ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4054

Studia nad Autorytaryzmem i Totalitaryzmem 43, nr 1
Wrocław 2021

https://doi.org/10.19195/2300-7249.43.1.21

JAKUB KOCIUBIŃSKI
ORCID: 0000-0002-4391-7439
Uniwersytet Wrocławski
jakub.kociubinski@uwr.edu.pl

Wykorzystywanie danych personalnych zgromadzonych przypadkowo podczas operacji bezzałogowych statków powietrznych w świetle standardów prawa do prywatności gwarantowanego w Europejskiej Konwencji o Ochronie Praw Człowieka — zarys problemu

Słowa kluczowe: prawo do prywatności, Europejska Konwencja o Ochronie praw Człowieka, bezzałogowe statki powietrzne, dane osobowe.

THE USE OF PERSONAL DATA COLLATERALLY COLLECTED BY UNMANNED AERIAL VEHICLES IN THE LIGHT OF STANDARDS SET OUT IN THE EUROPEAN CONVENTION ON HUMAN RIGHTS — A PROBLEM OUTLINE

Abstract

The rapid growth of data-gathering technologies on the one hand has provided public authorities with a valuable tool for counteracting crimes, but on the other gave rise to concerns over potentially excessive intrusion into persons' privacy. In order to mitigate the risk of authoritarian behavior stemming from a moral hazard arising out of ability to conduct an ever more effective surveillance, public authorities must impose certain self-limitations with regards to the usage of such data. In this context, the use of unmanned aerial vehicles, which may serve other non-invigilation purposes, may inadvertently lead to collecting someone's personal data.

This paper provides a propaedeutic analysis of legal challenges associated with collateral collection of personal data through unmanned aerial platforms operated by public bodies, and the subsequent use of said data. The analysis will be carried out through the lens of the standards set out in the European Convention on Human Rights (ECHR). In order to provide an answer to the paper's research question whether the current acquis on Article 8 of the ECHR setting out the basic right to privacy and exceptions thereof require adjustment, the analysis will begin with an overview of

the existing case-law dedicated to the ECHR's standards associated with collecting and processing personal data with an emphasis on its relevance to technical specificities of drones operations. The inquiry will then focus on standards associated with operating unmanned platforms during which personal data may be collaterally collected in public places. While it stands to reason that anyone within such a public space must reasonably expect that his or her privacy will be somewhat limited, a distinction must be made between mere recording and the subsequent use of such data for a different purpose that it was originally gathered. The next part of the analysis will cover a legal assessment of situations whereby sensors installed on a drone used by public authorities over public spaces will record persons within their domicile — place of living.

The analysis carried out in this paper has led to conclusion that while the core of the pre-existing ECHR's case-law can be successfully applied *per analogiam* to unmanned aerial platforms' operations, due to technical and operational factors there is no feasible way to provide adequate information about whether a monitoring is conducted, who is carrying it out, etc., in a similar manner as this is being done in the case of stationary close-circuit cameras. Therefore, it is necessary to place a greater emphasis on *ex officio* data anonymization.

Keywords: right to privacy, European Convention on Human Rights, unmanned aerial vehicles, personal data.

1. Wprowadzenie

Postęp technologiczny w zakresie gromadzenia i przetwarzania różnego rodzaju danych — obrazu, dźwięku, danych nawigacyjnych, biometrycznych itp. — dał władzom publicznym wartościowe narzędzia, które mogą być wykorzystane między innymi do zwalczania przestępczości czy innych zagrożeń dla porządku i bezpieczeństwa publicznego. Spowodował jednocześnie powstanie nowych wyzwań, wpisujących się w szeroką i stale aktualną debatę dotyczącą ochrony swobód obywatelskich przed autorytarnymi zakusami rządzących. Jednym z aspektów tego zagadnienia jest wykorzystanie możliwości, jakie niosą z sobą coraz popularniejsze, doskonalsze i tańsze bezzałogowe statki powietrzne, tak zwane drony[1]. Ze względu na możliwość przenoszenia różnego rodzaju sensorów i często niezauważonego dotarcia w niedostępne miejsca stanowią one wygodne narzędzie umożliwiające pełne wykorzystanie możliwości, jakie oferują wzmiankowane technologie gromadzenia informacji.

Postrzeganie dronów w kategorii narzędzia — zatem samego w sobie aksjologicznie neutralnego — mogącego posłużyć do ingerencji władzy w prywatną sferę jednostek ma dwa główne aspekty. Z jednej strony jest kwestia wykorzystywania bezzałogowych statków powietrznych z wyraźnym przeznaczeniem inwigilacji (abstrahując w tym miejscu od tego, czemu owa inwigilacja ma ostatecznie służyć). Z drugiej natomiast strony jest problem gromadzenia przez struktury państwowe danych dotyczących osób fizycznych przy okazji wykonywania in-

[1] W niniejszej analizie określenia dron, bezzałogowy statek powietrzny, platforma UAV (*unmanned aerial vechicle*) będą używane wymiennie wobec wszystkich statków wykorzystywanych w celach innych niż rekreacyjne, niezależnie od ich masy startowej.

nych, zupełnie niezwiązanych z tymi osobami zadań (tak zwana *collateral privacy intrusion*)[2]. Jako przykład można podać zarejestrowanie czyjegoś wizerunku, wskazującego, że dana osoba przebywała w konkretnym miejscu w konkretnym czasie, podczas dokonywania przeglądu jakiejś instalacji przy wykorzystaniu kamery zamontowanej na dronie. Samo gromadzenie danych jest kwestią czysto techniczną, determinowaną w zależności od tego, gdzie, kiedy i jak prowadzona jest operacja. Natomiast problem prawny — analizowany w niniejszym opracowaniu z perspektywy standardów Europejskiej Konwencji o Ochronie Praw Człowieka (dalej: Konwencja) — polega na tym, czy i jak można wykorzystywać zebrane w ten sposób dane[3]. Można stwierdzić, że jest to kwestia dotykająca samej istoty autorytaryzmu, gdyż władza, dysponując szerokim dostępem do informacji, będzie miała naturalną pokusę ich wykorzystania, gdy tymczasem powinna się samoograniczyć dla uniknięcia nadmiernej, naruszającej art. 8 Konwencji, ingerencji w życie prywatne jednostek.

2. Gromadzenie informacji za pomocą systemów „masowej obserwacji"

Naszkicowany powyżej problem nie jest w rzeczywistości nowy — nowe są kolejne technologie. Po raz pierwszy znalazł się on w głównym nurcie debaty na temat granic dozwolonej ingerencji władz publicznych w życie prywatne obywateli w związku z rozpowszechnieniem się technologii masowego monitoringu miejsc publicznych[4]. Można wobec tego przyjąć jako punkt wyjścia do dalszej dyskusji, że istniejący dorobek — zwłaszcza Europejskiego Trybunału Praw Człowieka (dalej: ETPCz) — dotyczący samego późniejszego wykorzystania zgromadzonych danych może z powodzeniem być zaimplementowany na potrzeby operacji dronów, natomiast ze względu na uwarunkowania techniczne przyjęta interpretacja

[2] Na potrzeby prowadzonej dyskusji opisywane pojęcie gromadzonych danych mogących stanowić naruszenie prywatności będzie tożsame z pojęciem danych osobowych w rozumieniu art. 4 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO), Dz.Urz. UE z 2016 r. L 119/1.

