„Krytyka Prawa", tom 15, nr 1/2023, s. 115–133, ISSN 2080-1084, e-ISSN 2450-7938, © 2023 Author.

ANASTAZJA GAJDA[1]

Wykorzystywanie systemów sztucznej inteligencji (SI) na zewnętrznych granicach Unii Europejskiej. Możliwości, zagrożenia i wyzwania[2]

Wpłynął: 21.05.2022. Akceptacja:22.08.2022

Streszczenie

Unia Europejska i jej państwa członkowskie coraz częściej sięgają po technologie sztucznej inteligencji (SI) w celu wzmocnienia kontroli granicznych. Jest to jeden z przejawów szerszego trendu podążania w kierunku tzw. inteligentnych granic Unii.

Artykuł prezentuje unijne inicjatywy dotyczące opracowywania i wdrażania technologii cyfrowych opartych na SI w celu poprawy kontroli i bezpieczeństwa granic zewnętrznych Unii. Analizie zostały poddane główne kierunki wykorzystywania SI, tj. w zakresie automatycznego rozpoznawania odcisków palców i twarzy, wykrywania emocji, profilowania algorytmicznego oraz monitorowania, analizy i prognozowania migracji.

Celem artykułu jest, z jednej strony, ukazanie, iż ostrożne wdrażanie i wykorzystywanie technologii opartej na SI w celu kontroli granic może przynieść wiele korzyści. Z drugiej zaś strony, korzyści te należy jednak zrównoważyć ze znaczącym zagrożeniem, jakie stwarzają te technologie dla ochrony praw podstawowych jednostki.

Słowa kluczowe: Unia Europejska, sztuczna inteligencja, zewnętrzne granice Unii, strefa Schengen, projekt IborderCtrl, projekt ROBORDER.

---

[1] Prof. SGH, dr hab. Anastazja Gajda – Szkoła Główna Handlowa w Warszawie (Polska); e-mail: agajda2@sgh.waw.pl; ORCID: 0000-0003-4446-1055.

[2] Badania wykorzystane w artykule nie zostały sfinansowane przez żadną instytucję.

 DOI: 10.7206/kp.2080-1084.574

„Krytyka Prawa", tom 15, nr 1/2023, s. 115–133, ISSN 2080-1084, e-ISSN 2450-7938, © 2023 Author.

ANASTAZJA GAJDA

Use of Artificial Intelligence (AI) Systems at the External Borders of the European Union. Opportunities, Threats and Challenges[3]

Abstract

The European Union and its Member States are increasingly turning to artificial intelligence (AI) technologies to enhance border controls. This is one of the manifestations of a broader trend of moving towards the so-called smart borders of the Union.

This article presents EU initiatives on the development and implementation AI-based digital technologies to improve the control and security of the Union's external borders. The main directions of the use of AI were analyzed, i.e. in the field of automatic recognition of fingerprints and faces, emotion detection, algorithmic profiling and monitoring, analysis and forecasting of migration.

The aim of the article is, on the one hand, to show that the careful implementation and use of AI-based technology for border control can bring many benefits. On the other hand, however, these benefits must be balanced with the significant threat posed by these technologies to the protection of the fundamental rights of the individual.

Keywords: European Union, artificial intelligence, external borders of the Union, Schengen area, IborderCtrl project, ROBORDER project.

[3] The research in this article has not been supported financially by any institution.

Wprowadzenie

Zabezpieczanie granic zewnętrznych Unii Europejskiej (dalej: UE lub Unii) i skuteczne nimi zarządzanie wymaga coraz lepszego wykorzystywania możliwości oferowanych przez najnowsze technologie, w tym przez wielkoskalowe systemy informacyjne UE. Systemy te tworzono w ciągu szeregu lat przede wszystkim właśnie z myślą o zapewnianiu bezpieczeństwa oraz kontroli granic i migracji. W ciągu ostatnich dziesięcioleci utworzono wiele takich systemów służących przechowywaniu danych osobowych obywateli państw trzecich, którzy chcą się dostać do strefy Schengen[4]. Każdy z tych systemów cechują odrębne: cele, zadania, podstawy prawne, zasady tworzenia i korzystania z nich, grupy użytkowników i kontekst instytucjonalny[5].

Zakłada się, że do końca 2023 r. wszystkie te wielkoskalowe systemy dotyczące granic, migracji, bezpieczeństwa i sprawiedliwości Unii będą w pełni operacyjne[6] i interoperacyjne (wszystkie one zostaną ze sobą połączone)[7]. Zagwarantuje to, że będą one „porozumiewać się" między sobą, tak by przez połączenie informacji nie zabrakło żadnej kontroli oraz by organy krajowe dysponowały kompletnymi, wiarygodnymi i dokładnymi informacjami, z pełnym poszanowaniem wymogów w zakresie ochrony danych[8].

Jednocześnie zarówno UE, jak i jej państwa członkowskie, podejmując wysiłki na rzecz wzmocnienia kontroli granicznych, skutecznego rozwiązywana problemu nielegalnej imigracji oraz zwalczania przestępczości transgranicznej, coraz częściej

---

4 Obecnie funkcjonujące wielkoskalowe systemy informacyjne Unii to: System Informacyjny Schengen (SIS), Wizowy System Informacyjny (VIS), Europejski zautomatyzowany system rozpoznawania odcisków palców (Eurodac), Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS), System wjazdu/wyjazdu, Europejski systemu przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN).

5 Zob. szeroko na ten temat: A. Gajda, *Najnowsze technologie i zarządzanie granicami zewnętrznymi Unii Europejskiej*, „Krytyka Prawa" 2020, 12(4), s. 50–69.

6 Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego i Rady, *Strategia na rzecz w pełni funkcjonującej i odpornej strefy Schengen*, COM(2021) 277 final, Bruksela 2.06.2021, s. 8 (dalej: *Strategia*).

7 C.B. Casagran, *Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU*, „Human Rights Law Review" 2021, 21(2), s. 433–457.

8 Szerzej na temat interoperacyjności zob.: A. Gajda, *Interoperacyjność unijnych systemów w zakresie bezpieczeństwa, ochrony granic i zarządzania migracjami*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace" 2019, 1(37), s. 143–165.

 DOI: 10.7206/kp.2080-1084.574

sięgają po technologie sztucznej inteligencji (dalej: SI)[9]. W *Strategii* z czerwca 2021 r. wyraźnie podkreśla się potrzebę jak najlepszego wykorzystania istniejących i przyszłych technologii w zarządzaniu granicami. Uwydatnia się także znaczenie opracowywania i wdrażania technologii sztucznej inteligencji na potrzeby egzekwowania prawa.

