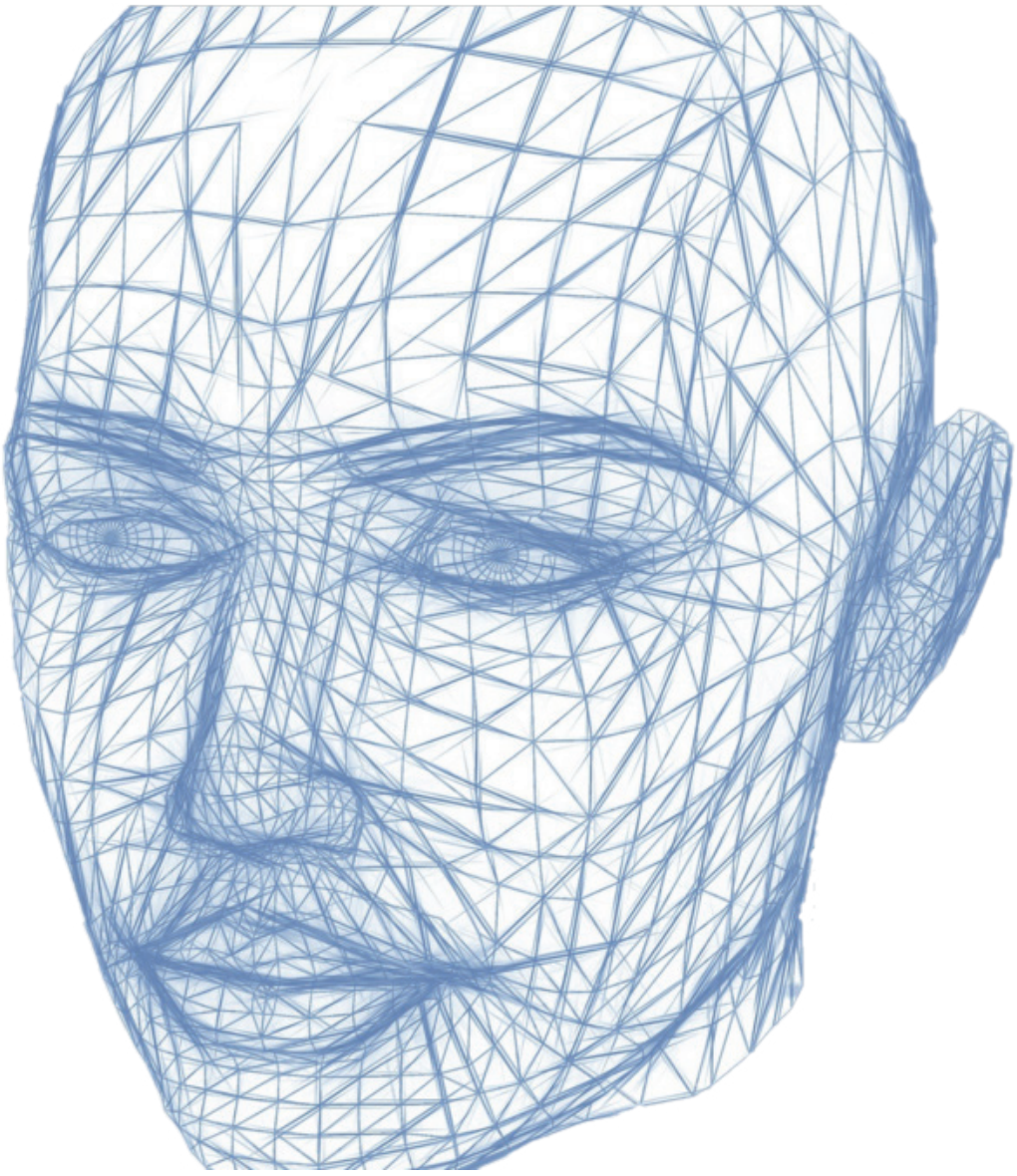

Internet i prawa obywatelskie w cyberprzestrzeni

w działaniach Rzecznika Praw Obywatelskich VII kadencji - lata 2015-2019

RZECZNIK PRAW OBYWATELSKICH

Na niniejszy zbiór składają się informacje regularnie publikowane na stronie Rzecznika Praw Obywatelskich, www.rpo.gov.pl
Wszystkie sprawy zostały podzielone na katerogie tematyczne, tak by mogli Państwo z łatwością zapoznać się z działaniami RPO w ramach wybranej dziedziny. Są wśród nich między innymi sprawy dotyczące:


alimentów


internetu i telekomunikacji


podatków


równości kobiet i mężczyzn


bezdomności


inwigilacji i prywatności


pomocy społecznej


seniorów


bioetyki


kierowców


pracowników


smogu


cudzoziemców, uchodźców i migrantów


książeczek mieszkaniowych


praw osób zatrzymanych


tortur i nieludzkiego traktowania


dykryminacji


lokatorów


praw żołnierzy i funkcjonariuszy


uciążliwych inwestycji


działalności gospodarczej i przedsiębiorców

mowy nienawiści i hejtu


prawa do sądu


wolności słowa


edukacji i szkół


ochrony środowiska


religii i wyznań


wykluczenia transportowego


emerytur i rent


osób pozbawionych wolności i KMPT


reprywatyzacji


zdrowia


instytucji finansowych i kredytów


osób z niepełnosprawościami


rolników i obrotu ziemią


zgromadzeń

Spis treści

1. Mowa nienawiści dotyka wszystkich. **Brońmy dzieci** - Adam Bodnar na obchodach Dnia Bezpiecznego Internetu o pięciu sposobach wsparcia dzieci 5
2. Podpis odbioru **przesyłek na tablecie**. RPO pyta, czy to bezpieczne 9
3. Krytyczna opinia RPO dla Senatu co do ustawy, która ma wdrażać unijną **„dyrektywę policyjną"** 9
4. Czy nauczyciel może zarekwirować **telefon komórkowy ucznia**? 11
5. Sesja 33 Kongresu Praw Obywatelskich: Nowe technologie, **sztuczna inteligencja a prawa człowieka** 11
6. Jak nasze dane mają przetwarzać organy zwalczające przestępczość? Opinia RPO do rządowego projektu wdrażającego unijną „dyrektywę policyjną" 13
7. Ministerstwo Cyfryzacji podjęło prace, aby obywatel mógł sprawdzić, czy dopisano go do **rejestru wyborców** 14
8. Bez szerokiego porozumienia nie będzie elektronicznej obywatelskiej inicjatywy ustawodawczej 15
9. W obronie obywateli, którzy 21 października nie mogli głosować. Wystąpienie RPO do PKW 15
10. Nie zostali dopisani do spisów wyborców - skarżą się RPO. Adam Bodnar pisze do Ministra Cyfryzacji 17
11. Dopisywanie się do rejestru wyborców przez E-PUAP. Rzecznik podejmuje interwencje po skargach od obywateli 18
12. O **patostreamingu** - prawnicy, naukowcy, przedstawiciele władz, organizacji pozarządowych i firm technologicznych, youtuberzy i dziennikarze 19
13. **Inwigilacja dwa lata później**. Sprawa wyroku ETPCz Sacharow (Zakharov) vs Rosja 21
14. Krytyczne uwagi Rzecznika o projekcie ustawy, która ma wdrażać dyrektywę policyjną UE 23
15. Sąd Najwyższy: kasacja RPO zasadna - **internet jest „miejscem publicznym"** 25
16. Sugestie Adama Bodnara dla międzyresortowego zespołu ds. przeciwdziałania propagowania faszyzmu i mowie nienawiści 26
17. RPO alarmuje: coraz mniej czasu na przyjęcie unijnej dyrektywy policyjnej 28
18. Adam Bodnar: sprawa **Cambridge Analytica** zagraża procesom demokratycznym i ochronie praw obywatelskich 29
19. RPO pisze do premiera ws. łagodniejszej sankcji za **nieświadome naruszenie praw autorskich** 30
20. RPO wycofuje wniosek do Trybunału Konstytucyjnego w sprawie inwigilacji 31
21. **Blokowanie kont** przez portale społecznościowe może naruszać wolność słowa - ocenia RPO 33
22. Podpisy pod obywatelskimi projektami ustaw - także drogą elektroniczną 34
23. Obywatel powinien sam decydować, na jakie strony wchodzi. Rzecznik pisze do Minister Finansów w sprawie **blokowania stron internetowych** 34
24. Kasacja Rzecznika na niekorzyść lidera stowarzyszenia Duma i Nowoczesność. Internet jest miejscem publicznym. 35
25. Dyrektywa policyjna - szansa dla obywateli czy legislacyjny pusty przebieg? 36
26. Wykorzystanie **internetu w szkole** - odpowiedź Ministerstwa Edukacji Narodowej 37
27. Polskie prawo w zakresie **retencji danych telekomunikacyjnych** powinno być dostosowane do wymogów prawa UE. RPO pisze w tej sprawie do Ministra Spraw Zagranicznych 37

28. Monitorowanie **korespondencji elektronicznej pracownika** stanowiło naruszenie jego prawa do poszanowania życia prywatnego i korespondencji 38

29. Minister Cyfryzacji o konieczności zmiany przepisów w sprawie retencji danych telekomunikacyjnych 38

30. Przed rozpoczęciem roku szkolnego RPO pyta: Jak uczniowie wykorzystują internet w szkole? 39

31. Odpowiedź Ministra Rozwoju i Finansów na wątpliwości Rzecznika dotyczące blokowania treści w internecie 40

32. RPO przestrzega: Przepisy ustawy o grach hazardowych mogą zostać wykorzystane do blokowania różnych treści w internecie 40

33. Ministerstwo Cyfryzacji po interwencji RPO przypomina resortowi sprawiedliwości: serwisy internetowe podmiotów publicznych powinny być **dostosowane do potrzeb osób z niepełnosprawnościami** już od 30 maja 2015 r. 41

34. Wystąpienie do minister cyfryzacji w sprawie nowych unijnych przepisów o ochronie danych osobowych 41

35. Niższy **VAT na e-booki** już wkrótce? Parlament Europejski przegłosował nowelizację dyrektywy 42

36. Wdrażanie Kodeksu postępowania dotyczącego **nielegalnego nawoływania do nienawiści w internecie.** Usuwanie mowy nienawiści z internetu może być skuteczniejsze 43

37. Ministerstwo Edukacji Narodowej odpowiada Rzecznikowi w sprawie **bezpieczeństwa cyfrowego dzieci i młodzieży** 44

38. Dostęp Policji do danych telekomunikacyjnych i internetowych. Jak Polska zareaguje na ważny wyrok Trybunału Sprawiedliwości UE? – odpowiedź MSWiA 45

39. RPO pyta Ministra Spraw Wewnętrznych i Administracji o zmiany w ustawie o Policji 46

40. Skarga kasacyjna RPO dotycząca odpowiedzialności osoby prowadzącej portal internetowy za **wpisy naruszające dobra osobiste** 46

41. Komendant Główny Policji odpowiada w sprawie uciążliwości związanych z **zabezpieczaniem sprzętu** komputerowego na potrzeby postępowania 47

42. Możliwość składania podpisów pod obywatelską inicjatywą legislacyjną drogą elektroniczną – Minister Cyfryzacji popiera postulat RPO 47

43. Rzecznik Praw Obywatelskich skarży ustawę antyterrorystyczną do Trybunału Konstytucyjnego 48

44. Wystąpienia do Ministra Cyfryzacji oraz Pełnomocnika Rządu ds. Społeczeństwa Obywatelskiego i Równego Traktowania **w sprawie przeciwdziałania mowie nienawiści i innym aktom nietolerancji** 51

45. Apel RPO do Prezydenta w sprawie **ustawy antyterrorystycznej** 52

46. Obywatelskie wysłuchanie publiczne ws. ustawy antyterrorystycznej - RPO przedstawia swoją opinię 53

47. Projekt ustawy o działaniach antyterrorystycznych – opinia RPO 53

48. Publiczne konsultacje RPO na temat projektu ustawy o działaniach antyterrorystycznych 54

49. Nielegalny handel billingami – informacja Komendanta Głównego Policji 55

50. Opinia GIODO dot. projektu ustawy o Policji 55

51. ETPC ws. niejawnego nadzorowania obywateli w związku ze **zwalczaniem terroryzmu** 56

52. Do MS ws. niejasnego brzmienia przepisu dotyczącego **przestępstw komputerowych** 57

53. Do MC oraz GIODO ws. dostępu służb do danych internetowych w projekcie ustawy o Policji 57

54. Odpowiedź Urzędu Komunikacji Elektronicznej ws. handlu bilingami telefonicznymi 58

55. Ważny wyrok Trybunału Sprawiedliwości ws. **ochrony danych w internecie** 58

56. Zastrzeżenia RPO ws. **kontroli operacyjnej służb** 58

MOWA NIENAWIŚCI DOTYKA WSZYSTKICH. BROŃMY DZIECI - ADAM BODNAR NA OBCHODACH DNIA BEZPIECZNEGO INTERNETU O PIĘCIU SPOSOBACH WSPARCIA DZIECI

data: 2019-02-05

- **Mamy coraz większy problem z mową nienawiści. Ostatnie wydarzenia, narastająca polaryzacja życia publicznego, podważanie autorytetów, nieustający spór polityczny, brak umiejętności cofnięcia się i przeproszenia – to wszystko sprawia że problem ten jest cały czas niezwykle poważny.**

- **W mowie nienawiści w gruncie rzeczy chodzi o to, że słowem możemy kogoś dotknąć, obrazić, naruszyć jego godność i poczucie bezpieczeństwa.**

- **Według RPO jednym z największych wyzwań jest odcinanie się dzieci od świata realnego i fakt, że to dzieci są często dla rodziców ekspertami od internetu.**

Adam Bodnar mówił o tym 5 lutego 2019 r. podczas konferencji zorganizowanej z okazji obchodów Dnia Bezpiecznego Internetu 2019 w Warszawie. Wydarzenie pod hasłem „Działajmy razem" zorganizowało Polskie Centrum Programu Safer Internet (PCPSI), które tworzą NASK i Fundacja Dajemy Dzieciom Siłę.

Jak zauważył RPO, życie w sieci to wiele możliwości, ale też ogromne niebezpieczeństwo. Nie tylko to oczywiste – zagrożenie dla prywatności, cyberprzestępczość, pornografia. A więc to, co jesteśmy w stanie względnie łatwo zidentyfikować czy przynajmniej nazwać. Zagrożenie to codzienna komunikacja. Dlaczego – bo nie mamy nad nią zupełnie kontroli, bo oddziałuje ona na dzieci podświadomie, bo wpływa na ich zachowania, bo nie są często przygotowane do wyrażania emocji. Bo to jest ich świat, do którego często nie mamy dostępu, albo którego nie rozumiemy (lub nie chcemy zrozumieć). Wciąż pojawiają się nowe rodzaje mediów społecznościowych, gier komputerowych, wszystkie z możliwością komentowania, która staje się często nowym narzędziem do wykluczania i hejtowania. Wśród znanych youtuberów – współczesnych herosów dla młodzieży, są tacy, którzy zaczęli żyć z pokazywania patologii. Dlatego w Biurze RPO podjęte zostały działania na rzecz powstrzymania zjawiska patostreamingu, który polega na pokazywaniu przemocy, poniżania drugiego człowieka.

Adam Bodnar zwrócił uwagę, że dzieci często prowadzą równoległe życie w sieci, to dla nich tak samo ważny świat, jak ten realny, czasem nawet ważniejszy. Aktywność w sieci to nie tylko kwestia codziennego życia, ale też statusu. Co także istotne, próby odłączenia się od internetu, rezygnacji z życia w sieci prowadzą do poczucia wykluczenia. – Jako dorośli nie jesteśmy często tego w stanie zrozumieć. Bo nawet jeśli jesteśmy coraz aktywniejsi w mediach społecznościowych, to jednak posiadamy umiejętność odłączenia się. Potrafimy nawiązywać relacje międzyludzkie i je prowadzić bez pośrednictwa sieci. Dzieci tak nie potrafią – podkreślał RPO.

Dlaczego trudno walczyć z mową nienawiści w sieci?

Niektórzy z twórców internetowych są bajecznie bogaci – dzieci chcą być influencerami, bo kojarzy im się to z sukcesem. I to dla nich dostępnym. Ale to oznacza też, że ich akceptują, powielają ich zachowania.

Dzieci są często ekspertami dla dorosłych od internetu – w jaki sposób rodzice mają zagwarantować bezpieczeństwo w sieci, korzystać z blokad i filtrów, kiedy dziecko potrafi szybciej i lepiej opanować wszystkie tajniki systemów.

Dzieci są od nas oddalone – zanurzone w grze (słuchawki), pochłonięte i wpatrzone w komórkę, a przy tym mają świadomość swojego prawa do prywatności i chcą z niego korzystać.

Co możemy zrobić?

Rozmawiać o wartościach – tłumaczyć dlaczego mowa nienawiści jest zła, wskazywać jak można mówić o uczuciach z szacunkiem dla drugiej strony, jak wyrażać swoje zdanie, przy jednoczesnym szukaniu przykładów z mediów, z których korzystają dzieci.

Trzeba podejmować nieustanną próbę zrozumienia jak wygląda świat w internecie - prośmy dzieci i młodzież o pokazanie, jak to działa, o wprowadzenie do tego świata.

Uczmy, że korzystanie z tego świata wiąże się z odpowiedzialnością – pokazujmy, co się stanie jeśli kogoś w sieci skrzywdzimy, na czym polega odpowiedzialność za słowo.

Nauczmy się razem z dziećmi, jak korzystać z mediów społecznościowych – jakie są regulaminy serwisów społecznościowych, jak zgłaszać niepożądane treści, z jakich mechanizmów można korzystać.

Na poziomie krajowym należy uznać, że bezpieczny internet to internet, z którego korzystamy świadomie i w którym dbamy o kulturę przekazu. To nie tylko ochrona przed znanymi już zagrożeniami, ale tymi, które pojawiają się każdego dnia.

Uczestnicy konferencji podkreślali również konieczność wspólnych działań rodziców i nauczycieli. Rozwój nowych technologii następuje bardzo dynamicznie, dlatego musimy współdziałać, aby móc towarzyszyć dzieciom w świecie online. Przeplatanie życia offline i online sprawia, że małe dzieci często nie potrafią ich rozróżnić, a wzrasta odsetek dzieci w wieku przedszkolnym korzystających regularnie z dostępu do sieci. Dziecięca wrażliwość i ufność niestety często przegrywa z manipulacją, a chęć zaistnienia przegrywa z uważnością i zdrowym rozsądkiem.

Dzień Bezpiecznego Internetu (DBI) obchodzony jest z inicjatywy Komisji Europejskiej od 2004 r. Jego głównym celem jest inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online oraz promocję pozytywnego wykorzystywania internetu. Ideą DBI jest podkreślanie siły współdziałania w dbaniu o cyfrowe bezpieczeństwo, zarówno na poziomie międzynarodowym, jak również lokalnym, łącząc zaangażowanie wielu instytucji, ale także rodziny, czyli najbliższego otoczenia dziecka.

Pełny tekst wystąpienia Adama Bodnara

Mowa nienawiści w sieciowym życiu naszych dzieci

W Polsce mamy coraz większy problem z mową nienawiści. Ostatnie wydarzenia, narastająca polaryzacja życia publicznego, podważanie autorytetów, nieustający spór polityczny, brak umiejętności cofnięcia się i przeproszenia - to wszystko sprawia, że problem ten jest cały czas niezwykle poważny.

Problem mowy nienawiści przenika wszystkie grupy społeczne. Starszych i młodzież. Polityków i działaczy.

Dzieci i rodziców.

Nie ma jednej definicji mowy nienawiści. Tradycyjnie chodzi o grupy dyskryminowane. Ale mowa nienawiści to może być także po prostu przemoc słowna. W gruncie rzeczy chodzi o to, czy słowem możemy kogoś dotknąć, obrazić, naruszyć jego godność, poczucie bezpieczeństwa.

Dwa lata temu dostałem od ucznia Kamila Zaka grafikę obrazującą problem mowy nienawiści. Grafika przypominała szubienicę.

