# *Veritas in caritate*

## Księga pamiątkowa ku czci Księdza Profesora Andrzeja Szostka MIC

Redakcja
o. Marcin Tkaczyk
Marzena Krupa
ks. Krzysztof Jaworski

Wydawnictwo KUL
Lublin 2016

Paweł Urbanovicz, Marek Smarzewski

# Bezpieczeństwo w cyberprzestrzeni a prawo karne

Cyberprzestrzeń stanowi jeden z obszarów, w obrębie których można zidentyfikować coraz liczniejsze zagrożenia dla bezpieczeństwa. W tym kontekście należy się odwołać do, wydanych przez Narodowy Instytut Standardów i Technologii dnia 12 lutego 2014 roku, *Ram dla polepszania cyberbezpieczeństwa krytycznych infrastruktur*, w których podnosi się, iż zagrożenia dla cyberbezpieczeństwa powstają ze względu na coraz większą złożoność i łączność w ramach infrastruktury krytycznej, podczas gdy narodowe i ekonomiczne bezpieczeństwo państwa uzależnione jest od jej niezawodnego funkcjonowania[1].

Cyberprzestrzeń to globalna domena w środowisku informacyjnym, obejmująca współzależne sieci infrastruktur informatycznych, w tym Internet, sieci telekomunikacyjne, systemy komputerowe, wbudowane procesory oraz sterowniki[2]. Należy zauważyć ścisły związek pomiędzy problematyką bezpieczeństwa w cyberprzestrzeni a prawem. Jeżeli bowiem prawo stanowi narzędzie do regulacji istotnych relacji międzyludzkich, w tym w ramach różnego typu stosunków istniejących w obrębie społeczeństwa, które coraz częściej istnieją i zachodzą w cyberprzestrzeni, powstaje konieczność ich odpowiedniego regulowania, a częścią prawa stają się regulacje we wskazanym przedmiocie. Odnosząc takie twierdzenie do dziedziny prawa karnego, można zaobserwować czyny poszczególnych jednostek noszące znamiona przestępstw – popełniane zarówno incydentalnie czy z mniejszą lub większą częstotliwością, jak i z nawyknienia bądź też zawodowo. Od lat obserwuje się narastającą w sieci Internet aktywność grup przestępczych o charakterze zorganizowanym, także ugrupowań terrorystycznych. Niejednokrotnie podnosi się wręcz tezę o przenoszeniu działalności takich grup czy organizacji do cyberprzestrzeni. Wydaje się jednak, że zjawisko to należało-

[1] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*. Dostępny w Internecie: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, s. 1 [dostęp: 2.11.2014].

[2] Zob. *Multinational Experiment 7. Outcome 3 – Cyber Domain. Objective 3.2. Information Sharing Network* z dnia 22 stycznia 2013 r. Dostępny w Internecie: http://csrc.nist.gov/cyberframework/rfi_comments/dod_js_j7_part_2_ 022713.pdf, s. 5 [dostęp: 2.11.2014].

by odnosić abstrakcyjnie do przestępstw, których istota pozwala na przyjęcie, iż mogą być one popełnione w cyberprzestrzeni.

Początek XXI wieku charakteryzuje się niezwykle szybkimi i dużymi zmianami w dziedzinie technologii informacyjnych, czyli technologii informacyjno-komunikacyjnych (TIK). Te zmiany doprowadziły do transformacji we wszystkich aspektach życia osób fizycznych w szczególności i całych państw w ogóle.

Zgodnie z definicją przyjętą przez UNESCO, technologia informacyjna (TI) stanowi zestaw wzajemnie powiązanych naukowych, technologicznych, inżynieryjnych dyscyplin, które badają metody efektywnej organizacji pracy ludzi, zajmujących się przetwarzaniem i przechowywaniem informacji. Pojęcie „TI" obejmuje swym zakresem technikę komputerową, metody organizacji i współdziałania tej techniki z ludźmi i urządzeniem produkcyjnym, ich praktyczne zastosowania, a także powiązane z tym społeczne, ekonomiczne, etyczne, prawne i inne problemy.