Artykuł przedstawia unijne inicjatywy dotyczące opracowywania i wdrażania technologii cyfrowych opartych na SI w celu poprawy kontroli i bezpieczeństwa granic zewnętrznych Unii. Analizie zostały poddane główne kierunki wykorzystywania SI, tj. w zakresie automatycznego rozpoznawania odcisków palców i twarzy, wykrywania emocji, profilowania algorytmicznego oraz monitorowania, analizy i prognozowania migracji. Zwraca się przy tym uwagę na zagrożenia płynące z niekontrolowanego stosowania technologii SI, potencjalnych naruszeń praw podstawowych jednostki, por. stronniczość i dyskryminacja, ochrona i bezpieczeństwo danych osobowych, niezgodne z prawem profilowanie, przejrzystość finansowania przez UE badań nad wykorzystywaniem systemów SI. Uwzględniono także aktualną sytuację w Unii w zakresie procedur prawodawczych, które zmierzają do przyjęcia rozporządzenia dotyczącego SI.

Sztuczna inteligencja w pracach Unii Europejskiej

Sztuczna inteligencja jest już częścią naszego życia – to nie jest *science fiction*. SI jest obecna w naszej rzeczywistości w różnych sytuacjach. W zasadzie korzystamy z niej codziennie[10].

W Unii dominuje pogląd, że rozwój systemów sztucznej inteligencji powinien odbywać się przy przestrzeganiu określonych reguł etycznych i prawnych. Takie podejście ma zapewnić rozwój sztucznej inteligencji respektujący zasady człowieczeństwa[11]. Świadczy o tym przedstawiony 21 kwietnia 2021 r. przez Komisję Europejską *Wniosek dotyczący rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji* (dalej: *Wniosek*)[12]. *Wniosek* jest pierwszym tego typu aktem

---

9 C. Dumbrava, *Artificial intelligence at EU borders. Overview of applications and key issues*, European Parliament, European Parliamentary Research Service PE 690.706 – July 2021, s. 1.

10 M. Hildebrandt, *The Artificial Intelligence of European Union Law*, „German Law Journal" 2020, 21(1), s. 74–79.

11 G. Carriço, *The EU and artificial intelligence: A human-centred perspective*, „European View" 2018, 17(1), s. 29–36.

12 Komisja Europejska, *Wniosek rozporządzenia Parlamentu Europejskiego i Rady ustanawiający zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniający niektóre akty ustawodawcze Unii*, COM(2021) 206 final, Bruksela, 21.04.2021 oraz *Załączniki do Wniosku* COM(2021) 206 final, Bruksela 21.04.2021.

prawnym na świecie. Stanowi konsekwencję podejmowanych w ciągu ostatnich lat przez różne organy UE licznych inicjatyw z zakresu prawnego uregulowania zjawiska sztucznej inteligencji[13].

Wniosek nie dotyczy wprost systemów sztucznej inteligencji, lecz sposobu, w jaki te systemy są wykorzystywane[14]. Komisja wyszła bowiem z założenia, że im wyższe jest ryzyko dla praw i wolności człowieka związane z konkretnym systemem, tym większe obowiązki dla jego twórców i podmiotów ten system wdrażających. W rezultacie systemy SI zostały podzielone na cztery kategorie, zgodnie z poziomem ryzyka, jakie niesie konkretny sposób ich użycia: minimalne, niskie, wysokie i niedopuszczalne.

Dla niniejszych rozważań istotne znaczenie ma to, że KE za systemy wysokiego ryzyka uznaje m.in. systemy sztucznej inteligencji przeznaczone do zdalnej identyfikacji biometrycznej osób fizycznych „w czasie rzeczywistym" i *post factum* (zob. załącznik nr III *Wniosku*). Korzystanie z nich w czasie rzeczywistym na potrzeby ochrony porządku publicznego w miejscach publicznych jest co do zasady zabronione. Wyjątki od tej zasady są ścisłe określone i regulowane. Tego rodzaju zastosowanie wymaga uzyskania zezwolenia sądu lub innego niezależnego organu oraz musi być odpowiednio ograniczone w odniesieniu do czasu, zasięgu geograficznego i przeszukiwania baz danych.

Choć to pierwszy projekt przyszłych przepisów unijnych i zapewne jeszcze podlegał będzie modyfikacjom, to można założyć, że podstawowe zasady (np. podejście oparte na ocenie ryzyka czy wytyczne skierowane do producentów i użytkowników SI) zostaną zachowane. Przyjęcie konkretnych rozwiązań prawnych ma sprawić, że Unia stanie się globalnym centrum wiarygodnej SI i będzie odgrywać główną rolę w jej dalszym rozwoju, uwzględniając zagrożenia z nią związane. Według założeń dzięki proponowanym przepisom systemy SI stosowane w UE staną się bardziej bezpieczne, przejrzyste, etyczne, bezstronne i kontrolowane przez człowieka.

---

13 *Wniosek* określa system sztucznej inteligencji jako „oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję" (art. 3 pkt 1 *Wniosku*).

14 M. Świerczyński, Z. Więckowski, *Sztuczna inteligencja w prawie międzynarodowym. Rekomendacje wybranych rozwiązań*, Warszawa 2021, s. 30–32.

 DOI: 10.7206/kp.2080-1084.574

Sztuczna inteligencja na granicach zewnętrznych Unii Europejskiej

W ostatnich latach zarówno KE, jak i wyspecjalizowane agencje unijne zajmujące się m.in. ochroną granic zewnętrznych UE (przede wszystkim Europejska Agencja Straży Granicznej i Przybrzeżnej – Frontex i Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości – eu-LISA) prowadziły badania, w których szczegółowo analizowano potencjalne możliwości stosowania SI w zarządzaniu granicami zewnętrznymi, przeciwdziałaniu nielegalnej imigracji i zapewnianiu bezpieczeństwa[15]. W 2020 r. Komisja powołała nawet Grupę ekspertów ds. sztucznej inteligencji w dziedzinie spraw wewnętrznych[16] w celu pomocy w przygotowaniu propozycji legislacyjnych i inicjatyw politycznych dotyczących sztucznej inteligencji[17].