Ale zamiast poszczególnych oczek sznura były słowa. Właśnie słowa nienawiści.

Słowa w około to m.in.:

- ***grubas,***
- ***lesba,***
- ***katol,***
- ***debil,***
- ***idiota,***
- ***ścierwo,***
- ***lizus,***
- ***kujon,***
- ***kebab,***
- ***beton,***
- ***gówno,***
- ***ćwok,***
- ***pedał,***
- ***parówa,***
- ***talib,***
- ***prosiak,***
- ***ułom,***
- ***Down,***
- ***moher.***

Z tymi słowami możemy się spotkać w różnych sytuacjach. Czasami usłyszymy je w sprzeczce między dziećmi, czasami na korytarzu, czasami wyrwie się w domu. Wtedy możemy reagować. Wytłumaczyć, powiedzieć, że tak nie wolno. Próbować wychowywać.

Ale nasze dzieci nie żyją tylko w domu, na ulicy, na zajęciach pozalekcyjnych czy pozaszkolnych. Dla nich świat równoległy to życie w sieci. Tam się dzieci spotykają, tam rozmawiają, tam spędzają wolny czas, prowadzą życie towarzyskie.

To jest dla nich tak samo ważny świat jak ten rzeczywisty.

Jako dorośli nie jesteśmy czesto tego w stanie zrozumieć. Bo nawet jesteśmy coraz aktywniejsi w mediach społecznościowych, to jednak posiadamy umiejętność odłączenia się. Potrafimy nawiązywać relacje międzyludzkie i je prowadzić bez pośrednictwa sieci. Dzieci tak nie potrafią. A jeśli już próbują, to ryzykują, że zostaną wykluczone w grupie. Dlaczego - bo nie wiedzą z czego śmieją się koledzy i koleżanki, kto komu dał ile lajków, co zostało zadane, jaki mem jest teraz interesujący oraz kto nagrał nową piosenkę. Aktywność w sieci to nie tylko kwestia codziennego życia, ale też statusu.

Nie ma tam Ciebie, to tak jakbyś nie istniał.

Ale życie w sieci to jest także niebezpieczeństwo.

Nie tylko to oczywiste - zagrożenie dla prywatności, cyberprzestępczość, pornografia. A więc to co jesteśmy w stanie względnie łatwo zidentyfikować czy przynajmniej nazwać. Zagrożenie to codzienna komunikacja. Dlaczego - bo nie mamy nad nią zupełnie kontroli, bo oddziałuje ona na dzieci podświadomie, bo wpływa na ich zachowania, bo nie są często przygotowane do wyrażania emocji. Bo to jest ich świat, do którego często nie mamy dostępu, albo którego nie rozumiemy (lub nie chcemy zrozumieć).

Zastanówmy się teraz, jak wygląda życie towarzyskie dzieci w sieci.

Ciekawi mnie, czy będą Państwo w ogóle te nazwy kojarzyli.

Media społecznościowe.

To już nie stary poczciwy Facebook czy nawet Instagram, ale także Snapchat. Ile przestrzeni do komentowania, zakładania grup, wymiany uwag. Skoro dorośli hejtują, to dlaczego dzieci miałyby być lepsze?. Też mogą czytać różne nienawistne strony czy zapoznawać się z newsami promującymi jedyny słuszny pogląd na temat islamu czy różnych wrażliwych grupa.

Nową platformą jest Tik Tok - wcześniej serwis Musical.ly, pozwalający na zamieszczanie muzyki i podkładów pod różne piosenki. Znowu - brzmi niewinnie. Ale aby zdobyć popularność trzeba się odpowiednio poruszać i zachowywać.

Siostry Godlewskie nie bez przyczyny stały się popularne. Mają naśladowców. Ale to z kolei powoduje hejt. I spirala się nakręca.

Gry komputerowe – czasy starego dobrego Arkanoida, Boulder Dasha, Tetrisa czy Heroes of Might and Magic minęły. Gry oznaczają pełne zanurzenie w fabule, ale także grę zespołową innych, którym w grze nie idzie, którzy nas akurat zabili, lub którzy nam przeszkodzili w grze. Counter Strike, Fortnite, League of Legends, Grand Theft Auto.

Wszędzie jest opcja komentowania na żywo.

Wszędzie dominuje przemoc

Skoro jesteśmy przy grach, to przejdźmy do youtuberów. Naszych współczesnych herosów dla młodzieży. Też nie są wybredni jeśli chodzi o słowa. Szczególnie ci ostrzejsi. Ale są tacy, którzy z tego zaczęli wręcz żyć, nie tylko ze słów, ale z pokazywania nienawiści i patologii. Tzw. patostreamerzy. Udaje się stopniowo ograniczać ich możliwości działania, ale czy za chwilę nie pojawią się w innym miejscu na youtube. Ale na youtube są też komentarze. No i czasami nie da rady ich przeczytać. Wczoraj próbowałem. Było ciężko.

Albo nabijanie się z najsłabszych - nagrywanie bezdomnych, jak kupuje im się whisky za 3000 zł i co oni mówią. No i nagrywanie filmu, nabijanie się. A pod spodem komentarz:

,,huj z ciebie gosciu, robisz fejm na ludziach nieporadnych zyciowo, myslisz ze masz 3k to jestes zajebisty, pajac zwykly,zal ogladac wykorzystywanie ludzi do bicia fejmu na yt, kupilbys im jakies ciuchy ,zabral do fryzjera, POMOC ZWYKLA, fredzlu bez ambicii jebal cie pies ,nie pozdrawiam „.

Niby empatycznie, ale przy okazji hejt. Przejrzałem trochę innych komentarzy.

Słownictwo tak bogate, że nawet Bralczyk i Miodek niektórych zwrotów nie uwzględnili. A do tego dialogi pomiędzy Guralem, Sebixem czy Rafonixem czy innymi streamerami. Generalnie jad, seks, wymiana hejtu, a pod spodem nagrań wierna publiczność z mocnymi komentarzami.

W każdym tym miejscu następuje proces sączenia nienawiści. Krok po kroku. W sposób często nawet niewidoczny. Z różnych miejsc.

Dlaczego z tym jest trudno walczyć?

Kilka przyczyn:

- niektórzy z twórców są bajecznie bogaci - dzieci chcą być influencerami czy progamerami, bo im się to kojarzy z sukcesem. I to dla nich dostępnym. Ale to oznacza, że ich akceptują, powielają ich zachowania - dzieci są dla nas ekspertami od internetu. W Rodzince.pl jest odcinek jak Agacie Kuleszy (czyli filmowej Marysi) chłopcy z rodzinki.pl zakładają konto na serwisie randkowym.

- W jaki sposób rodzice mają zastosować kontrolę rodzicielską, skoro dziecko potrafi w sposób błyskawiczny opanować te wszytskie tajniki Androida czy innego systemu operacyjnego, dzieci są od nas oddzielone - nie tylko zanurzeniem w grę, ale także poprzez słuchawki, mikrofon, wlepienie oczu w komórkę, w to, że mają prawo do prywatności. To utrudnia rodzicom i nauczycielom ingerencję.

Powstaje pytanie, co można zrobić.

Kilka sugestii, w jakim kierunku można pójść.

1. Mówmy o wartościach - dlaczego mowa nienawiści jest zła oraz, jak należy wyrażać uczucia - z nadzieją, że to także będzie stosowane w ich codziennym życiu. Trzeba szukać przykładów z ich życia, a nie sztucznych, z ,,Gazety Wyborczej" (której nie czytają) czy Twittera (którego nie używają).

2. Podejmujmy nieustanną próbę zrozumienia, jak wygląda ich sieciowy świat. To może być trudne, ale nie możemy od razu oddawać pola. Bez walki. Że to nie dla nas. Niech nas w ten świat wprowadzają. Niech pokazują, co jak działa. Nie chodzi o kontrolę. Ale zrozumienie.

3. Uczmy, że korzystanie z tego świata wiąże się z odpowiedzialnością. Co się stanie jak kogoś skrzywdzimy? Czy możemy mieć problemy w szkole? Czy nauczyciel może wszcząć postępowanie? Czy rodzice mogą ponieść odpowiedzialność? Uczmy, że słowo oznacza także odpowiedzialność.

4. N auczmy się wraz z dziećmi, jakie są regulaminy korzystania z mediów społecznościowych oraz jak zgłaszać niepożądane treści. To jest możliwe. Ale czy z tego korzystamy.

5. Uznajmy - na poziomie krajowym - że bezpieczny internet to internet, z którego korzystamy świadomie i w którym dbamy o kulturę przekazu. To nie tylko ochrona przed znanymi już zagrożeniami, ale tymi które występują na codzień.

PODPIS ODBIORU PRZESYŁEK NA TABLECIE. RPO PYTA, CZY TO BEZPIECZNE

data: 2018-12-28

- **Od pewnego czasu podpisujemy odbiór przesyłek na tablecie u listonosza czy kuriera; mamy wątpliwości czy to jest bezpieczne**
- **Taki podpis jest bowiem utrwalany nie na papierze, lecz jako elektroniczny zapis ciągu znaków**
- **Może się zatem zaliczać do danych biometrycznych, które podlegają szczególnej ochronie**
- **Rzecznik Praw Obywatelskich spytał Prezes Urzędu Ochrony Danych Osobowych o potencjalne zagrożenia z tym związane**

Obywatele zgłaszają wątpliwości związane z wykorzystywaniem urządzeń rejestrujących tzw. odręczny podpis biometryczny przez operatorów pocztowych, w tym Pocztę Polską, przy potwierdzaniu odbioru przesyłek.

Potwierdzanie odbioru przesyłek własnoręcznym podpisem od dawna było powszechną praktyką. Dopiero jednak jego elektroniczne utrwalanie wywołało wątpliwości związane z ochroną danych osobowych. Różnica jest bowiem zasadnicza: podpis na ekranie dotykowym jest utrwalany nie w postaci tuszu na kartce papieru, lecz w postaci elektronicznego zapisu ciągu znaków. Niepokój obywateli wynika z większej mobilności danych przetwarzanych w formie elektronicznej i – co za tym idzie - zwiększeniem ryzyka nieautoryzowanego dostępu.

Dane biometryczne objęto szczególną ochroną po wejściu w życie RODO (rozporządzenia 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). Art. 9. RODO wprowadził generalny zakaz przetwarzania danych biometrycznych w celu jednoznacznego zidentyfikowania osoby, ze wskazaniem wyjątków od tego. Według RODO dane biometryczne oznaczają „dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne".

Cechy te mogą zatem obejmować m.in. linie papilarne, wygląd siatkówki lub tęczówki oka, owal twarzy, kształt małżowiny usznej, geometrię ręki, układ naczyń krwionośnych dłoni, głos i jego barwę. Cechy behawioralne to np. charakter pisma, dynamika pisania i sposób poruszania się. Oznacza to, że podpis może zostać zaliczony do danych biometrycznych i jako taki podlega szczególnej ochronie.

Ze względu na wrażliwy charakter danych biometrycznych Rzecznik Praw Obywatelskich chce uzyskać więcej informacji na temat urządzeń stosowanych przez listonoszy, stosowanych zabezpieczeń oraz sposobu i okresu przechowywania zebranych danych.

Dlatego Adam Bodnar spytał prezes UODO Edytę Bielak-Jomaa, czy przetwarzanie danych biometrycznych podczas świadczenia usług pocztowych było przedmiotem jej zainteresowania; czy planuje działania w tej sprawie i jak ocenia potencjalne zagrożenia związane z tym zjawiskiem.

VII.520.76.2018

KRYTYCZNA OPINIA RPO DLA SENATU CO DO USTAWY, KTÓRA MA WDRAŻAĆ UNIJNĄ „DYREKTYWĘ POLICYJNĄ"

data: 2018-12-20

- **Uchwalona przez Sejm ustawa nie dokonuje właściwego wdrożenia „dyrektywy policyjnej" z 2016 r.**
- **Wprowadza bowiem zbyt wiele wyjątków, np. wyłącza np. spod ustawy pięć służb specjalnych**
- **Ustawa w wielu miejscach jest niespójna lub wręcz sprzeczna z prawem Unii Europejskiej**
- **Rzecznik przedstawił swe uwagi Senatowi, który pracuje nad ustawą**

14 grudnia 2018 r. Sejm uchwalił ustawę o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Rzecznik Praw Obywatelskich na etapie prac legislacyjnych poprzedzających skierowanie projektu przedstawiał swe uwagi, skierował również opinię do Marszałka Sejmu (niedołączoną przez niego do druku nr 2089).

Obecnie ustawą zajmuje się Senat. W związku z tym Rzecznik przedstawił Marszałkowi Senatu swe istotne wątpliwości, związane z poziomem przestrzegania praw i wolności człowieka i obywatela.

Ustawa ma wdrażać dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. Dotyczy ona uprawnień służb w przetwarzaniu danych i jest nazywana „drugą nogą" RODO, czyli rozporządzenia o tym, co wolno przedsiębiorcom i administracji robić z danymi osobowymi. Od 2017 r. Adam Bodnar występował do kilku resortów, wskazując że dyrektywa jest bardzo ważna z punktu widzenia obywatela. Została ona przyjęta 27 kwietnia 2016 r., weszła w życie 5 maja 2016 r., a zatem projektodawca miał praktycznie dwa lata na przygotowanie projektu.

Wyłączenia pięciu służb spod ustawy

Ustawa przewiduje wyłączenie z zakresu jej stosowania danych osobowych przetwarzanych w ramach realizacji ustawowych zadań służb specjalnych: ABW, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz CBA. Projektodawca tłumaczy, że wszystkie obszary działalności tych służb należą do przewidzianego przez dyrektywę wyjątku, jakim jest przetwarzanie danych „w związku z zapewnieniem bezpieczeństwa narodowego".

Rzecznik konsekwentnie nie zgadza się z tym stanowiskiem, czemu dał wyraz w opinii dla Sejmu. Nie wszystkie bowiem zadania ustawowe realizowane przez służby mieszczą się w zakresie pojęcia „bezpieczeństwo narodowe". Trzeba pamiętać, że z punktu widzenia prawa Unii Europejskiej pojęcie „bezpieczeństwo narodowe" nie może być utożsamiane z pojęciem „bezpieczeństwa wewnętrznego", o czym świadczą przepisy samego Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej. Również - przykładowo - zwalczanie terroryzmu nie jest uznawane w UE za domenę wyłączoną z zakresu prawa Unii.

Wyłączenie stosowania ustawy do danych osobowych z akt postępowania

Takie przepisy ustawy oznaczają, że nie będzie ona miała zastosowania do danych osobowych zawartych w aktach postępowań - prowadzonych na podstawie Kpk, Kpw, Kkw, Kks, ustawy o postępowaniu w sprawach nieletnich czy ustawy ws. rejestru sprawców przestępstw seksualnych. Takie wyłączenie nie jest zgodne z dyrektywą 2016/680. RPO zaznacza, że podobną opinię w tej sprawie ma MSZ.

Powierzenie nadzoru nad przetwarzaniem danych osobowych w sądach i prokuraturze instytucjom, które nie są niezależne od władzy wykonawczej

Ustawa stanowi, że – w zależności od sytuacji – albo Krajowa Rada Sądownictwa, albo prezesi sądów (lub odpowiedni prokuratorzy) będą mogli zażądać dostępu do wszelkich danych osobowych w prowadzonych postępowaniach w związku z realizacją zadań wynikających z konieczności nadzoru nad sposobem przetwarzania danych osobowych. Tymczasem z prawa UE jasno wynika, że nadzór nad przetwarzaniem danych osobowych może sprawować wyłącznie organ niezależny.

W ocenie Rzecznika takie rozwiązania prawne są wątpliwe, bowiem ani Krajowa Rada Sądownictwa, ani prezesi sądów nie mogą być dziś uznani za organy niezależne, zdolne do prowadzenia nadzoru w sposób wypełniający wymogi Karty Praw Podstawowych UE. W opinii do projektu ustawy KRS sama uznała się za niewłaściwą do sprawowania takiego nadzoru – wskazuje Rzecznik.

Poszerzenie wyłączeń dla informacji niejawnych

Rzecznik negatywnie ocenia wyłączenie przez ustawę spod ochrony danych przetwarzania informacji niejawnych. Budzi to bowiem zastrzeżenia Z punktu widzenia zakresu rodo oraz dyrektywy 2016/680, a przede wszystkim art. 51 Konstytucji. Obecnie wyłączeniu spod ustawy podlega tylko rejestracja zbioru danych przez administratorów danych niejawnych, a nie ich przetwarzanie.

Brak implementacji art. 17 dyrektywy

Dyrektywa nałożyła na państwa członkowskie obowiązek zapewnienia, że osoba, której dane dotyczą, będzie mogła wykonywać swoje prawa także za pośrednictwem właściwego organu nadzorczego, który ma informować daną osobę przynajmniej o fakcie przeprowadzenia wszelkich niezbędnych weryfikacji lub przeglądów. Ustawa daje wprawdzie możliwość złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ale ma przysługiwać ona wtedy, gdy dane osobowe są przetwarzane niezgodnie z prawem. Art. 17 dyrektywy dotyczy zaś sytuacji, w której osoba w ogóle nie ma pewności, że jej dane (i jakie) są przetwarzane.

RPO nie może się zgodzić z takim rozwiązaniem w ustawie. Istota art. 17 polega bowiem na możliwości dokonywania przez Prezesa UODO niezależnej oceny zasadności przetwarzania danych przez podmioty objęte zakresem dyrektywy. W ten sposób jeden z najistotniejszych przepisów dyrektywy 2016/680 nie znajdzie swojego odzwierciedlenia w polskim systemie prawnym – napisał Rzecznik do marszałka Senatu.

Wejście w życie ustawy i terminy na dostosowanie

Ustawa ma wejść w życie zasadniczo po 14 dniach od dnia ogłoszenia. Ale art. 102 ustawy przyznaje administratorom kolejny rok na dostosowanie zasad przetwarzania danych osobowych do środków technicznych i organizacyjnych wymaganych art. 39 ust. 2 ustawy. Dodatkowo, jeśli wymagałoby to niewspółmiernie dużego wysiłku lub nakładów, administrator będzie miał czas aż do 6 maja 2023 r.

Rzecznik przypomina, że dyrektywa była uchwalona w kwietniu 2016 r. Wyznaczanie teraz kolejnych terminów, a zwłaszcza tak odległych, musi być ocenione jako sprzeczne z dyrektywą. Takie rozwiązania są też rozbieżne z tym, co było wyzwaniem dla wszystkich, którzy od 25 maja 2018 r. stosują przepisy rodo i są nimi związani. - Żaden podmiot, który jest objęty zakresem stosowania rodo, nie był w tak doskonałej sytuacji, w jakiej mają być administratorzy objęci zakresem przepisów ustawy – podkreśla Rzecznik.

Nie wyjaśniono, dlaczego w takiej uprzywilejowanej sytuacji stawia się organy co do zasady publiczne, w porównaniu do sytuacji podmiotów prywatnych - w szczególności przedsiębiorców, którzy musieli ponieść często wysokie koszty dostosowania się do przepisów rodo w wyznaczonym terminie.

Rzecznik przekazał swe uwagi marszałkowi Senatu Stanisławowi Karczewskiemu z prośbą o ich uwzględnienie w toku prac nad ustawą.

VII.501.315.2014

CZY NAUCZYCIEL MOŻE ZAREKWIROWAĆ TELEFON KOMÓRKOWY UCZNIA?

data: 2018-12-17

Społeczność szkolna może funkcjonować tylko wtedy, gdy ustali sobie jasne zasady. To wszystkim ułatwia życie, bo wiadomo, co jest dopuszczalne i czego się w danej sytuacji spodziewać. Ważne, by zasady te były jasno sprecyzowane i by nie naruszały prawa powszechnego.

Statut szkoły może zabraniać korzystania z telefonów komórkowych i innych urządzeń elektronicznych w trakcie trwania zajęć. Nauczyciel może nakazać wyłączenie urządzenia lub umieszczenie go w widocznym miejscu na czas trwania lekcji. Szkoła nie ma jednak uprawnień do rekwirowania przedmiotów należących do uczniów. Osoby pełnoletnie lub rodzice osób niepełnoletnich mogą w każdej chwili zażądać zwrotu należących do nich, a przetrzymywanych przez szkołę, rzeczy.

