WIEDZA OBRONNA 2025, Vol. 293 No. 4
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/8tgzy788

BOGUSŁAW PACEK*
Polish Army Museum, Warsaw, Poland, Warsaw Fire Academy, Warsaw, Poland

ANTONI MARIUSZ KAMIŃSKI*
University of Warsaw, Warsaw, Poland

PRAWNE OGRANICZENIA STOSOWANIA TECHNOLOGII CYFROWYCH W KONTEKŚCIE BEZPIECZEŃSTWA NARODOWEGO

LEGAL RESTRICTIONS ON THE USE OF DIGITAL TECHNOLOGIES IN THE CONTEXT OF NATIONAL SECURITY

Abstrakt: Współczesne państwa demokratyczne stają przed trudnym wyzwaniem równoważenia dynamicznego rozwoju technologii cyfrowych z koniecznością zapewnienia bezpieczeństwa narodowego. Artykuł analizuje prawne zakazy i ograniczenia w stosowaniu technologii cyfrowych w pięciu sektorach bezpieczeństwa według klasyfikacji Barry'ego Buzana: militarnym, politycznym ekonomicznym, społecznym i ekologicznym. Pozwoliło to na identyfikację kluczowych dylematów, przed którymi stoją państwa o demokratycznych systemach w erze cyfrowej. Obejmują one m.in. dążenie do wykorzystania możliwości cyfrowej rewolucji przy jednoczesnym zminimalizowaniu nowych zagrożeń bezpieczeństwa; wprowadzaniu zakazów i ograniczeń przy zachowaniu standardów swobód obywatelskich; elastyczne regulacje prawne, które nie hamują rozwoju nowych technologii, ale pozwalają na skuteczne zarządzanie bezpieczeństwem; niwelowanie napięć między postępem technologicznym a normami etyczno-prawnymi.

Słowa kluczowe: technologie cyfrowe, bezpieczeństwo narodowe, regulacje prawne, państwa demokratyczne, prawo bezpieczeństwa.

Abstract: Contemporary democratic states face the imperative of balancing the dynamic development of digital technologies with the necessity of ensuring national security. This presents a significant challenge, particularly in the context of maintaining civil liberties standards. The article examines legal prohibitions and restrictions on the utilization of digital technologies across five security sectors, as classified by Barry Buzan: military, political, economic, societal, and environmental. It identifies key dilemmas confronting states with democratic systems in the digital era. These include endeavoring to capitalize on the opportunities presented by the digital revolution while mitigating new security threats; imposing prohibitions and restrictions while preserving standards of civil liberties; implementing flexible regulations that do not impede the development of new technologies, yet allow for effective security management; and addressing tensions between technological advancements and ethical and legal norms.

Keywords: digital technologies, national security, legal regulations, democratic states, security law.

* **prof. dr. hab. Bogusław Pacek**, Polish Army Museum, Warsaw, Poland, Warsaw Fire Academy, Warsaw, Poland
https://orcid.org/0000-0002-2476-6081 sekretariat@muzeumwp.pl
* **dr. hab. Antoni Mariusz Kamiński**, University of Warsaw, Warsaw, Poland
https://orcid.org/0000-0002-9169-5543 m.kaminski@akademia.mil.pl

Copyright (c) 2025 Bogusław Pacek and Antoni Mariusz Kamiński. This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

Wprowadzenie

Pod wpływem rozwoju cyfrowych technologii współczesne środowisko bezpieczeństwa ulega niezwykle dynamicznym zmianom. Wymaga to od państw szybkiego adoptowania się do nowych wyzwań, aby skutecznie reagować na powstające zagrożenia. W erze cyfrowej transformacji rozwój innowacyjnych technologii często wyprzedza tempo tworzenia regulacji prawnych, zarówno na poziomie krajowym, jak i międzynarodowym. Prowadzi to do paradoksu, gdy państwa z jednej strony inwestują i wspierają prace nad zaawansowanymi rozwiązaniami technologicznymi, a z drugiej strony wprowadzają obostrzenia i zakazy w ich stosowaniu argumentując to względami bezpieczeństwa narodowego.

Najczęściej tego typu restrykcje dotyczą państw niedemokratycznych i mają związek z łamaniem praw człowieka. Przykłady Chin, Rosji, Iranu czy Korei Północnej wyraźnie wskazują, że władze ograniczają stosowanie technologii cyfrowych, aby przede wszystkim uniemożliwić dostęp społeczeństwa do informacji i wolnych mediów, które zagrażają stabilności autorytarnych reżimów[1]. Jednak problem jest dużo bardziej złożony, gdyż w państwach demokratycznych również powstają sytuacje, kiedy względy bezpieczeństwa narodowego wymagają wprowadzenia restrykcyjnych regulacji, ale przy jednoczesnym zachowaniu swobód obywatelskich.

Celem artykułu jest analiza prawnych zakazów i ograniczeń w stosowaniu technologii cyfrowych w kontekście bezpieczeństwa w państwach demokratycznych. Opierając się na klasycznej koncepcji Barry'ego Buzana przyjęto, że bezpieczeństwo państwa to złożony proces utrzymania integralności i suwerenności w warunkach zewnętrznych i wewnętrznych zagrożeń, wykraczając poza tradycyjne ujęcie militarne. Dlatego analizę prawnych zakazów i ograniczeń w stosowaniu technologii cyfrowych przeprowadzono w pięciu wyszczególnionych przez Buzana współzależnych sektorach bezpieczeństwa[2]:

- bezpieczeństwie militarnym – obejmującym zdolności państwa do obrony przed zewnętrznymi zagrożeniami fizycznymi (np. konfliktem zbrojnym);
- bezpieczeństwie politycznym – skoncentrowanym na stabilność instytucji państwowych oraz zdolność do utrzymania suwerenności i legitymacji władzy w tym ograniczanie ryzyka manipulacji procesów politycznych (np. wyborów);
- bezpieczeństwie ekonomicznym – dotyczącym ochrony infrastruktury krytycznej, stabilności finansowej państwa oraz ochrony przed kryzysami gospodarczymi;
- bezpieczeństwie społecznym – skoncentrowanym na ochronie spójności społecznej, tożsamości kulturowej i prawie do prywatności;
- bezpieczeństwie ekologicznym – obejmującym przeciwdziałanie zagrożeniom dla środowiska oraz ochronie ekosystemów przed degradacją (np. przez nadmierną eksploatację zasobów).

W badaniach przyjęto następującą hipotezę roboczą: Dynamiczny rozwój technologii cyfrowych generuje wiele nowych zagrożeń bezpieczeństwa, które trudno jest przewidzieć z wyprzedzeniem.

