ustawa z 29.01.2004 r. – Prawo zamówień publicznych (Dz.U. z 2018 r. poz. 1986 ze zm.)
u.RM	– ustawa z 8.08.1996 r. o Radzie Ministrów (Dz.U. z 2012 r. poz. 392 ze zm.)
u.s.g.	– ustawa z 8.03.1990 r. o samorządzie gminnym (Dz.U. z 2018 r. poz. 994 ze zm.)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2019 r. poz. 123)
u.t.k.	– ustawa z 28.03.2003 r. o transporcie kolejowym (Dz.U. z 2017 r. poz. 2117 ze zm.)
u.z.k.	– ustawa z 26.04.2007 r. o zarządzaniu kryzysowym (Dz.U. z 2018 r. poz. 1401)
ustawa o KSC	– ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560)

z.t.p.	– rozporządzenie Prezesa Rady Ministrów z 20.06.2002 r. w sprawie „Zasad techniki prawodawczej" (Dz.U. z 2016 r. poz. 283, zał.)

Wprowadzenie

1. Geneza regulacji

Cyberprzestępczość odnosi się do szerokiego zakresu różnych działań przestępczych, w których jako podstawowe narzędzie lub jako główny cel są wykorzystywane komputery i systemy informacyjne[1]. Może ona obejmować przestępstwa tradycyjne (np. oszustwo, fałszerstwo, kradzież), przestępstwa związane z treścią (np. rozpowszechnianie pornografii dziecięcej w Internecie lub nawoływanie do nienawiści) oraz przestępstwa charakterystyczne wyłącznie dla komputerów i systemów informacyjnych (np. ataki na systemy teleinformatyczne, ataki odmowy usługi, przejmowanie mocy obliczeniowej, tworzenie i dystrybucję złośliwego oprogramowania)[2].

[1] E.C. Viano, Cybercrime, *Organized Crime, and Societal Responses: International Approaches*, Springer International Publishing 2018; J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015; J. Clough, *Principles of Cybercrime*, Cambridge 2015; S.W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Boston 2012.

[2] Aktualne zagrożenia wskazują m.in. raporty Europolu (Internet Organised Crime Threat Assessment 2018, Europol https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018), FBI's Internet Crime Complaint Center – IC3 (2017 INTERNET CRIME REPORT https://pdf.ic3.gov/2017_IC3Report.pdf), zespołu CERT Polska (Krajobraz bezpieczeństwa polskiego Internetu w 2017 roku, Raport z działalności CERT Polska za rok 2017, https://www.cert.pl/publikacje/) czy raporty zespołów sektorowych (Raport CERT Orange Polska 2017, https://cert.orange.pl/raporty-cert). W raportach oraz piśmiennictwie wskazuje się również rosnące straty finansowe powodowane przez cyberbezpiestępczość – zob. Raport MCAFEE, The Economic Impact of

Cyberbezpieczeństwo zwykle wiązane było z zabezpieczeniami i działaniami, które można wykorzystać zarówno w sferze cywilnej, jak i wojskowej w celu zachowania dostępności i integralności sieci, infrastruktury informacyjnej oraz poufności informacji w nich zawartych[3]. Według nowej polskiej ustawowej definicji jest to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