Pozbawienie prawa korzystania z telefonu po zakończeniu zajęć może być stosowane jako środek wychowawczy w stosunku do niepełnoletnich uczniów, powinno się to jednak odbywać za wiedzą i zgodą ich prawnych opiekunów, zgodnie z postanowieniami statutu.

Jeżeli szkoła wprowadzi obowiązek pozostawienia telefonów komórkowych na czas trwania zajęć w depozycie, ponosi odpowiedzialność za wynikłe z tego szkody (np. kradzież czy uszkodzenie sprzętu), a uczeń pełnoletni musi mieć zapewnioną możliwość dostępu do urządzenia kiedy tylko uzna to za konieczne.

Nawet w sytuacji, w której telefon komórkowy został zarekwirowany zgodnie z zasadami obowiązującymi w szkole, przeglądanie jego zawartości przez osoby trzecie, np. nauczycieli, stanowi naruszenie prawa do prywatności i jako takie jest niezgodne z prawem.

SESJA 33 KONGRESU PRAW OBYWATELSKICH: NOWE TECHNOLOGIE, SZTUCZNA INTELIGENCJA A PRAWA CZŁOWIEKA

data: 2018-12-15

- **Trzeba dbać o ochronę praw człowieka w kontekście nowych technologii**
- **Nie powinno się wprowadzać żadnej etyki dla samochodów autonomicznych**
- **Trzeba sprawdzać i kontrolować algorytmy, licząc się z tym, że prawdziwie przejrzyste będą one tylko dla specjalistów. Trzeba jednak realizować prawo do bycia poinformowanym**
- **Maszyny mogą dla nas zbierać dane; problemem będzie, gdy będą za nas podejmować ważne decyzje. A algorytmów nie mogą wyjaśniać inne algorytmy.**

Tematem dyskusji była przejrzystość algorytmów rządzących nowymi technologiami i możliwe zagrożenia, także wobec praw człowieka.

Nowe technologie zmieniają nasze życie. Godzimy się z tym, akceptujemy, korzystamy z możliwości, które dają, ułatwiamy sobie życie codzienne jeśli chodzi o komunikację, rozrywkę, usługi publiczne czy transportowe. Sztuczna inteligencja wkracza powoli do zakładów pracy, zastępuje pracowników, automatyzuje różne procesy. Jednak nie pozostaje to bez wpływu na prawa człowieka. Poświęcamy naszą prywatność na rzecz bezpieczeństwa i wygody. Stopniowo likwidowane są niektóre miejsca pracy. Wreszcie zaczynamy stawiać pytania etyczne jak dalece sztuczna inteligencja może zastępować człowieka oraz czy

człowiek może ustalić bariery jej rozwoju. Jak nigdy przedtem rzeczywistość z filmów science fiction wymaga już teraz od nas odpowiedniej refleksji. Czy dotychczasowe instrumenty prawne okażą się do tego wystarczające? Czy zdążymy z odpowiedzią na główne pytania i wyzwania etyczne zanim nowe technologie rozwiną się do tego stopnia, że nie będziemy mogli już wiele zrobić?

Paneliści:

- Aleksandra Przegalińska - doktoryzowała się w dziedzinie filozofii sztucznej inteligencji na UW, adiunkt w Center for Research on Organizations and Workplaces w Akademii Leona Kozminskiego
- Krzysztof Izdebski - prawnik, członek zarządu i dyrektor programowy Fundacji ePaństwo.
- Kamil Mamak - dr prawa, filozof i pasjonat nowych technologii.
- Filip Konopczyński - prawnik i kulturoznawca, specjalista Pracowni Badań Społecznych Naukowej i Akademickiej Sieci Komputerowej (NASK).
- Katarzyna Szymielewicz - prawniczka specjalizująca się w problematyce praw człowieka i nowych technologii. Współzałożycielka i prezeska Fundacji Panoptykon.

Relacja z panelu

Kamil Mamak: Wykorzystywanie algorytmów do sterowania autonomicznymi samochodami może rodzić liczne problemy prawne. Zwłaszcza, jeśli preferowałyby osoby znajdujące się poza pojazdem kosztem tych, które w nim są. Nie mówiąc nawet o preferencjach typu kobieta czy mężczyzna.

Aleksandra Przegalińska: Nie ma i nie będzie żadnych moralnych norm dla samochodów autonomicznych. Środowisko naukowe nie jest w stanie ich wypracować. Traumatyczne dla moich studentów było doświadczenie testu „dylematu wagonika" (czy w chwili wypadku drogowego, gdy możemy wybrać, jak skręcimy kierownicę i czy poświęcimy raczej osobę starszą, by nie zabić młodszej, czy zabić mężczyznę czy kobietę). Notabene w kulturach azjatyckich w tym teście była preferencja, by chronić starszych, a nie młodszych. Widzimy, że te maszyny są skuteczne, jeśli chodzi o zadania. Chciałoby się to stosować np. w diagnostyce medycznej, ale mamy kłopot, co dalej z tym robić.

Filip Konopczyński: Oczekiwanie, że można ustalić jednolitą etykę, jest zbyt daleko idące. To nie może być ostatecznie rozstrzygnięte, choć jest to starsze niż sama sztuczna inteligencja.

Przewortnie mówiąc, chciałbym, aby mój samochód miał osobowość prawną i to on odpowiadał, gdybym spowodował wypadek.

Nie jest niespodziewaną konsekwencją, że to roboty dziś zabijają. Wiele nowych technologii to wynik stosowania komercyjnego wcześniejszego inwestycji w technologie wojskowe.

Katarzyna Szymielewicz: Produkujemy olbrzymie ilości nowych technologii. Jesteśmy skazani na to, że to maszyny będą dla nas zbierać dane. Problem zaczyna się, gdy będzie to wkraczać na poziom decyzji. Bo decyzje o reklamach w sieci jesteśmy w stanie pozostawić samej sieci. Ale jak wyobrażamy sobie, że maszyny będą opiekować się osobami starszymi? Jest mnóstwo sfer w których algorytmy zwolnią nas z dylematów. Dlatego musimy tu ustalić granice. Możemy skonstruować taki algorytm, który będzie oceniał dla nas ten pierwszy algorytm – np., gdy okaże się, że ludzie w czerwonych autach częściej mają wypadki drogowe. Chodzi o to, by nie mieć takiego systemu citizen scoringu ludzi, jak w Chinach.

Krzysztof Izdebski: Facebooka używano do mordów w Birmie. Ludzki komponent zawsze będzie obecny. A jeśli maszyny przejęłyby nad nami kontrolę, to może byłoby i lepiej, jeśli mówimy o tej okrutnej historii ludzkości. Ważnym „bezpiecznikiem" będzie przejrzystość danych - tak, aby same algorytmy nie wyjaśniały innych algorytmów. Bo np. z algorytmów w Australli wynikało, że najniebezpieczniej jest w okolicach komisariatów policji – bo tam ludzie zgłaszają informacje o przestępstwach. Teoretycznie sztuczna inteligencja mogłaby przyspieszyć sprawy sądowe, ale jakim kosztem.

Najciekawsze głosy w dyskusji

Ludzie muszą być lepszymi ludźmi, by stosować nowe technologie. I bez autonomicznych samochodów wiemy co robić, żeby było bezpieczniej, a nie robimy tego. Nie musimy tu wymyślać etyki.

Konkluzje

- **Trzeba dbać o ochronę praw człowieka w kontekście nowych technologii**
- **Nie powinno się wprowadzać żadnej etyki dla samochodów autonomicznych**
- **Trzeba patrzeć na ręce algorytmom, choć ich przejrzystość zawsze będzie elitarna. Chodzi o realizację prawa do bycia poinformowanym**
- **System losowania sędziów w Polsce powinien być jasny – to kwestia tylko woli politycznej**

JAK NASZE DANE MAJĄ PRZETWARZAĆ ORGANY ZWALCZAJĄCE PRZESTĘPCZOŚĆ? OPINIA RPO DO RZĄDOWEGO PROJEKTU WDRAŻAJĄCEGO UNIJNĄ „DYREKTYWĘ POLICYJNĄ”

data: 2018-11-30

- **Rządowy projekt nie dokonuje właściwego wdrożenia dyrektywy z 2016 r. – wprowadza zbyt wiele wyjątków, wyłączając określone służby i organy spod ustawy**
- **Jest on w wielu miejscach niespójny lub sprzeczny z prawem Unii Europejskiej**
- **RPO przedstawia Marszałkowi Sejmu swe uwagi w nadziei, że parlament usunie usterki projektu**

Projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (druk nr 2989) przeszedł już w Sejmie pierwsze czytanie. Tymczasem zawiera propozycje, które wywołują istotne wątpliwości dotyczące przestrzegania praw i wolności człowieka i obywatela – pisze Adam Bodnar w wystąpieniu do marszałka Marka Kuchcińskiego. Ustawa ma wdrożyć dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. Dotyczy ona uprawnień służb w przetwarzaniu danych i jest nazywana „drugą nogą” RODO, czyli rozporządzenia o tym, co wolno przedsiębiorcom i administracji robić z danymi osobowymi.

W związku z pracami parlamentue Rzecznik przedstawia uwagi, które dotyczą spraw fundamentalnych z punktu widzenia praw jednostki i nie mogą być traktowane jako wyczerpujące zastrzeżenia i wątpliwości, które można podnieść pod adresem tego projektu i sposobu procedowania nad nim.

Od 2017 r. Adam Bodnar występował do kilku resortów, wskazując że dyrektywa jest bardzo ważna z punktu widzenia obywatela.

Wyłączenia dla służb

Projekt przewiduje wyłączenie z reguł dotyczących przetwarzania danych dla służb specjalnych: ABW, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz CBA. Projektodawca tłumaczy, że wszystkie obszary działalności tych służb należą do przewidzianego przez dyrektywę wyjątku, jakim jest przetwarzanie danych „w związku z zapewnieniem bezpieczeństwa narodowego”.

Rzecznik Praw Obywatelskich konsekwentnie nie zgadza się z tym stanowiskiem. Nie wszystkie bowiem zadania ustawowe realizowane przez służby mieszczą się w zakresie pojęcia „bezpieczeństwo narodowe”. Trzeba pamiętać, że z punktu widzenia prawa Unii Europejskiej pojęcie „bezpieczeństwo narodowe” nie może być utożsamiane z pojęciem „bezpieczeństwa wewnętrznego”, o czym świadczą przepisy samego Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej. Również - przykładowo - zwalczanie terroryzmu nie jest uznawane w UE za domenę wyłączoną z zakresu prawa Unii.

Wyłączenie stosowania ustawy do danych osobowych zawartych w aktach postępowania

Projekt przewiduje takie wyłączenie, co oznacza, że do danych osobowych zawartych w aktach postępowań, prowadzonych na podstawie Kpk, KPW, kkw, kks, ustawy o postępowaniu w sprawach nieletnich czy ustawy, która przewiduje utworzenie i prowadzenie rejestru sprawców przestępstw seksualnych, ustawa nie będzie miała zastosowania. Takie wyłączenie nie jest zgodne z dyrektywą 2016/680. RPO zaznacza, że podobną opinię w tej sprawie ma MSZ.

Powierzenie nadzoru nad przetwarzaniem danych osobowych w sądach i prokuraturze instytucjom, które nie są niezależne od władzy wykonawczej

Projekt przewiduje, że – w zależności od sytuacji – albo Krajowa Rada Sądownictwa, albo prezesi sądów (czy odpowiedni prokuratorzy) będą mogli zażądać dostępu do wszelkich danych osobowych w prowadzonych postępowaniach w związku z realizacją zadań wynikających z konieczności nadzoru nad sposobem przetwarzania danych osobowych. Tymczasem z prawa UE jasno wynika, że nadzór nad przetwarzaniem danych osobowych może sprawować wyłącznie organ niezależny. W ocenie Rzecznika takie rozwiązania prawne są wątpliwe, bowiem ani Krajowa Rada Sądownictwa, ani prezesi sądów nie mogą być dziś uznani za organy niezależne, zdolne do prowadzenia nadzoru w sposób wypełniający wymogi Karty Praw Podstawowych UE.

Poszerzenie wyłączeń dla informacji niejawnych

Projekt wyłącza też spod ochrony danych przetwarzanie informacji niejawnych. Także tę zmianę RPO ocenia negatywnie, bo wyłączenie stosowania przepisów o ochronie danych osobowych jest zbyt szerokie. Obecnie wyłączeniu spod ustawy podlega tylko rejestracja zbioru danych przez administratorów danych niejawnych, a nie ich przetwarzanie. Liczne niespójności, także wobec RODO pokazują, że na etapie prac rządowych nie dokonano prawidłowej analizy wszystkich problemów, jakie wiążą się z implementacją dyrektywy 2016/680 i koniecznością zapewnienia spójności rozwiązań między projektowaną ustawą a przepisami RODO.

Poważnym problemem jest także to, że choć projekt ma wdrażać do polskiego systemu prawnego dyrektywę z 27 kwietnia 2016 r., czyli sprzed ponad dwóch lat, w trakcie prac nad projektem zainteresowanym podmiotom wyznaczono zaledwie kilka dni na przedstawienie uwag. A później już nie poddano ich żadnej szerszej dyskusji z udziałem zainteresowanych.

VII.501.315.2014

MINISTERSTWO CYFRYZACJI PODJĘŁO PRACE, ABY OBYWATEL MÓGŁ SPRAWDZIĆ, CZY DOPISANO GO DO REJESTRU WYBORCÓW

data: 2018-11-28

- **Ministerstwo Cyfryzacji podjęło prace nad rozbudową systemu ePUAP - aby obywatel mógł sprawdzać stan realizacji wniosku o wpisanie do rejestru wyborców, a gmina miała ułatwioną analizę danych**
- **Tak resort cyfryzacji odpowiedział na wystąpienie RPO w sprawie skarg obywateli, którzy - korzystając z ePUAP - nie mogli dopisać się do rejestru podczas wyborów samorządowych**
- **Procedowanie wniosku leży po stronie gminy; wiele z nich nie sprostało wymogom i nie rozpatrzyło ich w ustawowym 3-dniowym terminie – wskazał resort**
- **W związku z przyszłorocznymi wyborami do Parlamentu Europejskiego oraz do Sejmu i Senatu Ministerstwo zorganizuje spotkanie z MSWiA i Krajowym Biurem Wyborczym w sprawie wsparcia procedur wyborczych**

Obywatele, którzy chcieli dopisać się przez ePUAP do rejestru wyborców, skarżą się RPO na uniemożliwienie im udziału w wyborach samorządowych 21 października 2018 r - mimo że zgłosili drogą elektroniczną wnioski o dopisanie do rejestru wyborców.

Zdecydowana większość skarg dotyczy wyborców, którzy skorzystali z usługi wyborczej on-line (strona Obywatel.gov.pl i uwierzytelnienie przy pomocy Profilu Zaufanego e-PUAP). Była ona prezentowana jako wygodna dla wyborców, nie wymagająca osobistej wizyty w urzędzie, udostępniona m.in. z myślą o wyborcach z niepełnosprawnościami. Część skarg dotyczy osób, które wniosek złożyły zbyt późno, aby mógł być on rozpatrzony w ustawowym 3-dniowym terminie (do 16 października włącznie). Jednak są też wyborcy, którzy złożyli go odpowiednio wcześnie, a to wskazuje na różnorodne trudności organizacyjne i techniczne, jakie uniemożliwiły skuteczny wpis do rejestru.

Skargi stały się podstawą wystąpienia Rzecznika Praw Obywatelskich z 24 października do Ministra Cyfryzacji. Adam Bodnar poprosił Marka Zagórskiego o stanowisko co do skuteczności i praktycznego działania usługi wyborczej on-line, mającej umożliwiać wpis do rejestru. Wystąpił też o informacje, ilu wyborców złożyło takie wnioski.

Odpowiedź Ministerstwa Cyfryzacji

Na wystąpienie RPO 22 listopada 2018 r. odpowiedział minister cyfryzacji Marek Zagorski. Poinformował, że z e-usługi Wpisz się do rejestru wyborców i Zgłoś zamiar głosowania korespondencyjnego na portalu obywatel.gov.pl do 2 listopada 2018 r. skorzystały 47 752 osoby.

Do 21 października 2018 r. przez platformę ePUAP wniosek o wpis do rejestru wyborców złożyło zaś 46 551 osób. Z tego 43 205 osób złożyło wniosek w terminie gwarantującym jego rozpatrzenie przed I turą wyborów samorządowych.

Po przesłaniu wniosku do urzędu gminy, przy wykorzystaniu platformy ePUAP, obywatel otrzymuje Urzędowe Poświadczenie Przedłożenia (UPP). Czyli korespondencja została skuteczne dostarczona na Elektroniczną Skrzynkę Podawczą urzędu. Od tego momentu gmina ma 3 dni na realizację wniosku, w tym na sprawdzenie, czy wnioskujący spełnia warunki stałego zamieszkania pod wskazanym adresem.

Przepis nie wskazuje w jaki sposób dokonuje się sprawdzenia. Kodeks wyborczy nie precyzuje listy dokumentów, które należy gminie przedstawić. Urzędy gmin mogą w rożny sposób sprawdzać, czy wnioskodawcy spełniają warunki stałego zamieszkania na obszarze danej gminy. Jeśli oczekują przedstawienia jakichś dokumentów, mogą wezwać obywateli do ich przedłożenia (również przez ePUAP).

- Właściwy organ ma trzy dni na wydanie decyzji, a w przypadku wydania decyzji o odmowie wpisania do rejestru wyborców, organ ma obowiązek niezwłocznego poinformowania o tym obywatela. Zatem dopełnienie przez organy obowiązków wynikających z Kodeksu Wyborczego pozwoliłoby zdecydowanej większości wyborców, którzy złożyli wnioski do 16 października włącznie, na wcześniejsze (jeszcze przed I turą wyborów) uzyskanie informacji o podjętej decyzji w sprawie złożonego przez nich wniosku – głosi pismo ministra.

Podkreślił, że platforma ePUAP, Profil Zaufany i podpis zaufany umożliwiają bezpieczną komunikację obywatela z administracją publiczną w rożnych sprawach, w tym co do wniosków o wpis do rejestru wyborców. Procedowanie przesłanego przez obywatela wniosku, tak jak to ma miejsce w przypadku wielu innych e-usług administracji, realizowanych przy wykorzystaniu platformy ePUAP, leży już natomiast po stronie gminy.

Do Ministerstwa Cyfryzacji wpłynęło kilkanaście skarg od obywateli na realizację ich wniosków o dopisanie do rejestru wyborców. W pierwszej kolejności dotyczyły one sytuacji, w których obywatele dowiadywali się o braku możliwości głosowania w lokalu wyborczym. Wskazuje to na brak rozpatrzenia wniosku i kontaktu w sprawie ewentualnego uzupełnienia wniosków oraz o braku wydania decyzji pozytywnej lub odmownej. W tych przypadkach obywateli informowano o przysługujących im środkach odwoławczych.

Przedstawione przez Rzecznika przykłady potwierdzają powyższą sytuację. Urzędy, które nie obsłużyły złożonych wniosków, wskazywały na ich niekompletność, wprowadzając tym samym użytkowników w błąd (w kontekście brzmienia art. 19 Kodeksu

wyborczego). Urzędy te nie sprostały wymogom elektronicznej administracji i Kodeksu Wyborczego, nie rozpatrzyły w ustawowym terminie wniosków złożonych drogą elektroniczną, nie poinformowały o tym obywateli, nie dając im szans na ewentualne przedłożenie dodatkowych dokumentów (w sytuacji gdy gmina zamierzała potwierdzić fakt zamieszkiwania na jej terenie właśnie w ten sposób), nie poinformowały obywateli o podjętych w ich sprawach decyzjach. Decyzje te były wydawane już po dniu wyborów, bez zachowania trzydniowego terminu.