Analiza raportów z przeprowadzonych badań wskazuje przede wszystkim na cztery główne obszary zastosowań sztucznej inteligencji, z których UE korzysta lub rozważa wykorzystanie w kontekście kontroli granic zewnętrznych i zapewniania ich bezpieczeństwa. Są to:

1) identyfikacja biometryczna (zautomatyzowana technologia rozpoznawania odcisków palców i twarzy),
2) technologie rozpoznawania emocji,
3) profilowanie algorytmiczne,
4) narzędzia SI do monitorowania, analizy i prognozowania migracji[18].

---

15 Zob.: Deloitte, *Opportunities and challenges for the use of artificial intelligence in border control, migration and security*, Vol. 1, *Main report*, May 2020, https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en (dostęp: 1.02.2022); Ecorys, *Feasibility study on a forecasting and early warning tool for migration based on Artificial Intelligence technology*, November 2020, https://op.europa.eu/lv/publication-detail/-/publication/946b0bc7-7006-11eb-9ac9-01aa75ed71a1/language-lv/format-PDF/source-search (dostęp: 1.02.2022); M.J. Flynn, *Study on technical requirements for data spaces in law enforcement*, June 2020, https://op.europa.eu/de/publication-detail/-/publication/0d02ee25-6c19-11eb-aeb5-01aa75ed71a1/language-de (dostęp: 1.02.2022); A. Renda, J. Arroyo, R. Fanni, M. Laurer, A. Sipiczki, T. Yeung, G. Maridis, M. Fernandes, G. Endrodi, S. Milio, V. Devenyi, S. Georgiev, G. de Pierrefeu, *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, April 2021, https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation (dostęp: 1.02.2022); eu-LISA, *Artificial Intelligence in the Operational Management of Large-scale IT Systems*, July 2020, https://www.eulisa.europa.eu/Publications/Reports/AI%20in%20the%20OM%20of%20Large-scale%20IT%20Systems.pdf (dostęp: 1.02.2022); Frontex, *Artificial Intelligence-based capabilities for European Border and Coast Guard*, March 2021, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf (dostęp: 1.02.2022).

16 Na temat Grupy i jej prac zob.: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3727&news=1 (dostęp: 1.02.2022).

17 Zob.: T. Bircan, E.E. Korkmaz, *Big data for whose sake? Governing migration through artificial intelligence*, „Humanities and Social Sciences Communications" 2021, 8(1), s. 1–5.

18 Zob.: A. Beduschi, *International migration management in the age of artificial intelligence*, „Migration Studies" 2021, 9(3), s. 576–596.

Zautomatyzowane technologie rozpoznawania odcisków palców i twarzy

W wielkoskalowych systemach informacyjnych UE dotyczących bezpieczeństwa granic coraz częściej uwzględnia się wykorzystywanie technologii biometrycznych w celu identyfikacji lub weryfikacji tożsamości. I tak, zautomatyzowana technologia identyfikacji odcisków palców jest obecnie wykorzystywana w trzech scentralizowanych systemach informacyjnych UE, tj. w systemach: SIS, Eurodac i VIS. Będzie wykorzystywana także w systemie wjazdu/wyjazdu oraz w systemie ECRIS-TCN, które mają się stać w pełni operacyjne w 2023 r.

Z kolei zautomatyzowana technologia rozpoznawania twarzy nie jest jeszcze używana w żadnym z tych systemów, ale we wszystkich systemach – z wyjątkiem ETIAS – ma przetwarzać obrazy twarzy w celu weryfikacji lub identyfikacji w najbliższej przyszłości. Wykorzystywanie systemów automatycznego rozpoznawania twarzy budzi wiele wątpliwości. Powszechnie uznaje się je jako jedne z najbardziej wrażliwych i podatnych na naruszenie praw podstawowych jednostki.

Warto wskazać, że istnieją różne rodzaje zastosowania rozpoznawania twarzy, m.in. weryfikacja/uwierzytelnianie (tj. porównywanie wizerunku twarzy obecnej osoby ze zdjęciem na dokumencie tożsamości, np. w ramach inteligentnych granic), identyfikowanie (tj. dopasowywanie zdjęcia do danych z danej bazy zdjęć) oraz wyodrębnianie wizerunku twarzy w czasie rzeczywistym z wykorzystaniem takich źródeł, jak materiały zarejestrowane przez system monitoringu wizyjnego i przeszukiwanie baz danych w celu dopasowania wizerunku. Każde z tych zastosowań ma inne konsekwencje pod względem ochrony praw podstawowych[19].

Bramki ABC (ang. *Automated Border Control*), czyli automatyczne bramki wykorzystywane do odprawy granicznej na lotniskach są przykładem wykorzystania technologii rozpoznawania twarzy[20]. Wraz ze stopniowym przyjmowaniem paszportów biometrycznych na całym świecie bramki ABC stają się powszechną formą kontroli bezpieczeństwa na lotniskach. Dzisiejsze systemy ABC obsługują szereg danych biometrycznych, w tym rozpoznawanie twarzy i (rzadziej) rozpoznawanie tęczówki. Bramka ABC dokonuje weryfikacji biometrycznej podróżnego – automatycznie porównuje dane zawarte w chipie biometrycznym dokumentu z wizerunkiem

[19] Zob. szeroko na ten temat: Fundamental Rights Agency, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, November 2019, s. 7, https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (dostęp: 1.02.2022).

[20] Szeroko na ten temat zob.: Frontex, *Best Practice Operational Guidelines for Automated Border Control (ABC) Systems*, September 2015, s. 10, https://frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_ABC.pdf (dostęp: 1.02.2022).

 DOI: 10.7206/kp.2080-1084.574

twarzy podróżnego i potwierdza, czy osoba przedstawiająca dokument do odprawy jest jego właścicielem.

Technologia rozpoznawania twarzy może być również wykorzystywana do nadzoru lotnisk i innych przestrzeni publicznych w czasie rzeczywistym poprzez analizę obrazu na żywo z kamer CCTV. Odbywa się to poprzez wyodrębnianie obrazów twarzy zarejestrowanych przez kamery i porównywanie ich z wizerunkami twarzy osób znajdujących się na listach obserwacyjnych. Jak jednoznacznie wynika z raportu z 2020 r.[21], w państwach unijnych bardzo szybko wdraża się systemy rozpoznawania twarzy do celów nadzoru publicznego, nie tylko na lotniskach, ale także w szkołach, na stadionach i w miejscach imprez masowych.