[1] Zob. więcej: E. Frantz, A. Kendall-Taylor, J. Wright, Digital Repression in Autocracies, V-Dem Institute, 2020.

[2] B. Buzan, People, States and Fear: The National Security Problem in International Relations, 1983, s. 75–83.

Dlatego częstą taktyką stosowaną przez państwa demokratyczne jest odwlekania uchwalenia regulacji prawnych na poziomie krajowym, obserwacja trendów i wprowadzanie prawnych zakazów i ograniczeń dotyczących stosowania technologii cyfrowych ze względu na bezpieczeństwo narodowe tylko w określonych przypadkach (przy uwzględnieniu standardów praw i wolności obywatelskich).

W badaniach zastosowano analizę i syntezę literatury przedmioty oraz źródeł pierwotnych (głównie aktów prawnych na poziomie międzynarodowym i krajowym), a także metodę studium przypadku (*case study*).

Bezpieczeństwo militarne

Ograniczenia dotyczące wykorzystania zaawansowanych technologii cyfrowych w obszarze bezpieczeństwa militarnego budzą szczególne kontrowersje. W tym przypadku państwa demokratyczne muszą balansować pomiędzy potrzebą zbudowania strategicznej przewagi nad zdolnościami bojowymi przeciwnika i zapewnienia skuteczności operacyjnej swoich sił zbrojnych, a koniecznością przestrzegania norm międzynarodowych i zasad etycznych. Największe dylematy powstają w związku z szybkim rozwojem Autonomous Weapon Systems (AWS), czyli zaawansowanymi technologicznie systemami zintegrowanymi z elementami sztucznej inteligencji, które po ich aktywacji mogą podejmować działania autonomicznie. Specyficzną kategorię AWS stanowią Lethal Autonomous Weapon Systems (LAWS), czyli systemy bojowe, które identyfikują i eliminują cele samodzielnie bez udziału człowieka w procesie decyzyjnym[3]. LAWS wywołują spory prawne dotyczące legalności ich użycia w kontekście międzynarodowego prawa humanitarnego konfliktów zbrojnych, zwłaszcza w aspekcie trudności z rozróżnieniem celów cywilnych od wojskowych. Dodatkowo budzą najwięcej wątpliwości etycznych ze względu na możliwość samodzielnego decydowania przez autonomiczne systemy o ludzkim życiu lub śmierci.

Należy podkreślić, że rozważania na temat etycznych i prawnych aspektów AWS i LAWS nie są już tylko teoretyczne, gdyż pojawiają się przykłady zastosowania tej broni w praktyce. Według raportu ONZ w 2020 roku podczas operacji „Peace Storm" libijskie siły rządowe (GNA-AF) użyły autonomicznych tureckich dronów Kargu-2 do atakowania wycofujących się grup zbrojnych powiązanych z Khalifem Haftarem. Zadanie było realizowane w trybie *fire, forget and find*, a systemy były zaprogramowane do autonomicznego atakowania celów bez potrzeby utrzymywania łączności między operatorem a dronem[4]. Z kolei władze Korei Południowej oficjalnie potwierdziły zainstalowanie w strefie zdemilitaryzowanej działka strażniczego SGR-A1. Choć producent tego systemu zaprzecza, że SGR-A1 pracuje w pełni autonomicznie, to wielu ekspertów międzynarodowych wskazuje, że system może działać zarówno w trybie z udziałem decyzji człowieka (*human-in-the-loop*), jak też w pełni autonomicznie (*human over the loop)*[5].

[3] N. Nnamdi, B.O. Eniola, B. Abegunde, Examining Lethal Autonomous Weapons through the Lens of International Humanitarian Law, „Scholars International Journal of Law, Crime and Justice" 2023, t. 6, nr 06, s. 229–230.

[4] Panel of Experts on Libya, Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973, S/2021/229, 2021.

[5] H.-Y. Liu, Categorization and legality of autonomous and remote weapons systems, „International Review of the Red Cross" 2012, t. 94, nr 886, s. 631.

Technologie LAWS są przedmiotem dużej międzynarodowej debaty na temat wprowadzenie restrykcyjnych ograniczeń prawnych ich użycia lub całkowitego zakazu. Grupa organizacji pozarządowych prowadząca kampanię „Stop Killer Robots" wskazała, że w 2019 roku 30 państw opowiada się za całkowitym zakazem LAWS[6]. Natomiast w październiku 2024 roku ONZ przyjęła rezolucję na temat LAWS w której potwierdzono konieczność zastosowanie prawa międzynarodowego w odniesieniu do autonomicznych systemów uzbrojenia oraz wyrażono zaniepokojenie potencjalnymi negatywnymi konsekwencjami systemów autonomicznych dla bezpieczeństwa globalnego[7]. Jednak biorąc pod uwagę fakt, że USA, Chiny i Federacja Rosyjska nadal intensywnie rozwijają prace badawcze nad systemami AWS i LAWS to przyjęcie międzynarodowych regulacji prawnych w tym zakresie może okazać się niezwykle trudne.

Niektóre państwa demokratyczne wprowadzają ograniczenia prawne w zastosowaniu technologii AWS i LAWS na poziomie krajowym. Przykładem są Stany Zjednoczone, gdzie Departament Obrony przyjął Dyrektywę 3000.09 dotyczącą wykorzystania autonomicznych i półautonomicznych funkcji w systemach uzbrojenia. Dyrektywa nie zakazuje autonomicznych systemów, ale nakłada dodatkowe wymagania techniczne i proceduralne. Nakazuje także, aby przy ich rozwoju nie wyeliminowano roli człowieka w krytycznych aspektach użycia siły. Bardzo istotne jest w tym przypadku zastrzeżenie dotyczące projektowania systemów autonomicznych w sposób umożliwiający dowódcom i operatorom odpowiedni poziom ludzkiej oceny w kwestii użycia siły (*appropriate levels of human judgment over the use of force*)[8]. Sformułowanie to stanowi podstawowy filar polityki USA w zakresie autonomicznych systemów uzbrojenia. Jego celem jest zapewnienie, że decyzje o użyciu siły pozostają pod kontrolą człowieka, nawet w systemach o wysokim stopniu autonomii.

