PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ OPERATORÓW BEZZAŁOGOWYCH STATKÓW POWIETRZNYCH

ANNA KONERT*

DOI: 10.26399/iusnovum.v15.2.2021.12/a.konert

1. WPROWADZENIE

Postęp technologiczny w zakresie bezzałogowych statków powietrznych (dalej BSP), zwanych potocznie dronami, wiąże się nierozerwalnie z prawem do prywatności oraz ochroną danych osobowych. Działalność prowadzona z wykorzystaniem dronów jest szczególnie wrażliwa z punktu widzenia danych osobowych, gdyż często wyposażone są one w urządzenia rejestrujące obraz lub dźwięk. Operator drona może z łatwością wchodzić w posiadanie dużej ilości danych kwalifikowanych jako dane osobowe, w tym wizerunku, lub też innych danych pozwalających zidentyfikować daną osobę, która nie wyraziła na to zgody[1].

Warunki użytkowania bezzałogowych statków powietrznych, wraz z elementami koniecznymi dla zapewnienia bezpiecznego wykonywania operacji z udziałem BSP, zostały określone przez przepisy prawa publicznego. W dniu 11 września 2018 r. weszło w życie rozporządzenie Parlamentu Europejskiego i Rady w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Bez-

* dr hab., profesor Uczelni Łazarskiego, Dziekan Wydziału Prawa i Administracji Uczelni Łazarskiego w Warszawie, e-mail: a.konert@lazarski.edu.pl, ORCID: 0000-0002-1188-7087

** Artykuł powstał jako efekt projektu badawczego „Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym." finansowanego przez Narodowe Centrum Nauki (nr 2017/27/B/HS5/00008).

[1] Zob. M. Ottavio, *Privacy and Data Protection Implications of the Civil Use of Drones*, Brussels: Directorate General for Internal Policies. Policy Department C: Citizens' Rights and Constitutional Affairs. Civil liberties, justice and home affair, 2015; R.L. Finn, D. Wright, *Privacy, Data Protection and Ethics For Civil Drone Practice: A Survey of Industry, Regulators and Civil Society Organisations*, „Computer Law & Security Review" 2016, vol. 32, iss. 2; M.E. Steward, *Privacy Aspects Of Drones: Is There a Gap In Australia's Laws In Relation To The Protection of Privacy From Private Civil Use of Remotely Piloted Aircraft Systems?: In Particular, Does The Legislation Addressing Data Protection, Trespass To Land and Private Nuisance Need To Be Reformed?*, Thesis Master in Air and Space Law, Leiden University, 2015 (niepublikowana).

pieczeństwa Lotniczego Unii Europejskiej oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 216/2008 (zwane nowym rozporządzeniem bazowym lub NBR – New Basic Regulation). W dniu 11 czerwca 2018 r. EASA opublikowała rozporządzenia delegowane i wykonawcze komisji w sprawie bezzałogowych statków powietrznych: Rozporządzenie delegowane Komisji (UE) 2019/945 z dnia 12 marca 2019 r. w sprawie bezzałogowych systemów powietrznych oraz operatorów bezzałogowych systemów powietrznych z państw trzecich[2], oraz Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych[3]. Celem wprowadzenia nowych regulacji jest przede wszystkim zapewnienie bezpieczeństwa przy wykonywaniu operacji bezzałogowymi statkami powietrznymi oraz ochrona prywatności, ochrona danych osobowych i ochrona środowiska, przy jednoczesnym umożliwieniu swobodnego dostępu do przestrzeni powietrznej dla BSP[4].

W niniejszym artykule zostanie dokonana analiza przepisów oraz dokumentów dotyczących ochrony danych osobowych w sytuacji ich przetwarzania przez operatorów dronów. Szczegółowe zagadnienia związane z wpływem przepisów o ochronie danych osobowych na rynek dronowy wraz z analizą praw i obowiązków operatorów dronów zostały przedstawione w artykule: A. Konert, M. Sakowska-Baryła, *Impact of the GDPR on the Unmanned Aircraft Sector*, „Air and Space Law" 2021. Ponadto te same Autorki dokonały analizy przepisów o ochronie danych osobowych oraz Kodeksu cywilnego w zakresie odpowiedzialności za naruszenie prawa do prywatności przez dziennikarzy używających dronów w artykule *Prawne uregulowania w zakresie używania bezzałogowych statków powietrznych przez media*, „International Journal of Legal Studies" 2020, t. 8, nr 2[5].

Celem niniejszego artykułu jest ustalenie obowiązków operatorów dronów (jako administratorów w rozumieniu przepisów o ochronie danych osobowych) oraz konsekwencji prawnych w sytuacji, w której dany rodzaj operacji wykonywanej przy użyciu drona (ze względu na swój charakter, zakres, kontekst i cele) z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Aby osiągnąć ten cel, należy, po pierwsze, wskazać na rodzaje operacji z udziałem dronów, co do których będą miały zastosowanie przepisy o ochronie danych osobowych, oraz po drugie, ustalić, w jakich sytuacjach mamy do czynienia z „wysokim ryzykiem naruszenia praw lub wolności osób fizycznych".

---

[2] Dz.Urz. UE L 152 z 11.06.2019.

[3] Dz.Urz. UE L 152/45 z 11.06.2019.