W prawie międzynarodowym cyberbezpieczeństwo nie stało się przedmiotem kompleksowej, wiążącej regulacji o zasięgu globalnym. Jest ono natomiast przedmiotem wielu rezolucji Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych, które są zaleceniami adresowanymi do państw członkowskich, niezawierającymi norm prawnie wiążących. Już rezolucja nr 45/121 93 z 14.12.1990 r. odnosiła się do zwalczania przestępstw komputerowych. W rezolucji nr 56/121 z 19.12.2001 r. wzywano państwa członkowskie do wprowadzenia regulacji obejmujących zwalczanie przestępstw dokonywanych z użyciem technologii informacyjnych oraz gwarantujących skuteczną ochronę integralności i dostępności danych w systemach komputerowych. Na jej podstawie zorganizowano – we współdziałaniu z Międzynarodowym Związkiem Telekomunikacyjnym [ITU] – Światowy Szczyt Społeczeństwa Informacyjnego. Szczyt odbywał się w dwóch fazach w grudniu 2003 r. w Genewie i w listopadzie 2005 r. w Tunisie, a przyjęte na nim deklaracje i kolejne rezolucje Zgromadzenia Ogólnego ONZ, m.in. nr 58/199 z 23.12.2003 r. i nr 64/211 z 21.12.2009 r., zalecały działania zorientowane szerzej, na „globalną kulturę cyberbezpieczeństwa" i kompleksowe wzmacnianie ochrony „informacyjnej infrastruktury krytycznej"[4]. Platformą współdziałania różnych

Cybercrime (https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es--economic-impact-cybercrime.pdf); J. Charatynowicz, *Ekonomiczne aspekty cyberprzestępczości. Zagrożenia związane z konwersją i transferem wirtualnych walut* [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Szczytno 2017, s. 157–172.

[3] G. Szpor (red.), *Jawność i jej ograniczenia*, t. 1, *Idee i pojęcia*, Warszawa 2016, s. 130–138; *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017.

[4] Szerzej por.: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 38–43 i cytowana tam literatura; J. Worona, *Cyberprzestrzeń a prawo międzynaro-*

grup interesariuszy po Światowym Szczycie stało się Forum Zarządzania Internetem (ang. *Internet Governance Forum*, IGF), organizator dorocznych konferencji światowych i krajowych[5].

Wcześniejsze postulaty opracowania globalnych strategii i planów skonkretyzowano rezolucją Zgromadzenia Ogólnego ONZ nr 65/230 z 21.12.2010 r., powierzając Biuru Narodów Zjednoczonych ds. Narkotyków i Przestępczości [UNODC] opracowanie i wdrożenie globalnego programu zwalczania cyberprzestępczości. W kolejnej dekadzie Zgromadzenie Ogólne ONZ przedłużyło mandat udzielony w Tunisie IGF na wypracowywanie dobrych praktyk w dziedzinie bezpieczeństwa w Internecie. Ramy międzynarodowej współpracy mającej na celu zwiększenie zaufania i bezpieczeństwa w społeczeństwie informacyjnym wyznaczała nadal ITU – agenda wyspecjalizowana ONZ ds. technologii informacyjnych i komunikacyjnych, zrzeszająca państwa i podmioty sektora prywatnego działające w obszarze łączności elektronicznej. Nie powiodły się natomiast próby uzgodnienia międzynarodowej regulacji traktatowej odnoszącej się do cyberprzestrzeni w ramach powołanej w 2004 r. Grupy Ekspertów Rządowych ONZ, której działalność ujawniła trudności w odnoszeniu do cyberprzestrzeni zasad międzynarodowego prawa humanitarnego i zróżnicowanie interesów państw członkowskich[6].

Przeciwdziałanie przestępczości komputerowej było też przedmiotem regionalnych aktów prawa międzynarodowego. Rada Europy już Zaleceniem nr R(89) 9 z 13.9.1989 r. wzywała kraje członkowskie do uwzględnienia w prawodawstwie krajowym minimalnej listy przestępstw komputerowych[7]. Po następnej dekadzie została sporządzona

dowe, Rozprawa doktorska UwB 2017 https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/5875/1/J_Worona_%20Cyberprzestrzen_a_%20prawo_miedzynarodowe_Status_quo_i_perspektywy.pdf.

[5] http://www.intgovforum.org/multilingual/content/about-mag; https://igf.nask.pl/igf/igf-polska/44, IGF-Polska.html.

[6] C. Banasiński, *Cyberbezpieczeństwo*..., s. 42.