Pojawiają się głosy, że takie systemy automatycznego rozpoznawania twarzy absolutnie nie powinny być wykorzystywane do kontroli granicznej ani w przestrzeni publicznej[22]. Także Parlament Europejski (dalej: PE) w *Rezolucji z 6 października 2021 r.* (dalej: *Rezolucja*)[23] wezwał do przyjęcia moratorium na korzystanie z systemów rozpoznawania twarzy do działań organów ścigania, które mają na celu zdalną identyfikację poprzez rozpoznawanie twarzy w miejscach publicznych, a także przy automatycznych bramkach kontroli granicznej wykorzystywanych do odprawy granicznej na lotniskach.

PE zwrócił uwagę na ryzyko stronniczości algorytmów w zastosowaniach SI. Podkreślał jednocześnie, iż ludzki nadzór i silne uprawnienia prawne są potrzebne, aby zapobiec dyskryminacji przez SI, zwłaszcza w kontekście egzekwowania prawa lub przekraczania granic. Zdaniem PE ostateczne decyzje muszą zawsze podejmować ludzie, a osoby monitorowane przez systemy oparte na SI muszą mieć dostęp do środków odwoławczych.

Wspólne stanowisko dotyczące m.in. systemów automatycznego rozpoznawania twarzy wystosowały także Europejska Rada Ochrony Danych (dalej: EROD) i Europejski Inspektor Ochrony Danych (dalej: EIOD)[24]. Organy te uznały, że ze

---

21 F. Chiusi, S. Fischer, N. Kayser-Bril, M. Spielkamp (eds.), *Automating Society Report 2020*, AlgorithmWatch, October 2020, https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf (dostęp: 1.02.2022).

22 Zob.: *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*, 7.06.2021, https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf (dostęp: 1.02.2022).

23 Zob.: Parlament Europejski, *Rezolucja Parlamentu Europejskiego z dnia 6 października 2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych* (2020/2016(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PL.pdf (dostęp: 1.02.2022).

24 Europejska Rada Ochrony Danych – Europejski Inspektor Ochrony Danych, *Wspólna opinia 5/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji („akt w sprawie sztucznej inteligencji")*, 18.06.2021, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_pl (dostęp: 1.02.2022).

względu na niezwykle wysokie ryzyko, jakie stwarza zdalna biometryczna identyfikacja osób w przestrzeni publicznej, należy wprowadzić ogólny zakaz „jakiegokolwiek wykorzystywania sztucznej inteligencji do automatycznego rozpoznawania cech ludzkich w przestrzeni publicznej, takich jak rozpoznawanie twarzy, chodu, odcisków palców, DNA, głosu, uderzeń w klawisze i innych sygnałów biometrycznych lub behawioralnych, w jakimkolwiek kontekście"[25]. EROD i EIOD wskazują także na konieczność wprowadzenia zakazu stosowania systemów SI wykorzystujących dane biometryczne do podziału osób fizycznych na grupy ze względu na pochodzenie etniczne, płeć, orientację polityczną i seksualną lub inne powody, ze względu na które dyskryminacja jest zakazana z mocy art. 21 Karty Praw Podstawowych Unii Europejskiej[26].

Technologia rozpoznawania emocji

Celem technologii rozpoznawania emocji jest wykrywanie stanów psychicznych i emocji na podstawie badania mimiki twarzy, często w połączeniu z innymi cechami fizjonomicznymi (takimi jak kierunek spojrzenia, gesty, głos, tętno, temperatura ciała, przewodność skóry itp.)[27].

Systemy rozpoznawania emocji oparte na SI w dużej mierze opierają się na teoriach opracowanych przez amerykańskiego psychologa P. Ekmana, który twierdził, że kłamstwo wyzwala niewerbalne ślady behawioralne, które można rozpoznać właśnie poprzez analizę mimiki (wyrazu) twarzy. Opierając się na twierdzeniu Ekmana, że ludzkie emocje można sklasyfikować w sześciu podstawowych kategoriach, tj. gniew, obrzydzenie, strach, szczęście, smutek i zaskoczenie, naukowcy zajmujący się SI starali się zautomatyzować rozpoznawanie tych podstawowych emocji, gdy pojawią się one w mimice twarzy[28].

Aplikacje do rozpoznawania emocji oparte na SI są już wdrażane w wielu obszarach i kontekstach. Są wykorzystywane m.in. do monitorowania zdrowia psychicznego, wykrywania nieuczciwych roszczeń ubezpieczeniowych, monitorowania zaangażowania uczniów (w tym do pomocy dzieciom z autyzmem w rozwijaniu umiejętności społecznych i emocjonalnych), oceny kandydatów do pracy i wykry-

---

25 Ibidem, pkt 32.

26 Zob.: Karta Praw Podstawowych Unii Europejskiej, Dz. Urz. UE z 7 czerwca 2016 r. C 202/389.

27 J. Sánchez-Monedero, L. Dencik, *The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2020, 25(3), s. 413–430.

28 Chociaż P. Ekman podobno wyraził wątpliwości co do niezawodności technologii automatycznego wykrywania emocji, zob.: K. Crawford, *Atlas of AI: The Real Worlds of Artificial Intelligence*, Yale University Press 2021; C. Dumbrava, op. cit., s. 16–17.

 DOI: 10.7206/kp.2080-1084.574

wania potencjalnych złodziei sklepowych. Takie aplikacje są również reklamowane jako przydatne w zapobieganiu przestępczości, kontroli bezpieczeństwa czy kontroli granicznej[29].

W kontekście kontroli granic warto wskazać, że w 2007 r. amerykańska Administracja Bezpieczeństwa Transportu wprowadziła system kontroli pasażerów za pomocą technik obserwacyjnych w celu wykrywania przejawów strachu i stresu podróżnych, które mogą prowadzić do identyfikacji potencjalnych terrorystów. System był krytykowany zarówno jako nieskuteczny, jak i dyskryminujący[30]. Z kolei w 2021 r. Brytyjska Agencja Graniczna przetestowała w punktach kontroli granicznej na lotniskach narzędzia oparte na SI do oceny stresu, lęku i oszustwa w oparciu o analizę termiczną ciała i mimiki twarzy[31].

Projekt IborderCtrl – sztuczna inteligencja do wykrywania kłamstw

Technologie rozpoznawania emocji stanowią jedno z najbardziej kontrowersyjnych zastosowań sztucznej inteligencji na granicach. Obecnie systemy wykrywania emocji nie są jeszcze wdrożone na granicach unijnych. Warto jednak wskazać, że w ramach wielu projektów i inicjatyw finansowych przez UE badano i pilotowano takie technologie mające służyć wzmocnieniu kontroli granic zewnętrznych Unii.