Należy podkreślić, że Dyrektywa 3000.09 dotyczy tylko instytucji nadzorowanych przez Departament Obrony i nie obejmuje innych departamentów rządowych i cywilnych agencji federalnych odpowiedzialnych za bezpieczeństwo państwa. Tak więc systemy AWS lub LAWS używane przez Centralną Agencję Wywiadowczą (CIA) nie muszą spełniać wymogu „ludzkiej kontroli" i zatrzymania ataku bez potwierdzenia operatora. Jest to bardzo istotne w kontekście realizacji przez CIA operacji *covert action*, których elementem są zabójstwa (*targeted killings*) również poza strefami konfliktów zbrojnych (jak np. Jemen czy Pakistan). Upubliczniony w 2016 roku na polecenie prezydenta Baracka Obamy raport amerykańskiej Wspólnoty Wywiadowczej (Intelligence Community) pokazał, że CIA wykorzystuje bezzałogowe statki powietrzne do eliminacji liderów międzynarodowego terroryzmu na dużą skalę. W latach 2009–2015 przeprowadzono łącznie 473 ataki, w których zginęło 2372–2581 przeciwników *(enemy combatants*) i od 64 do 116 osób niebędących celami ataków *(non- combatants*)[9]. Choć *covert action* są sprzeczne z zasadami

[6] Campaign to Stop Killer Robots, Country Views on Killer Robots, s. 1.

[7] United Nations General Assembly, Lethal autonomous weapons systems (Resolution 78/241, UN Doc A/79/251).

[8] Department of Defense, Autonomy in weapon systems (DoD Directive 3000.09), s. 3.

[9] Director of National Intelligence, Summary of Information Regarding U.S. Counterterrorism Strikes Outside Areas of Active Hostilities, 2016.

prawa międzynarodowego[10] to procedury ich realizacji są oficjalnie uregulowane w amerykańskim systemie prawnym. Zgodnie z przepisami sekcji 503e ustawy Ustawa National Security Act termin *covert action* oznacza działania rządu Stanów Zjednoczonych Ameryki mające na celu wywieranie wpływu na sytuację polityczną, ekonomiczną lub militarną poza granicami USA z zamierzeniem, że rola rządu Stanów Zjednoczonych Ameryki nie będzie jawna ani oficjalnie potwierdzona[11]. Na tej podstawie prezydent Stanów Zjednoczonych zatwierdza operacje, które realizowane są przez Centralną Agencję Wywiadowczą.

Oczywiście *covert action* (w tym *targeted killings*) to nie tylko domena USA, ale również wielu innych państw zarówno demokratycznych i niedemokratycznych[12]. Jednak w związku z szybkim rozwojem broni autonomicznej i zaawansowanej sztucznej inteligencji bardzo niepokojąco wyglądają scenariusze dotyczące przyszłości takich operacji. Dotyczy to np. autonomicznych mikrodronów zdolnych przez wiele dni samodzielnie śledzić cel (również w środowisku zurbanizowanym) i w odpowiednim momencie podjąć decyzję o jego eliminacji[13]. Taka perspektywa rodzi pytania o granice inwigilacji i ingerencji w suwerenność państw oraz zasadę proporcjonalności i rozróżniania w kontekście międzynarodowego prawa humanitarnego konfliktów zbrojnych. Pokazuje to również konieczność wprowadzenia regulacji prawnych na poziomie międzynarodowym dotyczących obostrzeń i zakazów użycia autonomicznych systemów uzbrojenia w określonych sytuacjach. Z drugiej strony przykład obecnych regulacji prawnych *covert action* na poziomie krajowym w USA i operacji CIA realizowanych na ich podstawie wskazuje, że w praktyce wszelkie ograniczenia mogą być bardzo trudne do wyegzekwowania.

Na zakończenie rozważań nad bezpieczeństwem militarnym należy zwrócić uwagę na aspekt personalny dotyczący żołnierzy i cywilnych pracowników wojska. Krajowe regulacje prawne lub wewnętrzne przepisy w siłach zbrojnych wprowadzają bowiem liczne ograniczania w korzystaniu z technologii cyfrowych. Skala i rodzaj tych obostrzeń jest bardzo różna i zależy głównie od natury zadań realizowanych przez daną formację. Najdalej idące ograniczenia dotyczą zazwyczaj funkcjonariuszy wywiadu i kontrwywiadu wojskowego, co wynika z tajnego charakteru ich pracy. Wytyczne zalecają m.in. unikanie publikowania zdjęć (zwłaszcza w mundurach), ujawniania lokalizacji czy informacji o pracy w sieci[14]. Największy problem z ujawnianiem wrażliwych danych w sieci przez żołnierzy dotyczy geotagowania jednostek. Po skandalu z aplikacją biegową Strava w 2018 roku w której ujawniono trasy biegowe i rowerowe amerykańskich żołnierzy stacjonujących na całym świecie (co umożliwiało identyfikację granic instalacji wojskowych) Pentagon wprowadził całkowity zakaz używania urządzeń z glokalizacją (m.in. smartfony i fitness

[10] Porównaj: M.C. Haas, S.-C. Fischer, The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order, „Contemporary Security Policy" 2017, t. 38, nr 2; D. Kretzmer, Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Defence?, „The European Journal of International Law" 2005, t. 16, nr 2; E.J. Sanchez, Intelligence Collection, Covert Operations, and International Law, „Intelligencer: Journal of U.S. Intelligence Studies" 2017, t. 23, nr 2.

[11] U.S. Congress, National Security Act of 1947 (Section 503), Pub. L. 80–253, Large 61 Stat. 495.

[12] M. Kamiński, Ewolucja wywiadu jako instytucji państwa, Warszawa 2021, s. 312–313.

[13] M.C. Haas, S.-C. Fischer, The evolution of targeted killing practices, op. cit., s. 285–288.

[14] Bureau of Justice Assistance, Developing a policy on the use of social media in intelligence and investigative activities: Guidance and recommendations, s. 29–30.

trackery) w strefach operacyjnych[15]. Z kolei turecki parlament w 2024 roku znowelizował ustawę o personelu sił zbrojnych wprowadzając zakaz korzystania z mediów społecznościowych przez żołnierzy. Bezpośrednią przyczyną wprowadzenia tak restrykcyjnych przepisów był incydent z żołnierzem sił specjalnych, który prowadził transmisję na żywo w aplikacji Tik Tok ujawniając słabe zabezpieczenia tureckich baz w północnym Iraku, co wykorzystali bojownicy Partii Pracujących Kurdystanu do ataków moździerzowych[16].