[3] Zarejestrowanie danych personalnych może oczywiście także nastąpić w wyniku użytkowania platform UAV przez osoby prywatne w celach albo zawodowych, albo czysto rekreacyjnych i w pewnych sytuacjach też może stanowić naruszenie Konwencji (zob. *per analogiam* sprawa *Von Hannover v. Niemcy*, skargi 40660/08 i 60641/08, wyrok z 7 lutego 2012 roku), natomiast niniejsze opracowanie skupia się tylko na sytuacjach, gdzie z dronów korzystają instytucje publiczne.

[4] Zob. między innymi T. Takahashi, *Drones and privacy*, „The Columbia Science and Technology Law Review" 2012, nr 16, s. 72–114; M. Zalnieriute, *An international constitutional moment for data privacy in the times of mass-surveillance*, „International Journal of Law and Information Technology" 2015, nr 23 (2), s. 99–133; T. Stahl, *Indiscriminate mass surveillance and the public sphere*, „Ethics and Information Technology" 2016, nr 18, s. 33–39.

dotycząca standardów samego zbierania informacji musi być wypracowana od podstaw lub przynajmniej zmodyfikowana.

W dorobku strasburskim w sprawach związanych ze stacjonarnymi systemami monitoringu, określanymi tam jako „masowa obserwacja" (*mass surveillance*), zwłaszcza w sprawach *Weber i Saravia* oraz *Liberty*, wskazano, że do systemów, które ze względu na swoją techniczną konfigurację mogą równocześnie gromadzić informacje o większej liczbie osób, zastosowanie znajdują takie same standardy dotyczące ochrony prywatności, wynikające z przepisu art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka, jak wobec działań zindywidualizowanych[5]. W rozstrzygnięciu sprawy *Zakharov* ETPCz doprecyzował, że obserwacja konkretnych, znanych wcześniej osób, czyli innym słowy działania podejmowane od początku z intencją zbierania informacji o właśnie tych osobach, wymaga istnienia uzasadnionego podejrzenia[6]. Natomiast samo zbieranie informacji za pomocą systemów „masowych" — na przykład przechowywanie nagrań — co do zasady nie wymaga istnienia podejrzenia wobec konkretnych osób[7]. Jest to zrozumiałe, ponieważ w przypadku wszystkich systemów obserwujących jakiś obszar, obserwowana może być potencjalnie nieograniczona liczba osób, które siłą rzeczy nie są wcześniej znane (przez co linia interpretacji daje się zastosować *per analogiam* do tytułowej kwestii). Kluczowa kwestią jest więc wcześniejsze zdefiniowanie kręgu jednostek podlegających obserwacji, bo to determinuje problem możliwości dalszego wykorzystania zgromadzonego materiału.

Natomiast w praktyce ocena w tym względzie wymyka się dychotomicznemu podziałowi na obserwowanie jednej osoby lub obserwowanie każdego, kto będzie w danym miejscu, jakby to *implicite* mogło wynikać z przytoczonego orzecznictwa. Instruktywny przykład stanowi sprawa *Szabó i Vissy*[8]. Obserwacja została wymierzona w członków konkretnej organizacji. Nie było więc wiadomo z góry, kto dokładnie będzie obserwowany, jakie ewentualnie podejrzenia dotyczą konkretnych osób, co ta obserwacja ujawni, jakie czyny itp. W uzasadnieniu władz publicznych dana organizacja jako całość uznawana była za zagrażającą bezpieczeństwu publicznemu, co ich zdaniem stanowiło podstawę do podjęcia działań inwigilacyjnych, których jednym z celów było także zidentyfikowanie członków danej organizacji i dopiero późniejsze ewentualne dalsze dochodzenie, jaka mogłaby być rola tych osób w nielegalnych działaniach, jeżeliby stwierdzono, że miały miejsce[9].

---

[5] Sprawy *Liberty i inni v. Zjednoczone Królestwo*, skarga 58243/00, wyrok z 1 czerwca 2008 roku, pkt 5 i 83; *Weber i Saravia v. Niemcy*, skarga 54934/00, decyzja z 29 czerwca 2006 roku, pkt 4 i 95.

[6] Sprawa *Roman Zakharov v. Rosja*, skarga 47143/06, wyrok z 4 grudnia 2015 roku, pkt 10.

[7] Sprawy *Association for European Integration and Human Rights i Ekimdzhiev v. Bułgaria*, skarga 62540/00, wyrok z 28 czerwca 2007 roku, pkt 79 i 80; *Iordachi i inni v. Mołdawia*, skarga 25198/02, wyrok z 10 lutego 2009 roku, pkt 51.

[8] Sprawa *Szabó i Vissy v. Węgry*, skarga 37138/14, wyrok 12 stycznia 2016 roku, pkt 7, 10 i 11.

[9] *Ibidem*.

Jeżeli więc użycie drona wiązać się będzie z gromadzeniem informacji wobec kogokolwiek przebywającego w danym miejscu, na przykład w pobliżu nadzorowanej instalacji, wówczas zastosowanie znajdzie schemat interpretacyjny stosowany w odniesieniu do stacjonarnych systemów obserwacji, takich jak kamery na budynkach. Wówczas fakt, że dany sensor znajdzie się na platformie UAV, będzie irrelewantną kwestią techniczną. Zatem samo wejście w posiadanie danych osobowych przy okazji operacji z użyciem dronów wykonywanych przez instytucje publiczne co do zasady nie narusza standardów Konwencji, natomiast w świetle linii interpretacji z przytoczonej sprawy *Szabó i Vissy* obserwacja miejsca ukierunkowana na gromadzenie informacji o osobach znajdujących się w danym miejscu będzie naruszała art. 8 Konwencji, jeśli samo przebywanie tam będzie legalne, czyli działanie byłoby wówczas wymierzone w krąg osób (*range of persons*), a nie polegałoby na, mówiąc ogólnie, ochronie obiektu[10]. Przy czym, jeśli rzeczywiście dane operacje z użyciem dronów mają służyć na przykład inspekcji infrastruktury, wówczas nie wystąpi *ex ante* cel inwigilacyjny, a bezpośrednie zainteresowanie konkretnymi osobami może pojawić się, jeżeli zarejestrowaniu „na żywo" uległby zamach na dany obiekt, więc nie byłaby to sytuacja pozwalająca zastosować szablon interpretacyjny ze sprawy *Szabó i Vissy.*

Skoro więc samo gromadzenie informacji nie jest *per se* niezgodne z Konwencją, to w kontekście tytułowego zagadnienia występują dwie kategorie sytuacji. Po pierwsze, kiedy dane zostały zebrane wobec osób przebywających w miejscu publicznym, i po drugie, wobec gromadzenia informacji, które co prawda ukierunkowane jest na miejsca publiczne (lub w których władza wprowadza ograniczenia dostępu), lecz podczas wykonywania operacji zostały zarejestrowane jednostki znajdujące się w miejscu zamieszkania.