[4] Por. A. Konert, *Odpowiedzialność operatora bezzałogowego statku powietrznego za opóźnienie lub odwołanie lotu*, „Ius Novum" 2021, nr 1, s. 155. Zob. szerzej P. Kasprzyk, *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym. Rozwój regulacji prawnych dotyczących bezpieczeństwa lotnictwa bezzałogowego*, Warszawa 2021; M. Ostrihansky, M. Szmigiero, *Prawo dronów. Bezzałogowe statki powietrzne w prawie Unii Europejskiej oraz krajowym*, Warszawa 2020; M. Osiecki, *Drony – przyszłość lotnictwa i wyzwanie legislacyjne. Kilka uwag o nowych regulacjach unijnych dotyczących bezzałogowych statków powietrznych*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, nr 7.

[5] https://ijols.com/resources/html/article/details?id=211785 (dostęp: 23.06.2021).

2. OCHRONA ADMINISTRACYJNA W ŚWIETLE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

Ochrona danych osobowych jest pewnego rodzaju wyspecjalizowaną konstrukcją, która służy ochronie tych samych wartości, które służą ochronie prawa do prywatności[6]. Dane osobowe podlegają ochronie cywilnoprawnej (art. 23 i n. k.c.) oraz administracyjnoprawnej.

Ochrona administracyjnoprawna uregulowana jest szczegółowo w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO). Rozporządzenie zaczęło obowiązywać bezpośrednio w krajowych porządkach prawnych od 25 maja 2018 r. i wprowadziło wiele zmian oraz rozszerzyło zakres obowiązków administratorów i podmiotów przetwarzających dane. Celem RODO, poza ochroną podstawowych praw i wolności osób fizycznych, jest też wyposażenie osób fizycznych oraz organów nadzorujących w skuteczne narzędzia reagowania na naruszenia przepisów tego rozporządzenia[7].

W ramach zmian dostosowujących do RODO, w Polsce uchwalono Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej: UODO) oraz zmiany w przepisach sektorowych. UODO zawiera w szczególności ograniczenia lub wyłączenia przepisów ustawy lub RODO (art. 2–6 ustawy), wskazuje na organy publiczne zobowiązane do wyznaczenia inspektora ochrony danych, zawiera przepisy dotyczące certyfikacji w zakresie ochrony danych osobowych, o której mowa w art. 42 RODO (art. 12–26), kodeksu postępowania, o których mowa w art. 40 RODO, wskazuje na Prezesa Urzędu Ochrony Danych Osobowych jako organ nadzorczy (art. 34–59 ustawy), określa postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych (art. 60–74 ustawy), a także wprowadza kontrolę przestrzegania przepisów o ochronie danych osobowych (art. 78–91 ustawy)[8].

---

[6] P. Sarnecki, Art. 47, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, III, red. L. Garlicki, Warszawa 2003, s. 4.

[7] Szerzej zob. M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2014; *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, oraz *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017.

[8] Szerzej zob. M. Rycak, *Komentarz do ustawy z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych* (Dz.U. nr 100, poz. 1087), Komentarz do Dziennika Ustaw Nr 37, rok V, 7 października 2001 r.

3. SPECYFIKA PRZEPISÓW OCHRONY DANYCH OSOBOWYCH ZE WZGLĘDU NA UŻYCIE BEZZAŁOGOWYCH STATKÓW POWIETRZNYCH

Przepisy rozporządzenia 2016/679 mogą mieć zastosowanie podczas wykonywania niektórych operacji z użyciem bezzałogowych statków powietrznych, jeśli ma miejsce przetwarzanie danych osobowych (w sposób zautomatyzowany lub nie) oraz gdy operator drona (administrator danych) prowadzi działalność w UE, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

Przepisy RODO mogą mieć zastosowanie w wielu przypadkach używania BSP. Dane gromadzone, przechowywane i przetwarzane, które zawierają „dane osobowe", takie jak imię i nazwisko, adres e-mail, numery telefonów lub zdjęcia lotnicze. muszą być zgodne z zasadami RODO[9]. Większość dronów na rynku to urządzenia zdolne do gromadzenia dużych ilości danych[10].

Zapisy lotów dokonane przez bezzałogowe statki powietrzne będą często zawierały dane osobowe, na przykład wizerunek danej osoby, jeśli twarz osoby jest wyraźnie widoczna. Dane te są najczęściej zbierane bez zgody podmiotów, których dotyczą. Jeśli jednak osoby są w oddali, a twarze – rozmyte, jest mało prawdopodobne, że zostaną uznane za dane osobowe. Jednakże identyfikacja nastąpić może w inny sposób, przykładowo poprzez lokalizację, widoczne numery adresowe, numery tablic rejestracyjnych, konkretną odzież itp. Przepisy RODO mają zastosowanie, gdy dron rejestruje szczegóły dotyczące cech fizycznych osoby, jej zachowania, życia prywatnego lub jej działalność zawodową[11]. Nie dochodzi do przetwarzania danych osobowych w sytuacji, gdy oprogramowanie drona automatycznie maskuje i anonimizuje dane osobowe.

W razie używania dronów do fotografowania, na przykład podczas ślubu, mapowania nieruchomości lub do jakiejkolwiek innej działalności komercyjnej, podlegają one RODO, ponieważ zawierają obrazy osób, które posiadają informacje identyfikacyjne. Nie dotyczy to sytuacji, w której zdjęcia są wykorzystywane w celach informacyjnych lub w sztuce. Należy wówczas uzyskać zgodę osoby na opublikowanie zdjęć. Ponadto przepisy RODO mają zastosowanie w sytuacji użycia dronów przy przeprowadzaniu inspekcji i monitorowaniu, kiedy osoby mogą być oznakowane lub zidentyfikowane[12].

---

[9] Według art. 4 RODO „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

[10] Cyt. za A. Konert, *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym. Zagadnienia cywilnoprawne*, Warszawa 2020, s. 160.