Bezpieczeństwo polityczne

W obszarze bezpieczeństwa politycznego interesującym zagadnieniem są ograniczenia i zakazy związane z bezpieczeństwem wyborów. W pierwszej dekadzie XXI wieku wydawało się, że nieuchronnie duża część państw demokratycznych wprowadzi głosowanie za pośrednictwem Internetu w celu ułatwienia obywatelom udziału w wyborach i zwiększenia frekwencji. Tymczasem na początku 2025 roku jedynym państwem, które w pełni korzysta z takiej możliwości jest Estonia. Po raz pierwszy Estończycy mogli zagłosować online w 2005 roku w wyborach samorządowych, ale tą drogę wybrało tylko 3% wyborców. Natomiast w wyborach parlamentarnych w 2023 roku swój głos za pośrednictwem Internetu oddało już ponad 51% głosujących, co stanowi rekord w historii estońskich wyborów[17]. Ciągle wzrastająca popularność głosowania online pokazuje, że Estończycy mają zaufanie do systemów obrony cybernetycznej swojego państwa i nie obawiają się obcej ingerencji i prób manipulacji głosami. Jest to o tyle zastanawiające, że w 2007 roku Estonia stała się celem zmasowanego ataku rosyjskich hackerów na infrastrukturę teleinformatyczną państwa określanego często jako pierwszy na świecie przypadek próby cybersabotażu w tak dużej skali[18]. Nie zniechęciło to jednak estońskich władz, które konsekwentnie rozwijają swój system „i-Voting" umożliwiając od października 2025 roku głosowanie nawet za pomocą aplikacji mobilnych w smartfonach.

Zupełnie inaczej zareagowały na wzrastające zagrożenia cyberbezpieczeństwa inne państwa demokratyczne, które w większości przypadków ograniczały lub wycofywały się z prób wprowadzenia możliwości głosowanie przez Internet. Tak było w przypadku Australii, gdzie władze stanu Nowej Południowej Walii wprowadziły w 2011 roku system „iVote" dla wyborców niepełnosprawnych i osób przebywających za granicą, zaś w 2020 roku rozszerzyły go na wszystkich wyborców przebywających poza swoim okręgiem wyborczym. Jednak podczas wyborów w 2021 roku nastąpiło przeciążanie systemu, co uniemożliwiło oddanie głosu tysiącom wyborców, a Sąd Najwyższy Nowej Południowej Walii nakazał powtórne głosowanie w trzech okręgach. Audyt ujawnił również błędy w kodzie źródłowym systemu (m.in. brak skutecznej weryfikacji głosów), co ostatecznie spowodowało decyzję władz o likwidacji „iVote" w 2023 roku[19]. Również

[15] Department of Defense, Use of Geolocation-Capable Devices, Applications, and Services, 2018.

[16] L. Kenez, Turkish military to enforce strict social media ban for soldiers after security breaches and ambushes, https://nordicmonitor.com/2024/06/turkish-military-enforces-strict-social-media-ban-for-soldiers-after-security-breaches-and-ambushes/ (dostęp 01.09.2025).

[17] National Electoral Committee of Estonia, Election results, https://data.ipu.org/parliament/EE/EE-LC01/election/EE-LC-01-E20230305/ (dostęp: 01.09.2025).

[18] M.A. Kamiński, Obrona Narodowa Republiki Estonii, Toruń 2018, s. 68.

[19] NSW Electoral Commission, Technology assisted voting: Final review report, 2023, s. 4.

we Francji wdrożono w 2012 roku system głosowania online w wyborach parlamentarnych dla wyborców przebywających za granicą. Jednak w 2017 roku na kilka tygodni przed kolejnymi wyborami wycofano się z tego rozwiązania po ostrzeżenia French Cybersecurity Agency (ANSSI), która uznała system za zbyt podatny na ataki cybernetyczne. Po pięciu latach prac i wprowadzeniu nowych zabezpieczeń ponownie umożliwiono głosowanie online dla obywateli francuskich za granicą, ale system nadal nie działał w pełni efektywnie, m.in. w 2023 roku sądy unieważniły wyniki w dwóch okręgach wyborczych z powodu błędów w dystrybucji kodów dostępu, zaś w 2024 roku serwis do głosowania miał awarie uniemożliwiającą dostęp części użytkowników[20]. Z projektów wprowadzenia cyfrowych technologii umożliwiających głosowanie w wyborach wycofały się również m.in. Szwajcaria, Norwegia, Finlandia, Irlandia i Holandia.

Obawy o bezpieczeństwo wyborów wzrosły dodatkowo po rosyjskiej ingerencji w amerykańską kampanię wyborczą w 2016 roku, która miała na celu podważenie zaufania obywateli do systemu demokratycznego oraz zdyskredytowanie kandydatki Partii Demokratycznej w wyborach prezydenckich Hillary Clinton. Skuteczność rosyjskich działań oraz skala ataku zaskoczyła amerykańskie instytucje rządowe i uwidoczniła liczne luki w systemie ochrony wyborów USA. W raporcie Office of the Director of National Intelligence (ODNI) opublikowanym w 2017 roku stwierdzono, że rosyjskie służby wywiadowcze, na polecenie prezydenta Władimira Putina, przeprowadziły zaawansowaną i wieloaspektową operację w celu podważenia zaufania do demokratycznego procesu wyborczego w USA. Jednym z jej kluczowych elementów były ataki hackerskie na systemy Partii Demokratycznej i publikacja skradzionych danych (m.in. maili Hillary Clinton) w serwisie WikiLeaks. Ponadto operacja obejmowała cyberataki na infrastrukturę wyborczą w różnych stanach oraz masową kampanię dezinformacji w mediach społecznościowych[21].

Po rosyjskim ataku przeprowadzono gruntowną reformę systemu ochrony wyborów w Stanach Zjednoczonych. Jednym z jej ważnych elementów była modernizacja infrastruktury wyborczej, a zwłaszcza wycofanie maszyn do głosowania typu Direct Recording Electronic (DRE), które umożliwiały tylko elektroniczne głosowanie i nie posiadały dodatkowego papierowego zapisu oddanych głosów. Jest to więc przykład ograniczenia technologii w pełni cyfrowych na rzecz systemów hybrydowych lub analogowych umożliwiających większe bezpieczeństwo i papierowy audyt. Jednocześnie należy podkreślić, że wymiana maszyn do głosowania typu DRE była przeprowadzona w bardzo dużej skali. Badania Brennan Center for Justice wykazały, że 2016 r. 22,4% zarejestrowanych wyborców mieszkało w okręgach, w których używano maszyn DRE bez papierowej kopii zapasowej, zaś w 2024 r. było to już tylko 1,4% amerykańskich wyborców[22].

Z kolei Holandia jest przykładem państwa, które całkowicie wycofało się z używania cyfrowych maszyn do głosowania. Holenderskie władze konsekwentnie wprowadzały elektroniczne systemy

[20] G. Wetherall-Grujić, French Overseas Voters Set New Online Voting Record, https://democracy-technologies.org/voting/france-new-online-voting-record/ (dostęp: 01.09.2025).