3. Rejestrowanie danych w miejscach publicznych

Przyjmuje się w orzecznictwie ETPCz, że osoba znajdująca się w miejscu publicznym musi liczyć się z tym, że jej zachowanie zostanie zarejestrowane i ocenione w szerokim tego słowa znaczeniu zarówno przez władze pod kątem występowania ewentualnych czynów niedozwolonych, jak i innych uczestników życia publicznego w kategoriach, mówiąc ogólnie, moralnych[11]. Niemniej jednak prowadzenie obserwacji w miejscach publicznych co do zasady nie wyłącza stosowania art. 8 Konwencji wobec relacji międzyludzkich zachodzących w przestrzeni pub-

[10] Zob. także sprawy *Roman Zakharov*, pkt 249 oraz *Társaság a Szabadságjogokért v. Węgry*, skarga 37374/05, wyrok z 14 kwietnia 2009 roku, pkt 36; *Nagla v. Łotwa*, skarga 73469/10, wyrok z 16 lipca 2013 roku, pkt 82.

[11] Zob. K. Hughes, *Photographs in public places and privacy*, „Journal of Media Law" 2009, nr 2, s. 159–171 i cytowane tam orzecznictwo oraz literatura.

licznej[12]. Stosowana w tym kontekście kategoria „życia prywatnego" może więc obejmować także aktywności mające miejsce poza miejscem zamieszkania czy stałego pobytu danej osoby[13]. Należy jednak odnotować, przywołując rozstrzygnięcia spraw *Peck* oraz *P.G. i J.H*, że nawet jeśli w miejscach publicznych może istnieć uzasadnione domniemanie prywatności — na przykład w wydzielonych obszarach (szatnie, toalety itp.) — to istnienie ochrony na gruncie Konwencji nie jest uzależnione od subiektywnego przeświadczenia danej osoby, że w tym miejscu powinna być poszanowana jego/jej prywatność[14].

Ocena, jakie konkretnie rodzaje aktywności byłyby objęte ochroną, jest mocno kazuistyczna, biorąc pod uwagę ogromną liczbę potencjalnych scenariuszy, dlatego nie jest możliwe stworzenie zestawu taksatywnych przesłanek. Natomiast pozostając na pewnym poziomie ogólności, w wyroku *P.G. i J.H* Trybunał wskazał, że wprawdzie osoba znajdująca się w miejscu, gdzie może być łatwo zauważona — w rozstrzygnięciu padł przykład przechodzenia przez ulicę — musi zakładać, że może podlegać obserwacji, jednak naruszenie prywatności mogłoby wystąpić, jeżeli ów materiał zostałby upowszechniony lub posłużyłby do ustalenia tożsamości, zakładając, że dana jednostka nie jest poszukiwana, gdyż ciąży na niej uzasadnione podejrzenie popełnienia przestępstwa, czyli władze szukają już konkretnej osoby[15]. Zatem naruszeniem nie będzie sfotografowanie czy nagranie uczestnika publicznego zdarzenia (demonstracji, koncertu itp.), gdyż udział w wydarzeniu ze względu na jego charakter implikuje wyrażenie zgody na upublicznienie materiałów z niego — analogiczne wyłączenie ograniczenia rozpowszechniania funkcjonuje na gruncie RODO[16].

Jednak należy odnotować, że w rozstrzygnięciu sprawy *Peck* ETPCz stanął na stanowisku, że upublicznienie zapisów monitoringu — na podstawie których możliwe będzie zidentyfikowanie danej osoby — może stanowić naruszenie pra-

[12] Sprawa *P.G. and J.H. v. United Kingdom*, skarga 44787/98, wyrok z 6 lutego 2001 roku, pkt 56.

[13] Sprawa *Nicolae Virgiliu Tănase v. Romania*, skarga 41720/13, wyrok z 25 czerwca 2019 roku, pkt 128–132. Zob. też sprawy *Uzun v. Niemcy*, skarga 35623/05, wyrok z 2 września 2010 roku, pkt 43; *Von Hannover v. Niemcy (no. 2)*, skargi 40660/08 i 60641/08, wyrok z 7 lutego 2012 roku, pkt 95; *Altay v. Turcja*, skarga 11236/09, wyrok z 9 kwietnia 2019 roku, pkt 49.

[14] Sprawy *P.G. i J.H. v. Zjednoczone Królestwo*, pkt 56–57; *Peck v. Zjednoczone Królestwo*, skarga 44647/98, wyrok z 28 stycznia 2003 roku, pkt 57–67; *Gillan i Quinton v. Zjednoczone Królestwo*, skarga 4158/05, wyrok z 12 stycznia 2010 roku, pkt 61. Zob. też sprawy *Halford v. Zjednoczone Królestwo*, skarga 20605/92, wyrok z 25 czerwca 1997 roku; *Peev v. Bułgaria*, skarga 64209/01, wyrok z 26 lipca 2007 roku, pkt 39.

[15] Sprawa *P.G. i J.H. v. Zjednoczone Królestwo*, *op. cit.*, pkt 57 i 58. Zob. też sprawa *Amann v. Szwajcaria*, skarga 27798/95, wyrok z 16 lutego 2000 roku, pkt 65 i 66.

[16] W decyzji *X v. Zjednoczone Królestwo* (skarga 5877/72, decyzja z 12 października 1973 roku) Komisja Praw Człowieka uznała, że przechowywanie zdjęć wykonanych na demonstracji nie będzie stanowić naruszenia art. 8 Konwencji. Zob. też *Kurier Zeitungsverlag und Druckerei GmbH (no. 2) v. Austria*, skarga 1593/06, z 19 czerwca 2012 roku; *Krone Verlag GmbH v. Austria*, skarga 27306/07, wyrok z 19 czerwca 2012 roku oraz w tym kontekście art. 9 lit. e RODO.

wa do prywatności, nawet jeżeli zarejestrowane zostały aktywności odbywające się w miejscu publicznym[17]. Należy zatem dokonać rozróżnienia, czy określone działania polegające na rejestrowaniu informacji podejmowane są przez osoby prywatne w celu zaspokojenia celów osobistych, takich jak na przykład nagrywanie koncertu, czy przez organy państwa dla realizacji celów publicznych[18]. W tym drugim przypadku w sprawie *Doerga* Trybunał wskazał, że przepisy regulujące wspomnianą działalność muszą być wystarczająco jasne i szczegółowe, aby przeciwdziałać ich arbitralnemu stosowaniu[19]. Przy spełnieniu powyższych przesłanek rejestrowanie informacji na przykład za pomocą dronów w miejscach publicznych będzie akceptowalne, jeżeli zebrane dane będą wykorzystywane dla ochrony bezpieczeństwa publicznego[20].

W naszkicowanej we wstępie sytuacji działania władz publicznych wykorzystujących technologie UAV są wprawdzie motywowane celami leżącymi w interesie publicznym — jest to nieco sztuczny konstrukt prawny, ale zarazem konieczne założenie wobec wszystkich aktywności władz — ale nie takimi konkretnie związanymi z bezpieczeństwem rozumianym jako zapobieganie przestępczości. Tutaj element bezpieczeństwa może występować na przykład, jeżeli dokonuje się przeglądu instalacji energetycznej czy linii kolejowej, ale nie jest to bezpieczeństwo związane z porządkiem publicznym ukierunkowanym na zagrożenia powodowane przez działanie ludzkie[21].