[11] Ibidem.

[12] Ibidem.

RODO nie ma również zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze (art. 2 ust. 2 lit. c).

Zgodnie z art. 2 ust. 2 lit. d przepisy RODO nie będą miały zastosowania do przetwarzania danych osobowych przez służby publiczne, które używają dronów, w ramach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych, lub wykonywania kar, w tym w celu ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom (tzw. *law enforcement*). Przykładowo używanie dronów rejestrujących obraz (gromadzących zdjęcia ludzi) przez policję w celu zapewnienia bezpieczeństwa państwowego nie będzie podlegało przepisom RODO. Problematyka używania dronów przez służby publiczne wymaga odrębnej analizy.

Realizacja prawa do prywatności i ochrony danych osobowych wspierana jest przez dwie koncepcje prawne: *privacy by design* (zasada prywatności w fazie projektowania oznacza takie podejście do projektowania, w którym istnieje konieczność zachowania odpowiedniego poziomu prywatności, oraz informowania o tym użytkowników na każdym etapie tworzenia produktu tak, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową), oraz *privacy by default* (zasada prywatności w ustawieniach domyślnych, czyli koncepcja według której wyłącznie dane osobowe konieczne do realizacji danego celu powinny podlegać przetwarzaniu, a ponadto jedynie przez okres niezbędny do jego realizacji)[13].

Planując operacje bezzałogowym statkiem powietrznym, operatorzy dronów i piloci powinni dążyć do zminimalizowania wpływu na prywatność i dane osobowe ludzi na ziemi zarówno w fazie projektowania, jak i w ustawieniach domyślnych, czyli przy planowaniu lotu, ustalając konkretny tor lotu, przy używaniu wyposażenia BSP oraz przy zarządzaniu zgromadzonymi danymi[14]. W fazie planowania lotu operator BSP powinien odpowiedzieć na następujące pytania:

- Gdzie i kiedy powinien odbyć się lot?
- Jaka jest okolica lotu?
- Jakie informacje, przed, w trakcie i po locie, należy rozpowszechniać i komu?
- Kiedy należy włączyć czujniki danych i kiedy dane powinny być rejestrowane?[15]

Używając wyposażenia BSP, operator powinien odpowiedzieć na następujące pytania:

- Jakie wyposażenie i funkcje powinien posiadać BSP?
- Jaki sprzęt nie jest konieczny?
- W jaki sposób zagwarantowane zostanie bezpieczeństwo danych?

---

[13] Szerzej zob. A. Konert, M. Sakowska-Baryła, *Impact of the GDPR on the Unmanned Aircraft Sector*, „Air and Space Law" 2021. Koncepcje *privacy by design* oraz *privacy by default* zostały zdefiniowane w przepisach rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.

[14] Kodeks postępowania w zakresie prywatności (Privacy Code of Conduct) dostępny jest na stronie: https://dronerules.eu/assets/files/PCC_DR_final-for-printing_9-November-2018.pdf (dostęp: 08.01.2021), s. 11.

[15] Ibidem.

- W jaki sposób zgromadzone dane zostaną zminimalizowane?
- Czy piloci wiedzą, jak obsługiwać sprzęt?[16]

Wreszcie, przy zarządzaniu zgromadzonymi danymi, operator BSP powinien odpowiedzieć na następujące pytania:

- W jaki sposób gromadzone dane będą przetwarzane bezpiecznie?
- Jak dane będą przechowywane i przesyłane?
- W jaki sposób zgromadzone dane zostaną zminimalizowane?
- Jak i kiedy dane osobowe zostaną zanonimizowane lub usunięte?
- Komu zostaną udostępnione dane i pod jakimi warunkami?[17]

4. KODEKS POSTĘPOWANIA W ZAKRESIE PRYWATNOŚCI (PRIVACY CODE OF CONDUCT)

Kodeks postępowania w zakresie prywatności, uchwalony w 2018 r. w ramach projektu DroneRules PRO, stanowi praktyczny przewodnik po wymogach dotyczących prywatności i ochrony danych dla operatorów i pilotów dronów[18].

Kodeks ten ma pomóc w kierowaniu działaniami operatorów i pilotów dronów podczas wykonywania działań komercyjnych z ich wykorzystaniem. Kodeks może pomóc przedsiębiorstwom w planowaniu działalności i ustanowieniu sformalizowanego zestawu zasad postępowania, aby ułatwić przestrzeganie wymogów określonych w RODO. Nie jest on prawnie wiążącym dokumentem i powinien być wykorzystywany jako źródło wskazówek i wiedzy wraz z innymi zasobami dostępnymi na stronie internetowej DroneRules.eu[19].

Kodeks zawiera rekomendacje dla operatorów i pilotów dronów, mające na celu zminimalizowanie wpływu na prywatność i dane osobowe ludzi na ziemi podczas wykonywania operacji w różnych rodzajach przestrzeni. W razie więc wykonywania operacji w przestrzeni publicznej, jak na ulicach, w parkach, na plaży itp., operatorzy dronów i piloci nie powinni celować w lub systematycznie nagrywać ludzi bez ich wiedzy i zgody. Należy także unikać prowadzenia operacji w tym samym miejscu przez dłuższy czas, chyba że jest to konieczne do celów operacji. Wówczas należy wyraźnie poinformować osoby mieszkające, pracujące i przechodzące regularnie w tym obszarze o szczegółach operacji[20].