Jednym z nich był projekt iBorder Ctrl (*Inteligentny Przenośny System Kontroli Granic*)[32], który został przetestowany w latach 2016–2019 na Węgrzech, Łotwie i w Grecji. Otrzymał 4,5 mln EUR dofinansowania ze środków unijnych w ramach programu „Horyzont 2020". Zastosowano w nim technologię, która służyła do analizowania 38 mikrogestów, tak aby rozpoznać, czy dana osoba kłamie, czy nie[33].

Procedura przekraczania granicy z wykorzystaniem iBorderCtrl miała na celu ograniczać interwencje celników do minimum, co przekładać się miało na przyspieszenie kontroli granicznych i przyczynić się do poprawy bezpieczeństwa

29 C. Dumbrava, op. cit., s. 16–17.

30 O. Schwartz, *Don't look now: why you should be worried about machines reading your emotions*, „The Guardian" 6.03.2019, https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science (dostęp: 1.02.2022).

31 C. Dumbrava, op. cit., s. 17.

32 Zob.: iBorderCtrl – *Intelligent Portable Border Control System*, https://cordis.europa.eu/project/id/700626 (dostęp: 1.02.2022).

33 Projekt iBorderCtrl zawierał komponent wykrywający kłamstwa o nazwie ADDS (*Automatic Deception Detection System*) firmy „Silent Talker", start-upu obsługiwanego przez naukowców z Manchester Metropolitan University.

granic[34]. Zastosowana w projekcie procedura była dwuetapowa. W pierwszym etapie osoba podróżująca wypełniała aplikację online i skanowała swoje dokumenty identyfikacyjne, w tym paszport z niezbędnymi wizami. Następnie odbywała ona zautomatyzowaną rozmowę z wirtualnym celnikiem (sztuczną inteligencją), który zadawał szereg pytań, m.in. o ich trasę podróży, zamiary czy o przedmioty znajdujące się w bagażu. W tym czasie kamera internetowa rejestrowała reakcje pytanych osób poprzez skanowanie ruchów twarzy i oczu. Odpowiednie zaprojektowane algorytmy na tej podstawie miały analizować, czy dana osoba kłamie, czy też mówi prawdę. Następnie podróżni otrzymywali kod QR, który był przedstawiany podczas rzeczywistej kontroli granicznej.

W przypadku zarejestrowania fałszywych odpowiedzi podróżny miałby być odsyłany do prawdziwych funkcjonariuszy straży granicznej, którzy podejmowaliby odpowiednie działania i decydowali, czy mogą przepuścić takiego „podejrzanego" podróżnego. Takie działania miałyby polegać m.in. na powtórnym sprawdzeniu dokumentów oraz informacji z poprzednich odpraw, a także na przeprowadzeniu weryfikacji biometrycznej. Natomiast ci podróżni, którzy przeszliby test SI, musieliby wykonać jedynie kilka podstawowych czynności.

Procedura stosowana w ramach tego projektu wzbudziła szereg obaw dotyczących jej skuteczności i uczciwości[35]. Niezależne badania pokazały, że skuteczność wyniosła niecałe 76%[36]. Ponadto poddawana badaniu w ramach projektu grupa osób nie była odpowiednio dobrana, gdy weźmie się pod uwagę takie czynniki, jak płeć czy pochodzenie etniczne. Dlatego dokładność uzyskanych wyników, jego bardzo ogólne podejście i implikacje były kontestowane[37]. Analizy wykazały bowiem, że algorytmy zastosowane w systemie iBorderCtrl uwzględniają takie zmienne, jak pochodzenie etniczne, co nasuwa podejrzenie o dyskryminację[38]. Takie algorytmy powinny natomiast uwzględniać różnice kulturowe i środowiskowe.

Warto też wskazać, że jeden z posłów do PE P. Breyer złożył pozew przeciwko KE do Sądu UE, w którym domagał się wyjaśnienia decyzji o finansowaniu systemu

---

34 Zob. ciekawie na ten temat: M. Pfeifer, *Intelligent Borders? Securitizing Smartphones in the European Border Regime*, „Culture Machine" 2021, 20, https://culturemachine.net/wp-content/uploads/2021/09/Michelle-Pfeifer.pdf (dostęp: 1.02.2022).

35 R. Gallagher, L. Jona, *We tested Europe's new lie detector for travelers – and immediately triggered a false positive*, „The Intercept" 26.07.2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector (dostęp: 1.02.2022).

36 Zob.: K. Crockett, A. Antoniades, W. Khan, G.E. Boultadakis, *Intelligent deception detection through Machine Based interviewing*, „Conference Paper" 2018, 1, https://www.researchgate.net/publication/328399576_Intelligent_Deception_Detection_through_Machine_Based_Interviewing (dostęp: 1.02.2022).

37 M. Forti, *AI-driven migration management procedures: fundamental rights issues and regulatory answers*, „BioLaw Journal – Rivista di BioDiritto" 2021, 2, s. 440.

38 Ibidem.

 DOI: 10.7206/kp.2080-1084.574

iBorderCtrl i odtajnienia informacji na temat tego projektu[39]. Polityk twierdził, że nie ma żadnego dowodu naukowego na (słuszność) wykorzystywania SI do wykrywania kłamstw. W skardze wskazywał także na brak przejrzystości w odniesieniu do rzeczywistego działania systemu wykrywania kłamstw i wyraził obawy, że ta technologia może być również wykorzystywana do celów komercyjnych przez podmioty prywatne.

Także PE w *Rezolucji*[40] wyraził swoje zaniepokojenie projektami badawczymi finansowanymi w ramach projektu „Horyzont 2020", takimi jak projekt iBorderCtrl. Wezwał do zaprzestania finansowania badań dotyczących systemów biometrycznych i zakazu ich wdrażania. Parlament Europejski uznał również, że zarówno bramki kontroli granicznej, które wykorzystują automatyczne rozpoznawanie, jak i projekt iBorderCtrl powinny zostać usunięte przez używające je państwa członkowskie UE. Wezwał KE do wszczęcia postępowań wobec tych państw członkowskich Unii, które uchybiają przyjętym zobowiązaniom.

Profilowanie algorytmiczne

Profilowanie algorytmiczne oraz systemy wspomagania decyzji w zarządzaniu migracją i granicami są coraz częściej wykorzystywane i wdrażane na całym świecie[41]. Algorytmy sztucznej inteligencji mogą być również wykorzystywane do przesiewania danych (osobowych i nieosobowych) w celu identyfikacji nieznanych osób, które mogą być przedmiotem zainteresowania władz.