Nawet jeśli platformy UAV są wykorzystywane (co coraz częściej ma miejsce) do ochrony jakiegoś obszaru przed niepożądaną ingerencją osób trzecich, czyli działań *stricte* związanych z zapobieganiem działań przestępczych, to równocześnie zarejestrowaniu mogą podlegać osoby postronne znajdujące się w pobliżu, wobec których nie ma podejrzeń, że dopuściły się jakiegokolwiek czynu zabronionego, oczywiście przy założeniu, że ich zachowanie nie powoduje uzasadnionych podejrzeń, że chcą naruszyć ten obszar.

---

[17] Sprawa *Peck v. Zjednoczone Królestwo*, skarga 44647/98, wyrok z 28 stycznia 2003 roku, pkt 44.

[18] Sprawa *Friend i Countryside Alliance i inni v. Zjednoczone Królestwo*, skargi 16072/06 i 27809/08, decyzja z 24 listopada 2009 roku, pkt 41 i 42.

[19] Sprawa *Doerga v. Holandia*, skarga 50210/99, wyrok z 27 kwietnia 2004 roku, pkt 53.

[20] Sprawa *Perry v. Zjednoczone Królestwo*, skarga 63737/00, wyrok z 17 lipca 2003 roku, pkt 38.

[21] Konieczność opisowego doprecyzowania zadań z zakresu szeroko pojętego bezpieczeństwa jest przynajmniej częściowo spowodowana tym, że w języku polskim pod tym pojęciem rozumie się zarówno zabezpieczenie osób i mienia przed skutkami wypadków, awarii itp., jak i ingerencji osób trzecich, czyli kategorii, które w języku angielskim określa się odpowiednio jako *safety* i *security*. Pojawiające się w tym kontekście określenie „porządek publiczny" nie jest do końca adekwatne, bo implikuje szeroki kontekst ochrony — kraj, ustrój itp. — podczas gdy bezpieczeństwo w kontekście zagadnień opisywanych w niniejszym opracowaniu, czyli nieinwigilacyjnych działań dronów, w trakcie których „przy okazji" doszło do rejestracji danych osobowych, odnosi się do sytuacji, w których głównym celem rejestrującego jest *safety*.

Zastosowanie Konwencji nie może więc być ograniczone do wykorzystania dronów, które są specyficznie ukierunkowane na zbieranie informacji o ludziach, ale ochrona gwarantowana przez system strasburski obejmuje również działania szeroko pojętych podmiotów państwowych, które wykonywane są w innym celu, ale mogą — niekoniecznie zgodnie z intencją władz — ingerować w życie prywatne jednostek[22].

Bazując na istniejącym orzecznictwie, jeżeli więc podczas realizowania operacji z wykorzystaniem platform UAV, polegającej na, ogólnie mówiąc, inspekcji jakiegoś obszaru czy instalacji, doszłoby do zarejestrowania danych pozwalających zidentyfikować daną osobę (nie musi to być tylko wizerunek twarzy ale na przykład obraz umożliwiający odczytanie tablicy rejestracyjnej samochodu czy zarejestrowanie danych GPS z jakiegoś urządzenia należącego do danej osoby), to przechowywanie tych danych do późniejszego wykorzystania przez państwo w celu niedopowiadającym oryginalnemu przeznaczeniu mogłoby — co do zasady — stanowić naruszenie prawa do prywatności, chronionego przez Konwencję[23]. Powyższe, dosyć kategoryczne poprzez swoją ogólność, twierdzenie wymaga jednak pewnego doprecyzowania.

Dane pozwalające na identyfikację jednostek, zebrane podczas działań niezwiązanych z szeroko rozumiana ochroną porządku publicznego, mogą być wykorzystane jako materiał dowodowy, ale tylko wtedy, jeśli wobec danej osoby toczy się postepowanie i w jego toku okaże się, że wspomniane materiały mogą pozwolić na ustalenie pewnych faktów istotnych dla danego postepowania (na przykład dowód, że podejrzany przebywał/nie przebywał w określonym miejscu w określonym czasie)[24]. Natomiast niedozwolone w świetle standardów Konwencji, zinterpretowanych w rozstrzygnięciach *Klass* i *Rotaru*, będzie zidentyfikowanie nagranych osób, których działania nie dają żadnych podstaw do podejrzeń o popełnienie przestępstwa bądź które nie są poszukiwane, i zarchiwizowanie danych na potrzeby przyszłego wykorzystania w na razie nieznanym celu[25]. Jest to aspekt szerszego

[22] Zob. *per analogiam* sprawa *Egeland i Hanseid v. Norwegia*, skarga 34438/04, wyrok z 16 lipca 2009 roku oraz między innymi R. Finn, D. Wright, *Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications*, „Computer Law & Security Review" 2012, nr 28 (2), s. 184–194.

[23] Kluczową kwestią pozostanie więc dalsze wykorzystanie danych. W wyrokach *Rotaru v. Rumunia* i *Klass v. Niemcy* (odpowiednio: skarga 28341/95, wyrok z 4 maja 2000 roku; skarga 5029/71, wyrok z 6 września 1978 roku) Trybunał stwierdził, że wykorzystanie zebranych „przypadkowo" danych do wszczętego później postepowania stanowi naruszenie art. 8 Konwencji.

[24] W każdym przypadku musi istnieć możliwość wglądu do zebranych informacji i skuteczna możliwość dokonywania sprostowań. Zob. sprawa *Dumitru Popescu v. Rumunia (no 2)*, skarga 71525/01, wyrok z 26 kwietnia 2007 roku, pkt 81. Z tego powodu musi być prawnie zagwarantowana możliwość przygotowania weryfikującej ekspertyzy przez odpowiedni podmiot publiczny lub podmiot prywatny, niezależny od władzy publicznej. Zob. sprawa *Segerstedt-Wiberg i inni v. Szwecja*, skarga 62332/00, wyrok z 6 czerwca 2006 roku, pkt 88.

[25] Sprawy *Rotaru v. Rumunia*, pkt 46 i *Klass v. Niemcy*, pkt 51. Istniejące orzecznictwo nie dotyczy dokładnie opisanych w tekście sytuacji, bo koncentruje się na kwestiach nagrywania w trak-

problemu tak zwanych „owoców zatrutego drzewa", pojawiający się zwłaszcza w sferze procedury karnej. Chodzi tu o sytuacje, gdzie dowód sam w sobie jest wartościowy, natomiast został zebrany z naruszeniem standardów, przez co może być skutecznie zakwestionowany[26]. Zakładając, że władza publiczna nie odrzuca standardów Konwencji w świadomy sposób i w sensie systemowym, to samoograniczenie w zakresie przetwarzania danych jest wręcz niezbędne, tym bardziej że od strony technicznej nie ma żadnych przeszkód do zanonimizowania danych osób postronnych na potrzeby wykorzystywania zarejestrowanego materiału zgodnie z jego oryginalnym przeznaczeniem i archiwizacji uprzedniej identyfikacji zarejestrowanych osób.