Wykonując operacje w pobliżu przestrzeni prywatnych (domy, tarasy, ogrody i prywatne pojazdy), operatorzy dronów i piloci powinni tak zaplanować tor lotu i kąty, pod którymi dane są przechwytywane przez czujniki dronów, aby zminimalizować ryzyko nagrania ludzi w ich prywatnych domach, obiektach biznesowych lub w pojeździe, chyba że jest to konieczne do celów operacji[21]. Zaleca się, by nie

---

[16] Ibidem.
[17] Ibidem.
[18] Kodeks dostępny jest na stronie: https://dronerules.eu/assets/files/PCC_DR_final-for-printing_9-November-2018.pdf (dostęp: 08.01.2021).
[19] Ibidem, s. 3.
[20] Ibidem, s. 12.
[21] Ibidem, s. 13.

wykonywać operacji dronem nad nieruchomościami prywatnymi na wysokościach poniżej 20 metrów bez zgody właścicieli lub najemców nieruchomości[22].

Wreszcie rekomendacje dotyczą także tak zwanych wrażliwych miejsc, czyli obszarów lub budynków, w których mogą znajdować się dzieci, osoby starsze, osoby chore psychicznie, uchodźcy, więźniowie itp. Będą to więc szkoły, przedszkola lub place zabaw, domy starców, ośrodki dla uchodźców, więzienia itp. Do wrażliwych miejsc zalicza się również obiekty, w których mogłyby zostać ujawnione wrażliwe lub potencjalnie zawstydzające informacje o ludziach wchodzących lub wychodzących, takich jak budynki religijne, siedziba partii politycznych, szpitale lub kliniki pchychiatryczne itp. W takich sytuacjach operatorzy dronów i piloci powinni zaplanować tory lotu i kąty, pod którymi dane są przechwytywane przez czujniki dronów, w taki sposób, aby zminimalizować ryzyko nagrania ludzi wewnątrz tych obiektów lub w trakcie wchodzenia lub wychodzenia z nich, chyba że jest to konieczne do celów operacji. Ponadto należałoby dokładnie zaplanować czas lotu, na przykład porę dnia i dzień tygodnia tak, aby zminimalizować ryzyko nagrania osób w tych lokalizacjach. Oznacza to, że nie powinno się wykonywać operacji BSP przy kościele w trakcie trwania mszy lub przy szpitalu w trakcie dowozu rannych z wypadku karetką pogotowania ratunkowego. Należy poinformować odpowiednich przedstawicieli takich lokalizacji o szczegółach operacji[23].

Należy także pamiętać o strefach zakazanych dla operacji BSP, ustalanych zwykle przez przepisy krajowe[24] lub przez tak zwany *geofencing*[25].

5. OCENA SKUTKÓW

5.1. ZASADY OGÓLNE

Jeżeli dany rodzaj operacji wykonywanych przy użyciu bezzałogowych statków powietrznych (ze względu na swój charakter, zakres, kontekst i cele) z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to zgodnie z art. 35 ust. 1 RODO operator BSP (jako administrator) przed rozpoczęciem przetwarzania ma obowiązek dokonać tak zwanej oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (Data Protection Impact Assessment, DPIA).

Rozporządzenie wyraźnie wskazuje, że DPIA jest wymagana w szczególności w przypadku systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwa-

---

[22] EASA, Draft acceptable means of compliance (AMC) and guidance material (GM): https://www.easa.europa.eu/sites/default/files/dfu/Draft%20AMC%20%20GM%20to%20draft%20Regulation%20…-…%20and%20to%20the%20draft%20Annex%20%28Part-U….pdf (dostęp: 08.01.2021).

[23] Privacy Code of Conduct, op. cit., s. 13.

[24] Zob. P. Kasprzyk, *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym*, op. cit.

[25] BSP powinien być wyposażony przez system ostrzegania oraz mieć aktualne bazy danych lokalizacji.

rzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie. W pozostałych przypadkach taka ocena musi być dokonywana przez każdy podmiot samodzielnie, uwzględniając przykładowo wielkość, strukturę organizacyjną, możliwości techniczne, zakres i rodzaj danych, czy też cel ich przetwarzania. Ustawodawca nie wskazuje więc konkretnych środków i procedur w zakresie bezpieczeństwa, takich jak kontrola dostępu, szyfrowanie, sposoby monitorowania procesów przetwarzania itp. Zobowiązanie podmiotów do samodzielnego przeprowadzania oceny ryzyka umożliwia skoncentrowanie się na sytuacjach najwyższego ryzyka. Wiele motywów preambuły RODO (np. 75, 76, 77, 84, 86, 89) oraz jego przepisów (np. art. 34, 35, 36) dotyczy ryzyka lub wysokiego ryzyka. Pojęcie ryzyka używane w tych przepisach można zdefiniować jako „wpływ niepewności na cele", czyli że ryzyko jest czymś negatywnym, co może niekorzystnie wpłynąć na osiągnięcie celu przez wywołanie niepożądanych skutków ubocznych[26].

Ocena skutków dla ochrony danych to proces, który pomaga organizacjom w identyfikowaniu i minimalizowaniu ryzyka związanego z prywatnością. Jest ona wymagana zawsze wtedy, gdy:

– dany rodzaj przetwarzania jest wskazany w przepisie prawa, czyli np. art. 53 ust. 3 RODO 9 (w przypadku systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie),
– dany rodzaj przetwarzania jest wskazany w wykazie podanym do publicznej wiadomości przez krajowy organ nadzorczy (art. 35 ust. 4 RODO),
– poziom ryzyka został uznany za wysoki przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania[27].