Należy zwrócić uwagę na główne kierunki wdrażania nowoczesnych technologii informacyjnych. Są to w szczególności: modelowanie matematyczne i komputerowe; bazy danych i wiedzy; systemy eksperckie i inteligentne; narzędzia technologii planowania i zarządzania; e-mail; zintegrowane pakiety aplikacyjne i środowiska; środki, metody i techniki grafiki komputerowej, multimediów i animacji; hipertekst i technologie WWW, dostęp do rozproszonych zasobów internetowych; technologie chmurowe; narzędzia projektowania i technologia CASE i inne.

W tym kontekście należy zwrócić uwagę na znany aksjomat, zgodnie z którym technologie informacyjne są w zasadzie technologiami komputerowymi, technologiami internetowymi. Z technicznego punktu widzenia Internet jest zbiorem zasobów informacyjnych oraz systemów połączonych ze sobą kanałami i zjednoczonych w sieci, w której wymiana informacji odbywa się na bazie jednolitego systemu standardów i protokołów. Ten ostatni fakt oznacza, że Internet nie tylko integruje zasoby komunikacyjne i technologiczne, ale również materialne, finansowe, intelektualne, humanitarne, polityczne i inne, oraz zróżnicowanie form regulacji procesów społecznych. Wspomniana integracja większości najważniejszych zasobów związanych z działalnością człowieka, grup ludzi i całych państw (e-administracja, cyfrowa dyplomacja, e-edukacja, e-bankowość i inne) tworzy tzw. cyberprzestrzeń. Cyberprzestrzeń nie tylko stanowi złożony obiekt techniczny, ale także wspólnotę osób, które wstępują ze sobą w różne relacje i różne komunikacje w obszarze informacji. Pozostaje bowiem sferą działań społecznych związanych z ruchem i przekształcaniem informacji w sieci World Wide Web.

Najnowsze trendy w rozwoju stosunków związanych z bezpiecznym korzystaniem z cyberprzestrzeni wskazują, iż niektóre kwestie z nią związane muszą być przedmiotem regulacji na płaszczyźnie zarówno prawa krajowego, jak i międzynarodowego. Takie twierdzenie znajduje swe uzasadnienie w istniejących zagrożeniach dla systemów internetowych (i nie tylko), które są związane

z działaniami różnych grup hakerów (w tym międzynarodowych), naruszających integralność i poufność informacji oraz wpływających na realizację głównego interesu państwa, a mianowicie w przedmiocie zapewnienia bezpieczeństwa narodowego. Zagrożenia te można podzielić na wewnętrzne i zewnętrzne. Do pierwszych należą: utrata informacji z powodów przyczyn wewnętrznych; wyciek poufnych danych; fałszerstwo dokumentów przez pracowników; wprowadzenie złośliwego oprogramowania szpiegującego przez któregoś z pracowników firmy; upublicznienie czy rozpowszechnianie przez pracowników w Internecie danych dyskredytujących firmę itp.