W przypadku miejsc publicznych — ogólnodostępnych lub z ograniczonym dostępem, ale niebędących miejscem zamieszkania — istnienie zasadnego oczekiwania prywatności będzie przede wszystkim determinowane przez otrzymanie informacji o możliwości obserwacji. Ten warunek będzie spełniony dla miejsc zasadniczo ogólnodostępnych, jeśli w danej sytuacji „przeciętna", myśląca racjonalnie osoba powinna zakładać możliwość bycia obserwowaną[27]. Choć, jak wspomniano, ocena w przypadku miejsc z ograniczonym dostępem (takich, gdzie istnieć może domniemanie prywatności) jest bardziej zniuansowana, gdyż pozostaje jeszcze ustalenie, czy rzeczywiście wspomniane domniemanie powinno zachodzić; generalnie przyjmuje się jednak, że zbieranie informacji „z ukrycia" (*covert*) jest niedopuszczalne w świetle Konwencji (jeżeli nie mamy do czynienia z podejrzanym), dlatego — zakładając, że samo rejestrowanie byłoby dozwolone — w praktyce dla zneutralizowania ryzyka naruszenia prawa do prywatności wystarczające jest umieszczenie informacji o prowadzonym zbieraniu informacji. Może to być na przykład tabliczka informacyjna na ścianie, że pomieszczenie objęte jest monitoringiem[28]. O ile tego typu rozwiązania dobrze sprawdzają się w przypadku systemów stacjonarnych, o tyle nie nadają się one do prostej implementacji wobec dronów, które, można powiedzieć, z samej definicji są „ukrytymi" środkami obserwacji. Nawet jeżeli sam statek powietrzny jest widoczny, to obserwowana osoba właściwie nigdy nie będzie w stanie samodzielnie stwierdzić, czy taka inwigilacja rzeczywiście jest prowadzona. Immanentnie powiązane kwestie niemożności stwierdzenia, czy obserwacja jest prowadzona, i pewnej uciążliwości obecności drona, nie w kontekście na przykład powodowanego przez niego hała-

cie demonstracji czy innego rodzaju imprez masowych. Zob. też R. Finn, D. Wright, *op. cit.* oraz sprawa *Friedl v. Austria*, skarga 15225/89, wyrok z 31 stycznia 1995 roku.

[26] W orzecznictwie strasburskim zob. między innymi sprawy *Ćwik v. Polska*, skarga 31454/10, wyrok z 5 listopada 2020 roku; *Ramanauskas v. Litwa*, skarga 74420/01, wyrok z 5 lutego 2008 roku.

[27] Niemniej jeżeli zarejestrowana nie jest osobą publiczną, kimś nieszukającym żadnego publicznego rozgłosu (ani tym bardziej kimś poszukiwanym), upublicznienie zgromadzonego materiału będzie naruszeniem prawa do prywatności. Zob. sprawa *Rodina v. Łotwa*, skargi 48534/10 i 19532/15, wyrok z 14 maja 2020 roku, pkt 131.

[28] Zob. sprawa *Doerga v. Holandia*, pkt 53.

su, tylko psychologicznego dyskomfortu, że być może prowadzona jest inwigilacja, powróci także w odniesieniu do możliwości naruszenia prywatności w domu.

W rozstrzygnięciu sprawy *Reklos i Davoulis* Trybunał zajął stanowisko, że gromadzenie materiału fotograficznego w celach niezwiązanych z inwigilacją konkretnych osób — czyli na przykład podczas kontrolowania jakiejś instalacji — ale pozwalającego na identyfikację, będzie naruszać prawo do prywatności, jeżeli te osoby nie wyrażą zgody na bycie nagrywanym i nie będą miały możliwości skutecznego żądania zanonimizowania materiału[29]. Ogólnie rzecz biorąc, powyższa interpretacja jest zasadna, niemniej jednak jej stosowanie w stosunku do operacji z użyciem platform UAV napotyka praktyczne problemy, wynikające z operacyjnej charakterystyki działania omawianej technologii. O ile bowiem w przypadku systemów stacjonarnych dany obszar może być z powodzeniem oznaczony jako miejsce obserwowane — tak się dzieje w przypadku monitoringu (gdzie jeszcze na tabliczce może być na przykład adres e-mailowy albo telefon kontaktowy do instytucji gromadzącej dane) — to analogicznej czynności nie da się wykonać w przypadku drona. Obserwowana jednostka może nie mieć w ogóle świadomości, że w pobliżu znajduje się platforma UAV; w pobliżu może być także kilka dronów, należących do zupełnie różnych użytkowników, których przeznaczenie nie jest tej osobie znane; urządzenie może znajdować się w sporej odległości, a znajdujące się na pokładzie sensory i tak mogą z powodzeniem zarejestrować dane identyfikujące; wreszcie dana osoba może być świadoma obecności platformy UAV, ale nie wiedzieć, czy jest prowadzona obserwacja umożliwiająca jej identyfikację, bądź nie ma wiedzy, do kogo ów dron należy, czyli nie wie, wobec kogo miałaby zgłaszać ewentualne żądanie anonimizacji danych.

4. Operacje w miejscach publicznych prowadzące do naruszenia prywatności domu

Dom — miejsce chronione przez art. 8 Konwencji — określa się w orzecznictwie strasburskim w sposób funkcjonalny jako fizycznie zdefiniowaną przestrzeń, w której rozwija się życie rodzinne i prywatne, przy czym nie ma znaczenia, czy i jakiego rodzaju „węzeł" prawny — prawo własności, tytuł użytkowania — łączy ją z osobą, której prywatność podlega ochronie[30]. Ochrona na gruncie Konwencji obejmuje nie tylko wtargnięcie do domu, ale, co istotne w kontekście opisywanego

[29] Sprawa *Reklos i Davoulis v. Grecja*, skarga 1234/05, wyrok z 15 stycznia 2009 roku, pkt 40.

[30] Zob. sprawy *Buckley v. Zjednoczone Królestwo*, skarga 20348/92, wyrok z 18 stycznia 2001 roku, pkt 54; *Prokopovich v. Rosja*, skarga 58255/00, wyrok z 18 listopada 2004 roku, pkt 35–39; *Khamidov v. Rosja*, skarga 72118/01, wyrok z 15 listopada 2007 roku, pkt 128; *McCann v. Zjednoczone Królestwo*, skarga 19009/04, wyrok z 13 maja 2008 roku, pkt 46.

zagadnienia, także uniemożliwienie lub utrudnienie korzystania z jego wygód[31]. W kontekście tytułowej problematyki naruszenie prywatności można więc rozpatrywać w dwóch zasadniczych, powiązanych z sobą aspektach. Pierwszym będzie kwestia rejestrowania danych dotyczących osób znajdujących się w domu — w powyższym rozumieniu. Natomiast drugi dotyczy możliwości naruszenia prywatności poprzez samą obecność platformy UAV, wykonującej swoje nieinwigilacyjne zadania w pobliżu czyjegoś miejsca zamieszkania.