[21] Office of the Director of National Intelligence (ODNI), Assessing Russian activities and intentions in recent US elections: The analytic process and cyber incident attribution, 2017.

[22] R. Edlin, M. Maier, W. Stewart, Costs for Replacing Voting Equipment in 2024, https://www.brennancenter.org/our-work/analysis-opinion/costs-replacing-voting-equipment-2024 (dostęp: 01.09.2025).

w lokalach wyborczych od lat 60-tych XX wieku i z czasem zdecydowana większość głosów oddawana była z użyciem urządzeń cyfrowych. Jednak w 2006 roku grupa „Wij vertrouwen stemcomputers niet" ujawniła poważne luki w systemach zabezpieczeń elektronicznych maszyn do głosowania, które umożliwiały manipulację wynikami oraz naruszały tajność głosowania (przez emisję specyficznych sygnałów dźwiękowych). Kiedy niezależne komisje potwierdziły brak przejrzystości systemu holenderski rząd w 2008 roku podjął decyzję o wycofaniu cyfrowych maszyn z lokali wyborczych i powrót do głosowania za pomocą papierowych kart[23].

Bezpieczeństwo ekonomiczne

W aspekcie bezpieczeństwa ekonomicznego kluczowym elementem jest ochrony infrastruktury krytycznej, wrażliwych danych oraz technologii strategicznych przed zagrożeniami zewnętrznymi (m.in. cyberatakami, złośliwym oprogramowaniem i szpiegostwem przemysłowym). Atak na systemy związane m.in. z energetyką i zaopatrzeniem w surowce (elektrownie, sieci przesyłowe, gazociągi, rafinerie), wodociągami (ujęcia wody, przepompownie, oczyszczalnie), finansami (banki, systemy płatności, giełdy) czy łącznością (sieci telekomunikacyjne, centra danych, systemy 5G), mogłyby spowodować katastrofalne skutki dla bezpieczeństwa narodowego i gospodarki państwa. Dlatego w wielu sektorach związanych z infrastrukturą krytyczną stosuje się ograniczenia w użyciu technologii cyfrowych. Jednym z najskuteczniejszych sposobów zabezpieczania wrażliwych systemów przed zagrożeniami zewnętrznymi jest metoda *air gap* polegająca na fizycznym odizolowaniu systemów komputerowych lub sieci od zewnętrznych połączeń (w tym Internetu), co znacząco ogranicza ryzyko cyberataków i szpiegostwa przemysłowego. Air Gap jest stosowane m.in. w niemieckich elektrowniach jądrowych do ochrony systemów SCADA, czy też w holenderskim systemie zarządzania tamami przeciwpowodziowymi[24]. Choć Air Gap ogranicza stosowania cyfrowych technologii przez odcięcie systemów od zewnętrznych źródeł to nie eliminuje jednak wszystkich zagrożeń. Przykładem może być skuteczny cybersabotaż amerykańskich i izraelskich służb wywiadowczych z użyciem wirusa Stuxnet, który zaimplementowano do wewnętrznego systemu laboratorium w Natanz w Iranie w celu zniszczenia elementów infrastruktury służących do prac nad bronią jądrową.

Ograniczenia lub zakazy stosowaniu cyfrowych technologii dotyczą również urządzeń *Internet of Things* (IoT), czyli fizycznych obiektów wyposażonych w sensory, oprogramowanie i technologie komunikacyjne, które umożliwiają przetwarzanie i wymianę danych przez sieć internetową bez bezpośredniego udziału człowieka. Jest to jeden z najbardziej dynamicznie rozwijający się segmentów rynku technologicznego, który w 2024 stanowił już 19% jego globalnej wartości, zaś prognozy ekonomiczne wskazują, że do 2030 roku liczba urządzeń IoT na świecie przekroczy 40 miliardów[25]. Jednocześnie urządzenia IoT są bardzo podatne na ataki cybernetyczne, co

[23] B. Goldsmith, H. Ruthrauff, Case Study Report on Electronic Voting in the Netherlands, „International Foundation for Electoral Systems" 2009, s. 272–274.

[24] Porównaj: R.L. Perez, F. Adamsky, R. Soua, T. Engel, Forget the Myth of the Air Gap: Machine Learning for Reliable Intrusion Detection in SCADA Systems, „EAI Endorsed Transactions on Security and Safety" 2019, t. 6, nr 19; Waterschap Vechtstromen, The Watermachine: multifunctional area for flood protection and improved water quality - Kristalbad, Enschede, European Environment Agency (EEA), 2017.

[25] A. Krishnan, A. Taparia, D. Paraskevopoulos, E. Pasqua, State of IoT Summer 2024, s. 2-5.

stanowi powszechny problem z punktu widzenia konsumentów korzystających z IoT, ale również stwarza poważne zagrożenia dla instytucji państwowych. Dlatego Kongres Stanów Zjednoczonych uchwalił w 2020 roku ustawę Internet of Things Cybersecurity Improvement Act, która wprowadza zakaz zakupu i użytkowania przez amerykańskie agencje rządowe urządzeń IoT, które nie spełniają określonych wymogów bezpieczeństwa ustanawianych przez National Institute of Standards and Technology[26].

Ograniczenia w stosowaniu cyfrowych technologii w kontekście bezpieczeństwa ekonomicznego dotyczą również pojazdów autonomicznych. Choć samochody autonomiczne nie weszły jeszcze do powszechnego użytkowania i ciągle pozostają w fazie testowej, to prognozy wskazują, że w przyszłości zrewolucjonizują one rynek transportu i wpłyną na masową utratę miejsc pracy przez kierowców[27]. Poszczególne państwa wprowadzały pewne ograniczenia w testowaniu autonomicznych pojazdów na drogach publicznych z uwagi na bezpieczeństwo ruchu drogowego. Tak był m.in. w Niemczech, gdzie do 2021 roku regulacje prawne wymagały podczas testów fizycznej obecności kierowcy w autonomicznym pojeździe, który mógł przejąć sterowanie w sytuacjach awaryjnych[28]. Jednak istnieją też przykłady restrykcyjnej polityki państwa wobec branży autonomicznych pojazdów ze względu na ochronę miejsc pracy kierowców. W 2017 roku w Indiach rząd zakazał stosowania tej technologii tłumacząc, że w kraju o tak wysokim bezrobociu wprowadzenie samochodów autonomicznych mogłoby spowodować, że 7-8 milionów ludzi dodatkowo zostałoby pozbawionych pracy[29].