Wyciągając wnioski z zaistniałej sytuacji, Ministerstwo Cyfryzacji podjęło prace nad rozbudową systemu ePUAP o moduł umożliwiający sprawdzenie stanu sprawy przez użytkownika oraz nad rozwiązaniami, które ułatwią gminom analizę posiadanych danych.

Ponadto, przed drugą turą wyborów, zwiększono działania informacyjne i rozszerzono opis usługi Wpisz się do rejestru wyborców na portalu obywatel.gov.pl. Podkreślono fakt, iż po złożeniu wniosku podlega on rozpatrzeniu przez gminę:

Wysłanie wniosku nie oznacza wpisania do rejestru wyborców. Decyzję o wpisaniu (lub odmowie wpisania) do rejestru wyborców urząd podejmie w ciągu 3 dni od złożenia wniosku. Urząd w tym czasie zweryfikuje twoją deklarację. Urzędnik może odmówić wpisania cię do rejestru wyborców — jeśli uzna, że nie mieszkasz tam, gdzie deklarujesz. Dostaniesz wtedy pisemną odmowę. W takiej sytuacji możesz złożyć skargę.

Mając na uwadze zbliżający się rok, w którym odbędą się wybory do Parlamentu Europejskiego i wybory parlamentarne, zorganizujemy spotkanie z właścicielami biznesowymi procesu - Ministerstwem Spraw Wewnętrznych i Administracji i Krajowym Biurem Wyborczym - w sprawie ewentualnego doprecyzowania procesów wspierających procedury wyborcze – zapowiedział ponadto minister Marek Zagórski.

VII.602.40.2018

BEZ SZEROKIEGO POROZUMIENIA NIE BĘDZIE ELEKTRONICZNEJ OBYWATELSKIEJ INICJATYWY USTAWODAWCZEJ

data: 2018-11-08

- **Wprowadzenia elektronicznej obywatelskiej inicjatywy ustawodawczej wymaga szerokiego konsensusu politycznego.**
- **Dopiero wtedy możliwe byłoby rozważenie technicznych aspektów i rozwiązań, za pomocą których obywatele będą mogli podejmować inicjatywę ustawodawczą.**
- **Technicznie jest to mozliwe do wprowadzenia.**

Minister Cyfryzacji odpowiedział tak na jego wystąpienie Rzecznika. - Wprowadzanie ewentualnych zmian w tym obszarze wymaga szerokiej dyskusji oraz wskazania wiodącego organu, który upoważniony zostanie do zainicjowania i pokierowania pracami zmierzających w postulowanym kierunku. W przypadku podjęcia takich decyzji Ministerstwo Cyfryzacji będzie czynnie wspierało inicjatywę.

Jednym z kluczowych zagadnień jest zapewnienie rozliczalności zbiórki głosów poparcia pod obywatelskimi projektami ustaw. Musi to gwarantować, że oddany głos będzie niepodważalnie powiązany zarówno z danymi identyfikującymi obywatela popierającego projekt, jak i z dokumentem elektronicznym zawierającym treść popieranego projektu. Umożliwienie gromadzenia poparcia pod obywatelskimi projektami ustaw z wykorzystaniem środków komunikacji elektronicznej oraz podpisów elektronicznych należy ocenić jako możliwe do realizacji.

VII.600.9.2015.

W OBRONIE OBYWATELI, KTÓRZY 21 PAŹDZIERNIKA NIE MOGLI GŁOSOWAĆ. WYSTĄPIENIE RPO DO PKW

data: 2018-11-02

- **Urzędy nie były przygotowane na tak duży wpływ wniosków on-line o dopisanie się do rejestru wyborców - uważa RPO**
- **Obywatele zakładali, że brak odpowiedzi na wniosek oznacza wpisanie do rejestru - w lokalu wyborczym czekało ich bolesne rozczarowanie**
- **Wielu wniosków nie rozpatrzono w terminie; wyborcy dostawali wręcz mylne informacje; nie byli też zawiadamiani o odmowie wpisania do rejestru**
- **W ocenie obywateli wszystko to podważa zaufanie do praworządnego państwa**

Do Rzecznika Praw Obywatelskich wpłynęło wiele skarg od obywateli, którzy nie mogli głosować w wyborach samorządowych 21 października 2018 r - mimo że zgłosili on-line wnioski o dopisanie do rejestru wyborców. Rzecznik zwrócił się do przewodniczącego Państwowej Komisji Wyborczej Wojciecha Hermelińskiego o stanowisko co do skuteczności i praktycznego działania usługi wyborczej on-line, mającej umożliwiać wpis do rejestru.

Wcześniej RPO pytał też o to Ministra Cyfyzacji; wystąpił także o wyjaśnienia w sprawach konkretnych skarg m.in. do prezydentów miast.

Skargi składają obywatele, którzy skorzystali z usługi wyborczej on-line (strona Obywatel.gov.pl i Profil Zaufany e-PUAP), chcąc dopisać się do rejestru wyborców. Usługa ta była szeroko prezentowana jako wygodna dla wyborców, będącą efektem współpracy ekspertów Ministerstwa Cyfryzacji, MSWiA, PKW oraz Centralnego Ośrodka Informatyki. Tymczasem usługa nie działała prawidłowo, co spowodowało, że skuteczne złożenie wniosku i wpisanie do rejestru wyborców nie było możliwe.

Pani Magdalena podkreślała np. brak informacji, że trzeba było przesłać skan umowy wynajmowanego mieszkania w mieście, gdzie chciało się głosować. Ponadto e-PUAP pozwalał na przesłanie tylko dwóch załączników.

„Wezwanie do uzupełnienia braków w nierealnym terminie jednego dnia uważam za łamanie moich praw obywatelskich" – pisał z kolei pan Rafał; jego wniosek odrzucono wobec braku potwierdzenia zamieszkania w danym mieście.

Z kolei pan Maciej uzupełnił wniosek zgodnie z wezwaniem, ale nie dostał żadnej decyzji - dopiero w lokalu wyborczym dowiedział się, że nie dopisano go do rejestru.

Trudności te spowodowały poważne wzburzenie i krytykę wyborców. Pisali do RPO np.:

„to niedopuszczalne, aby komukolwiek odmówiono prawa do głosu tym bardziej, jeżeli wypełnił wcześniej wszystkie warunki zawarte w ustawie pozostawiając organowi odpowiedni czas na wydanie decyzji w konkretnej sprawie",

„uważam, że w dniu dzisiejszym zostałem pozbawiony konstytucyjnego prawa umożliwiającego oddanie głosu w wyborach",

„procedowanie w ten sposób jest skandaliczne, wbrew wszelkim regułom prawa administracyjnego i postępowania w tym zakresie".

„powszechne występowanie problemów przy tego typu wnioskach podważa zaufanie obywateli do praworządnego Państwa",

„słucham od dwóch dni z zażenowaniem wypowiedzi, a to PKW a to przedstawiciela Ministerstwa Cyfryzacji, że należę może do grupy ciamajdów, oferm życiowych, które zrobiły coś za późno lub nie potrafią obsługiwać <świetnie działającego systemu>".

Ponadto do RPO wpłynęły informacje o trudnościach w praktycznym stosowaniu nakładek na karty do głosowania, sporządzanych w alfabecie Braille'a. Przed wyborami RPO wskazywał PKW, że gdy wyborca zażąda w lokalu takiej nakładki, ma ona być dopiero dowieziona z urzędu gminy, a wyborca musi czekać. Rzecznik pytał też PKW, czy przewidziano sytuację, gdy nakładek zażąda wielu wyborców w różnych lokalach jednej gminy.

Wpłynęła także skarga obywatela na bezpodstawne pozbawienie go, wraz z ojcem, praw wyborczych w wyniku pisma sądu do gminy. „Sąd przez swoje błędy pozbawił nas prawa do głosowania" - głosi skarga. RPO wystąpił już w tej sprawie do sądu.

Były też skargi na niemożność głosowania przez osoby znajdujące się w więzieniach i aresztach śledczych. Zgodnie ze stanowiskiem PKW, jeśli są one zameldowane w innych gminach niż miejsce odbywania kary, to nie mogą się dopisywać do rejestru tam, gdzie ją odbywają. Według RPO osoby takie powinny mieć realnie zagwarantowane prawa wyborcze.

Z analizy wniosków wynikają następujące problemy związane z korzystaniem z usługi wyborczej on-line. Wyborcy wskazują na **brak jasnych komunikatów, lub wręcz mylne informacje** w ramach usługi wyborczej oferowanej na stronie obywatel.gov.pl:

przekazując wniosek o wpis do rejestru wyborców i załączając wskazane w systemie dokumenty, obywatele nie wiedzieli, że powinni się liczyć z dalszą procedurą (podejmowaną przez wójta/burmistrza/ prezydenta miasta) w celu sprawdzenia, czy dana osoba na stałe mieszka na obszarze gminy - co może oznaczać konieczność dołączenia kolejnych dokumentów;

z powodu niepełnej informacji o procedurze wpisu do rejestru wyborców obywatele różnie interpretowali brak odpowiedzi na taki wniosek. W większości zgłoszonych przypadków uznawali to jako dokonanie skutecznego wpisu. Było to założeniem błędne, o czym jednak dowiadywali się dopiero w lokalach wyborczych,

wyborcy byli informowani na stronie obywatel.gov.pl, że składając wniosek do 16 października, zostaną wpisani do rejestru. W części przypadków okazało się to informacją nieprawdziwą,

ponadto wyborcy wskazywali na fakt błędnego złożenia wniosku o dopisanie się do spisu wyborców, a nie do rejestru wyborców (co miało wynikać miało z braku jasnych i jednoznacznych komunikatów).

Analiza prowadzi też do wniosku o **braku skoordynowania usługi wyborczej on-line co do procedur stosowanych przez urzędy gmin/miast:**

w części przypadków odmowy wpisania do rejestru dokonywano wyłącznie na podstawie załączonych do wniosku dokumentów, które oceniano jako niewystarczające (tymczasem ich liczba była technicznie ograniczona; nie było również informacji o innych, dodatkowo wymaganych dokumentach),

wniosek wraz z wymaganymi załącznikami uznawano za zawierający braki i wzywano w krótkim terminie jednego dnia do uzupełnienia o dodatkowe dokumenty. W praktyce okazywało się to trudne do wykonania,

nie informowano wyborców ani o wpisaniu do rejestru, ani o odmowie wpisania. Pozbawiało to obywateli możliwości złożenia skargi do sądu (sąd rozpoznaje taką skargę w 3 dni; decyzja sądu jest ostateczna),

zupełnie nie uwzględniano wniosków o wpisanie do rejestru wyborców, wpływających systemem ePUAP.

Wiele urzędów gmin/miast **miało ogromne trudności z terminowym rozpatrzeniem wniosków o wpisanie do rejestru (przede wszystkim z uwagi na ich dużą liczbę)** - wskazuje Rzecznik. W wielu przypadkach terminy te nie zostały dochowane. Trudności tych nie przewidziano w fazie projektowania usługi on-line.

Problemy z wpisem do rejestrów wyborców dodatkowo obciążyły członków obwodowych komisji wyborczych w dniu wyborów. Musieli wyjaśniać sytuację wyborców, którzy nie znaleźli się w rejestrach.

Dlatego zastępca RPO Stanisław Trociuk poprosił Wojciecha Hermelińskiego o stanowisko PKW w sprawie skuteczności i adekwatności usługi wyborczej on-line, szczególnie w kontekście jej funkcjonowania. Zwrócił się też o informacje o funkcjonowaniu usługi zgłaszania z wykorzystaniem Profilu Zaufanego zamiaru głosowania korespondencyjnego przez wyborców z niepełnosprawnościami.

VII.602.40.2018

NIE ZOSTALI DOPISANI DO SPISÓW WYBORCÓW - SKARŻĄ SIĘ RPO. ADAM BODNAR PISZE DO MINISTRA CYFRYZACJI

data: 2018-10-29

- **Obywatele, którzy chcieli dopisać się przez ePUAP do rejestru wyborców, skarżą się RPO na problemy, jakie uniemożliwiły im udział w wyborach samorządowych**
- **Pani Magdalena podkreśla brak informacji, że trzeba było przesłać skan umowy wynajmowanego mieszkania w mieście, gdzie chciało się głosować; ponadto e-PUAP pozwalał na przesłanie tylko dwóch załączników**
- **Wezwanie do uzupełnienia braków w nierealnym terminie jednego dnia uważam za łamanie moich praw obywatelskich – pisze z kolei pan Rafał; jego wniosek odrzucono wobec braku potwierdzenia zamieszkania w danym mieście**
- **Z kolei pan Maciej uzupełnił wniosek zgodnie z wezwaniem, ale nie dostał żadnej decyzji - dopiero w lokalu wyborczym dowiedział się, że nie dopisano go do rejestru**

Takie m.in. sygnały od obywateli, którzy nie mogli głosować w wyborach samorządowych 21 października 2018 r - mimo że zgłosili przez e-PUAP wnioski o dopisanie do rejestru wyborców - stały się podstawą wystąpienia Rzecznika Praw Obywatelskich do Ministra Cyfryzacji. Adam Bodnar poprosił Marka Zagórskiego o stanowisko co do skuteczności i praktycznego działania usługi wyborczej on-line, mającej umożliwiać wpis do rejestru. Ponadto Rzecznik wystąpił o wyjaśnienia w sprawach konkretnych skarg do prezydentów miast.

Zaniepokojny RPO bada sprawę

Sygnały od obywateli Rzecznik przyjął z zaniepokojeniem. Z racji wagi sprawy dla realizacji zasady powszechności wyborów, RPO zdecydował sprawę zanalizować.

Zdecydowana większość skarg dotyczy wyborców, którzy zdecydowali się skorzystać z usługi wyborczej on-line (strona Obywatel.gov.pl i uwierzytelnienie przy pomocy Profilu Zaufanego e-PUAP). Była ona prezentowana jako wygodna dla wyborców, nie wymagająca osobistej wizyty w urzędzie, udostępniona m.in. z myślą o wyborcach z niepełnosprawnościami.

Pewna część skarg dotyczy osób, które odpowiedni wniosek złożyły zbyt późno, aby mógł być on rozpatrzony w ustawowym terminie (do 16 października włącznie). Jednak są też wyborcy, którzy złożyli go odpowiednio wcześnie, a to wskazuje na różnorodne trudności organizacyjne i techniczne, jakie uniemożliwiły skuteczny wpis do rejestru wyborców i w efekcie – wzięcie udziału w wyborach.

Na co skarżą się obywatele

Na brak możliwości swobodnego dołączania załączników. Dodatkowe załączniki były zaś - przynajmniej w części przypadków - uznawane za konieczne w procedurze wpisu.

Np. pani Magdalena, która złożyła wniosek 16 października, nie mogła oddać głosu. W lokalu wyborczym dostała numer do Urzędu gminy. W rozmowie telefonicznej usłyszała, że wniosku rozpatrzyć nie zdążyli. W skardze pisała: „Po chwili jednak pani stwierdziła, że sprawdzi mój wniosek. Kiedy to zrobiła, pojawił się zarzut, że nie wysłałam skanu umowy najmu. Moje pytanie brzmi: w którym momencie składania wniosku zostałam o to poproszona? Odpowiedź: w żadnym. Jedynym wymaganym skanem był skan dowodu osobistego, który zamieściłam. Wiem też że w oficjalnej komunikacji podana była informacja, że taki dokument w ogóle nie jest wymagany. Oprócz tego e-PUAP ograniczał możliwość wymaganych załączników do dwóch, czyli przód i tył dowodu. Kiedy powiedziałam to pani z Urzędu Miasta, odpowiedziała <ale my wymagamy takiego dokumentu, a e-PUAP to osobny system i ja nie wiem dlaczego nie ma tutaj takiego pola>”.

Na chaos i brak precyzyjnych informacji

W innej skardze obywatel wskazywał na problemy organizacyjne i techniczne: „Po przyjściu do lokalu wyborczego otrzymałem informację, że nie zostałem dopisany na listę i poproszono mnie skontaktowanie się z Urzędem Gminy […]. W trakcie połączenia dostałem odpowiedź, że nie ma mnie na liście pomimo terminowego złożenia wniosku oraz dołączenia skanu dokumentu tożsamości. Zapytano mnie również o to, czy dołączyłem dokument potwierdzający to, że mieszkam pod wskazanym adresem. Nigdzie w systemie nie było to wymagane, ani nikt o tym nie informował, ponadto nie było nawet miejsca na dołączenia takiej liczby załączników. Po zapytaniu o to gdzie można zgłosić sprawę usłyszałem, że pani sprawdzi jeszcze raz i faktycznie sprawdziła. Tutaj przechodzimy do najbardziej kuriozalnej sytuacji bo pani po ponownym sprawdzeniu stwierdziła, że mój wniosek został rozpatrzony pozytywnie […] pomimo tego pani stwierdziła jednak, że urząd nie ma mojego wniosku i ePuap to oddzielny system”.

Na nieuwzględnienie tego, że obywatel nie może uzupełnić wniosku w jeden dzień

Także pan Rafał dostał informację, że jego elektroniczny wniosek został odrzucony 15 października z powodu „braku dokumentu potwierdzającego zamieszkanie we Wrocławiu”. Został wezwany do uzupełnienia braków w ciągu jednego dnia od otrzymania pisma. W skardze do RPO napisał: „Brak informacji o tym, że taki dokument powinien zostać załączony uważam za karygodny. Brak pola w tym formularzu na załączenie dokumentu potwierdzającego zamieszkanie uważam, za celowe wprowadzenie w błąd i próbę oszukania mnie jako wyborcę. Wezwanie do uzupełnienia braków w nierealnym terminie jednego dnia uważam za łamanie moich praw obywatelskich”.

Do uzupełnienia wniosku z 15 października w ciągu jednego dnia został wezwany także pan Maciej. Uczynił to za pośrednictwem e-PUAP 17 października o godz. 13:56. „Nie otrzymałem żadnej decyzji - ani o dokonaniu wpisu, ani o odmowie. W dniu wyborów ok. godz. 19:30 udałem się do lokalu wyborczego. Okazało się, że nie zostałem dopisany do rejestru wyborców” – wskazał w swej skardze. Przewodniczący komisji wyborczej poinformował go, że otrzymał informacją, iż nie został dopisany do rejestru wyborców z uwagi na fakt, iż wniosek złożono zbyt późno.

Na to, że korespondencja z urzędami urywała się przed zakończeniem sprawy

W skardze do RPO pan Donat pisał, że 15 października wnioskował przez e-PUAP o dopisanie do spisu wyborców w mieście, gdzie aktualnie mieszka. „Do dnia dzisiejszego nadal nie otrzymałem żadnej odpowiedzi (…) Pracownicy PKW twierdzą, że mam udowadniać, że mieszkam tu, gdzie mieszkam, ale we wniosku nie ma takich informacji” - dodał.

Wyborcy skarżą się także na brak jakichkolwiek wiadomości w odpowiedzi na złożone wnioski lub zamieszczanie na stronie obywatel.gov.pl mylących ich informacji.

Skarżąca pisała” „Na stronie obywatel.gov.pl widniała oficjalna informacja, że do 16 października można poprzez konto w serwisie e-PUAP składać wniosek o dopisanie do grona wyborców zgodnie z miejscem zamieszkania”. Mimo złożenia wniosku w tym terminie, nie został on jednak rozpatrzony do dnia wyborów. Skarżąca zauważyła: „Jako obywatel widziałam wyraźną informację <Masz jeszcze 2h na złożenie wniosku, aby dopisać się do listy wyborców i zagłosować w najbliższych wyborach samorządowych>. Przy tak jasnym komunikacie, podanym na oficjalnej, państwowej stronie czuję się bezpiecznie, że nawet jeśli złożę wiosek o 23:30 to odpowiednie organy mają wystarczającą ilość czasu aby go rozpatrzyć […] Gdybym wiedziała, że nie będę dopisana do listy wyborców w […], najpewniej udałabym się wcześniej do urzędu, lub wróciła do miejsca zameldowania aby oddać głos”.

Prośba do Ministra Cyfryzacji

- Uprzejmie proszę Pana Ministra o przedstawienie stanowiska w sprawie skuteczności i adekwatności przyjętych procedur usługi wyborczej on-line mającej umożliwiać wyborcom wpis do rejestru wyborców, szczególności w kontekście jej funkcjonowania w praktyce – napisał Adam Bodnar do ministra Marka Zagórskiego.