Dopuszczalne ograniczenia prawa do prywatności, skodyfikowanego w przepisie art. 8 Konwencji, podobnie jak wszystkie inne dopuszczalne odstępstwa od praw chronionych tym aktem, muszą być wprowadzone za pomocą ustaw, być proporcjonalne i niezbędne dla społeczeństwa demokratycznego[32]. Natomiast istniejące orzecznictwo dotyczące standardów ochrony prywatności w domu główny nacisk kładzie na wtargnięcia związane z rewizjami i zatrzymaniami, czyli sytuacje, gdzie są one jednoznacznie ukierunkowane na konkretną akcję wobec konkretnej osoby. Dlatego w kontekście omawianego zagadnienia konieczne jest stosowanie tego orzecznictwa *per analogiam*, uzupełnione przez dorobek dotyczący ukrytego monitoringu w miejscach publicznych. Chociaż należy zastrzec, że w tytułowym przypadku nie jest dokonywana jakakolwiek fizyczna ingerencja, gdyż dron cały czas znajduje się poza terenem posesji. Natomiast adekwatność dorobku poświęconego ukrytej obserwacji wynika z tego, że także w miejscach publicznych mogą istnieć wydzielone obszary, gdzie jednostka powinna oczekiwać prywatności, przez co relacja zasady do wyjątku stanowi pasujący element[33]. Jeżeli więc zgodnie z dorobkiem art. 8 Konwencji oczekiwanie prywatności jest wobec domu przyjmowane *a priori*, wówczas ocena wspomnianej sytuacji obserwacji przy użyciu platformy UAV wpisuje się w szablon interpretacyjny nagrywania z ukrycia, bez zgody.

W orzeczeniu w sprawie *Ismayilova* Trybunał określił takie działanie jako „szczególnie poważne i rażące" naruszenie art. 8 Konwencji i „niezwykle mocną" ingerencję w życie prywatne[34]. Z kolei w rozstrzygnięciu *Söderman* ETPCz wskazał, że stanowi to naruszenie „integralności osobistej", odnotowując, że związane ze wspomnianym nagrywaniem poczucie wrażliwości, bycia wyeksponowanym samo w sobie wystarczy do stwierdzenia naruszenia art. 8 Konwencji, zwłaszcza jeśli sytuacja dotyczy dzieci[35].

[31] Sprawy *López Ostra v. Hiszpania*, skarga 16798/90, wyrok z 9 grudnia 1994 roku, pkt 51; *Giacomelli v. Włochy*, skarga 59909/00, wyrok z 2 listopada 2006 roku, pkt 76; *Moreno Gomez v. Hiszpania*, skarga 4143/02, wyrok z 16 listopada 2004 roku, pkt 53; *Oluic v. Chorwacja*, skarga 61260/08, wyrok z 20 maja 2010 roku.

[32] Sprawa *L.M. v. Włochy*, skarga 60033/00, wyrok z 8 lutego 2005 roku, pkt 29 i 31.

[33] Zob. między innymi sprawy *López Ribalda i inni v. Hiszpania*, skargi 1874/13 i 8567/13, wyrok z 17 października 2019 roku; *Bărbulescu v. Rumunia*, skarga 61496/08, wyrok z 5 września 2017 roku.

[34] Sprawa *Ismayilova v. Rosja*, skarga 37614/02, wyrok z 29 listopada 2007 roku, pkt 116.

[35] Sprawa *Söderman v. Szwecja*, skarga 5786/08, wyrok z 12 listopada 2013 roku, pkt 81 i 85.

Można stwierdzić, że w odniesieniu do powyższej sytuacji naruszenie ma taki sam charakter jak „przypadkowe" zarejestrowanie informacji w miejscu publicznym i późniejsze oportunistyczne ich wykorzystanie przeciwko zarejestrowanym osobom, które *ex ante* nie były celem żadnego postępowania, jednak powaga wspomnianego naruszenia byłaby większa z racji tego, że oczekiwanie dotyczące poziomu prywatności w domu jest znacznie wyższe niż w przypadku miejsc publicznych. O ile zgodnie z istniejącym orzecznictwem osoba znajdująca się w przestrzeni publicznej musi liczyć się z tym, że jej działania zostaną zarejestrowane i poddane ocenie (w szerokim tego słowa znaczeniu), to w prywatnej przestrzeni analogiczne domniemane nie zachodzi[36]. Tym samym, choć w przypadku informacji gromadzonych w miejscach publicznych wskazuje się, że obserwowany/obserwowana powinien/powinna mieć skuteczną możliwość żądania anonimizacji danych, to w miejscu prywatnym analogiczny zabieg powinien być prowadzony z urzędu[37].

Kontrowersje budzi natomiast sytuacja, w której zarejestrowane zostałoby działanie *prima facie* przestępcze mające miejsce w domu[38]. Z jednej strony można wówczas powoływać się na stan wyższej konieczności — ochronę bezpośrednio zagrożonego życia — dla uzasadnienia interwencji, jeśli przestępstwo rzeczywiście wiązałoby się z takim ryzykiem. Natomiast powyższa interpretacja jest zasadna tylko wtedy, gdyby operator platformy UAV miał podgląd „na żywo", bo tylko wtedy istniałaby konieczność natychmiastowej interwencji. Natomiast jeżeli materiał uległby zarejestrowaniu i wzmiankowane przestępstwo zostałoby ujawnione dopiero później, podczas jego analizy na potrzeby wykonania zadania, dla którego został zebrany, to wówczas wymagana możliwość skutecznego żądania anonimizacji byłaby fikcyjna, a poza tym doszłoby do wykorzystania danych bez wyroku sądu i wcześniejszego istnienia uzasadnionego podejrzenia wobec konkretnych osób, czyli w sytuacji wskazywanej wcześniej jako niedopuszczalna na gruncie Konwencji[39]. Powyższe rozważania na razie pozostają spekulacją, gdyż Trybunał nie został jak dotąd skonfrontowany z koniecznością zbadania któregoś z naszkicowanych powyżej scenariuszy, natomiast biorąc pod uwagę dynamikę wzrostu wykorzystania technologii UAV, szansa ich wystąpienia nie jest jedynie teoretyczna.

Przechodząc do drugiego aspektu sygnalizowanego na początku tej części opracowania, skoro naruszeniem art. 8 Konwencji może być także uniemożliwie-

[36] Zob. The Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg 23 stycznia 2017 roku.

[37] Analogiczne rozwiązania są rekomendowane przez Radę Europy (zob. *ibidem*.), ponadto funkcjonują na gruncie RODO.

[38] *Prima facie* w tym sensie, że pobieżna obserwacja danej aktywności daje uzasadnione podejrzenie, że ma się do czynienia z przestępstwem.