Ponadto w związku z dużą popularnością technologii „chmury" niedawno pojawiła się osobna klasa zagrożeń, związanych z wykorzystaniem tych technologii w przedsiębiorstwach. Zagrożenia te obejmują powyżej wymienione i kilka innych rodzajów, w szczególności: niezapewnienie przez *service providera* usług, które są bardzo ważne dla biznesu; przechwytywanie danych przekazywanych między *providerem* a klientem; dostęp do danych przez repozytorium (przechowalnię) w chmurze, zrealizowany przez nieautoryzowanego użytkownika. Przez zewnętrzne lub internetowe zagrożenia zwykle rozumie się złośliwe oprogramowania (*malware*). Obecnie są tysiące rodzajów takich programów, które działają w różny sposób i mają ścisłą klasyfikację. Wszystkie złośliwe programy łączy to, że są one stworzone specjalnie do nieuprawnionego użycia, zniszczenia, blokowania, modyfikacji lub kopiowania informacji, naruszenia pracy komputerów lub sieci komputerowych, wprowadzenia zmian w kodzie aplikacji. Historia programów destrukcyjnych rozpoczęła się od wirusów komputerowych. Prosty wirus infekuje zazwyczaj jeden komputer. Wirusy „nie wykorzystują" serwisów sieciowych do swojego rozprzestrzeniania się i przenikania do innych komputerów. Kopia wirusa trafia na inne komputery w sieci tylko wtedy, gdy zainfekowany obiekt (plik) jest aktywowany na innym komputerze. Wirusy sieciowe lub robaki, które są najbardziej znane użytkownikom, mają zdolność do replikacji w komputerach połączonych w sieci. Robaki otrzymały swoją nazwę ze względu na ich zdolność do przenikania do komputera bez pomocy użytkownika. Do najczęściej wykorzystywanych przez cyberprzestępców należy zaliczyć trojany („konie trojańskie"). Główną cechą trojana jest to, że pozwala on na zdalny dostęp do obcego komputera, serwera, wraz ze wszystkimi płynącymi stąd konsekwencjami.

Według danych Kaspersky Lab w 2012 roku 96% wszystkich zarejestrowanych ataków (ponad pół miliarda) zostało zrealizowanych przez 20 programów destrukcyjnych, przy czym 87,4% z nich przeprowadzono za pomocą Malicious URL (środki dystrybucji – *spam i phishing*). Według tego samego źródła w pierwszym kwartale 2014 roku ataki na aplikacje mobilne najczęściej (22,77%) zostały wykonane za pomocą Trojana – Trojan SMS.AndroidOs.Stealer.a[3].

[3] Zob. http://securelist.ru/analysis/malware-quarterly/19176/razvitie-informacionnyx-ugroz-v-pervom-kvartale-2014-goda/ [dostęp: 11.11.2014].

Wiele zagrożeń internetowych przenika do komputera użytkownika za pośrednictwem przeglądarki. Głównym instrumentem infekcji przez przeglądarki są *exploity*. Otwierają one drogę dla cyberprzestępców do infekowania komputera. Cyberprzestępcy często monitorują ogólnodostępne sieci Wi-Fi i przechwytują dane przesyłane przez kanały publiczne. Tak więc przestępca może uzyskać dostęp do danych bankowych, haseł, kont i innych cennych informacji użytkownika. Z uwagi na to, że zasoby internetowe (np. serwery WWW) mają ograniczenia dotyczące liczby jednocześnie przetwarzanych transakcji, dość popularnym rodzajem cyberprzestępczości stały się ataki typu „odmowa w usłudze" (*Denial of Service*), co prowadzi do tego, że uprawnieni użytkownicy nie otrzymują dostępu do „zasobów własnych" (np. rachunków bankowych).

Nawet krótka analiza pokazuje całą powagę i globalną skalę problemu. Na znaczenie i doniosłość rozważanego zagadnienia wskazują odpowiednie decyzje ONZ. W tym miejscu trzeba przede wszystkim odwołać się do rezolucji Zgromadzenia Ogólnego ONZ nr 64/25 z dnia 2 grudnia 2009 roku[4] oraz rezolucji Zgromadzenia Ogólnego ONZ nr 67/27 z dnia 3 grudnia 2012 roku[5].