Wystąpił też o informacje, ilu wyborców złożyło wnioski do 16 października, a ilu po tym dniu (z uwzględnieniem gmin, do których były kierowane). Zwrócił się również o podanie, ilu wniosków nie rozpatrzono do 21 października.

W związku z szerszą analizą procedur głosowania, Rzecznik poprosił także o informację o funkcjonowaniu tej usługi w przypadku zgłaszania zamiaru głosowania korespondencyjnego.

VII.602.40.2018

DOPISYWANIE SIĘ DO REJESTRU WYBORCÓW PRZEZ E-PUAP. RZECZNIK PODEJMUJE INTERWENCJE PO SKARGACH OD OBYWATELI

data: 2018-10-23

- **RPO dostaje skargi od osób, które nie mogły głosować w wyborach samorządowych 21 października, mimo że zgłosiły przez E-PUAP wnioski o dopisanie do rejestru wyborców**
- **Rzecznik zapytał już Prezydenta Warszawy o to, ilu osób w stolicy dotyczył ten problem**

Jeden z obywateli napisał np. do RPO, że wniosek przez ePUAP skierował w poniedziałek przedwyborczy, załączył skan dokumentu poświadczającego, gdzie mieszka, a mimo to nie znalazł się na liście wyborców. Komisja poinformowała go „o dużej częstotliwości występowania takiego zdarzenia".

Rzecznik prosi zatem o dane, ilu wyborców złożyło wniosek o wpis do rejestru wyborców z wykorzystaniem Profilu Zaufanego (ePUAP) do 16 października włącznie, a ilu po dniu 16 października 2018 r. (z uwzględnieniem urzędów dzielnic, do których były kierowane). Prosi też o podanie liczby wniosków, które nie zostały rozpatrzone do 21 października 2018 r.

VII.602.41.2018, VII.602.45.2018, VII.602.52.2018, VII.602.52.2018

O PATOSTREAMINGU - PRAWNICY, NAUKOWCY, PRZEDSTAWICIELE WŁADZ, ORGANIZACJI POZARZĄDOWYCH I FIRM TECHNOLOGICZNYCH, YOUTUBERZY I DZIENNIKARZE

data: 2018-10-18

- **Jak zmierzyć się ze zjawiskiem patostreamingu? RPO zorganizował w swoim Biurze w Warszawie okrągły stół w tej sprawie. W spotkaniu uczestniczyła wiceminister cyfryzacji Wanda Buk, oraz 30 innych ekspertów.**
- **Patostreaming to pokazywanie przemocy i wulgarnych treści, niekiedy będących łamaniem prawa, po to, by oglądający to przez internet widzowie płacili nadawcy. W Polsce w ostatnich latach zjawisko nasila się w sposób nie znany w innych krajach**
- **To wulgarne, poniżające materiały, często pełne przemocy fizycznej i słownej, nierzadko nagrywane pod wpływem alkoholu lub innych środków odurzających z lekceważeniem prawa i zasad współżycia społecznego.**
- **Mają dużą oglądalność, a ich nadawcy na tym zarabiają. Dostają też pieniądze za to, że zrobią coś odrażającego czy okrutnego: może to być znęcanie się nad osobą bliską, bicie, poniżanie….**
- **Mogą to oglądać dzieci, często bez wiedzy rodziców o istnieniu takiego zagrożenia**

Zjawisko jest stosunkowo nowe, ale powstało na ten temat kilka reportaży[1]. Rzecznik dostał dopiero jedną skargę (od sąsiadów nadawcy takich treści, czyli patostreamera). Nie ma takich skarg resort cyfryzacji, Ministerstwo Sprawiedliwości szuka na razie narzędzi do opisu problemu. Ale o skali zjawiska alarmują organizacje pozarządowe, wychowawcy, psychologowie, badacze społeczni.

- Coraz więcej osób zwraca uwagę na mowę nienawiści
i się jej sprzeciwia. Patologiczne treści w internecie
często idą dalej – naruszają nietykalność cielesną innych osób,
promują przemoc, utrwalają negatywne stereotypy.
Najczęściej dostępne są na popularnych platformach
bez ograniczeń wiekowych.
Zorganizowaliśmy w Biurze Rzecznika Praw Obywatelskich
spotkanie ludzi, dla których punktem wyjścia jest godność jako
nienaruszalna podstawowa wartość.
Patostreaming jest jaskrawym przykładem łamania godności i nie
ma na to naszej zgody w przestrzeni publicznejm,
jaką jest Internet
– mówi Zuzanna Rudzińska-Bluszcz, inicjatorka spotkania,
odpowiedzialna w BRPO za strategiczne postępowania sądowe.

Z dyskusji wynikało, że patostreaming jest zjawiskiem, które na tak szeroką skalę pojawiło się tylko w Polsce. Przedstawiciel Google'a podkreślał, że podobnych zgłoszeń firma nie ma z innych krajów. Prawdopodobnie więc zjawisko to jest skutkiem głębszych procesów zachodzących w naszym społeczeństwie, na co wskazywali też inni uczestnicy spotkania. Przemoc i agresja słowna obecna jest przecież nie tylko w internecie i nie tylko w formach „ludowych" – dziennikarze i politycy nie stronią od agresywnych komentarzy, programy typu „reality show" są nadawane w dużych stacjach telewizyjnych, przemoc i mowa nienawiści jest częścią kultury masowej i debaty politycznej. Większość z nas przestaje na to reagować, przyzwyczaja się,

Zebrani ustalili więc, że choć prostych rozwiązań tu nie będzie, to na pewno skuteczna okaże się współpraca i wskazywanie konkretnych rozwiązań, które krok po kroku mogą zmierzać do ograniczenia zjawiska patostreamingu. Kluczowe znaczenie ma tu współpraca, a rola trzeciego sektora jest nie do przecenienia, co podkreślali przedstawiciele władz.

Trzeba wykorzystywać istniejące rozwiązania prawne i uczyć się z nich korzystać

1. Musimy uczyć się reagować na przemoc i patologię w internecie. Ci, którzy się na internecie znają, powinni w tym wspierać rodziców i wychowawców oraz pomoc społeczną

2. Trzeba się nauczyć problem opisywać w mediach tak, by nie przysparzał złej sławy twórcom patostreamingu, bo oni żywią się tą złą sławą

3. Trzeba utrudniać dostęp do tych treści – ale też i zarabianie na nich (i pokusę sponsorowania patostreamingu)

To tylko pierwsze propozycje – kolejne zostaną wspólnie wypracowane na podstawie dwugodzinnej dyskusji w Biurze RPO. Prowadzili ją zastępca RPO i mec. Zuzanna Rudzińska Bluszcz, a wzięli w niej udział:

- Wanda Buk, wiceministra cyfryzacji
- Jan Kostrzewa dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Sprawiedliwości
- Marcin Olender, Google
- Michał Białek, Wykop.pl
- Alek Tarkowski, Centrum Cyfrowe
- Marcin Bochenek, Państwowy Instytut Badawczy
- Maciej Tanaś, NASK, doradca RPD
- Karol Paciorek, youtuber:
- Maciej Budzich, blogger
- Artur Kurasiński, blogger
- Kamil Bolek, Lifetube
- Wojciech Kardyś, Goog for you
- Konrad Dulkowski i Rafał Gaweł, Ośrodek Monitorowania Zachowań Rasistowskich
- Łukasz Wojtasik i Marta Wojtas, Dajemy Dzieciom Siłę
- Rafał Szymański, Porcelanowe aniołki
- Krzysztof „Ator" Woźniak", blogger
- Dominika Bychowska-Siniarska, HFPC.
- Ludmiła Ananikova, Gazeta Wyborcza
- Maciej Młynarczyk, Prokuratura Rejonowa Warszawa Praga Północ
- Grażyna Stanek, prokurator w ss, Lex Superomnia
- Maria Rotkiel, psycholożka
- Marcin Zimoń, Komenda Stołeczna Policji,wydział prewencji
- Agata Malinowska, pełnomocniczka Komendanta Stołecznego Policji ds. Praw Człowieka.

A także przedstawiciele BRPO: Michał Hara, Piotr Sobota, Agnieszka Jarzębska i Joanna Jakubczak, a także Dariusz Supeł, który oprócz tego, że w pracuje w BRPO jest także wychowawcą i przewodniczącym ZHP.

Gdy przedmiotem przekazu jest zdarzenie mogące wypełniać znamiona czynu zabronionego (np. znęcanie, pobicie):

Eksperci BRPO zwracają uwagę na dostępne już przepisy. W przypadku patostreamingu policja powinna prowadzić czynności sprawdzające, czy zachodzi podejrzenie zaistnienia przestępstwa lub wykroczenia

Problem polega na tym, że przedmiotem patostreamów często są zachowania stanowiące przestępstwa ścigane z oskarżenia prywatnego albo na wniosek (znieważenie, zniesławienie, naruszenie nietykalności cielesnej, zniszczenie cudzej rzeczy). Może być też tak, że prezentowane w patrostreamie treści są zainscenizowane lub nie odpowiadają deklaracjom ich autorów (np. mieszane substancje są inne od deklarowanych). Wtedy można ewentualnie rozważyć odpowiedzialność z art. 286 § 1 k.k. Spełnione są bowiem wszystkie trzy przesłanki zaistnienia przestępstwa oszustwa (działanie w celu uzyskania korzyści majątkowej, wprowadzenie innej osoby w błąd i doprowadzenie jej do niekorzystnego rozporządzenia mieniem).

Gdy sam przekaz może wypełniać znamiona czynu zabronionego:

Możliwe jest ściganie takich czynów, popełnionych za pośrednictwem internetu
Pozwalają na to

- art. 52a kodeksu wykroczeń (publiczne nawoływanie do popełnienia przestępstwa, publiczne nawoływanie do przeciwdziałania przemocą aktowi stanowiącemu źródło powszechnie obowiązującego prawa, publiczne pochwalanie popełnienia przestępstwa)
- art. 141 k.w. (dopuszczanie się nieobyczajnego wybryku, zamieszczenie w miejscu publicznym nieprzyzwoitego ogłoszenia, napisu lub rysunku albo używanie słów nieprzyzwoitych
- art. 117 § 3 kodeksu karnego (publiczne nawoływanie do wszczęcia wojny napastniczej lub publiczne pochwalanie wszczęcia lub prowadzenia takiej wojny
- art. 135 § 2 k.k. (publiczne znieważenie Narodu lub Rzeczypospolitej Polskiej art. 133 k.k., publiczne znieważenie Prezydenta RP)
- art. 196 k.k. (obrażanie uczuć religijnych poprzez publiczne znieważenie przedmiotu czci religijnej lub miejsce przeznaczone do publicznego wykonywania obrzędów religijnych)
- art. 200b k.k. i inne. (publiczne pochwalanie lub propagowanie zachowania o charakterze pedofilskim

Trzeba pamiętać, że internet to miejsce publiczna.Wynika to z orzeczenie Sądu Najwyższego z dnia 17 kwietnia 2018 r. sygn. akt IV KK 296/17 wydane po rozpoznaniu kasacji Rzecznika Praw Obywatelskich, w którym Sąd Najwyższy rozważając kwestie odpowiedzialności za czyn z art. 141 k.w. stwierdził, między innymi, że „w przypadku wykorzystania Internetu do umieszczenia w nim nieprzyzwoitego ogłoszenia, napisów lub rysunków albo używania za jego pośrednictwem słów nieprzyzwoitych, miejscem publicznym w rozumieniu art. 141 k.w. są serwisy WWW takie jak: portale informacyjne, portale korporacyjne, z tym że w przestrzeni dla potencjalnych klientów, otwarte fora dyskusyjne, blogi, vlogi (tzw. videoblogi), do których dostęp nie jest limitowany, a zatem nie zabezpieczony loginem i hasłem, ograniczającymi możliwość uzyskania dostępu do wyodrębnionej przestrzeni internetowej dla internautów przez właściciela serwisu”.

Co więcej Sąd Najwyższy uznał, że „w kontekście pojęcia miejsce publiczne odnoszącego się do przestrzeni wirtualnej nie jest istotne gdzie fizycznie znajduje się serwer sprzętowy, na którym udostępniany jest serwis internetowy”.

[1] m.in. https://uwaga.tvn.pl/uwaga-po-uwadze,2680,n/patologia-na-zywo-czyli-swiat-patostreamerow,273874.html; http://wyborcza.pl/duzyformat/7,127290,23229085,sekspiosenki-cypisa-i-popka-na-youtubie-ogladaja-dzieci-z-podstawowki.html

INWIGILACJA DWA LATA PÓŹNIEJ. SPRAWA WYROKU ETPCZ SACHAROW (ZAKHAROV) VS ROSJA

data: 2018-09-24

- **Jak wygląda sytuacja w Polsce dwa lata po zwiększeniu uprawnień służb specjalnych w zakresie inwigilacji?**
- **Jakie wnioski wynikają dla nas ze sprawy Sacharow przeciw Rosji?**

24 września 2018 r. odbyła się w Biurze RPO konferencja dotycząca inwigilacji. Uczestniczył w niej bohater słynnej sprawy „inwigilacyjnej” przed Europejskim Trybunałem Praw Człowieka Roman Sacharow (Zakharov).

Przeszło dwa lata temu rozpoczął się proces nadający polskim służbom uprawnienia, które mogą godzić w prawa obywateli w zakresie ich prywatności. Tzw. ustawa inwigilacyjna weszła w życie w lutym 2016 r., a „antyterrorystyczna” – w lipcu 2017 r.

Jak dziś, po miesiącach stosowania nowych zapisów, wygląda sytuacja? Jak przestrzegane jest prawo do prywatności? Czy wobec wycofania przez Rzecznika Praw Obywatelskich wniosków o stwierdzenie niekonstytucyjności tych ustaw z Trybunału Konstytucyjnego jesteśmy skazani na niekontrolowane i wszechwładne służby?

Sprawa Sacharowa

Roman Sacharow w 2015 r. wygrał przed Europejskim Trybunałem Praw Człowieka sprawę przeciwko Rosji (skarga nr 47143/06) dotyczącą użycia systemu informatycznego SORM Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej do podsłuchiwania rozmów i przechwytywania korespondencji elektronicznej.

- Kiedy przeczytałem wyrok w sprawie Sacharow przeciw Rosji, pomyślałem najpierw: kim jest człowiek, który odważył się stanąć przeciw potężnemu państwu, słynącemu z tego, że swoich przeciwników ściga także za granicą? To jeden ze współczesnych bohaterów walki o prawa człowieka – przedstawiał gościa Marcin Mrowicki z BRPO.

- Jak wyglądała sytuacja w Rosji 12 lat temu, kiedy złożył Pan wniosek do ETPCz? – pytał Romana Sacharowa Adam Bodnar.

Sacharow opowiadał, że skargę złożył w 2006 r. jako pracownik fundacji zajmującej się wolnością słowa i jako dziennikarz. Wykonując swoje obowiązki, kontaktował się bowiem z osobami, które prosiły o zachowanie tego w tajemnicy, a potem okazywało się, że o tych kontaktach wiedzą rosyjscy politycy.

W owym czasie - podkreślał - w Rosji panowało przekonanie, że kwestie praw człowieka i wolności słowa są traktowane przez władze poważnie – np. stanowisko rosyjskiego rzecznika praw obywatelskich były analizowane, a kontrolowane przez państwo media przekazywały oprócz propagandy także informacje. Fundacja, z którą współpracował Sacharow, miała współpracowników także wśród urzędników. – Mieliśmy jeszcze wolność słowa i możliwość wykonywania pracy dziennikarskiej, a postawa konformistyczna nie przeważała – opowiadał Sacharow.

- Dlatego na podejrzenia, że informacje o moich kontaktach trafiają do polityków rosyjskich, postanowiłem zareagować. Nie chciałem składać skargi przeciw mojemu państwu, wystąpiłem więc przeciwko firmom telefonii komórkowej. Żyliśmy w czasach jeszcze sporej otwartości w dziedzinie gospodarczej. Złożenie pozwu udało się i dostawałem duże wsparcie od różnych prawników i organizacji. O sprawie otwarcie pisały media, zwłaszcza biznesowe.

Skarga dotyczyła tego, że operatorzy komórkowi zgodzili się na zainstalowanie urządzeń pozwalających na przechwytywanie informacji bez zgody sądu. Podstawą do instalowania tych urządzeń był niepublikowany oficjalnie załącznik do rozporządzenia ministra.

Roman Sacharow przegrał sprawę przed rosyjskimi sądami. Uzasadniły one, że nie przedstawił wystarczających dowodów, że on i jego rozmówcy padli ofiarą inwigilacji.

Wtedy sprawa trafiła do ETPCz. Sacharow powołał się na art. 8 Europejskiej Konwencji Praw Człowieka (prawo do prywatności).

ETPCz stwierdził naruszenie Konwencji:
choć formalnie do inwigilacji trzeba mieć w Rosji zgodę sądu,
ale obowiązek ten można łatwo obejść. Jeśli tak skonstruowane
jest prawo, to człowiek nie musi już dowodzić,
że był inwigilowany. Wystarczy, że jest taka możliwość
(jest regulacja prawna, która umożliwia takie działania).
Ponadto prawo rosyjskie nie gwarantuje skutecznych środków
odwoławczych obywatelowi, który podejrzewa,
że jest inwigilowany).

- Pamiętam, że po wyroku podeszli do mnie sędziowie z Białorusi, akurat tam obecni, i gratulowali nam – mówił Roman Sacharow.

Wyrok nie został jednak nigdy wykonany.

Zupełnym przypadkiem wyrok został ogłoszony w dniu, w którym prezydent Putin podpisał nowe prawo dające pierwszeństwo konstytucji rosyjskiej nad prawem międzynarodowym, jeśli wymaga tego „ochrona interesu Rosji" - opowiadał dalej Sacharow.

Relacjonował, że już przed ogłoszeniem wyroku pole debaty publicznej zawężało się. - Już nie rozmawialiśmy w pracy o tym, co uważamy o sprawie Krymu, służby specjalne dopytywały się moich przełożonych, czy naprawdę „potrzebny jest im ten Sacharow", złodzieje próbowali mi ukraść telefon komórkowy (charakterystyczne, że nie pieniądze ani karty kredytowe).

- Wtedy już byłem przekonany, że wyrok ETPCz nie zostanie w Rosji wykonany. Nie byliśmy już państwem demokratycznym – bo sądy nie były już niezależne i to gwałtownie zmieniło sytuację. Parlament przestał być miejscem debaty, a debatę publiczną zastąpiła propaganda.

- A dziś? Czy może Pan powiedzieć, jak wygląda życie dziennikarzy w Rosji? – pytał Adam Bodnar.

- Nadal w miarę niezależna jest prasa lokalna: jeśli nie krytykuje władz centralnych, może publikować materiały niewygodne dla władz lokalnych. Nikt nie łamie tam praw dziennikarzy. Ale narastającym problemem jest autocenzura. Jednocześnie coraz więcej jest spraw karnych za komentarze w sieci, a nawet za lajki (ludzie dostają mandaty, a nawet wyroki więzienia za coś co napisali albo tylko udostępnili w sieci kilka lat temu), Służby specjalne mają pełen dostęp do paneli administracyjnych w rosyjskich sieciach społecznościowych. Operatorzy tych sieci mają obowiązek przechowywania (retencji) kompletu danych przez pół roku.

Sacharow zauważył, że choć powodem tak intensywnego zbierania danych o obywatelach ma być bezpieczeństwo państwa, to system jest tu niewydolny i w razie realnego zagrożenia służby rosyjskie i tak zwracają się o pomoc do Amerykanów. Tak szeroko zakrojona inwigilacja skuteczna jest natomiast w powstrzymywaniu opozycji i zwykłych ludzi, których – nawet jeśli popierają rząd – może kusić, by zalajkować „nieprawomyślny" wpis.