Wysokie ryzyko naruszenia praw lub wolności osób fizycznych występuje w szczególności wtedy, gdy gromadzone dane osobowe są wykorzystywane do ustalenia, czy osoby fizyczne otrzymują określone świadczenia, na przykład projekty budowlane lub infrastrukturalne; gdy regularnie nagrywa się osoby wchodzące lub wychodzące z budynków religijnych, placówek medycznych, posterunków policji, siedziby partii politycznej lub domów publicznych itp., a także gdy

[26] Jak rozumieć podjeście oparte na ryzyku? Poradnik RODO Podejście oparte na ryzyku, UODO maj 2018, https://www.uodo.gov.pl/pl/383/208 (dostęp: 14.01.2021).

[27] Jak stosować podejście oparte na ryzyku? Poradnik RODO Podejście oparte na ryzyku, UODO maj 2018, https://www.uodo.gov.pl/pl/383/208 (dostęp: 14.01.2020). Tam zob. tabelę szacowania poziomu ryzyka, s. 22.

wykonuje się operacje dronem regularnie lub przez dłuższy czas nad tym samym obszarem[28].

Jednorazowe zdarzenia lub operacje, których dotyczy tylko ograniczona liczba osób, najprawdopodobniej nie kwalifikują się jako stwarzające „wysokie ryzyko naruszenia praw lub wolności osób fizycznych".

Ocenę ryzyka należy dokonać dla każdej operacji lub można zastosować tę samą ocenę dla zestawu podobnych operacji. Podobne operacje obejmują również operacje prowadzone wspólnie przez kilka podmiotów. Ta sama ocena może być zatem stosowana przez dwóch operatorów BSP ściśle ze sobą współpracujących podczas danej operacji.

Ocena pozwoli określić sposób ochrony praw osób, których dane osobowe są przetwarzane. Odpowiedzi na pytania, które należy zadać w takiej ocenie, powinny określać proporcjonalność i przejrzystość działań operatora BSP oraz wskazywać na stopień poinformowania osób, których dane dotyczą, a także określać prawa osób, których dane są przetwarzane.

Podczas przeprowadzania oceny zaleca się zaangażowanie ekspertów i zainteresowanych stron. Powinno się też zasięgnąć wskazówek inspektora ochrony danych (DPO), jeśli jest wyznaczony zgodnie z art. 35 ust. 2 RODO. Będzie on również odpowiedzialny za monitorowanie wdrażania oceny skutków w zakresie ochrony danych w praktyce.

Ocena nie jest konieczna w przypadku, gdy operator BSP nie jest administratorem danych i umownie przeniósł tę rolę na kogoś innego lub gdy operacja dronem objęta jest wyjątkiem od przeprowadzenia oceny, określonym przez właściwy organ ochrony danych, lub też gdy operacje BSP prowadzi się w celu wypełnienia innych lub konkurujących obowiązków prawnych lub zadania w interesie publicznym, pod warunkiem, że w trakcie procesu legislacyjnego przeprowadzono ocenę skutków[29].

5.2. PODRĘCZNIK I SZABLON OCENY WPŁYWU NA PRYWATNOŚĆ

W ramach projektu DroneRules PRO powstał podręcznik i szablon oceny wpływu na prywatność (*A Privacy Impact Assessment Handbook and Template*)[30]. Szablon zapewnia ustrukturyzowane podejście do bezpieczeństwa w operacjach BSP oraz stanowi zestaw pytań, które pomogą operatorom dronów zidentyfikować główne informacje na temat operacji drona, poprzez rozważenie ewentualnych zagrożeń dla prywatności, i określić odpowiednie zabezpieczenia. W szablonie należy uwzględnić informacje dotyczące:

- operacji BSP – lokalizacja, trasa lotu, czas trwania i kontekst,
- używanego sprzętu,

---

[28] DroneRules PRO, *A Privacy Impact Assessment Handbook and Template*, s. 7, https://dronerules.eu/assets/files/DRPRO_Data_Protection_Impact_Assessment_EN.pdf (dostęp: 24.01.2021).

[29] Ibidem, s. 9.

[30] https://dronerules.eu/assets/files/DRPRO_Data_Protection_Impact_Assessment_EN.pdf (dostęp: 24.01.2021).

- ryzyka związanego z ochroną danych,
- praktyk zarządzania danymi w odniesieniu do zebranych danych[31].

Szablon składa się z pięciu kroków:

Krok 1: Prawny obowiązek przeprowadzenia Oceny skutków.
Krok 2: Mapowanie operacji BSP oraz przepływu danych osobowych.
Krok 3: Zidentyfikowanie ryzyka związanego z ochroną danych.
Krok 4: Rozwiązania minimalizujące ryzyko związane z ochroną danych.
Krok 5: Wyniki Oceny skutków.

Obowiązkiem operatora BSP jest przede wszystkim ustalenie, czy potrzebuje dokonać Oceny skutków, opierając się na przepisach RODO (art. 35). W ramach kroku 2 szablon zawiera tabelę z pytaniami, które mają pomóc w stworzeniu mapy operacji wykonywanych z udzialem BSP, ich kontekstu i przepływu danych osobowych, co z kolei ma pomóc w ocenie charakteru, zakresu, celu operacji oraz w identyfikacji źródeł wszelkich zagrożeń dla prywatności i ochrony danych (w jaki sposób te dane będą gromadzone, rejestrowane, przetwarzane i zanonimizowane lub usunięte). Należy więc odpowiedzieć na następujące pytania: Jaki rodzaj operacji się wykonuje? Jakie dane osobowe będą gromadzone? Co stanie się z danymi osobowymi po ich przechwyceniu przez drona? Czy zostanie to nagrane lub przesłane? W jaki sposób będzie to przesyłane, przechowywane i przetwarzane oraz w jakim celu?[32] Jakim osobom lub organizacjom będą udostępniane dane osobowe? Czy dane osobowe będą udostępniane organizacjom spoza UE? W jaki sposób dane osobowe będą usuwane? Jak długo dane osobowe w formie umożliwiającej identyfikację osób będą przechowywane? W jaki sposób dane zostaną usunięte? Którzy pracownicy mają dostęp do danych osobowych?[33] Czy organizacja zobowiązała się do przestrzegania oficjalnie zatwierdzonych kodeksów postępowania, aby pomóc w spełnieniu wymogów ochrony danych?[34]