Przyjmując, że równowaga w obrębie globalnego społeczeństwa informacyjnego oparta jest na stymulującym rozwoju w człowieku wartości demokratycznych (swobodna wymiana informacji i wiedzy, wzajemna tolerancja i szacunek dla godności innych ludzi), można stwierdzić, że kwestia statusu prawnego użytkownika w cyberprzestrzeni, jego odpowiedzialność za działania w tym obszarze jest kluczową kwestią z punktu widzenia prawa technologii informatycznych. Wydaje się, że takie założenie jest istotne i znajduje konfirmację w stwierdzonych znacznych szkodach powodowanych przez cyberprzestępczość. Zgodnie z danymi opublikowanymi przez Centrum Strategicznych i Międzynarodowych Studiów w raporcie z czerwca 2014 roku uszczerbki spowodowane cyberprzestępczością są szacowane na kwotę od 375 do 575 miliardów dolarów rocznie[6]. Cyberprzestępczość stanowi zatem niewątpliwe zjawisko wywołujące poważny deficyt dla bezpieczeństwa, skutkujące – jak można zaobserwować w relacji do określonych jego przejawów – realnymi szkodami w dziedzinie dóbr chronionych przez prawo.

Należy przy tym zauważyć, iż stan, w którym brakuje bezpieczeństwa, może być często uzależniony od zachowań samej jednostki w cyberprzestrzeni. Podejmując określone działania, naraża się ona nieraz na negatywne efekty czynów popełnianych przez cyberprzestępców. Nierzadko jednak przyczynę braku bezpieczeństwa stanowi niedostateczne zabezpieczenie sieci domowych, publicznych czy w obrębie instytucji.

Nie powinno budzić zdziwienia, iż pośród instytucji czy osób prawnych najbardziej narażone na niebezpieczeństwo pokrzywdzenia w wyniku przestępstw

[4] Zob. http://research.un.org/en/docs/ga/quick/regular/64 [dostęp: 11.11.2014].

[5] Zob. tamże.

[6] Zob. http://csis.org/event/2014-mcafee-report-global-cost-cybercrime [dostęp: 11.11.2014].

popełnianych w sieci teleinformatycznej czy za jej pośrednictwem są organizacje należące do sektora bankowego i ubezpieczeniowego lub funkcjonujące w obszarze usług. W coraz większym stopniu wzrasta również liczba czynów zabronionych, godzących w działalność informacyjną prowadzoną przez instytucje administracji publicznej[7], m.in. przez atakowanie i blokowanie stron zawierających informacje publiczne. Nie należy przy tym zapominać, iż ofiarami cyberprzestępców padają również poszczególne osoby fizyczne, pozostające często w nieświadomości bycia pokrzywdzonymi.

Ograniczając nawiązanie do typologii przyjętej w ustawie z dnia 6 czerwca 1997 roku – *Kodeks karny*[8], do przestępstw, których ofiarą jednostka może się stać w cyberprzestrzeni, zaliczamy m.in.: *hacking*; nielegalny podsłuch komputerowy; utrudnianie dostępu i niszczenie informacji; sabotaż informatyczny; przestępstwa seksualne popełnione na szkodę małoletniego; oszustwo komputerowe, *cyberstalking*, kradzież tożsamości; fałszerstwo komputerowe.

W procesie globalizacji i coraz bardziej dynamicznego rozwoju technologii informatycznych i rozrastania się sieci Internet oraz związanego z tym wzrostu skomplikowania w jej obrębie problematyczną kwestią pozostaje prawne definiowanie rzeczywistości powiązanej z tymi zjawiskami. Na gruncie prawa karnego brakuje już nawet powszechnie akceptowanej definicji cyberprzestępczości. Ogólnie rzecz ujmując, można jednak definiować cyberprzestępczość jako zachowania odnoszące się do wykorzystywania technologii informacyjnych (komputerów i sieci komputerowych) do popełniania przestępstw[9].

W prawie karnym niedostatki związane z funkcjonującą siatką pojęciową dostrzegalne są w odniesieniu do niektórych typów przestępstw. Ustawodawca posługuje się przykładowo pojęciem „systemu teleinformatycznego", innym razem „sieci teleinformatycznej". Ponadto w części szczególnej *Kodeksu karnego* można odnaleźć określenie „sieć telekomunikacyjna". Używa się także pojęcia „systemu informatycznego" jako przedmiotu czynności wykonawczej. Ustawodawca formułuje także termin „system komputerowy". W relacji do przywołanych kategorii pojęciowych należy zauważyć, że w większości ich znaczenie jest określone w obowiązujących aktach prawnych. Niemniej rozumienie części z nich można by uznać za częściowo zdezaktualizowane w związku z rozwojem technologii informacyjnych, inne zaś nie zawsze odpowiadają terminologii przyjętej w obowiązującym ustawodawstwie.