Inwigilacja w Polsce dwa lata później

- Sprawa Sacharow przeciw Rosji jest od dawna wyznacznikiem standardów europejskich. I to do niej stale odnoszą się wszyscy, którzy analizują ochronę praw obywatelskich po zmianie przepisów inwigilacyjnych w Polsce – mówiła w kolejnym panelu konferencji dr Barbara Grabowska-Moroz (Helsińska Fundacja Praw człowieka)

Ten panel prowadził Mirosław Wróblewski, dyrektor Zespołu Prawa Konstytucyjnego i Europejskiego w Biurze RPO

O tym, jak służby w Polsce sukcesywnie dostawały nowe uprawnienia – kosztem obywateli – od początku 2016 r. (ustawa policyjna, ustawa antyterrorystyczna, przepisy dotyczące „owoców zatrutego drzewa"), opowiadał mec. Marcin Mrowicki z BRPO: Służby dostały bardzo szeroki dostęp do informacji o naszej aktywności w sieci, a wiele z tych informacji nie jest – nawet post factum – kontrolowane przez sądy.

RPO alarmował, zanim ostatecznie przepisy te weszły w życie, następnie zaskarżył je do Trybunału Konstytucyjnego.

- Niestety, na początku 2017 r. TK zaczął manipulować przy składach wyznaczonych do oceny tych spraw (zmiany składu pełnego na skład pięcioosobowy, bez podstawy prawnej i włączenie do składu osób których status sędziowski jest kwestionowany). Z tego powodu RPO swoje wnioski wycofał – mówił mec. Mrowicki (patrz załącznik - wybrane fragmenty Informacji Rocznej RPO za rok 2017).

**- Nasza nowa ustawa inwigilacyjna ma z pozoru niewinny przepis,
że służby mają co pół roku sprawozdawać sądom podejmowane działania.
Początkowo wydawało się nam, że taka kontrola
jest po prostu niewystarczająca i na tym należy się skupić.
Ale w praktyce kluczowy okazał się początkowo nie rzucający się w oczy przepis,
że te sprawozdania sądowe są objęte przepisami o informacji niejawnej.
Bo to on wprowadził dodatkową zmianę: służby nie chcą już ujawniać
jakichkolwiek informacji o skali kontroli bilingów,
powołując się właśnie na przepisy o informacji niejawnej
– mówił Wojtek Klicki z Panoptykonu.**

Także sądy administracyjne zmieniły podejście do odmów dostępu do informacji publicznej ze strony służb. Zmienione prawo sprawiło, że na szali wartości bezpieczeństwo zaczyna znaczyć więcej niż wolność jednostki.

Elementem ochrony danych osobowych – tzw. drugą nogą RODO – miała być ustawa wdrażająca dyrektywę policyjną. To tu miały zostać opisane zasady ochrony prywatności w relacjach z państwem. Ustawa miała być gotowa do maja, w momencie wejścia w życie RODO. Nie jest gotowa do dziś, a informacje o stanie projektu napawają niepokojem (ma ona wyłączyć obrót informacjami niejawnymi z przepisów o ochronie danych osobowych).

Co to znaczy? - pytał panelistów dyr. Wróblewski.

- że znacząco osłabła ochrona praw człowieka
- że nowe przepisy pod pretekstem zwiększania bezpieczeństwa niszczą zaufanie do państwa. A bez zaufania bezpieczeństwo jest iluzoryczne
- że problemu nie rozwiąże wdrożenie dyrektywy policyjnej
- że dziś skarga z Polski na te przepisy zostałaby przez ETPCz uznana za zasadną

Ale nadal nadzieja jest w sądach i w tym, jak się ukształtuje orzecznictwo w tej kluczowej dla praw człowieka sprawie.

KRYTYCZNE UWAGI RZECZNIKA O PROJEKCIE USTAWY, KTÓRA MA WDRAŻAĆ DYREKTYWĘ POLICYJNĄ UE

data: 2018-05-02

- **Wyłączenie pięciu służb specjalnych z ustawy wprowadzającej unijną dyrektywę policyjną z 2016 r. może być sprzeczne nie tylko z samą dyrektywą, ale i z Konstytucją RP**
- **Rzecznik Praw Obywatelskich w dużej części krytycznie ocenia rządowy projekt ustawy, który ma wprowadzać do polskiego prawa dyrektywę Parlamentu Europejskiego i Rady UE 2016/680, dotyczącą przetwarzania danych osobowych przez organy ścigania**
- **RPO krytykuje także złożenie projektu w ostatnim możliwym terminie, skoro na jego przygotowanie MSWiA miało prawie dwa lata. Na zgłaszanie uwag resort przeznaczył tylko 10 dni**

Od 2017 r. Adam Bodnar występował do kilku resortów, wskazując że dyrektywa jest bardzo ważna z punktu widzenia obywatela. Ułatwia ona wymianę danych między państwami członkowskimi, a zarazem wzmacnia prawa osób, których te dane dotyczą. Przyznaje jednostce prawo uzyskania informacji od służb, czy jej dane są zbierane i przetwarzane oraz prawo do skargi na te działania do niezależnego organu nadzorczego.

28 marca 2018 r. Rzecznik po raz kolejny wyraził zaniepokojenie brakiem prac nad wprowadzeniem dyrektywy do polskiego prawa. W piśmie do szefa MSWiA wskazał, że przepisy niezbędne do jej wykonania mają być stosowane przez państwa członkowskie od 6 maja - Polska może nie dotrzymać tego terminu. Wystąpił wtedy do ministra Joachima Brudzińskiego o pilną informację na temat stanu prac nad projektem odpowiedniej ustawy.

Projekt na ostatnią chwilę

20 kwietnia 2018 r. MSWiA poinformowało o umieszczeniu dzień wcześniej na stronach Rządowego Centrum Legislacji projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

W odpowiedzi zastępca RPO Stanisław Trociuk napisał, że wyznaczenie 10-dniowego terminu na przedstawienie uwag do projektu nie tylko nie pozwala na ich pełne opracowanie, ale jest też sprzeczne z Regulaminem pracy Rady Ministrów. Przypomniał, że dyrektywa została przyjęta 27 kwietnia 2016 r. i weszła w życie 5 maja 2016 r., a zatem projektodawca miał prawie dwa lata na przygotowanie projektu. Przedstawienie go w ostatnim możliwym terminie RPO ocenił krytycznie.

Ustawa nie obejmie pięciu tajnych służb

- **Rzecznik negatywnie ocenia propozycję wyłączenia spod ustawy danych osobowych przetwarzanych w ramach realizacji zadań Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego.**

Zdaniem RPO nie wszystkie bowiem zadania tych służb mieszczą się w zakresie pojęcia „bezpieczeństwo narodowe" - co uzasadniałoby wyłączenie dopuszczalne przez dyrektywę. Z punktu widzenia prawa UE pojęcie „bezpieczeństwo narodowe" nie może być jednak utożsamiane z pojęciem „bezpieczeństwa wewnętrznego". Działalność CBA nie ma np. bezpośredniego związku z „bezpieczeństwem narodowym".

Dlatego nie można się zgodzić się z pozostawieniem poza obowiązkiem stosowania przepisów o ochronie danych osobowych co najmniej pięciu służb specjalnych. Może to oznaczać - przynajmniej w części - nie tylko sprzeczność z postanowieniami dyrektywy, ale przede wszystkim z art. 51 Konstytucji RP (mowa w nim m.in., że władze nie mogą gromadzić innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym).

Z zadowoleniem RPO przyjął zaś, że w skierowanym już do Sejmu projekcie nowej ustawy o ochronie danych osobowych uwzględniono jego uwagi w sprawie Prezesa Urzędu Ochrony Danych Osobowych. Będzie to nowy, niezależny organ nadzorczy właściwy zarówno i do unijnego rozporządzenia RODO, i tej dyrektywy.

RPO jest z kolei zaniepokojony informacjami o problemach budżetu PUODO i nieprzygotowaniem stosowania nowych przepisów od maja (RODO ma być stosowane od 25 maja - tego samego dnia przestanie obowiązywać ustawa o ochronie danych z 1997 r.). Należy to rozstrzygnąć jak najszybciej, by możliwe było sprawne wykonywanie nowych obowiązków od początku obowiązywania przepisów ustawy o ochronie danych osobowych oraz ustawy o ochronie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości - wskazuje Stanisław Trociuk.

Szczegółowe uwagi RPO

Według Rzecznika obok przepisów, które zasadniczo oddają treść postanowień dyrektywy, projekt zawiera również rozwiązania mogące wypaczyć ich sens i istotę:

nie przewiduje realizacji dyrektywy, gdyż nie gwarantuje istoty prawa dostępu - czyli informacji o tym, jakie dane osobowe są przetwarzanie i wszelkich dostępnych informacji o ich pochodzeniu;

wprowadza możliwość żądania usunięcia danych osobowych z jawnych ich zbiorów. Tymczasem dyrektywa nie przewiduje takiego ograniczenia tylko do zbiorów jawnych;

zapis projektu, że decyzje PUODO nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych, wykracza poza zakres dyrektywy. Dany podmiot ma być wprawdzie zobowiązany do przywrócenia zgodnego z prawem sposobu przetwarzania danych, jednak mogą one już być zebrane wcześniej wbrew przepisom prawa;

szczególnie niezgodny z dyrektywą jest zapis, który uzależnia przekazanie informacji osobie, której dane dotyczą, od niezbędności do ochrony jej żywotnych interesów lub innej osoby. Takiego wymogu dyrektywa nie przewiduje;

Rzecznik ma wątpliwości, czy projekt realizuje zapisane w dyrektywie prawo jednostki do wniesienia skargi do organu nadzorczego, gdy uznaje ona, iż przetwarzanie jej danych narusza przepisy. Żaden zapis projektu nie wskazuje bowiem wprost na możliwość wniesienia skargi. Mowa jest w nim, że PUODO działa z urzędu lub na wniosek osoby zainteresowanej;

projekt wymienia tylko zażalenie, które nie prowadzi do wszczęcia postępowania, a zwłaszcza nie kończy się decyzją PUODO i ewentualną skargą na nią do sądu administracyjnego (co przewiduje projekt). Można argumentować, że prawo do skargi wynika z zasad Kodeksu postępowania administracyjnego, jednak dla pewności prawnej zapis o przysługującej skardze powinien znaleźć się w ustawie - podkreśla RPO;

zabrakło też możliwości wniesienia sprawy do sądu, niezależnie od postępowania administracyjnego i sądowoadministracyjnego - co dyrektywa gwarantuje;

weryfikacji zebranych danych osobowych służby mają dokonywać nie rzadziej niż co 10 lat (dziś jest to 5 lat). W projekcie brak wyjaśnienia, dlaczego 10 lat ma być okresem właściwym.

Konkluzje RPO

Z punktu widzenia ochrony praw jednostki przedstawiony projekt nie może zostać oceniony całkowicie pozytywnie - podsumowuje Stanisław Trociuk. Przyznał, że sama dyrektywa nie jest doskonała, ale Trybunał Sprawiedliwości UE w przyszłości będzie miał okazję do wypowiedzi na jej temat.

Dyrektywa jest aktem ogólnym, pozostawiającym wiele miejsca na uznanie krajowego ustawodawcy. Jego decyzje muszą jednak uwzględniać standardy Karty Praw Podstawowych UE oraz zapewniać spójność systemu tworzonego w ramach całej UE.

Szczególnej rozwagi wymagają uwagi RPO do projektu ustawy dotyczące systemu środków ochrony prawnej, czy też praw osoby, której dane dotyczą - napisał Trociuk. „Wprowadzanie ograniczeń albo blankietowych wyłączeń od reguł ogólnych, wyłączanie określonych służb z reżimu przepisów o ochronie danych osobowych, czy też rozszerzanie uprawnień innych służb stoi w sprzeczności z podstawowym celem dyrektywy, jakim jest ochrona praw podstawowych i wolności osób fizycznych" - brzmi konkluzja pisma.

Uwagi RPO do projektu Trociuk poddał ministrowi Brudzińskiemu pod rozwagę, prosząc o poinformowanie o sposobie ich wykorzystania w pracach legislacyjnych.

VII.501.315.2014

SĄD NAJWYŻSZY: KASACJA RPO ZASADNA - INTERNET JEST „MIEJSCEM PUBLICZNYM"

data: 2018-04-17

- **Internet jest miejscem publicznym w rozumieniu prawa - potwierdził Sąd Najwyższy**
- **Uwzględniając kasację Rzecznika Praw Obywatelskich, SN nakazał ponowne zbadanie sprawy Mateusza S.**
- **Lidera stowarzyszenia Duma i Nowoczesność obwiniono o umieszczenie w miejscu publicznym (czyli w internecie) nieprzyzwoitych napisów i rysunków**

W 2017 r. sąd umorzył sprawę Mateusza S. za opublikowanie w sieci naklejek z tzw. „zakazem pedałowania". Uznał bowiem, że internet nie jest „miejscem publicznym". Skutecznie zakwestionował to RPO.

Za co odpowiadał Mateusz S.

Opublikowane obrazki były stylizowane na drogowe znaki zakazu. Przedstawiały m.in. dwa ludziki w pozycji sugerującej seks analny, z tekstem m.in. „Zakaz pedałowania, homoseksualiści wszystkich krajów, leczcie się".

Policja postawiła Mateuszowi S. zarzut z art. 141 Kodeksu wykroczeń. Za umieszczenie nieprzyzwoitych rysunków i napisów w miejscu publicznym przewiduje on karę ograniczenia wolności, do 1,5 tys. zł grzywny albo karę nagany.

W 2017 r. Sąd Rejonowy w Wodzisławiu Śląskim umorzył sprawę. Przyznał, że rysunki przez część odbiorców mogą zostać uznane za nieprzyzwoite. Stwierdził jednak, że umieszczenie ich w sieci nie wypełnia znamion wykroczenia, gdyż internet nie jest miejscem publicznym w myśl art. 141 Kw. Według sądu wszystkie treści dostępne w sieci stanowią jedynie „zapis danych w komputerach".

RPO złożył kasację

W kasacji na niekorzyść Mateusza S. Adam Bodnar dowodził, że sąd błędnie przyjął, iż internet nie jest miejscem publicznym - w efekcie niezasadne umorzył postępowanie.

W kasacji Rzecznik podkreślał, że działanie w miejscu publicznym musi być podjęte w przestrzeni dostępnej dla ogółu, do której nieograniczony dostęp ma nieokreślona liczba ludzi. Skoro zatem osoba przekazuje w sieci treści do nieokreślonego kręgu podmiotów, to strona internetowa jest miejscem publicznym w rozumieniu art. 141 Kw. „Wbrew przekonaniu wyrażonemu przez sąd rejonowy, internet nie jest jedynie zapisem danych w komputerach, lecz stanowi on ogólnoświatową sieć, system" - napisał Adam Bodnar.

RPO wniósł by SN uchylił umorzenie i zwrócił sprawę Mateusza S. sądowi w Wodzisławiu Śląskim.

SN podzielił stanowisko Rzecznika

SN podzielił stanowisko RPO, że w rozumieniu art. 141 Kw internet jest miejscem publicznym. Wskazał, że zaskarżone postanowienie Sądu Rejonowego nie było uzasadnione w sposób rzetelny. Argumenty, na które powoływał się sąd, umarzając postępowanie, SN uznał za anachroniczne.

Według SN treści publikowane w internecie, choć fizycznie rzeczywiście znajdują się na dyskach twardych, to jednak tworzą „pewną przestrzeń". Jeśli są zaś dostępne na stronie internetowej, na którą każdy bez ograniczeń może wejść, to tym samym jest to miejsce publiczne.

Zarazem SN zwrócił uwagę, że nie każda strona internetowa może być traktowana jako przestrzeń publiczna. „Dostęp do

niektórych treści wymaga np. zalogowania się i w takich sytuacjach pojawić się może wątpliwość czy mówimy o przestrzeni publicznej" - wyjaśniał sędzia sprawozdawca.

SN uchylił postanowienie o umorzeniu sprawy i zwrócił ją sądowi rejonowemu do ponownego rozpoznania.

Duma i Nowoczesność stała się znana, gdy w lesie pod Wodzisławem w 2017 r. jej członkowie świętowali rocznicę urodzin Adolfa Hitlera, co sfilmowała ukryta kamera TVN24. Zarzuty propagowania nazistowskiego ustroju usłyszało w tej sprawie siedem osób, w tym Mateusz S. W oddzielnym trybie sąd zbada wniosek starosty wodzisławskiego o rozwiązanie stowarzyszenia.

Komentarz Marka Łukaszuka, dyrektora zespołu prawa karnego w Biurze RPO:

Następstwem wykładni językowej terminu internet musi być uznanie, że strona internetowa jest miejscem publicznym w rozumieniu art. 141 Kw. W orzecznictwie SN wyraźnie wskazuje się, że miejsce publiczne jest miejscem dostępnym dla nieokreślonej liczby osób i że może być nim także internet.

RPO w pełni identyfikuje się też z poglądem Trybunału Konstytucyjnego, który we wrześniu 2015 r. stwierdził, że za miejsce publiczne w myśl Kodeksu wykroczeń należy uznać także internet.

Dzisiejszy wyrok wspiera dotychczasowe orzecznictwo. Ma też swoisty walor edukacyjny. Tym rozstrzygnięciem sąd wypełnia swoją rolę, określoną w ustawie o SN, a dotyczącą kształtowania orzeczeń sądów powszechnych, nie tylko w tej konkretnej sprawie.

BPK.511.37.2017

SUGESTIE ADAMA BODNARA DLA MIĘDZYRESORTOWEGO ZESPOŁU DS. PRZECIWDZIAŁANIA PROPAGOWANIA FASZYZMU I MOWIE NIENAWIŚCI

data: 2018-04-12

- **Komercyjni dostawcy internetu powinni być zobowiązani do informowania organów ścigania o przestępstwach mowy nienawiści - proponuje Rzecznik Praw Obywatelskich**
- **Należałoby też przyjąć definicję mowę nienawiści, wykraczającą poza dziś ścigane przestępstwa motywowane nienawiścią z powodu przynależności narodowej, etnicznej, rasowej, wyznaniowej lub bezwyznaniowości**
- **Powinien także powstać niezależny organ, który we współpracy z branżą internetową i organizacjami pozarządowymi opracowałby kodeks dobrych praktyk**

Adam Bodnar przedstawił szefowi MSWiA Joachimowi Brudzińskiemu dziewięć sugestii dla międzyresortowego zespołu ds. przeciwdziałania propagowaniu faszyzmu i innych ustrojów totalitarnych oraz przestępstwom nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość.

Rzecznik z satysfakcją przyjął powołanie tego zespołu przez premiera - na wniosek szefa MSWiA. Zadeklarował wszelkie możliwe wsparcie jego prac.

Zespołowi zlecono zidentyfikowanie problemów w ściganiu przestępstw motywowanych nienawiścią oraz opracowanie założeń ewentualnych zmian w celu wyeliminowanie tych zjawisk. Problematyka zwalczania tego rodzaju przestępczości pozostaje w kręgu moich zainteresowań - podkreślił Adam Bodnar.

Niemal połowa przestępstw z nienawiści – w internecie

RPO przekazał ministrowi uwagi dotyczące przygotowania odpowiednich narzędzi w celu ograniczeniu zjawiska mowy nienawiści w internecie. Jak podkreślił, chodzi o wypowiedzi propagujące ideologie rasistowskie, faszyzm lub inne ideologie totalitarne oraz nawołujące do nienawiści lub znieważających poszczególne osoby lub grupy osób ze względu na określone cechy, jak narodowość, przynależność etniczna, wyznanie lub bezwyznaniowość, ale także wiek, niepełnosprawność, orientacja seksualna czy tożsamość płciowa.

Ze statystyk Prokuratury Krajowej wynika, że w 2016 r., z 1631 śledztw o przestępstwa z nienawiści, 701 tj. ponad 40 proc., dotyczyło czynów popełnionych w internecie. Tendencja ta utrzymywała się w pierwszej połowie 2017 r.

W sugestiach działań dla zespołu Adam Bodnar powołał się na dorobek Unii Europejskiej, a także ciał traktatowych ONZ oraz Rady Europy.