Krok 3 ma na celu określenie, w jaki sposób wymagania dotyczące ochrony danych dotyczą przetwarzania danych. Pytania zawarte w tej części mają na celu pomoc przy rozważaniu ryzyka związanego z użytkowaniem drona. Po zidentyfikowaniu zagrożeń dla prywatności i ochrony danych, operator BSP zostanie poproszony o wybranie prawdopodobieństwa i poziomu istotności ryzyka, aby ustalić ich potencjalny wpływ na osoby fizyczne. W ramach kroku 3 szablon zawiera

[31] Ibidem, s. 4. Szablon należy wypełnić przed rozpoczęciem lotu, co zapewni wystarczającą ilość czasu na wdrożenie w praktyce wszelkich zidentyfikowanych zabezpieczeń. Ocena nie jest jednak ćwiczeniem jednorazowym i należy ją dostosować do wszelkich zmian wprowadzanych do operacji BSP. Należy zapisać kopię Oceny w archiwach i użyć jej jako dowodu w celu uzupełnienia zgodności z RODO.

[32] W tej części tabeli należy opisać wszelkie urządzenia – sprzęt i oprogramowanie – które będą używane, i będą służyć do przechwytywania, rejestrowania, przesyłania i przechowywania danych osobowych.

[33] W tej części tabeli należy napisać uzasadnienie posiadania przez nich dostępu do danych osobowych.

[34] Ibidem, s. 10–13.

sześć oddzielnych tabel z pytaniami, na koniec których należy dokonać oddzielnej oceny ryzyka[35].

[35] W ramach pierwszej tabeli (zgodna z prawem podstawa I cel) należy odpowiedzieć (oraz opisać) na następujące pytania: Jaki jest cel operacji BSP i przetwarzania danych osobowych? Czy ten cel jest wystarczająco określony, wyraźny i uzasadniony? Czy cel wymaga przetwarzania danych osobowych? Czy dalsze cele przetwarzania danych osobowych są przewidywalne na późniejszym etapie? Jeśli tak, to jakie mogą być? Czy są zgodne z pierwotnym celem, czy też są nieoczekiwane i niezwiązane z pierwotnym celem? Jaka jest podstawa prawna przetwarzania danych osobowych przez drona? Czy potrafisz wskazać potencjalne słabości polegania na wybranej przez operatora BSP podstawie prawnej? W ramach drugiej tabeli (minimalizowanie ryzyka) należy odpowiedzieć na następujace pytania: W jaki sposób plan operacji BSP umożliwia gromadzenie jedynie małej ilości danych osobowych, tak małej, jak jest to konieczne do celów lotu? W jaki sposób minimalizowane jest przetwarzanie danych osobowych i wrażliwych danych osobowych? Czy zespół pilotujący drona jest wystarczająco świadomy kontekstu i precyzyjnych celów operacji, aby umożliwić im wykonanie lotu i ograniczenie go do niezbędnego minimum? Czy wdrożono jakieś środki techniczne w celu zminimalizowania gromadzenia lub zatrzymywania niepotrzebnych danych? Jeśli tak, jakie one są? Czy jest procedura zatrzymywania danych? Jeśli tak, należy opisać krótko procedurę lub wskazać, gdzie można ją znaleźć. Jak długo przechowywane są dane osobowe i jak się je usuwa? W ramach trzeciej tabeli (przejrzystość operacji) należy odpowiedzieć na następujące pytania: Czy misja drona jest widoczna i przejrzysta z punktu widzenia osób na ziemi? Czy dron jest widoczny? Czy zespół pilotujący jest widoczny? Czy członkowie zespołu pilotującego są przeszkoleni w zakresie obsługi dronów w sposób uwzględniający prywatność i w jaki sposób mają się komunikować z osobami w terenie? W jaki sposób ludzie na ziemi i lokalne firmy będą informowane o locie dronem przed operacją lub w trakcie? Czy kanały komunikacji, które wybrał operator BSP do informowania ludzi o swoich działaniach przed lotem i podczas lotu, mogą być skuteczne? Czy są jasne, zrozumiałe i czy dotrą do zamierzonej publiczności? W ramach czwartej tabeli (udostępnianie danych osobowych stronom trzecim) należy odpowiedzieć na następujące pytania: Czy jest umowa wyjaśniająca relacje i podział obowiązków z osobami trzecimi, którym udostępnia się dane? Czy po udostępnieniu stronom trzecim dane będą przetwarzane do celów innych niż pierwotnie zamierzony cel ich gromadzenia? Jeśli tak, to czym są i na jakie osoby potencjalnie mogą mieć wpływ? Czy którakolwiek ze stron, którym udostępnia się dane osobowe, będzie zlokalizowana poza UE? Jeśli tak, to czy istnieją środki prawne zapewniające ochronę danych osobowych, takie jak decyzja Komisji Europejskiej w sprawie odpowiedniej ochrony danych, międzynarodowe zobowiązanie państwa trzeciego, klauzule umowne lub indywidualna zgoda? Czy są pisemne zasady dotyczące ujawniania przechwyconych danych właściwym organom? W ramach piątej tabeli (zapewnienie indywidualnych praw i wolności w praktyce) należy odpowiedzieć na następujące pytania: W jaki sposób osoby, których dane osobowe są przetwarzane, mogą korzystać z prawa dostępu? Jak osoby fizyczne mogą skorzystać z prawa do przenoszenia danych? Jak osoby fizyczne mogą skorzystać z prawa do sprostowania i usunięcia swoich danych osobowych? W jaki sposób osoby fizyczne mogą skorzystać ze swoich praw do sprzeciwu wobec przetwarzania lub ograniczyć przetwarzanie? Czy piloci i inni pracownicy przechodzą ciągłe szkolenia w zakresie przestrzegania ochrony danych podczas lotu, a następnie podczas przetwarzania danych? Czy procedury korzystania z przysługujących im praw są szybkie, skuteczne i łatwo dostępne z punktu widzenia osób fizycznych? Czy w organizacji istnieją mechanizmy kontrolne zapewniające zgodność pracowników z tymi zasadami i procedurami? Jeśli tak, w jaki sposób działają te mechanizmy? W ramach ostatniej tabeli (dokładność i bezpieczeństwo danych) należy odpowiedzieć na następujące pytania: W jaki sposób (cyber-)bezpieczeństwo zebranych danych osobowych jest zapewnione w organizacji podczas gromadzenia (podczas lotu), podczas przechowywania oraz podczas udostępniania innym organom (podczas transferów)? Czy stosuje się procedury lub praktyki w celu zapewnienia dokładności i bezpieczeństwa wyposażenia drona przed lotem? Czy są jakieś wewnętrzne