Oprócz weryfikacji i identyfikacji znanych osób algorytmy SI są również wykorzystywane do identyfikacji osób nieznanych będących przedmiotem zainteresowania na podstawie określonych profili ryzyka. Profilowanie algorytmiczne dla oceny indywidualnych zagrożeń bezpieczeństwa oraz ryzyka nielegalnej migracji jest obecnie opracowywane w ramach systemu VIS oraz systemu ETIAS. Zautomatyzowana, oparta na danych wywiadowczych ocena ryzyka jest przeprowadzana przez państwa członkowskie w ramach wymiany między nimi danych o pasażerach.

---

39 Zob.: Skargę wniesioną 15 marca 2019 r. *Breyer przeciwko Komisji*, sprawa T-158/19.

40 Zob.: pkt 31 *Rezolucji*.

41 Zob.: P. Molnar, L. Gill., *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*, Citizen Lab and International Human Rights Program (Faculty of Law, University of Toronto) Research Report No. 114, University of Toronto, September 2018, s. 3 i n.

Narzędzia SI do monitorowania, analizy i prognozowania migracji

Wspomagana przez sztuczną inteligencją analiza przepływów migracyjnych i tendencji w przestępczości transgranicznej (wykrywanie zagrożeń i analiza ryzyka) staje się powszechnym narzędziem kontroli granicznej[42]. W badaniu przeprowadzonym w 2020 r.[43] dla KE przeanalizowano wykonalność opracowania narzędzi SI do prognozowania i wczesnego ostrzegania w celu oceny kierunku i intensywności nielegalnych przepływów migracyjnych do UE i w jej obrębie oraz w celu zapewnienia wczesnych ostrzeżeń i prognoz. W badaniu stwierdzono, że „można zbudować dobrze działający system prognozowania", chociaż jego wiarygodność nie mogłaby być odpowiednio oceniona z wyprzedzeniem.

Wyspecjalizowane agencje UE (zwłaszcza Frontex, EASO, Europol) wykorzystują technologie oparte na SI na granicach zewnętrznych UE w celu monitorowania, analizowania i prognozowania trendów migracyjnych i zagrożenia dla bezpieczeństwa[44].

Projekt ROBORDER – drony napędzane sztuczną inteligencją do nadzorowania granic

Ze środków UE (w ramach programu „Horyzont 2020") finansowany był także w latach 2017–2021 projekt ROBORDER[45]. Dotyczył utworzenia autonomicznego systemu nadzoru granic Europy. Zgodnie z tym projektem system strzegący granic UE mają współtworzyć – napędzane sztuczną inteligencją – drony latające, wodne, podwodne i naziemne, zdolne do funkcjonowania zarówno samodzielnie, jak w rojach. Aby przekazywany przez nie obraz był pełny, sieć miała obejmować także radary, aparaty fotograficzne, mikrofony i kamery, a także przenośne czujniki na pokładach pojazdów bezzałogowych (kamery optyczne i termowizyjne, czujniki ruchu itp.)[46].

---

42 Frontex, *Artificial Intelligence-based capabilities, final report*, 17.3.2021, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf (dostęp: 1.02.2022).

43 Ecorys, *Feasibility study on…*, s. 8.

44 Zob.: J. Bither, A. Ziebarth, *Automating decision-making in migration policy: a navigation guide*, November 2021, s. 26 i n., https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2021-11/Automating%20Decision-Making%20in%20Migration%20Policy_Bither%20and%20Ziebarth.pdf (dostęp: 1.02.2022).

45 ROBORDER – *Autonomous Swarm of Heterogeneous Robots for Border Surveillance*, czyli *Autonomiczny rój heterogenicznych robotów do nadzorowania granic.*

46 Szeroko na temat tego projektu zob.: https://roborder.eu/ oraz „Border Security Report", Vol. 26, September–October 2021, https://border-security-report.com/wp-content/uploads/2021/09/BSRSepOct2021.pdf (dostęp: 1.02.2022).

 DOI: 10.7206/kp.2080-1084.574

Twórcy projektu twierdzą, że te urządzenia (roboty) będą w stanie identyfikować ludzi i decydować, czy stanowią zagrożenie. Jeśli ustalą, że dana osoba mogła popełnić przestępstwo, powiadomią straż graniczną. W ten sposób uzyskuje się narzędzie, zgodnie z założeniami twórców, do walki z nielegalną imigracją, przemytem narkotyków, broni, a także do monitorowania wycieków ropy z tankowców i platform wiertniczych.

Projekt ten od samego początku wzbudzał szereg kontrowersji. Zakres władzy, jaką może dawać swym użytkownikom ROBORDER, wywołuje niepokój wielu osób i instytucji. Pojawiają się pytania o etykę, prawa człowieka i komercyjne zastosowania[47]. Ponoć zainteresowanie „rojem robotów monitorujących granice" wykazują już firmy prywatne. Nie można także ignorować potencjału projektu do zastosowań wojskowych. Roje inteligentnych dronów zdolnych rozpoznawać ludzi mogą stać się śmiertelnym zagrożeniem np. dla osób próbujących przedostać się na terytoriom strefy Schengen.

Można mieć słuszne wątpliwości, że ROBORDER i podobne projekty zlecają zbyt dużo pracy organów ścigania podmiotom innym niż ludzie i mogą z łatwością zostać użyte przeciwko ludziom na obszarach przygranicznych. Znane są już bowiem przypadki użycia dronów wyposażonych nie tylko w czujniki, lecz także uzbrojonych w paralizatory, gaz pieprzowy, gumowe kule i inną broń. Mogą wyniknąć z tego poważne konsekwencje, gdy połączy się taką technologię z podejmowaniem decyzji w oparciu o sztuczną inteligencję i wykorzystywaniem jej w politycznie obciążonych strefach przygranicznych. Wydaje się jednak, że to tylko kwestia czasu, kiedy drony podejmą działania w celu powstrzymania ludzi.

Wskazuje się także, że projekt może również naruszać warunki swojego finansowania. Jak wynika bowiem z dokumentów dotyczących projektu ROBORDER (uzyskanych dzięki unijnym przepisom o przejrzystości i dostępie do dokumentów) został on w większości sfinansowany z unijnego grantu badawczego w wysokości 8 milionów euro przeznaczonego dla projektów, które mają wyłącznie charakter niewojskowy. Jednak twórcy projektu przyznają, że część proponowanego systemu obejmuje także technologię wojskową lub taką, która będzie mogła być łatwo przekształcona do celów wojskowych.