Propozycje RPO dla zespołu

wyznaczenie niezależnego organu doradczego lub punktu kontaktowego, który we współpracy z branżą internetową i organizacjami pozarządowymi opracowałby kodeks dobrych praktyk. Czuwałby też nad egzekwowaniem obowiązków

dostawców usług internetowych w przeciwdziałaniu mowie nienawiści;

zapewnienie takiemu niezależnemu organowi uprawnień do rozpatrywania skarg na działalność administratorów stron internetowych, prowadzenia postępowań wyjaśniających oraz wymierzania proporcjonalnych sankcji administracyjnych w razie stwierdzenia uchybień.

doprecyzowanie zasad współpracy dostawców usług internetowych z organami ścigania, w tym - uregulowanie zakresu gromadzonych danych oraz terminu ich udostępnienia organom ścigania;

nałożenie na komercyjnych dostawców usług internetowych obowiązku informowania organów ścigania o przestępstwach związanych z mową nienawiści oraz o działalności organizacji, o których mowa w art. 13 Konstytucji RP (odwołujących się do totalitarnych metod i praktyk nazizmu, faszyzmu i komunizmu, dopuszczających nienawiść rasową i narodowościową);

nałożenie na dostawców usług internetowych obowiązku wprowadzenia formularza umożliwiającego zgłaszanie on-line przypadków mowy nienawiści

doprecyzowanie obowiązku dostawców usług do usunięcia mowy nienawiści lub uniemożliwienia dostępu do nich w określonym terminie od otrzymania wiarygodnej wiadomości (według wytycznych KE wpisy powinny być usuwane w ciągu doby od zgłoszenia); zgłaszający powinien móc się odwołać od odmowy usunięcia wpisu do sądu lub organu administracyjnego;

nałożenie na największych, komercyjnych dostawców usług internetowych obowiązku monitorowania przechowywanych danych w kierunku identyfikacji i usuwania mowy nienawiści;

opracowanie i prowadzenie publicznie dostępnej listy zaufanych podmiotów zgłaszających;

wprowadzenie ustawowego zakazu stosowania mowy nienawiści w internecie, kwalifikowanej na podstawie definicji przyjętej przez Komitet Ministrów Rady Europy.

Komentarze gorsze niż artykuły

RPO przypomniał wyrok Europejskiego Trybunału Praw Człowieka z 16 czerwca 2015 r. w sprawie Delfi przeciwko Estonii. Sprawa dotyczyła odpowiedzialności dostawcy internetu za komentarze pod artykułami. Sam artykuł mieścił się w granicach dopuszczalnej krytyki. To komentarze do tego artykułu stanowiły mowę nienawiści lub nawoływanie do przemocy. Dostawca kwestionował wyroki estońskich sądów, które zobowiązały go do zadośćuczynienia za naruszenie dóbr osobistych, mimo że obraźliwe komentarze zostały usunięte przez administratora w dniu, w którym pokrzywdzony o to się zwrócił (po 6 tygodniach od zamieszczenia komentarzy).

ETPCz nie stwierdził naruszenia art. 10 Europejskiej Konwencji Praw Człowieka. Uznał, że komercyjny charakter działalności portalu obligował administratora do szczególnej staranności przy publikowaniu nienawistnych komentarzy, a środki, które miały przeciwdziałać zamieszczaniu bezprawnych treści, były niewystarczające. Według ETPCz część wpisów można było zakwalifikować jako mowę nienawiści lub nawoływanie do przemocy, czyli jako wypowiedzi, które stanowią najbardziej skrajne nadużycie wolności słowa i nie są objęte ochroną art. 10 EKPC.

Był to kolejny argument za tym, że administratorzy komercyjnych portali informacyjnych, które umożliwiają użytkownikom komentowanie materiałów dziennikarskich, muszą liczyć się z szerokim zakresem obowiązków w stosunku do wpisów stanowiących mowę nienawiści. Jak podkreślił ETPCz, obowiązki te nie obejmują co prawda konieczności stosowania tzw. premoderacji, ale w praktyce, aby sprostać wymogom, administratorzy powinni usuwać bezprawne wpisy z własnej inicjatywy.

Przepisy zbyt łagodne dla mowy nienawiści w sieci

RPO podkreśla, że przeciwdziałanie mowie nienawiści w sieci wymaga szczególnych mechanizmów kontrolnych ze strony dostawców internetu. Obecny art. 15 ustawy o świadczeniu usług drogą elektroniczną w sposób zbyt szeroki zwalnia administratorów komercyjnych serwisów z obowiązków postmoderacji w zakresie mowy nienawiści.

Rzecznik przywołał uzasadnienie wyroku Sądu Najwyższego z 30 września 2016 r (I CSK 598/15). SN uznał, że na art. 15 ustawy nie może powołać się administrator portalu internetowego, który liczy się z możliwością bezprawnych wpisów, a nie podejmuje działań, mimo zatrudniania pracowników usuwających wpisy naruszające interesy ekonomiczne administratora. Ponadto istniejący system automatycznej filtracji używanego przez internautów słownictwa nie jest skuteczny.

Dostawcy powinni zawiadamiać organy ścigania

Zdaniem Rzecznika, z uwagi na fakt, że mowa nienawiści stanowi szczególny przejaw bezprawnego działania, w odniesieniu do treści uzasadniających podejrzenie przestępstwa zasadne byłoby wprowadzenie obowiązku zawiadamiania przez dostawców internetu organów ścigania - i to pod groźbą proporcjonalnej sankcji administracyjnej.

W stosunku do dostawców usług internetowych RPO uznaje za niewystarczający art. 304 ust. 1 Kodeksu postępowania karnego, który nakłada na każdego społeczny obowiązek zawiadomienia o podejrzeniu przestępstwa. Skoro przyjąć, że administratorzy komercyjnych serwisów są zobowiązani do postmoderacji zamieszczanych treści w kierunku wykrywania mowy nienawiści, to usunięcie bezprawnej treści bez zawiadomienia organów ścigania, prowadzić będzie do zniszczenia jedynych dowodów przestępstwa.

W celu uniknięcia takich sytuacji zasadne jest nałożenie na administratorów obowiązku zawiadomienia o popełnieniu przestępstwa, a także obowiązku należytego zabezpieczenia materiału dowodowego. Byłoby to skuteczną odpowiedzią na wyzwanie, jakim jest zwalczanie mowy nienawiści w internecie. Wpisywałoby się też w liczne rekomendacje organizacji międzynarodowych. Istotne jest przy tym doprecyzowanie zasad współpracy dostawców z organami ścigania.

Poszerzyć zakres pojęcia mowa nienawiści

Rekomendacje międzynarodowych organów ochrony praw człowieka odnoszą się do pojęcia mowy nienawiści, które jest różnie definiowane. Zasadne byłoby wprowadzenie ustawowej definicji mowy nienawiści. Zdaniem Rzecznika warto rozważyć, czy jej zakres nie powinien wykraczać poza katalog przestępstw motywowanych nienawiścią, określonych w art. 119 ust. 1, art. 256 ust. 1 i art. 257 Kodeksu karnego (z powodu przynależności narodowej, etnicznej, rasowej, politycznej, wyznaniowej lub z powodu bezwyznaniowości).

Dzięki temu użytkownik zamieszczający w sieci treści mieszczące się w definicji mowy nienawiści - ale nie będące przestępstwem motywowanym nienawiścią - poprzez odpowiednią reakcję dostawcy internetu zostanie niejako ostrzeżony, zanim zacznie sięgać po sformułowania będące przestępstwem.

RPO podkreślił, że najszerzej stosowaną definicją mowy nienawiści jest ta zawarta w rekomendacji nr R 97 (20) Komitetu Ministrów Rady Europy w kwestii wypowiedzi szerzących nienawiść. Zgodnie z nią, za mowę nienawiści powinna zostać uznana każda forma wypowiedzi, która rozpowszechnia, podżega, propaguje lub usprawiedliwia nienawiść rasową, ksenofobię, antysemityzm lub inne formy nienawiści oparte na nietolerancji, włączając w to nietolerancję wyrażaną w formie agresywnego nacjonalizmu lub etnocentryzmu, dyskryminacji lub wrogości wobec mniejszości, migrantów lub osób wywodzących się ze społeczności imigrantów.

Adam Bodnar wskazał, że w praktyce definicja ta jest obecnie stosowana przez Ministerstwo Sprawiedliwości i MSWiA. Nie bez znaczenia jest przy tym fakt, że definicja ta, jako wypracowana na forum Rady Europy, zapewnia największą kompatybilność z orzecznictwem ETPCz.

XI.518.50.2017

RPO ALARMUJE: CORAZ MNIEJ CZASU NA PRZYJĘCIE UNIJNEJ DYREKTYWY POLICYJNEJ

data: 2018-04-11

- **Rzecznik Praw Obywatelskich jest zaniepokojony brakiem prac nad wprowadzeniem do polskiego prawa unijnej dyrektywy policyjnej, która dotyczy przetwarzania danych osobowych przez organy ścigania**
- **Przepisy niezbędne do wykonania dyrektywy mają być stosowane przez państwa członkowskie od 6 maja - Polska może nie dotrzymać tego terminu, co według RPO grozi m.in.ogromną niepewnością prawną**
- **Adam Bodnar ma też wątpliwości, czy planowane przez rząd wyłączenie działań ABW i CBA spod tej dyrektywy nie będzie z nią sprzeczne**

Rzecznik wystąpił do szefa MSWiA Joachima Brudzińskiego o pilną informację na temat stanu prac nad ustawą wdrażającą dyrektywę 2016/680 z 27 kwietnia 2016 r. Pismo związane z tą sprawą oraz z projektem nowej ustawy o ochronie danych RPO wysłał też marszałkowi Sejmu Markowi Kuchcińskiemu.

Czym jest dyrektywa policyjna

Od 2017 r. Adam Bodnar wskazywał, że dyrektywa 2016/680 jest bardzo ważna z punktu widzenia obywatela i występował w tej sprawie do kilku resortów. Z jednej strony ułatwia ona wymianę danych między państwami członkowskimi, a z drugiej – wzmacnia prawa osób, których te dane dotyczą. Przyznaje też jednostce uprawnienie złożenia skargi oraz uzyskania informacji, czy jej dane są przetwarzane.

Dyrektywa przewiduje też przyjęcie sankcji za naruszenie przepisów przyjętych na jej podstawie. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

Dyrektywa jest aktem dość ogólnym, pozostawiającym wiele miejsca na uznanie krajowego ustawodawcy. Wszelkie decyzje muszą jednak uwzględniać standardy Karty Praw Podstawowych UE oraz zapewniać spójność systemu tworzonego w ramach całej UE.

Polska może nie zdążyć wprowadzić dyrektywy

27 marca 2018 r. Rada Ministrów przyjęła projekt ustawy o ochronie danych osobowych. Ma być on szybko uchwalony tak, by mogła ona wejść w życie 25 maja. Ustawę będzie się stosować do ochrony osób w związku z przetwarzaniem danych osobowych w zakresie określonym przez unijne rozporządzenie RODO. Ma być ono stosowane w Polsce od 25 maja 2018 r.

Jak napisał Adam Bodnar, tego samego dnia przestanie obowiązywać ustawa o ochronie danych z 1997 r., która wyznaczała dotychczas ramy przetwarzania danych osobowych w Polsce. Tymczasem do dziś nie przedstawiono projektu, który implementowałby dyrektywę 2016/680 do polskiego prawa. Projekt taki ostatnio wpisano do wykazu prac legislacyjnych Rady Ministrów, co może oznaczać, że wkrótce zostanie przedstawiony.

Według RPO obecnie nie tylko jest prawdopodobne, że do 6 maja właściwe przepisy nie zostaną przyjęte, ale również, że od 25 maja w ogóle nie będzie żadnych przepisów regulujących kwestie związane z dyrektywą. Do 25 maja zaplanowano bowiem w chwili obecnej jedynie dwa posiedzenia Sejmu.

Adam Bodnar ma obawy, że niedotrzymanie terminu nie tylko naruszyłoby polskie zobowiązania wynikające z członkostwa w UE i obowiązku przestrzegania wiążącego prawa międzynarodowego. Może to również mieć poważne skutki dla obywateli, związane ze standardem ochrony danych osobowych w obszarze dyrektywy.

Ponadto zastrzeżenia RPO budzi opis zakresu implementacji z dokumentu rządu. Np. całkowite wyłączenie spod dyrektywy służb specjalnych (w tym ABW i CBA) może być z nią sprzeczne. Nie wszystkie bowiem działania np. ABW mieszczą się w pojęciu „bezpieczeństwa narodowego" i nie wszystkie będą automatycznie mogły być pozostawione poza zakresem dyrektywy.

Zdaniem Rzecznika kwestie te powinny były być odpowiednio skonsultowane. Wydaje się, że ponownie wykorzystano model prac, w którym pomija się możliwość jakiejkolwiek dyskusji lub też pozostawia się zainteresowanym podmiotom bardzo krótki czas na zgłoszenie uwag, które nie będą przedmiotem pogłębionej analizy.

Zastrzeżenia RPO do projektu nowej ustawy o ochronie danych

W wystąpieniu do Marszałka Sejmu RPO z satysfakcją odnotował te zapisy projektu nowej ustawy o ochronie danych, które prowadzą do zapewnienia niezależności Prezesa Urzędu Ochrony Danych Osobowych (PUODO).

Do projektu wprowadzono jednak również zmiany, które mogą obniżyć standard prawa do ochrony danych osobowych w porównaniu do gwarantowanego przez RODO, ale głównie przez Konstytucję. RPO szczególnie zwraca uwagę na daleko idące wyłączenia i ograniczenia praw osób, których dane dotyczą - w przypadku przetwarzania ich przez administratorów realizujących zadania publiczne. Taki administrator nie będzie w wymienionych przypadkach informował osoby, której dane dotyczą, o zmianie celu przetwarzania oraz przysługujących jej prawach.

Ani projekt ustawy ani jego uzasadnienie nie zawierają analizy zasadności przyjmowania proponowanych ograniczeń. Tym samym nie jest jasne, czy cel i zakres wprowadzonych ograniczeń będą mogły być uznane za „niezbędne w demokratycznym państwie prawnym" i czy takie ograniczenie prawa do prywatności będzie mogło być uznane za zgodne z art. 47 i art. 51 w zw. z art. 31 ust. 3 Konstytucji.

VII.501.315.2014

ADAM BODNAR: SPRAWA CAMBRIDGE ANALYTICA ZAGRAŻA PROCESOM DEMOKRATYCZNYM I OCHRONIE PRAW OBYWATELSKICH

data: 2018-04-04

- **Sprawa typu Cambridge Analytica rodzi zagrożenie nie tylko dla prawa do prywatności użytkownika internetu, ale również dla szeroko pojętych procesów demokratycznych i ochrony praw obywatelskich - przestrzega Rzecznik Praw Obywatelskich**

- **Dlatego Adam Bodnar spytał Generalną Inspektor Ochrony Danych Osobowych, czy prowadzi postępowanie w tej sprawie oraz czy polskie prawo wystarczająco odpowiada na takie zagrożenia**

- **RPO ocenia, że na prawidłową realizację praw użytkowników serwisów społecznościowych typu Facebook może wpłynąć wchodzące w maju w życie unijne rozporządzenie ogólne o ochronie danych (RODO)**

Adam Bondar napisał do szefowej GIODO Edyty Bielak-Jomaa, mając na względzie zagrożenia dla ochrony danych osobowych, wynikające z działań firm typu Cambridge Analytica.

Chodzi o wykorzystanie danych 50 milionów użytkowników Facebooka w taki sposób, aby wpłynąć na wyniki wyborów prezydenckich w USA. Jak donosiły media, firma Cambridge Analytica tworzyła psychologiczne profile użytkowników, by móc kierować do nich przekazy o określonej, dopasowanej treści, które mogły oddziaływać na ich wybory, w tym polityczne. Na takie działania miał zgadzać się Facebook. Ta sama firma mogła też wpłynąć na wyniki referendum w sprawie Brexitu.

Zagrożenia wynikające z tzw. mikrotargetowania

Jak podkreślił RPO, cała sprawa uwypukla o wiele szersze zagadnienie, związane z udostępnianiem danych osobowych oraz wykorzystywaniem ich - bez świadomości albo za zgodą wyrażoną przez użytkownika poprzez zaakceptowanie skomplikowanego regulaminu - do wpływania na wybory i decyzje użytkownika. To rodzi zagrożenie nie tylko dla prawa do prywatności użytkownika sieci internetowej, ale również dla szeroko pojętych procesów demokratycznych i ochrony praw obywatelskich w kraju.

Adam Bodnar przypomniał, że w sprawie Cambridge Analytica działania podjął brytyjski Komisarz ds. Informacji, który wszczął postępowanie w sprawie wykorzystania danych osobowych. Sprawdza on m.in. okoliczności, w jakich dane pozyskane z Facebooka mogły zostać wykorzystane w szczególności do tzw. mikrotargetowania wyborców.

To technika znana w kampaniach wyborczych na świecie i wykorzystywana przez partie polityczne. Polega na przeszukiwaniu rynku, by wyłowić potencjalnych wyborców i do nich konkretnie kierować swój przekaz. Dzięki temu partia identyfikuje osoby, które jest w stanie z ogromnym prawdopodobieństwem przekonać do swoich poglądów. Możliwe jest bowiem powiązanie treści

przekazywanego komunikatu ze szczególnymi zainteresowaniami potencjalnego wyborcy. Z jednej strony mikrotargetowanie może stanowić korzyść dla osoby, polegającą na pozyskaniu informacji, ale z drugiej strony - zagrożenie dla jej prywatności oraz ogólnie zagrożenie dla mechanizmów demokratycznych w państwie prawa.

RPO powołał się na badaczy tematu, według których uświadomienie sobie takiej techniki może prowadzić do efektu mrożącego. Ludzie przypuszczający, że ich zachowanie jest monitorowane, mogą dostosowywać swoje zachowanie tak, by uniknąć zainteresowania. Wiąże się to też z brakiem komfortu użytkowników sieci, co może prowadzić do ograniczenia aktywności, by uniknąć możliwości zbierania informacji o sobie.

Przy tej technice wysoce prawdopodobne jest naruszanie zasad ochrony danych osobowych. Nie zawsze bowiem wszystkie informacje przekazywane przez portale muszą być oparte na zgodzie użytkownika. Ponadto nawet jeśli zgoda była, to dane mogą być wykorzystywane w celu innym niż ten, do którego zostały zebrane.

Według RPO dzięki adresowaniu konkretnego przekazu do konkretnego odbiorcy można maksymalnie zwiększyć lub też maksymalnie zmniejszyć zaangażowanie wyborcze. Partie polityczne mogą wykorzystywać te techniki do wpływania na poparcie, ale także na powstrzymanie się wyborców od głosowania na przeciwników politycznych. Wykorzystywanie techniki polegającej na tym, że informacje określonej treści pojawiają się wyłącznie u docelowej grupy odbiorców, a nie u wszystkich korzystających z danej platformy, może spowodować przekształcenie potencjalnych wyborców w obiekty manipulacji. Może też doprowadzić do zmniejszenia sfery debaty politycznej, przy jednoczesnym zwiększeniu polaryzacji politycznej. Ponadto jest to również powiązane z łatwym rozpowszechnianiem się tzw. fake news. W ten sposób część potencjalnych wyborców może w ogóle zostać wykluczona z procesu wyborczego.

Jak można zaradzić zagrożeniom

Wpływ na lepszą ochronę w Europie może mieć treść przepisów prawa UE, w tym mające wkrótce być stosowane rozporządzenie ogólne o ochronie danych osobowych (RODO), ale także mające być wkrótce przyjęte rozporządzenie w sprawie e-prywatności. „Przepisy te mogą wpłynąć na prawidłową realizację praw osób, w szczególności w odniesieniu do zakresu informacji gromadzonych na nasz temat przez firmy typu Facebook, ale także poprzez możliwość wglądu w swój pełny profil w celu skorygowania lub usunięcia danych" – uznał Adam Bodnar. Jak wynika z oświadczenia Marka Zuckerberga, Facebook zmienił już politykę - obecnie transfer danych bez zgody użytkowników naruszałby regulamin serwisu.