Kolejnym problemem jest niejednokrotnie niedostateczne dookreślenie znamion czynów zabronionych, które mogą być popełnione w cyberprzestrzeni. Brak precyzyjnego ujęcia znamion powoduje osłabienie zasady gwarancyjno-

---

[7] Zob. C. Sarzana, *Informatica, internet e diritto penale*, Milano 2010, s. 109–110.

[8] Dz.U. 1997, nr 88, poz. 553 ze zm.

[9] E. Kraemer-Mbula, P. Tang, H. Rush, *The cybercrime ecosystem: Online innovation in the shadows?*, "Technological Forecasting & Social Change" 80 (2013), Iss. 3, s. 543.

ści i trudności w jasnym rozgraniczeniu, jakie zachowania w nich się mieszczą. Ważnym zagadnieniem pozostaje też zbyt szerokie określanie niektórych typów przestępstw. Jako przykład można wskazać na kwestię posiadania w celu rozpowszechniania pornografii i na problematyczność wypełnienia znamion w przypadku pobierania tego typu treści za pomocą programu P2P, bez świadomości sposobu jego funkcjonowania i w związku z tym przy braku świadomości jednoczesnego ich rozpowszechniania. Tak samo wysoce kontrowersyjna jest kryminalizacja uzyskania dostępu do treści pornograficznych z udziałem małoletniego. Należałoby przyjąć, iż warunkiem odpowiedzialności karnej jest wówczas umyślność działania – może dojść bowiem do niezamierzonego uzyskania dostępu do takich materiałów, np. w wyniku przesłania spamu na e-mail, wyskakujących okienek, tzw. *pop-ups* bądź też zmodyfikowanych hiperłączy[10]. Stwierdzenie takie znajduje swe oparcie już w samym rozumieniu czynu stanowiącego „[...] tylko takie działanie, którego człowiek jest świadomym i wolnym sprawcą"[11].

Wartą uwagi materią pozostaje potrzeba harmonizacji prawa krajowego, europejskiego i międzynarodowego w kontekście przeciwdziałania cyberprzestępczości. To właśnie luki w prawie krajowym i międzynarodowym sprawiają, że utrudnione jest wykrywanie i ściganie cyberprzestępstw. Przyczyną jest zwłaszcza kwestia ich odmiennej typizacji w poszczególnych państwach. Skoro Internet stanowi narzędzie międzynarodowej komunikacji, oznacza to, iż rozwiązania prawne zapewniające bezpieczeństwo w jego obrębie powinny być stanowione i obowiązywać w globalnej skali. Stąd przyjmowanie jednolitego prawodawstwa skierowanego przeciwko nadużywaniu nowych technologii dla przestępczych celów stanowi punkt centralny dla osiągnięcia ogólnoświatowego cyberbezpieczeństwa. Zagrożenia mogą powstać w zasadzie gdziekolwiek, dlatego konieczne jest tworzenie międzynarodowych rozwiązań i organizowanie na takim szczeblu współpracy w prowadzeniu postępowań karnych oraz w stanowieniu przepisów o charakterze materialnym i procesowym[12]. Stąd cyberprzestępczość jest zjawiskiem szeroko dyskutowanym i rozważanym w różnych gremiach. Istnieje bowiem konieczność kategoryzacji jej elementów składowych, ich uporządkowania i uświadamiania w kwestii zagrożeń zeń płynących.

Prawdopodobnie najistotniejszym aktem prawnym[13] – w analizowanym przedmiocie – pozostaje *Konwencja Rady Europy o cyberprzestępczości* z dnia 23 li-

[10] Por. M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 200.