[39] Zob. sprawy *Rotaru v. Rumunia*, pkt 43 i 44; *Malone v. Zjednoczone Królestwo*, skarga 8691/79, wyrok z 26 kwietnia 1985 roku, pkt 67 i 68; *Kennedy v. Zjednoczone Królestwo*, skarga 26839/05, wyrok z 18 maja 2010 roku, pkt 152.

nie lub utrudnienie korzystania z wygód domu, to można argumentować, że sama obecność drona w pobliżu posesji może powodować dyskomfort[40]. Ocena w tym względzie jest jednak w znacznej mierze subiektywna, gdyż ów brak poczucia komfortu może nie wynikać z hałasu — który na ogół nie jest duży — tylko z obawy przed ewentualną obserwacją[41]. Osoba przebywająca w domu nie ma możliwości stwierdzenia, czy taka obserwacja jest prowadzona, czy w ogóle dany dron wyposażony jest w urządzenia umożliwiające tego rodzaju działania, czy należy do jednostek publicznych, czy też osób prywatnych, jakie zadania wykonuje itp. Tym bardziej że obserwacja może być prowadzona „na żywo", bez zapisu zgromadzonych danych, przez co później nie będzie się dało udowodnić, że miała ona miejsce, co, abstrahując od tego, czy rzeczywiście sytuacja miała miejsce, może stanowić okoliczność powołaną jako wzmocnienie poczucia dyskomfortu.

Wzmiankowany subiektywny charakter braku komfortu jest o tyle istotny, że w sytuacji stale rosnącej popularności technologii UAV i coraz szerszego wachlarza jej zastosowań, nie wydaje się, żeby można było realistycznie zakładać, że każdy dron znajdujący się w polu widzenia posesji został tam umieszczony w celu inwigilacji. Tu oczywiście dużo będzie zależało od tego, jak konkretnie zachowuje się dane urządzenie — czy jest stale w polu widzenia posesji, czy pojawia się regularnie itp. — ale poza ogólną przesłanką wskazująca na możliwości naruszenia prywatności poprzez uciążliwość samo obserwowanie drona niewiele daje, bo istniejące technologie pozwalają prowadzić obserwację pozwalającą na identyfikację jednostki, niezależnie od tego, czy jest to zamierzone działanie, z tak dużej odległości, że obecność tego typu urządzenia nie będzie uciążliwa, a być może w ogóle nie będzie zauważalna. Oczywiście tutaj postulatem *de lege ferenda* będzie ustalenie zasad operacji uniemożliwiających szczególnie uciążliwe operacje, ale sama obecność platform UAV jest po prostu znakiem czasów.

5. Podsumowanie

W 1928 roku sędzia Sądu Najwyższego w Stanach Zjednoczonych Louis D. Brandeis napisał, że największym zagrożeniem dla wolności jednostki są działania osób, które mają dobre intencje, ale ich gorliwość nie idzie w parze ze zrozumieniem konsekwencji[42]. Choć od sformułowania powyższego poglądu upłynęło niemal sto lat i postęp technologiczny dokonał w tym czasie ogromnego kroku

[40] Nie ma bezpośrednio pasującego orzecznictwa, ale zob. *per analogiam* sprawy *Powell i Rayner v. Zjednoczone Królestwo*, skarga 9310/81, wyrok z 21 lutego 1990 roku; *Galev i inni v. Bułgaria*, skarga 18324/04, decyzja z 29 września 2009 roku.

[41] R. Clarke, L. Bennett Moses, *The regulation of civilian drones' impacts on public safety*, „Computer Law & Security Review" 2014, nr 30, s. 289–290.

[42] Sprawa *Olmstead v. Stany Zjednoczone Ameryki*, 277 U.S 438, 485, 1928 (zdanie odrębne), cyt. za: T. Takahshi, *op. cit.*, s. 113.

naprzód, powyższe stwierdzenie pozostaje w pełni aktualne. Wyzwania stojące przed władzami publicznymi, dotyczące wykorzystania „przypadkowo" zebranych podczas działań, które nie mają na celu inwigilacji, danych polegają, ogólnie mówiąc, na dostrzeganiu konsekwencji, którymi w tym przypadku będzie możliwe naruszenie prawa do prywatności gwarantowanego na gruncie Konwencji. Od rządzących wymaga się więc pewnego samoograniczenia; mówiąc nieco eufemistycznie, powstrzymania się od pokusy wykorzystania informacji, których gromadzenie staje się łatwiejsze dzięki coraz doskonalszym technologiom.

Można powiedzieć, że trzon orzecznictwa strasburskiego, który dotyczy gromadzenia danych w kontekście prawa do prywatności, zasadniczo daje się zastosować *per analogiam* do działalności platform bezzałogowych. Niemniej jednak przeprowadzona analiza wykazała, że potencjalnie problematyczna pozostaje kwestia informowania o obserwacji, która co prawda nie jest wymierzona w konkretne osoby, ale może ze względu na uwarunkowania techniczne prowadzić do zgromadzenia danych osobowych. O ile w przypadku systemów stacjonarnych informacje na temat działania monitoringu w miejscach publicznych co do zasady wyeliminują ryzyko naruszenia art. 8 Konwencji, o tyle przypadku dronów jest to fizycznie niewykonalne. Tym samym znacznemu utrudnieniu ulega — patrząc z perspektywy czysto technicznej — spełnienie wymogu zapewnienia możliwości skutecznego żądania anonimizacji danych, jeśli zostały zebrane w miejscach/sytuacjach, gdzie występuje oczekiwanie prywatności. Wspominane samoograniczenie władzy dotyczy więc przede wszystkim standardów dotyczących anonimizacji/ograniczania dostępu, gdyż w przypadku dronów udostepnienie informacji, czy gromadzone są dane, kto to robi, dlaczego i do kogo zgłaszać się w kwestii wglądu do zebranych materiałów i roszczenia anonimizacji, jest technicznie niewykonalne. Jednocześnie, choć prawo Unii Europejskiej znajduje się poza zakresem niniejszej analizy, zasadne jest odnotowanie, że duża cześć rozwiązań, które stanowiłyby odpowiedź na wskazane w tekście niedopasowanie istniejącego orzecznictwa ETPCz do niektórych wyzwań stawianych przez technologie UAV, funkcjonuje na gruncie prawa UE w ramach RODO, zatem obowiązuje już w państwach należących też do Rady Europy. Wydaje się, że te rozwiązania mogą stanowić użyteczną inspirację da trybunału w Strasburgu, choć oczywiście nie dyrektywę interpretacyjną w ścisłym tego słowa znaczeniu. W kontekście ewolucji dorobku orzeczniczego ETPCz należałoby zatem postulować odejście od wymaganego standardu dotyczącego istnienia żądania anonimizacji danych i uznanie za naruszające art. 8 Konwencji zebranie danych niesłużących inwigilacji bez następującej z urzędu anonimizacji. Wymagałoby to w pierwszym rzędzie spojrzenia na funkcjonujące w państwach-sygnatariuszach Konwencji rozwiązania dotyczące zasad gromadzenia informacji, gdyż tutaj możliwe jest wprowadzenie *ex ante* rozwiązania systemowego.

Bibliografia

Literatura

Clarke R., Bennett Moses L., *The regulation of civilian drones' impacts on public safety*, „Computer Law & Security Review" 2014, nr 30, DOI: https://doi.org/10.1016/j.clsr.2014.03.007.

Finn R., Wright D., *Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications*, „Computer Law & Security Review" 2012, nr 28 (2), DOI: https://doi.org/10.1016/j.clsr.2012.01.005.

Hughes K., *Photographs in Public Places and Privacy*, „Journal of Media Law" 2009, nr 2.