[7] P. Csonka, *Council of Europe activities in the field of computer related crime* [w:] *Legal aspects of computer-related abuse*, red. A. Adamski, Poznań 1994, s. 89–104; S. Redo,

23.11.2001 r. w Budapeszcie Konwencja Rady Europy o cyberprzestępczości, przyjęta po 13 latach także przez Polskę, która stała się stroną tej umowy jako 40 państwo członkowskie Rady Europy[8].

Do wzrostu znaczenia konwencji budapesztańskiej przyczyniał się także stan prawa Unii Europejskiej, w którym – odsyłając do niej jako podstawy międzynarodowej współpracy – problematykę cyberbezpieczeństwa podejmowano długo głównie w aktach o charakterze programowym oraz regulacjach fragmentarycznych. Skupianie się na ogromnych korzyściach, które przynosi cyfrowy świat, przesłaniało jego podatność na zagrożenia. Dopiero przed kilku laty wzrastająca w alarmującym tempie liczba zamierzonych bądź przypadkowych incydentów naruszających bezpieczeństwo w Internecie, zmieniła to podejście[9].

W unijnej strategii cyberbezpieczeństwa z 2013 r. zwrócono uwagę, że zagrożenia mogą mieć różne źródła – w tym przestępcze, motywowane politycznie, terrorystyczne lub inicjowane przez państwo, jak również mogą być efektem klęsk żywiołowych i niezamierzonych błędów. Zauważono, że mogą powodować zakłócenia nie tylko w sferze wirtualnej, ale i realnej, w świadczeniu podstawowych

Prevention and control of computer related crime from the United Nations perspective [w:] *Legal aspects of computer-related abuse*, red. A. Adamski, Poznań 1994, s. 71–87.

[8] Dz.U. z 2015 r. poz. 728; szerzej por. A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę* [w:] *Internet. Ochrona wolności, własności, bezpieczeństwa*, red. G. Szpor, Warszawa 2011, s. 345–356; A. Adamski, *Europejskie standardy prawno-karnej ochrony sieci i informacji oraz ich implementacja do prawa polskiego* [w:] *Internet. Strategie bezpieczeństwa*, red. G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 23–46.

[9] Np. dyrektywa 2013/40/UE Parlamentu Europejskiego i Rady z 12.08.2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218, s. 8). Aktualnie prowadzone są m.in. prace nad regulacją transgranicznego dostępu do dowodów elektronicznych (Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final – 2018/0107, Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters Brussels, 5.2.2019 COM(2019) 70 final).

Komentarz omawia przepisy dotyczące cyberbezpieczeństwa, czyli odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług. Komentowana ustawa nakłada nowe obowiązki na podmioty publiczne, a także dostawców usług cyfrowych oraz operatorów usług kluczowych z sektorów: energetyki, transportu, bankowości i finansów, ochrony zdrowia, zaopatrzenia w wodę, infrastruktury cyfrowej.

W książce zostały poruszone w szczególności takie zagadnienia jak:

- identyfikacja i rejestracja operatorów usług kluczowych, a także ich obowiązki,
- zadania Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego działających na poziomie krajowym,
- obsługa incydentów,
- kompetencje organów właściwych do spraw cyberbezpieczeństwa,
- sposób sprawowania nadzoru i kontroli operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa,
- transgraniczny charakter zagrożeń,
- zakres strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Książka jest przeznaczona dla wszystkich podmiotów objętych krajowym systemem cyberbezpieczeństwa. Powinna okazać się przydana nie tylko dla prawników, ale także dla funkcjonariuszy publicznych i przedsiębiorców z wielu sektorów. Może też zainteresować pracowników naukowych i studentów kierunków takich jak: prawo, administracja, informatyka, obronność i bezpieczeństwo.

9788381604420 W01P01

ISBN 978-83-8160-442-0

9 788381 604420

ZAMÓWIENIA:
INFOLINIA 801 04 45 45, FAX 22 535 80 01
ZAMOWIENIA@WOLTERSKLUWER.PL
WWW.PROFINFO.PL

CENA 159 ZŁ (W TYM 5% VAT)