Bezpieczeństwo społeczne

W kontekście bezpieczeństwa społecznego trwa duża dyskusja na temat ograniczenia dostępu dzieci i młodzieży do urządzeń cyfrowych (zwłaszcza smartfonów) podczas zajęć w szkole. W raporcie UNESCO „Global Education Monitoring Report 2023" wskazano, że nadużywanie telefonów podczas lekcji obniża koncentrację i wyniki oraz może wpływać na pogłębienie dysproporcji między uczniami o różnym statusie materialnym. Jednocześnie jednak podkreślono, że decyzje o zakazie telefonów nie powinny mieć uniwersalnego charakteru tylko wynikać z analizy lokalnych uwarunkowań, bez presji technologicznej lub komercyjnej. W raporcie podano również, że w 2023 roku tylko 14% krajów na świecie prawnie zakazywało używania telefonów w szkołach[30]. Należy jednak zaznaczyć, że jest wśród nich bardzo duża reprezentacja państw członkowskich Unii Europejskiej. Jedynie Dania, Polska i Niemcy nie wprowadziły dotąd ogólnokrajowego zakazu używania telefonów komórkowych przez uczniów (choć szkoły mogą wprowadzać własne

[26] U.S. Congress, Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. 116-207, 134 Stat. 1001.

[27] R. Kurzweil, The Singularity Is Nearer: When We Merge with AI, 2024, s. 219.

[28] M. Urlich, Autonomously driving cars and the lawin Germany, „Wiadomości Ubezpieczeniowe" 2019, t. 4, nr 2019/4, s. 18–19.

[29] S. Edelstein, India Moves to Ban Self-Driving Cars to Protect Jobs, https://www.thedrive.com/tech/12830/india-moves--to-ban-self-driving-cars-to-protect-jobs (dostęp: 01.09.2025).

[30] UNESCO, Global Education Monitoring Report 2023: Technology in education – A tool on whose terms?, 2023, s. 158.

ograniczenia). Pozostałe państwa UE zakazały lub znacznie ograniczyły używania tego typu urządzeń w szkołach podstawowych i średnich[31].

Ograniczenia używania cyfrowych technologii dotyczą również sektora telemedycyny, której skokowy wzrost nastąpił podczas pandemii Covid-10. Według danych z raportu „The COVID-19 Pandemic and the Future of Telemedicine" w 2020 roku 21% wszystkich konsultacji lekarskich w krajach OECD odbyło się zdalnie (wzrost o 11%). Ponadto duża część państw OECD podczas kryzysu Covid-19 zliberalizowała swoje przepisy prawne dotyczące usług medycznych świadczonych zdalnie (np. zniosła wymóg fizycznej obecności pacjenta) i przepisywania recept online. Jednak w 16 przypadkach były to tylko rozwiązania tymczasowe i po zakończeniu pandemii przywrócono bardziej restrykcyjne regulacje. Na przykład w Korei Południowej telemedycyna jest obecnie dopuszczalna, ale tylko na najwyższych poziomach alertu epidemicznego[32].

Z bezpieczeństwem społecznym jest również związana ochrana danych osobowych. Ma to istotne znaczenie zwłaszcza w państwach Unii Europejskiej, gdzie obowiązują przepisy RODO. Z tego powodu dynamiczny rozwój sztucznej inteligencji, a zwłaszcza dużych modeli językowych budzi szereg wątpliwości dotyczących standardów ochrony prywatności. Było to podstawą podjęcia działań przez włoski Urząd Ochrony Danych Osobowych (Garante per la Protezione dei Dati Personali), który w marcu 2023 roku tymczasowo zablokowała dostęp do ChatGTP na obszarze Włoch. Agencja wskazała na brak przejrzystości w zakresie przetwarzania danych użytkowników oraz potencjalne ryzyko dla prywatności, zwłaszcza w przypadku osób niepełnoletnich. W rezultacie OpenAI twórca ChatGTP musiało dostosować swój model do wymagań RODO[33]. Z podobnych powodów w styczniu 2025 roku zablokowano na terenie Włoch chiński model DeepSeek zaraz po jego debiucie na rynku.

Bezpieczeństwo ekologiczne

W aspekcie bezpieczeństwa ekologicznego ograniczenia lub zakazy używania cyfrowych technologii wiążą się najczęściej z ich negatywnym wpływem na środowisko naturalne, emisją CO_2, lub nadmiernym zużywaniem surowców. Restrykcje są wprowadzane zarówno przez instytucje międzynarodowe i państwa, jak też lokalne społeczności, które chcą chronić unikalne ekosystemy.

Na poziomie międzynarodowym przykładem jest regulacja Unii Europejskiej dotycząca ekoprojektu dla produktów zrównoważonych (ESPR). Rozporządzenie stanowi kluczowy element strategii Unii Europejskiej na rzecz bezpieczeństwa ekologicznego, integrując wymogi zrównoważonego projektowania produktów oraz ograniczając negatywny wpływ technologii cyfrowych na środowisko. Rozporządzenie umożliwia Komisji Europejskiej wprowadzanie zakazów stosowania technologii o wysokim wpływie środowiskowym, co w praktyce oznacza ograniczenie produkcji urządzeń o krótkiej żywotności oraz eliminację technologii, które nie spełniają nowych

[31] L. Chadwick, Which countries in Europe have banned or want to restrict smartphones in schools?, https://www.euronews.com/next/2024/12/29/which-countries-in-europe-have-banned-or-want-to-restrict-smartphones-in-schools (dostęp: 01.09.2025).

[32] OECD, The COVID-19 Pandemic and the Future of Telemedicine. OECD Health Policy Studies, OECD Publishing, 2023, 28-36.

[33] S. Milano, J.A. McGrane, S. Leonelli, Large language models challenge the future of higher education, „Nature Machine Intelligence" 2023, t. 5, nr 4, s. 332–333.

wymogów, m.in. takich jak brak możliwości wymiany baterii czy nieefektywne zarządzanie energią[34].

Z kolei państwa skandynawskie zastosowały restrykcyjną politykę wobec przemysłu kryptowalut ze względu na bardzo wysokie zużycie energii elektrycznej generowane przez ten sektor. W Norwegii nowe przepisy wprowadziły obowiązek formalnej rejestracji wszystkich centrów danych zajmujących się kopaniem kryptowalut, co pozwoliło władzom na monitorowanie ich działalność oraz blokowanie projektów uznanych za „niepożądane". Dodatkowo zniesienie ulg podatkowych na energię elektryczną wykorzystywaną przez koparki kryptowalut znacząco wpłynęło na rentowność tego sektora. Podobna sytuacja miała miejsce w Szwecji, której północne regiony uchodziły za jedne z głównym europejskich centrów lokacji koparek kryptowalut. Jednak najwyższa w Europie podwyżka podatków dla przemysłu kryptowalut wprowadzona przez szwedzki rząd w 2023 roku (podatek wzrósł o 6000%) spowodowało exodus firm z tego sektora i zmniejszenie aktywności koparek kryptowalut w takich regionach jak Norrbotten i Västerbotten nawet o 90%[35].