Stahl T., *Indiscriminate mass surveillance and the public sphere*, „Ethics and Information Technology" 2016, nr 18, DOI: https://doi.org/10.1007/s10676-016-9392-2.

Takahashi T., *Drones and Privacy*, „The Columbia Science and Technology Law Review" 2012, nr 16.

Zalnieriute M., *An international constitutional moment for data privacy in the times of mass-surveillance*, „International Journal of Law and Information Technology" 2015, nr 23 (2), DOI: https://doi.org/10.1093/ijlit/eav005.

Orzecznictwo

Altay v. Turcja, skarga 11236/09, wyrok ETPCz z 9 kwietnia 2019 roku.

Amann v. Szwajcaria, skarga 27798/95, wyrok ETPCz z 16 lutego 2000 roku.

Association for European Integration and Human Rights i Ekimdzhiev v. Bułgaria, skarga 62540/00, wyrok ETPCz z 28 czerwca 2007 roku.

Bărbulescu v. Rumunia, skarga 61496/08, wyrok ETPCz z 5 września 2017 roku.

Buckley v. Zjednoczone Królestwo, skarga 20348/92, wyrok ETPCz z 18 stycznia 2001 roku.

Ćwik v. Polska, skarga 31454/10, wyrok ETPCz z 5 listopada 2020 roku.

Doerga v. Holandia, skarga 50210/99, wyrok ETPCz z 27 kwietnia 2004 roku.

Dumitru Popescu v. Rumunia (no 2), skarga 71525/01, wyrok ETPCz z 26 kwietnia 2007 roku.

Egeland i Hanseid v. Norwegia, skarga 34438/04, wyrok ETPCz z 16 lipca 2009 roku.

Friedl v. Austria, skarga 15225/89, wyrok ETPCz z 31 stycznia 1995 roku.

Friend i Countryside Alliance i inni v. Zjednoczone Królestwo, skargi 16072/06 i 27809/08, decyzja EKPCz z 24 listopada 2009 roku.

Galev i inni v. Bułgaria, skarga 18324/04, decyzja EKPCz z 29 września 2009 roku.

Giacomelli v. Włochy, skarga 59909/00, wyrok ETPCz z 2 listopada 2006 roku.

Gillan i Quinton v. Zjednoczone Królestwo, skarga 4158/05, wyrok ETPCz z 12 stycznia 2010 roku.

Halford v. Zjednoczone Królestwo, skarga 20605/92, wyrok ETPCz z 25 czerwca 1997 roku.

Iordachi i inni v. Mołdawia, skarga 25198/02, wyrok ETPCz z 10 lutego 2009 roku.

Ismayilova v. Rosja, skarga 37614/02, wyrok ETPCz z 29 listopada 2007 roku.

Kennedy v. Zjednoczone Królestwo, skarga 26839/05, wyrok ETPCz z 18 maja 2010 roku.

Khamidov v. Rosja, skarga 72118/01, wyrok ETPCz z 15 listopada 2007 roku.

Klass v. Niemcy, skarga 5029/71, wyrok ETPCz z 6 września 1978 roku.

Krone Verlag GmbH v. Austria, skarga 27306/07, wyrok ETPCz z 19 czerwca 2012 roku.

Kurier Zeitungsverlag und Druckerei GmbH (no. 2) v. Austria, skarga 1593/06, wyrok ETPCz z 19 czerwca 2012 roku.

L.M. v. Włochy, skarga 60033/00, wyrok ETPCz z 8 lutego 2005 roku.
Liberty i inni v. Zjednoczone Królestwo, skarga 58243/00, wyrok ETPCz z 1 czerwca 2008 roku.
López Ostra v. Hiszpania, skarga 16798/90, wyrok ETPCz z 9 grudnia 1994 roku.
López Ribalda i inni v. Hiszpania, skargi 1874/13 i 8567/13, wyrok ETPCz z 17 października 2019 roku.
Malone v. Zjednoczone Królestwo, skarga 8691/79, wyrok ETPCz z 26 kwietnia 1985 roku.
McCann v. Zjednoczone Królestwo, skarga 19009/04, wyrok ETPCz z 13.5.2008 roku.
Moreno Gomez v. Hiszpania, skarga 4143/02, wyrok ETPCz z 16 listopada 2004 roku.
Nicolae Virgiliu Tănase v. Rumania, skarga 41720/13, wyrok ETPCz z 25 czerwca 2019 roku.
Olmstead v. Stany Zjednoczone Ameryki, 277 U.S 438, 485 (1928), wyrok Sądu Najwyższego Stanów Zjednoczonych z 4 czerwca 1928 roku.
Oluic v. Chorwacja, skarga 61260/08, wyrok ETPCz z 20 maja 2010 roku.
P.G. and J.H. v. Zjednoczone Królestwo, skarga 44787/98, wyrok ETPCz z 6 lutego 2001 roku.
Peck v. Zjednoczone Królestwo, skarga 44647/98, wyrok ETPCz z 28 stycznia 2003 roku.
Peev v. Bułgaria, skarga 64209/01, wyrok ETPCz z 26 lipca 2007 roku.
Perry v. Zjednoczone Królestwo, skarga 63737/00, wyrok ETPCz z 17 lipca 2003 roku.
Powell i Rayner v. Zjednoczone Królestwo, skarga 9310/81, wyrok ETPCz z 21 lutego 1990 roku.
Ramanauskas v. Litwa, skarga 74420/01, wyrok ETPCz z 5 lutego 2008 roku.
Reklos i Davoulis v. Grecja, skarga 1234/05, wyrok ETPCz z 15 stycznia 2009 roku.
Rodina v. Łotwa, skargi 48534/10 i 19532/15, wyrok ETPCz z 14 maja 2020 roku.
Roman Zakharov v. Rosja, skarga 47143/06, wyrok ETPCz z 4 grudnia 2015 roku.
Rotaru v. Rumunia, skarga 28341/95, wyrok ETPCz z 4 maja 2000 roku.
Segerstedt-Wiberg i inni v. Szwecja, skarga 62332/00, wyrok ETPCz z 6 czerwca 2006 roku.
Söderman v. Szwecja, skarga 5786/08, wyrok ETPCz z 12 listopada 2013 roku.
Szabó i Vissy v. Węgry, skarga 37138/14, wyrok ETPCz z 12 stycznia 2016 roku.
Társaság a Szabadságjogokért v. Węgry, skarga 37374/05, wyrok ETPCz z 14 kwietnia 2009 roku.
Uzun v. Niemcy, skarga 35623/05, wyrok ETPCz z 2 września 2010 roku.
Von Hannover v. Niemcy (no. 2), skargi 40660/08 i 60641/08, wyrok ETPCz z 7 lutego 2012 roku.
Von Hannover v. Niemcy, skargi 40660/08 i 60641/08, wyrok ETPCz z 7 lutego 2012 roku.
Weber i Saravia v. Niemcy, skarga 54934/00, decyzja EKPCz z 29 czerwca 2006 roku.
X v. Zjednoczone Królestwo, skarga 5877/72, decyzja EKPCz z 12 października 1973 roku.

Akty prawne

Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO), Dz.Urz. UE z 2016 r. L 119/1.
The Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Strasbourg 23 stycznia 2017 roku.