Krok 4 pomaga znaleźć rozwiązania odpowiadające ryzykom zidentyfikowanym w kroku 3, które mogą obejmować zabezpieczenia techniczne (środki bezpieczeństwa, środki techniczne w celu zminimalizowania gromadzonych lub przechowywanych danych lub ochrony ich przed nieautoryzowanym dostępem) oraz gwarancje proceduralne (wewnętrzne wytyczne dotyczące zachowania i postępowania z danymi). W tej części znajduje się zestaw pytań przewodnich do każdej z sześciu części kroku 3 i kilka sugerowanych rozwiązań w celu zabezpieczenia danych osobowych, które można wdrożyć w praktyce. Ta lista ma pomóc w myśleniu o rozwiązaniach chroniących prywatność i dane osobowe osób. Nie jest jednak wyczerpująca. Operator BSP powinien sam zdecydować, jakie zabezpieczenia są dla niego dostępne, i i wybrać najbardziej odpowiednie dla danej operacji[36].

Ostatni krok to wyniki Oceny skutków. W tej części znajduje się sfinalizowana lista wszystkich zidentyfikowanych ryzyk i zabezpieczeń. Ta sekcja pomaga stworzyć łatwą do sprawdzenia listę kontrolną, z której można skorzystać przed i w trakcie wykonywania operacji dronem. Wyniki Oceny mają na celu przypomnienie operatorom (oraz odpowiednim podmiotom w organizacji) o zabezpieczeniach, które muszą wdrożyć, aby wesprzeć podejście do ochrony prywatności od samego początku wykonywania operacji dronem, a także stanowi arkusz referencyjny prywatności dla pilotów i personelu zaangażowanego w operację[37].

W ramach projektu DroneRules PRO powstała także lista kontrolna przed lotem dla pilotów. Ma ona na celu sprawdzenie wiedzy pilotów dotyczącej prywatności i ochrony danych istotnych[38].

5.3. SANKCJE I ODPOWIEDZIALNOŚĆ CYWILNA

W zależności od charakteru naruszenia, kary za niezgodność mogą wahać się od 10 mln EUR do 20 mln EUR, a w przypadku przedsiębiorstwa – w wysokości od 2 do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (art. 83 RODO).

Odpowiedzialność cywilna za szkody (zarówno majątkowe, jak i niemajątkowe) z tytułu naruszenia przepisów o ochronie danych osobowych uregulowana została w rozporządzeniu 2016/679 (w art. 79 i art. 82). W zakresie natomiast nieuregulowanym tym rozporządzeniem stosuje się przepisy Ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny. Tak też stanowi art. 92 UODO. Ustawa określa właściwość sądu oraz zasady prceduralne związane z dochodzeniem roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych. Dochodzenie więc roszczeń na podstawie RODO czy UODO nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych jako

zasady postępowania w przypadku naruszenia danych – nieupoważniony dostęp do danych osobowych przez osoby wewnętrzne lub zewnętrzne? Ibidem, s. 14–29.

[36] Ibidem, s. 30–36.

[37] Ibidem, s. 37.

[38] https://dronerules.eu/assets/files/DRPRO_Pre_Flight_Checklist_EN.pdf (dostęp: 24.01.2021).

dóbr osobistych, do których stosuje się przepisy Kodeksu cywilnego (art. 23 i n. k.c.). UODO wyodrębniła więc w sposób pośredni nowe dobro osobiste w postaci danych osobowych[39].

6. PODSUMOWANIE

W Preambule RODO czytamy między innymi, że „szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych (…). Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych" (pkt 6). Bez znaczenia więc, jak duży nastąpi postęp technologiczny dotyczący wykonywania operacji bezzałogowymi statkami powietrznymi – dane osobowe osób fizycznych muszą być chronione.

Przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 nadały koncepcjom *privacy by design* oraz *privacy by default* moc powszechnie obowiązującą, przyczyniając się do ochrony prywatności i danych osobowych w całym procesie technologicznym, zaczynając już od fazy projektowania. Operatorzy dronów mają więc obowiązek zminimalizowania wpływu na prywatność i dane osobowe ludzi na ziemi zarówno w fazie projektowania, jak i przy planowaniu lotu, oraz przy zarządzaniu zgromadzonymi danymi.

Zastosowanie przepisów RODO do operatorów bezzałogowych statków powietrznych zależy od tego, w jaki sposób operatorzy korzystają z takich danych, a także co robią następnie z zarejestrowanymi danymi. W razie zastosowania przepisów RODO oraz w wypadku dokonywania systematycznej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, wymagane jest dokonanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Ocena ta to proces, który pomaga organizacjom w identyfikowaniu i minimalizowaniu ryzyka związanego z prywatnością i powinna koncentrować się *na znalezieniu i* wdrożeniu środków, które w jak największym stopniu zminimalizują *ryzyko* związane z naruszeniem tych praw i wolności.

W niniejszym artykule przedstawione zostały rekomendacje w zakresie charakteru i zawartości merytorycznej oceny. Ponadto zostało wskazane, na co operatorzy powinni zwracać szczególną uwagę w trakcie wykonywania operacji przy użyciu dronów, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

---

[39] Cyt. za A. Konert, *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym…*, op. cit., s. 173–174.

BIBLIOGRAFIA

Finn R.L., Wright D., *Privacy, Data Protection and Ethics For Civil Drone Practice: A Survey of Industry, Regulators and Civil Society Organisations*, „Computer Law & Security Review" 2016, vol. 32, iss. 2.

Kasprzyk P., *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym. Rozwój regulacji prawnych dotyczących bezpieczeństwa lotnictwa bezzałogowego*, Warszawa 2021.

Konert A., *Odpowiedzialność operatora bezzałogowego statku powietrznego za opóźnienie lub odwołanie lotu*, „Ius Novum" 2021, nr 1.

Konert A., Sakowska-Baryła M., *Impact of the GDPR on the Unmanned Aircraft Sector*, „Air and Space Law" 2021.

Konert A., Sakowska-Baryła M., *Prawne uregulowania w zakresie używania bezzałogowych statków powietrznych przez media*, „International Journal of Legal Studies" 2020, t. 8, nr 2.

Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018.

Osiecki M., *Drony – przyszłość lotnictwa i wyzwanie legislacyjne. Kilka uwag o nowych regulacjach unijnych dotyczących bezzałogowych statków powietrznych*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, nr 7.

Ostrihansky M., Szmigiero M., *Prawo dronów. Bezzałogowe statki powietrzne w prawie Unii Europejskiej oraz krajowym*, Warszawa 2020.

Ottavio M., *Privacy and Data Protection Implications of the Civil Use of Drones*, Brussels: Directorate General for Internal Policies. Policy Department C: Citizens' Rights and Constitutional Affairs. Civil liberties, justice and home affair, 2015.

RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017.

Rycak M., *Komentarz do ustawy z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych* (Dz.U. nr 100, poz. 1087), Komentarz do Dziennika Ustaw Nr 37, rok V, 7 października 2001 r.

Sarnecki P., Art. 47, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, III, red. L. Garlicki, Warszawa 2003, s. 4.

Sakowska-Baryła M., *Prawo do ochrony danych osobowych*, Wrocław 2014.

Steward M.E., *Privacy Aspects of Drones: Is There a Gap In Australia's Laws In Relation To The Protection of Privacy From Private Civil Use of Remotely Piloted Aircraft Systems?: In Particular, Does The Legislation Addressing Data Protection, Trespass To Land and Private Nuisance Need To Be Reformed?*, Thesis Master in Air and Space Law, Leiden University, 2015 (niepublikowana).

PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ OPERATORÓW BEZZAŁOGOWYCH STATKÓW POWIETRZNYCH

Streszczenie

W niniejszym artykule zostanie dokonana analiza przepisów oraz dokumentów dotyczących ochrony danych osobowych w sytuacji ich przetrwarzania przez operatorów bezzałogowych statków powietrznych, ze szczególnym uwzględnieniem obowiązku tworzenia tak zwanej

oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w razie, gdy operatorzy wykonują operacje przy użyciu dronów, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Słowa kluczowe: bezzałogowe statki powietrzne, drony, prawo dronów, RODO, koncepcje *privacy by design* oraz *privacy by default*, ochrona prawa do prywatności, ochrona danych osobowych, ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych

PERSONAL DATA PROCESSING BY UNMANNED AERIAL VEHICLES' OPERATORS

Summary

This article will analyze the provisions and documents regarding the protection of personal data when using an unmanned aerial vehicle, with particular emphasis on the obligation to create the so-called Data Protection Impact Assessment in the event that operators perform operations using drones which, due to their nature, scope, context and objectives, are likely to result in a high risk of violating the rights or freedoms of natural persons.

Key words: unmanned aerial vehicles, drones, drone law, GDPR, privacy by design and privacy by default, protection of the right to privacy, personal data protection, assessment of the consequences of planned processing operations for personal data protection

Konert A., *Przetwarzanie danych osobowych przez operatorów bezzałogowych statków powietrznych*, „Ius Novum" 2021 (15) nr 2, s. 25–39. DOI: 10.26399/iusnovum.v15.2.2021.12/a.konert

Konert, A. (2021) 'Personal data processing by unmanned aerial vehicles' operators'. *Ius Novum* (Vol. 15) 2, 25–39. DOI: 10.26399/iusnovum.v15.2.2021.12/a.konert