[47] Z. Campbell, *Swarms of drones, piloted by artificial intelligence, may soon patrol Europe's borders*, „The Intercept" 11.05.2019, https://theintercept.com/2019/05/11/drones-artificial-intelligence-europe-roborder/ (dostęp: 1.02.2022).

Wnioski

W ramach Unii Europejskiej prowadzone są badania, w jaki sposób można rozwijać i przyjmować technologie SI w celu poprawy kontroli granic zewnętrznych i zapewniania bezpieczeństwa. Szereg aplikacji do identyfikacji biometrycznej, wykrywania emocji, oceny ryzyka i monitorowania migracji oparte na SI zostało już wdrożonych lub przetestowanych na granicach UE.

Ostrożne wdrażanie technologii opartej na SI w celu kontroli granic może przynieść wiele korzyści, m.in. zwiększoną zdolność wykrywania oszustw i nadużyć, lepszy i szybszy dostęp do informacji istotnych w procesie podejmowania decyzji, a także wzmocnioną ochronę osób szczególnie narażonych. Korzyści te należy jednak zrównoważyć ze znaczącym zagrożeniem, jakie stwarzają te technologie dla ochrony praw podstawowych jednostki (m.in. ryzyko stronniczości i dyskryminacji, naruszenie ochrony danych osobowych i prywatności czy ryzyko niezgodnego z prawem profilowania – np. wizerunki twarzy mogą ujawniać pochodzenie etniczne).

Istnieją poważne wątpliwości co do podstaw naukowych i wiarygodności algorytmów wykrywania emocji opartych na SI. W przypadku finansowania przez UE projektu skoncentrowanego na rozwoju technologii wykrywania emocji istnieje potrzeba wzmocnienia przejrzystości i nadzoru nad finansowaniem przez UE badań nad sztuczną inteligencją, w szczególności w obszarach wiążących się z poważnymi konsekwencjami, takimi jak granice i bezpieczeństwo.

Projekt iBorderCtrl stanowi przykład, jak wykorzystywanie systemów SI na granicach zewnętrznych Unii może wywoływać niepokojące skutki. Oparty na SI system do wykrywania kłamstw był odpowiedzialny za sprawdzanie wiarygodności i prawdziwości oświadczeń podróżnych podczas kontroli granicznych w celu wjazdu na terytorium strefy Schengen. System zadawał pytania i skanował mikroekspresję twarzy podróżnych. Jeśli algorytm był sceptyczny, to kierował osobę do dalszej kontroli. Funkcjonowanie tego systemu jest niejasne i niezrozumiałe dla użytkowników. Istnieje również uzasadniona obawa, że w dyskryminujący sposób uwzględnia on zmienne, takie jak pochodzenie etniczne lub narodowość osób poddawanych badaniu. Projekt otrzymał finansowanie z unijnego programu „Horyzont 2020". Został wprawdzie potraktowany jako „tylko" projekt pilotażowy. Jednak takie „testowanie" może mieć jednak dalej idące konsekwencje. Wiadomo, że tradycyjne, obsługiwane przez człowieka wariografy są niewiarygodne, a „dowody" za ich pomocą uzyskane są niedopuszczalne w wielu jurysdykcjach sądowych. Tutaj mamy do czynienia z technologią testowaną przy bardzo małym

 DOI: 10.7206/kp.2080-1084.574

nadzorze i bez określenia odpowiedzialności za potencjalne błędy przez nią popełnione[48].

Dyskusje na temat SI, w szczególności w mediach, często jawią się jako zaciekła walka między pesymistami, którzy postrzegają ją jako narzędzie destrukcji (zniszczenia) a optymistami, którzy widza ją z kolei jako narzędzie zbawienia. Oba obozy wydają się zgadzać, co do tego, że technologie oparte na sztucznej inteligencji są potężnymi narzędziami, które będą wywoływały daleko idące konsekwencje w wielu dziedzinach. Groźne jest przekonanie, że te technologie ze swoją niszczycielską mocą są nieuniknione, niezależnie od tego, co możemy z tym zrobić[49].

Taki rodzaj determinizmu technologicznego może blokować poważną debatę na temat tego, czy i jak technologie oparte na sztucznej inteligencji powinny być rozwijane i wdrażane. Na przykład, twierdzenie, że rozpoznawanie emocji jest możliwe i deklarowanie, że oparte na nim technologie są „przyszłością" kontroli granicznych i bezpieczeństwa, nie mówi wiele o celowości i akceptowalności takich technologii. Ślad takich deterministycznych tendencji można odnaleźć w niedawnym sprawozdaniu eu-LISA[50]. Wskazano tam, że wdrożenie SI nie jest kwestią „czy", ale „kiedy" i „w jakim stopniu". Warto wskazać na interesującą analogię między obecnym pośpiechem w przyjmowaniu technologii cyfrowych a sposobem, w jaki ludzkość zajęła się wcześniejszymi wyzwaniami technologicznymi. I tak fakt, iż samochody mogą poruszać się z prędkością 250 kilometrów na godzinę, nie powstrzymał organów regulacyjnych przed nakładaniem ograniczeń prędkości jazdy ze względu na ochronę bezpieczeństwa publicznego. Innymi słowy, „tylko dlatego, że niektóre technologie są możliwe, nie oznacza to, że powinny być akceptowane"[51].

Bibliografia

Beduschi A., *International migration management in the age of artificial intelligence*, „Migration Studies" 2021, 9(3).

Bircan T., Korkmaz E.E., *Big data for whose sake? Governing migration through artificial intelligence*, „Humanities and Social Sciences Communications" 2021, 8(1).

Bither J., Ziebarth A., *Automating decision-making in migration policy: a navigation guide*, November 2021, https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2021-

[48] Zob.: P. Szostak, *Drony i algorytmy przeciwko uchodźcom. Europa buduje wirtualny mur*, 16.09.2021, https://wyborcza.biz/biznes/7,177150,27578472,drony-i-algorytmy-przeciwko-uchodzcom.html (dostęp: 1.02.2022).

[49] C. Dumbrava, op. cit., s. 31.

[50] eu-LISA, *Artificial Intelligence…*, s. 32.

[51] E.M. Kuskonmaz, E. Guild, *Covid-19: A New Struggle over Privacy, Data Protection and Human Rights*? European Law Blog, 4.05.2020, https://europeanlawblog.eu/2020/05/04/covid-19-a-new-struggle-over-privacy-data-protection-and-human-rights/ (dostęp: 1.02.2022).