Interesującym elementem w ograniczaniu technologii cyfrowych w kontekście bezpieczeństwa ekologicznego jest inicjatywa francuskich agencji rządowych ARCEP, ADEME i ARCOM postulujących zmniejszenie rozdzielczości streamingu wideo. W ramowym dokumencie ekoprojektowania usług cyfrowych z 2024 roku oficjalnie zarekomendowano platformom streamingowym nadającym we Francji przejście z rozdzielczości 4K na domyślną rozdzielczość 720p dla trybu „standardowego" i 480p dla trybu „oszczędności energii" w usługach VOD. Ponadto wskazano łącznie 78 wytycznych mających na celu istotną redukcję środowiskowego śladu cyfrowego, zmniejszenia zużycia energii i emisji CO_2 związanych z transferem danych. Platformy streamingowe ignorujące zalecenia mogą podlegać kontrolom i sankcjom finansowym[36].

Z kolei w Ameryce Południowej w regionach Amazonii lokalne społeczności wprowadziły zakaz używania systemów GPS. Badania naukowe wykazały, że ścieżki wytyczane za pomocą technologii GPS przez turystów i firmy wydobywcze prowadziły do tworzenia sztucznych krawędzi leśnych, które wpływały na zmianę mikroklimatu (m.in. wzrost temperatury, spadek wilgotności) i przyspieszały obumieranie drzew. Ponadto współrzędne GPS były wykorzystywane do nielegalnego pozyskiwania drewna, wydobycia złota lub zakładania plantacji. Dlatego społeczność Cofán w Ekwadorze wprowadziła zakaz udostępniania współrzędnych świętych miejsc (m.in. góry Marudi), a w 2022 r. Sąd Konstytucyjny uznał prawo Cofán do konfiskaty sprzętu i wydalania intruzów ze swego terytorium. Natomiast w Brazylii społeczność Borari zabroniła przewodnikom turystycznym korzystania z GPS na terenach chronionych. Grzywna za złamanie zakazu

[34] European Union, Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for setting ecodesign requirements for sustainable products.

[35] N. Smith, Countries Say No to Energy Guzzling Bitcoin Mines, https://www.greenpeace.org/usa/countries-say-no-to-bitcoin-mines/ (dostęp: 01.09.2025).

[36] Arcep, Arcom, ADEME, General Policy Framework for the Ecodesign of Digital Services, 2024.

wynosi 5000 BRL, a jako dowody w postępowaniach sądowych są wykorzystywane nagrania z fotopułapek z geotagami[37].

Podsumowanie

Analiza prawnych zakazów i ograniczeń w stosowaniu cyfrowych technologii w zakresie bezpieczeństwa militarnego, politycznego, ekonomicznego, społecznego i ekologicznego pozwoliła pozytywnie zweryfikować hipotezę roboczą oraz wskazać na kilka kluczowych dylematów z którymi musza się mierzyć państwa demokratyczne we współczesnym świecie.

Po pierwsze, jest to dążenie do jak najlepszego wykorzystania możliwości jakie stwarza cyfrowa rewolucja, a zwłaszcza dynamiczny rozwój sztucznej inteligencji i autonomicznych urządzań. Może to zapewnić szybki wzrost gospodarczy, podniesienie poziomu zamożności obywateli oraz standardów życia. Dodatkowo zastosowanie innowacyjnych technologii może wpłynąć na zwiększenie bezpieczeństwa państwa i uzyskanie przewagi nad potencjalnym wrogim podmiotem. Dlatego państwa inwestują i wspierają cyfrową rewolucję i chcą być beneficjentami zmian jakie niesie ze sobą to zjawisko.

Po drugie, szybki rozwój cyfrowych technologii stwarza również liczne nowe zagrożenia dla bezpieczeństwa państwa. Co więcej, mimo wielu wysiłków nie wszystkie tendencje związane z wpływem na bezpieczeństwo da się przewidzieć wcześniej. W praktyce kolejne zagrożenia ujawniają się zazwyczaj po pewnym czasie od wprowadzenia danej technologii na rynek. Jest to paradoks zjawiska cyfrowej rewolucji, w którym jednocześnie zachodzą procesy zwiększające bezpieczeństwo państwa oraz stwarzające nowe i skomplikowane zagrożenia. Państwa muszą więc wykazać dużą elastyczność i szukać odpowiedniego balansu między innowacją a ryzykiem. Z jednej strony nie mogą hamować rozwoju cyfrowych technologii, bo to spowoduje, że nie nadążą za tempem zmian technologicznych i pozostaną w tyle. Z drugiej strony muszą uważnie śledzić wpływ tych procesów na bezpieczeństwo i reagować wprowadzając ograniczenia i zakazy.

Po trzecie, dynamiczny rozwój nowych technologii bardzo często wyprzedza regulacje prawne. Wiąże się to z kolejnym problemem, który muszą rozwiązać państwa oraz instytucje międzynarodowe. Jest to zasadnicze pytanie o to, czy wczesne zmiany legislacyjne dotyczące danej technologii nie wpłynął negatywnie na jej rozwój lub zahamują możliwości zaawansowanych badań. Dlatego można zaobserwować typową tendencję do odwlekania w czasie uchwalania nowych przepisów prawnych i dłuższej obserwacji trendów. Duże znaczenie odgrywają w tym względzie doświadczenia państw, które są pionierami we wdrażaniu określonej technologii lub zastosowały nowe rozwiązania prawne w odpowiedzi na zagrożenia bezpieczeństwa.

Po czwarte państwa demokratyczne wprowadzając zakazy i ograniczenia w stosowaniu technologii cyfrowych ze względu na bezpieczeństwo narodowe muszą również uwzględnić bardzo istotny czynnik zachowania standardów praw i wolności obywatelskich. To bardzo istotna różnica w porównaniu z państwami niedemokratycznymi, które często pod pozorem ochrony

[37] A. Moloney, In Ecuador's Amazon, indigenous forest defense gains legal ground, https://www.context.news/nature/long-read/in-ecuadors-amazon-indigenous-forest-defense-gains-legal-ground (dostęp: 01.09.2025).

bezpieczeństwa państwa łamią prawa człowieka. W przypadku systemów demokratycznych ochrona praw i wolności obywatelskich stanowi podstawę funkcjonowania państwa, a odpowiednie instytucje stoją na straży ich przestrzegania. Wszelkie zakazy i ograniczenia muszą więc być zgodne z konstytucyjnymi zasadami.