[11] A. Szostek, *Pogadanki z etyki*, Częstochowa 1998, s. 48. Zob. również tenże, *Rola natury czynu w argumentacji etycznej. Na marginesie dyskusji wokół norm ogólnie ważnych we współczesnej teologii*, „Roczniki Filozoficzne" 27 (1979), z. 2, s. 103.

[12] M. Obiso, G. Fowlie, *Toward a Global Approach to Cybersecurity*, w: K.J. Andreasson (ed.), *Cybersecurity. Public Sector Threats and Responses*, CRC Press 2012 [dostęp: 10.11.2014].

[13] W tym miejscu należałoby zwrócić uwagę na znaczny dorobek prawny Unii Europejskiej w zakresie zwalczania cyberprzestępczości i jej przeciwdziałania.

stopada 2001 roku[14], ratyfikowana przez Polskę na mocy ustawy z dnia 12 września 2014 roku[15]. Rzeczpospolita Polska, wyrażając zgodę na ratyfikację *Konwencji*, zastrzegła jednak, że warunek wykonania wniosku o pomoc wzajemną dotyczącego przeszukania lub uzyskania dostępu przy użyciu podobnych metod, zajęcia lub podobnego zabezpieczenia albo ujawnienia przechowywanych danych, w odniesieniu do przestępstw innych niż określone w art. 2–11 *Konwencji*, będzie stanowiła podwójna karalność tych przestępstw[16].

Poczynione ustalenia uzasadniają konstatację, iż dla uzyskania jednolitości w zakresie rozwiązań prawnych dotyczących wykrywania cyberprzestępczości, przede wszystkim zaś jej skutecznego ścigania i rozstrzygania w przedmiocie odpowiedzi na bezprawie przez nią wywołane, nieodzowne jest wyeliminowanie sprzeczności istniejących w obrębie systemu prawnego i niepozwalających na implementowanie niezbędnych norm w tym zakresie. Konieczne jest przy tym, ze względu na globalny charakter sieci Internet, przenoszenie instrumentów służących jej zwalczaniu i zapobieganiu na poziom międzynarodowy.

Nie deprecjonując przy tym potrzeby istnienia moralności społecznej, z uwagi na specyfikę cyberprzestrzeni, błędem byłoby przyjęcie założenia o funkcjonowaniu w jej obrębie użytkowników na podstawie pewnych powszechnie przyjętych zasad moralnych czy etycznych[17]. Cyberprzestrzeń stanowi miejsce, w obrębie którego występują rozmaite zagrożenia. Stąd wynika uzasadnienie dla regulacji i kontroli. Im bowiem mniejsza dowolność w – dających się ocenić jako nieetyczne bądź sprzeczne z uznanymi wartościami – zachowaniach przedsiębranych w cyberprzestrzeni, tym wprost proporcjonalnie spada stan niebezpieczeństwa dla dóbr prawnie chronionych. Swoją drogą trzeba ważyć zasadność regulacji, gdyż często niesie ona za sobą równoczesne ograniczenie praw i wolności jednostki.

---

[14] Zob. polskie tłumaczenie konwencji o cyberprzestępczości. Dostępny w Internecie: http://nowetechnologie.umk.pl/wp-content/uploads/2013/04/Konwencja-o-cyberprzestepczosci.pdf [dostęp: 10.11.2014].

[15] Dz.U. 2014, poz. 1514.

[16] Zob. http://www.prezydent.pl/download/gfx/prezydent/pl/defaultaktualnosci/2072/51/1/konwencja_re_ o_cybeprzestepczosci.rtf [dostęp: 10.11.2014].

[17] Por. A. Szostek, *Jeszcze o specyfice wartości moralnej. Na marginesie artykułu M.A. Krąpca „Decyzja – bytem moralnym"*, „Roczniki Filozoficzne" 31 (1983), z. 2, s. 84–85.