11/Automating%20Decision-Making%20in%20Migration%20Policy_Bither%20and%20Ziebarth.pdf (dostęp: 1.02.2022).

Campbell Z., *Swarms of drones, piloted by artificial intelligence, may soon patrol Europe's borders*, „The Intercept" 11.05.2019, https://theintercept.com/2019/05/11/drones-artificial-intelligence-europe-roborder/ (dostęp: 1.02.2022).

Carriço G., *The EU and artificial intelligence: A human-centred perspective*, „European View" 2018, 17(1).

Casagran C.B., *Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU*, „Human Rights Law Review" 2021, 21(2).

Chiusi F., Fischer S., Kayser-Bril N., Spielkamp M. (eds.), *Automating Society Report 2020*, AlgorithmWatch, October 2020, https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf (dostęp: 1.02.2022).

Crawford K., *Atlas of AI: The Real Worlds of Artificial Intelligence*, Yale University Press 2021.

Crockett K., Antoniades A., Khan W., Boultadakis G.E, *Intelligent deception detection through Machine Based interviewing*, „Conference Paper" 2018, 1, https://www.researchgate.net/publication/328399576_Intelligent_Deception_Detection_through_Machine_Based_Interviewing (dostęp: 1.02.2022).

Deloitte, *Opportunities and challenges for the use of artificial intelligence in border control, migration and security*, Vol. 1, *Main report*, May 2020, https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en (dostęp: 1.02.2022).

Dumbrava C., *Artificial intelligence at EU borders. Overview of applications and key issues*, European Parliament, European Parliamentary Research Service PE 690.706 – July 2021.

Ecorys, *Feasibility study on a forecasting and early warning tool for migration based on Artificial Intelligence technology*, November 2020, https://op.europa.eu/lv/publication-detail/-/publication/946b0bc7-7006-11eb-9ac9-01aa75ed71a1/language-lv/format-PDF/source-search (dostęp: 1.02.2022).

eu-LISA, *Artificial Intelligence in the Operational Management of Large-scale IT Systems*, July 2020, https://www.eulisa.europa.eu/Publications/Reports/AI%20in%20the%20OM%20of%20Large-scale%20IT%20Systems.pdf (dostęp: 1.02.2022).

Europejska Rada Ochrony Danych – Europejski Inspektor Ochrony Danych, *Wspólna opinia 5/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji („akt w sprawie sztucznej inteligencji")*, 18.06.2021, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_pl (dostęp: 1.02. 2022).

Flynn M.J., *Study on technical requirements for data spaces in law enforcement*, June 2020, https://op.europa.eu/de/publication-detail/-/publication/0d02ee25-6c19-11eb-aeb5-01aa75ed71a1/language-de (dostęp: 1.02.2022).

Forti M., *AI-driven migration management procedures: fundamental rights issues and regulatory answers*, „BioLaw Journal – Rivista di BioDiritto" 2021, 2.

 DOI: 10.7206/kp.2080-1084.574

Frontex, *Artificial Intelligence-based capabilities for European Border and Coast Guard*, March 2021, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf (dostęp: 1.02.2022).

Frontex, *Artificial Intelligence-based capabilities, final report*, 17.03.2021, https://frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf (dostęp: 1.02.2022).

Frontex, *Best Practice Operational Guidelines for Automated Border Control (ABC) Systems*, September 2015, https://frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_ABC.pdf (dostęp: 1.02.2022).

Fundamental Rights Agency, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, November 2019, https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (dostęp: 1.02.2022).

Gajda A., *Najnowsze technologie i zarządzanie granicami zewnętrznymi Unii Europejskiej*, „Krytyka Prawa" 2020, 12(4).

Gajda A., *Interoperacyjność unijnych systemów w zakresie bezpieczeństwa, ochrony granic i zarządzania migracjami*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace" 2019, 1(37).

Gallagher R., Jona L., *We tested Europe's new lie detector for travelers – and immediately triggered a false positive*, „The Intercept" 26.07.2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector (dostęp: 1.02.2022).

Hildebrandt M., *The Artificial Intelligence of European Union Law*, „German Law Journal" 2020, 21(1).

Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego i Rady, *Strategia na rzecz w pełni funkcjonującej i odpornej strefy Schengen*, COM(2021) 277 final, Bruksela 2.06.2021.

Komisja Europejska, *Wniosek rozporządzenia Parlamentu Europejskiego i Rady ustanawiający zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniający niektóre akty ustawodawcze Unii*, COM(2021) 206 final, Bruksela, 21.04.2021 oraz *Załączniki do Wniosku* COM(2021) 206 final, Bruksela 21.04.2021.

Kuskonmaz E.M., Guild E., *Covid-19: A New Struggle over Privacy, Data Protection and Human Rights*?, European Law Blog, 4.05.2020, https://europeanlawblog.eu/2020/05/04/covid-19-a-new-struggle-over-privacy-data-protection-and-human-rights/ (dostęp: 1.02.2022).

Molnar P., Gill L., *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*, Citizen Lab and International Human Rights Program (Faculty of Law, University of Toronto) Research Report No. 114, University of Toronto, September 2018.

Parlament Europejski, *Rezolucja Parlamentu Europejskiego z dnia 6 października 2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych* (2020/2016(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PL.pdf (dostęp: 1.02.2022).

Pfeifer M., *Intelligent Borders? Securitizing Smartphones in the European Border Regime*, „Culture Machine" 2021, 20, https://culturemachine.net/wp-content/uploads/2021/09/Michelle-Pfeifer.pdf (dostęp: 1.02.2022).

Renda A., Arroyo J., Fanni R., Laurer M., Sipiczki A., Yeung T., Maridis G., Fernandes M., Endrodi G., Milio S., Devenyi V., Georgiev S., de Pierrefeu G., *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, April 2021, https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation (dostęp: 1.02.2022).

Sánchez-Monedero J., Dencik L., *The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2020, 25(3).

Schwartz O., *Don't look now: why you should be worried about machines reading your emotions*, „The Guardian" 6.03.2019, https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science (dostęp: 1.02.2022).

Szostak P., *Drony i algorytmy przeciwko uchodźcom. Europa buduje wirtualny mur*, 16.09.2021, https://wyborcza.biz/biznes/7,177150,27578472,drony-i-algorytmy-przeciwko-uchodzcom.html (dostęp: 1.02.2022).

Świerczyński M., Więckowski Z., *Sztuczna inteligencja w prawie międzynarodowym. Rekomendacje wybranych rozwiązań*, Warszawa 2021.

 DOI: 10.7206/kp.2080-1084.574