Wreszcie po piąte, w państwach demokratycznych zauważalne są pewne napięcia między nieuniknionym postępem technologicznych a uniwersalnymi zasadami etycznymi. Dotyczy to zwłaszcza tak kontrowersyjnej kwestii jak Lethal Autonomous Weapon Systems. Brak międzynarodowych regulacji i mechanizmów kontroli sprawia, że państwa zmuszone są do podejmowania trudnych moralnie decyzji, czy dalej rozwijać LAWS (które mogą stać się istotnym elementem przyszłych wojen), czy też ze względu na ogólnoludzkie wartości ograniczyć badania nad tą bronią (co może wiązać się z utratą przewagi nad przeciwnikiem). Mamy więc tu do czynienia z kolejnym konfliktem między efektywnością operacyjną a normami etyczno-prawnymi.

BIBLIOGRAFIA

REFERENCES LIST

PIŚMIENNICTWO

LITERATURE

Arcep, Arcom, ADEME, *General Policy Framework for the Ecodesign of Digital Services*, 2024.

Bureau of Justice Assistance, *Developing a policy on the use of social media in intelligence and investigative activities: Guidance and recommendations*, 2013.

Buzan B., *People, States and Fear: The National Security Problem in International Relations*, 1983.

Campaign to Stop Killer Robots, *Country Views on Killer Robots*, 2019.

Chadwick L., *Which countries in Europe have banned or want to restrict smartphones in schools?*, https://www.euronews.com/next/2024/12/29/which-countries-in-europe-have-banned-or-want-to-restrict-smartphones-in--schools .

Edelstein S., *India Moves to Ban Self-Driving Cars to Protect Jobs*, https://www.thedrive.com/tech/12830/india--moves-to-ban-self-driving-cars-to-protect-jobs.

Edlin R., Maier M., Stewart W., *Costs for Replacing Voting Equipment in 2024,* https://www.brennancenter.org/our-work/analysis-opinion/costs-replacing-voting-equipment-2024.

Frantz E., Kendall-Taylor A., Wright J., *Digital Repression in Autocracies*.

Goldsmith B., Ruthrauff H., *Case Study Report on Electronic Voting in the Netherlands*, „International Foundation for Electoral Systems", 2009.

Haas M.C., Fischer S.-C., *The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order*, „Contemporary Security Policy" 2017, t. 38, nr 2.

Kamiński M., *Ewolucja wywiadu jako instytucji państwa*, Warszawa 2021.

Kamiński M.A., *Obrona Narodowa Republiki Estonii*, Toruń 2018.

Kenez L., *Turkish military to enforce strict social media ban for soldiers after security breaches and ambushes*, https://nordicmonitor.com/2024/06/turkish-military-enforces-strict-social-media-ban-for-soldiers-after-security-breaches-and-ambushes.

Kretzmer D., *Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Defence?*, „The European Journal of International Law" 2005, t. 16, nr 2.

A. Krishnan, A. Taparia, D. Paraskevopoulos, E. Pasqua, *State of IoT Summer 2024*, 2024.

Kurzweil R., *The Singularity Is Nearer: When We Merge with AI*, 2024.

Liu H.-Y., *Categorization and legality of autonomous and remote weapons systems*, „International Review of the Red Cross" 2012, t. 94, nr 886.

Milano S., McGrane J.A., Leonelli S., *Large language models challenge the future of higher education*, „Nature Machine Intelligence" 2023, t. 5, nr 4.

Moloney A., *In Ecuador's Amazon, indigenous forest defense gains legal ground*, https://www.context.news/nature/long-read/in-ecuadors-amazon-indigenous-forest-defense-gains-legal-ground.

Nnamdi N., Eniola B.O., Abegunde B., *Examining Lethal Autonomous Weapons through the Lens of International Humanitarian Law*, „Scholars International Journal of Law, Crime and Justice" 2023, t. 6, nr 06.

NSW Electoral Commission, *Technology assisted voting: Final review report*, 2023.

OECD, *The COVID-19 Pandemic and the Future of Telemedicine. OECD Health Policy Studies*, OECD Publishing, 2023.

Perez R.L., Adamsky F., Soua R., Engel T., *Forget the Myth of the Air Gap: Machine Learning for Reliable Intrusion Detection in SCADA Systems*, „EAI Endorsed Transactions on Security and Safety" 2019, t. 6, nr 19.

Sanchez E.J., *Intelligence Collection, Covert Operations, and International Law*, „Intelligencer: Journal of U.S. Intelligence Studies" 2017, t. 23, nr 2.

Smith N., *Countries Say No to Energy Guzzling Bitcoin Mines*, https://www.greenpeace.org/usa/countries-say--no-to-bitcoin-mines.

UNESCO, *Global Education Monitoring Report 2023: Technology in education – A tool on whose terms?*, 2023.

Urlich M., *Autonomously driving cars and the law in Germany*, „Wiadomości Ubezpieczeniowe" 2019, t. 4, nr 2019/4.

Waterschap Vechtstromen, *The Watermachine: multifunctional area for flood protection and improved water quality - Kristalbad, Enschede*, European Environment Agency (EEA), 2017.

Wetherall-Grujić G., *French Overseas Voters Set New Online Voting Record*, https://democracy-technologies.org/voting/france-new-online-voting-record.

ŹRÓDŁA

SOURCES

Department of Defense, *Autonomy in weapon systems (DoD Directive 3000.09)*, 2023.

Department of Defense, *Use of Geolocation-Capable Devices, Applications, and Services*, 2018.

Director of National Intelligence, *Summary of Information Regarding U.S. Counterterrorism Strikes Outside Areas of Active Hostilities*, 2016.

European Union, *Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for setting ecodesign requirements for sustainable products*, 2024.

National Electoral Committee of Estonia, *Election results*, https://data.ipu.org/parliament/EE/EE-LC01/election/EE-LC01-E20230305.

Office of the Director of National Intelligence (ODNI), *Assessing Russian activities and intentions in recent US elections: The analytic process and cyber incident attribution*, 2017.

Panel of Experts on Libya, *Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973, S/2021/229*, 2021.

United Nations General Assembly, *Lethal autonomous weapons systems (Resolution 78/241, UN Doc A/79/251)* [w:] 2024.

U.S. Congress, Internet of Things Cybersecurity Improvement Act of 2020, Pub. L. 116-207, 134 Stat. 1001.

U.S. Congress, National Security Act of 1947 (Section 503), Pub. L. 80–253, Large 61 Stat. 495.

OPEN ACCESS

Copyright (c) 2025 Bogusław Pacek and Mariusz Antoni Kamiński

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License