Zdaniem RPO po wejściu w życie w RODO w maju sytuacja powinna zmienić się tak, że jasno określone zostaną te reguły, które dotyczą prawa właściwego do oceny działań rozmaitych aplikacji. Przekazywanie naszych danych osobowych innym firmom w celach marketingowych, w tym brokerom danych, którzy agregują dane z różnych źródeł i tworzą własne profile, będzie wymagało świadomej, poinformowanej zgody. Jednak można spodziewać się, że wiele firm nadal będzie dokonywało takiej interpretacji przepisów, która będzie sprzyjała kontynuowaniu prowadzenia przez nie działalności w dotychczasowym kształcie.

Techniki takie mogą być wykorzystywana również przez inne firmy i na inne sposoby. Jeżeli potwierdziłyby się obawy wskazujące na istotne zagrożenia dla prawa do prywatności i podstawowych reguł demokracji, konieczne byłoby podjęcie szerszej dyskusji w kierunku wypracowania stosownego rozwiązania. Musiałoby one spełniać wymogi wynikające z ogólnych standardów ochrony praw człowieka, np. art. 10 Konwencji o ochronie praw człowieka i podstawowych wolności.

Do tego jednak potrzebne są dokładniejsze badania i analiza sytuacji. Nie jest to łatwe w sytuacji, w której partie polityczne nie są skłonne do ujawniania informacji, np. o wydatkach na marketing polityczny i kreowanie wizerunku. To tylko potwierdza, że konieczne jest znalezienie rozwiązań, które doprowadziłyby do znalezienia sposobu na kontrolę politycznego mikrotargetowania - podkreślił Adam Bodnar.

Dlatego spytał on GIODO, czy prowadzi analizy tego typu przypadków i czy w ocenie szefowej urzędu ustawodawstwo polskie odpowiada na sygnalizowane zagrożenia dla ochrony danych osobowych. Prosił także o informację, czy w tej konkretnej sprawie – tak, jak w Wielkiej Brytanii – zostanie podjęte postępowanie GIODO. Zwrócił się także o ocenę, czy przepisy RODO oraz przyszłego rozporządzenia o e-prywatności będą w stanie zapobiec takim zagrożeniom.

VII.520.14.2018

RPO PISZE DO PREMIERA WS. ŁAGODNIEJSZEJ SANKCJI ZA NIEŚWIADOME NARUSZENIE PRAW AUTORSKICH

data: 2018-03-15

- **Nieświadome naruszenie autorskich praw majątkowych nie powinno rodzić takiej samej odpowiedzialności jak działanie umyślne, podjęte np. w celach zarobkowych – uważa Rzecznik Praw Obywatelskich**
- **Adam Bodnar podkreśla, że w epoce cyfrowego dostępu do dóbr kultury trudno jest uzyskać wiarygodną informację o legalności ich udostępniania**
- **RPO napisał w tej sprawie do premiera Mateusza Morawieckiego, ponieważ dwukrotnie na jego wcześniejsze wystąpienia nie odpowiedział Minister Kultury i Dziedzictwa Narodowego**

Obecnie Prawo autorskie przyznaje osobom, których autorskie prawa majątkowe zostały naruszone, roszczenie o zapłatę kwoty pieniężnej odpowiadającej dwukrotności stosownego wynagrodzenia za zgodę na korzystanie z utworu. Wysokość roszczenia jest niezależna od winy użytkownika praw autorskich. „Skutkiem tego, takie same sankcje grożą osobie, która umyślnie narusza autorskie prawa majątkowe np. w celach zarobkowych, jak i osobie, która takie prawa narusza w sposób nieświadomy" – głosi pismo Adama Bodnara do premiera .

Według RPO rozwiązanie takie narusza zasady sprawiedliwości społecznej. Jest też o tyle niesprawiedliwe, że powszechna i masowa eksploatacja dóbr kultury w środowisku cyfrowym znacznie utrudnia użytkownikom uzyskanie wiarygodnej informacji o legalności ich udostępniania. Transgraniczny charakter udostępniania i nowe jego formy (jak np. licencje Creative Commons, aplikacje społecznościowe czy streamingowe) powodują, iż wielu użytkowników nie jest w stanie ocenić, czy eksploatacja danego dobra kultury odbywa się na podstawie zezwolenia uprawnionych podmiotów.

Dlatego RPO uznał, że dopuszczalność roszczeń o zapłatę dwukrotności wynagrodzenia – nawet w przypadku nieumyślnego naruszenia – wydaje się nieuprawnioną ingerencją w sferę wolności majątkowej użytkowników utworów chronionych Prawem autorskim.

Adam Bodnar przypomniał, że w czerwcu 2015 r. Trybunał Konstytucyjny orzekł (sygn. SK 32/14) niezgodność z normami konstytucyjnymi roszczenia o zapłatę trzykrotności wynagrodzenia - w przypadku zawinionego naruszenia autorskich praw majątkowych. Orzeczenie to trzeba odnieść właśnie do niezawinionego naruszenia, które dziś może być – na równi z zawinionym – podstawą roszczenia o zapłatę dwukrotności wynagrodzenia.

Na konieczność podjęcia działań legislacyjnych w celu zmiany przepisów RPO zwracał uwagę już w wystąpieniu z 1 sierpnia 2016 r. do prof. Piotra Glińskiego, ministra kultury i dziedzictwa narodowego. „Niestety, pomimo wagi zasygnalizowanego problemu, istotnego z punktu widzenia zgodności norm Prawa autorskiego ze standardami konstytucyjnymi, na powyższe wystąpienie nie otrzymałem żadnej odpowiedzi, chociaż zwracałem się o to ponownie do Ministra Kultury i Dziedzictwa Narodowego pismem z 27 listopada 2017 r." – napisał Adam Bodnar.

W tej sytuacji poprosił on Prezesa Rady Ministrów o spowodowanie udzielenia odpowiedzi zawierającej niezbędne wyjaśnienia dotyczące tego doniosłego społecznie problemu.

IV.715.1.2016

RPO WYCOFUJE WNIOSEK DO TRYBUNAŁU KONSTYTUCYJNEGO W SPRAWIE INWIGILACJI

data: 2018-03-14

- **Rzecznik praw obywatelskich Adam Bodnar wycofał z Trybunału Konstytucyjnego wniosek, w którym kwestionował znowelizowane w 2016 r. przez PiS zasady prowadzenia inwigilacji przez służby specjalne.**
- **Według RPO przepisy te naruszają kluczowe prawa i wolności obywatelskie, gwarantowane przez Konstytucję RP i prawo europejskie.**
- **Adam Bodnar nie widzi jednak szansy na niezależne i merytoryczne rozpoznanie tej sprawy przez Trybunał.**
- **Szczególne obawy RPO budzi w tych przepisach możliwość nieograniczonego zbierania przez służby, bez żadnej realnej kontroli, danych o aktywności obywateli w internecie oraz bilingów telefonicznych. Zdaniem RPO powinny być one pobierane tylko przy najpoważniejszych przestępstwach i jedynie wtedy, gdy inne metody są nieskuteczne.**

Sprawa dotyczy m.in. tego, jakie dane mogą o nas zbierać służby specjalne i co z tymi danymi mogą zrobić. Dziś RPO nie widzi szansy na niezależne i merytoryczne rozpoznanie swojego wniosku. Mają go bowiem oceniać w Trybunale osoby, których nie tylko status sędziowski ale bezstronność w sprawie uprawnień służb może być kwestionowana. RPO obawia się, że w takiej sytuacji wyrok Trybunału mógłby zamrozić stan prawny, który jest niezgodny ze standardami konstytucyjnymi i europejskimi. Adam Bodnar nie chce przyłożyć do tego ręki.

Wycofanie wniosku z Trybunału nie oznacza, że RPO zaprzestanie działań, aby zasady inwigilacji odpowiadały standardom konstytucji oraz prawa europejskiego. W tym kontekście RPO wyraża nadzieję na bezpośrednie stosowanie konstytucji i europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności przez polskie sądy.

„Przepisy Konstytucji stosuje się bezpośrednio, chyba że Konstytucja stanowi inaczej" - stanowi polska ustawa zasadnicza. Np. w kwietniu 2017 r. Sąd Apelacyjny we Wrocławiu uznał za niedopuszczalną prawnie prowokację CBA z 2007 r. wobec rzekomo skorumpowanych architektów. Wskazał na niezgodność odpowiednich przepisów z Konstytucją i obowiązującymi konwencjami. W marcu 2017 r. Sąd Najwyższy zastosował zaś Konstytucję bezpośrednio w sprawie umieszczenia w ośrodku w Gostyninie mężczyzny, który odbył wyrok za próbę gwałtu.

RPO nie przestanie także domagać się utworzenia niezależnego organu kontrolującego służby specjalne. Rzecznik będzie się też nadal domagał wykonania wniosków wynikających z opinii Komisji Weneckiej. Ponadto będą prowadzone działania edukacyjne pokazujące zagrożenia wynikające z tej ustawy dla obywateli i zasad państwa prawa.

Ustawa „inwigilacyjna" i kto ją ma oceniać

Ustawa „inwigilacyjna" została przyjęta w styczniu 2016 r. Była procedowana jako projekt poselski, a zatem nie była poddawana konsultacjom i uzgodnieniom - tak jak w przypadku projektów rządowych. Formalnie jej celem było wykonanie wyroku TK z 30 lipca 2014 r., który zakwestionował część zapisów ustaw regulujących działalność służb. Zaskarżył je wówczas m.in. RPO, który od lat wskazywał, że przepisy mogą naruszać prawa obywateli. Ustawa z 2016 r. znacząco jednak poszerzyła kompetencje służb specjalnych wobec obywateli.

Dlatego w lutym 2016 r. RPO Adam Bodnar zaskarżył do Trybunału Konstytucyjnego najważniejsze artykuły nowelizacji. Ocenił, że nie tylko nie realizują one wyroku TK z 2014 r., ale „w poważnym zakresie naruszają konstytucyjne prawa i wolności człowieka oraz standardy wyznaczone w prawie międzynarodowym".

Pierwotnie Trybunał miał się zająć sprawą w pełnym składzie (to co najmniej 11 z 15 sędziów TK). W styczniu 2017 r. sędzia Julia Przyłębska zdecydowała, że sprawę zbada skład tylko pięcioosobowy.

Sprawozdawcą ma być Mariusz Muszyński - wybrany pod koniec 2015 r. przez Sejm na stanowisko już obsadzone przez sędziego wybranego w październiku 2015 r., który nie został zaprzysiężony przez prezydenta Andrzeja Dudę. Do składu trafili też Justyn Piskorski i Jarosław Wyrembak, czyli także osoby zajmujące wcześniej obsadzone miejsca w Trybunale (jak stwierdził to Trybunał w wyroku z 9 marca 2016 r.). Weszli oni bowiem do Trybunału w miejsce osób, które zajęły w 2015 r. obsadzone miejsca, a zmarły w ostatnim czasie - Lecha Morawskiego i Henryka Ciocha.

Rzecznik wnosił o wyłączenie ze składu Mariusza Muszyńskiego i Justyna Piskorskiego. Wniosek złożył, zanim Trybunał poinformował go o kolejnej zmianie w składzie orzekającym. Sędzia Sławomira Wronkowska-Jaśkiewicz została decyzją prezes TK zastąpiona przez Jarosława Wyrembaka. Przewodniczącym składu został sędzia Michał Warciński. W składzie był też sędzia Leon Kieres.

W połowie lutego TK odwołał wyznaczony na 21 lutego termin w sprawie. 21 lutego TK nie wyłączył ze składu Mariusza Muszyńskiego i Justyna Piskorskiego. Jak podkreślał RPO, za wyłączeniem Muszyńskiego przemawiały nie tylko wątpliwości co do jego statusu, ale i wobec bezstronności przy ocenie aktów regulujących działalność służb specjalnych - w związku z zarzutami w mediach dotyczących jego powiązań ze służbami. TK uznał ten zarzut za „niepoparty jakimikolwiek dowodami, oparty na niepotwierdzonych doniesieniach prasowych".

Co mogą służby specjalne

RPO co do zasady nie kwestionuje możliwości stosowania różnych form inwigilacji przez służby specjalne. Podkreśla jednak, że wymogi bezpieczeństwa nie oznaczają, iż zasady inwigilacji mają nie podlegać ograniczeniom wynikającym z konstytucyjnych praw i wolności. Powinny być wynikiem kompromisu między bezpieczeństwem obywateli a ich prawem do prywatności. W ocenie RPO nowela przyznaje zaś priorytet pierwszej wartości.

Najważniejsze zarzuty wniosku RPO dotyczyły naruszenia prawa do prywatności i ochrony danych osobowych obywateli.

RPO zakwestionował przepisy o uprawnieniach służb do kontroli operacyjnej. Tak określa się stosowanie przez nie podsłuchów, podglądu, kontroli korespondencji (także elektronicznej) i przesyłek oraz uzyskiwanie treści smsów. Służby mogą prowadzić takie działania tylko za zgodą sądu.

Wniosek dotyczy też zasad pobierania przez służby danych telekomunikacyjnych, internetowych i pocztowych obywateli - na co zgoda sądu nie jest już potrzebna. Dane telekomunikacyjne to: numer telefonu komórkowego, jego lokalizacja, spisy połączeń i numer IP komputera. Dane internetowe m.in. identyfikują internautę i ukazują zakres każdorazowego korzystania przezeń z sieci (adresy odwiedzanych stron, wpisy w wyszukiwarce itp.).

W wyniku zmiany przepisów służby dostały dostęp do danych internetowych za pomocą stałego łącza. Pobieranie danych nie musi się wiązać z żadnym toczącym się postępowaniem. Służby nie muszą już - tak jak przedtem - składać pisemnych wniosków do dostawców usług internetowych i wykazywać, na potrzeby jakiego postępowania dane są im potrzebne.

Oznacza to, że dane te mogą być zbierane nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania najpoważniejszym przestępstwom, którym inaczej nie da się przeciwdziałać (jak wskazują standardy wynikające z Konstytucji i prawa europejskiego), ale także wtedy, gdy jest to dla służb wygodne.

Zdaniem RPO taki dowolny dostęp służb do tych danych oznacza ryzyko poważnych nadużyć. Służby mogą na tej podstawie np. precyzyjnie odtwarzać różne aspekty życia prywatnego obywatela, zbierać dane o trybie życia, poglądach, upodobaniach czy skłonnościach.

W noweli nie ma zapisu pozwalającego obywatelowi dowiedzieć się, że państwo ingerowało w jego prawa i wolności, podsłuchując go lub pobierając jego bilingi. Gdyby był o tym poinformowany, choćby post factum, mógłby zaskarżyć to do sądu, który oceniłby zasadność takiej inwigilacji. Teraz nie jest to możliwe. Obywatel nie dostanie takiej informacji nawet wtedy, gdy podczas inwigilacji nie wykryto niczego, co uzasadniałoby jej prowadzenie.

RPO kwestionuje brak realnej kontroli pobierania danych obywateli. Sąd okręgowy ma wprawdzie prawo do kontroli, ale jedynie na podstawie zbiorczych półrocznych sprawozdań służb. Sąd nie musi, ale tylko może weryfikować, czy dane pobrano zasadnie. Tymczasem Konstytucja zakazuje pozyskiwania, gromadzenia i udostępniania innych informacji o obywatelu niż niezbędne. Po kontroli sąd może jedynie poinformować poszczególną służbę o jej wynikach, ale nie może zarządzić np. zniszczenia zgromadzonych danych.

W praktyce ta kontrola sądów ma charakter iluzoryczny - dowodzi Adam Bodnar. Tajne sprawozdania służb nie są informacją publiczną, choć zawierają informacje dotyczące liczby pozyskanych danych telekomunikacyjnych, pocztowych lub internetowych i kwalifikacji prawnej czynów, w związku z którymi o nie wystąpiono.

Kolejnym zarzutem wobec noweli jest nieproporcjonalni długi czasu trwania kontroli operacyjnej - do 18 miesięcy. RPO kwestionuje, że przez półtora roku służby mogą podsłuchiwać obywatela lub czytać jego korespondencję - niezależnie od tego, czy po tym będzie na tej podstawie wszczęte postępowanie karne.

Ponadto nowela ograniczyła chronioną prawem tajemnicę zawodów zaufania publicznego, np. adwokatów czy radców prawnych. Zdobyte podczas inwigilacji tajemnice mogą być wykorzystane w postępowaniu karnym, gdy „jest to niezbędne ze względu na dobro wymiaru sprawiedliwości, a okoliczność ta nie może być ustalona na podstawie innego dowodu". Taki nieostry zapis może prowadzić do rażącego naruszenia fundamentalnego prawa jednostki - prawa do obrony. A przecież adwokat ma obowiązek zachować w tajemnicy wszystko, czego się dowiedział udzielając pomocy prawnej

Komisja Wenecka też krytykowała nowelę

W czerwcu 2016 r. Komisja Wenecka uznała, że nowela nadaje służbom zbyt szerokie kompetencje, które mogą uderzać bezpośrednio w prawo do prywatności obywateli. Oceniła m.in., że

- dostęp służb do najbardziej wrażliwych danych telekomunikacyjnych i internetowych powinien wymagać uprzedniej zgody sądu;
- nadzór nad zbieraniem mniej wrażliwych danych powinien sprawować niezależny organ, a jednostka powinna być informowana o ich pobraniu;
- system składania sądom ogólnych sprawozdań przez służby będzie nieskuteczny.

Rząd zignorował rekomendacje Komisji. Zalecała ona m.in. by pozyskiwanie najważniejszych danych telekomunikacyjnych i internetowych ograniczyć do najgroźniejszych sytuacji; by skrócić czas przechowywania danych oraz zadbać o nienaruszanie tajemnicy adwokackiej.

II.519.109.2015

BLOKOWANIE KONT PRZEZ PORTALE SPOŁECZNOŚCIOWE MOŻE NARUSZAĆ WOLNOŚĆ SŁOWA - OCENIA RPO

data: 2018-03-13

- **Blokowanie i kasowanie kont użytkowników oraz usuwanie komentarzy przez portale społecznościowe może być uznane za naruszenie wolności słowa - ocenia Rzecznik Praw Obywatelskich**
- **Według RPO filtrowanie napastliwych treści na Facebooku jest nieskuteczne, kryteria kasowania profili są niejasne, a cały proces jest zapewne zautomatyzowany**
- **Państwo polskie powinno koniecznie ustosunkować się do tego problemu - napisał zastępca RPO Stanisław Trociuk do Ministerstwa Cyfryzacji**

W liście do Marka Zagórskiego, sekretarza stanu w Ministerstwie Cyfryzacji, Stanisław Trociuk zwrócił uwagę na potrzebę zapewnienia większej przejrzystości funkcjonowania Facebooka i innych tego typu portali społecznościowych. Powołał się na wpływające do Biura RPO liczne skargi dotyczące blokowania lub usuwania kont. Skarżący wskazują, iż dochodzi do tego ze względu na ich przekonania bądź określone wypowiedzi. Obywatele skarżą się też na usuwanie komentarzy na Facebooku.

Według RPO dotychczasowa praktyka wskazuje, iż filtrowanie napastliwych treści na Facebooku jest nieskuteczne. Niejasne są kryteria kasowania profili. Można zakładać, że jest to proces zautomatyzowany .

„W ocenie Rzecznika tego typu działania mogą zostać uznane za ograniczenie, a nawet naruszenie konstytucyjnie chronionej wolności słowa. Wobec tego państwo polskie powinno koniecznie ustosunkować się do wskazanego problemu" - głosi list Stanisława Trociuka.

W listopadzie 2016 r. w Biurze RPO zorganizowano debatę pt. „Facebook - mowa nienawiści - wolność słowa. Wyzwanie cywilizacyjne i prawnicze czy kryzys wartości?". Brali w niej udział przedstawiciele administracji, naukowcy, aktywiści na rzecz wolności w internecie, działacze organizacji praw człowieka, zabiegających o wolność słowa i reprezentujących prawa mniejszości, a także ruchów nacjonalistycznych, których profile na Facebooku wtedy skasowano.

Debata potwierdziła problem blokowania lub usuwania kont na Facebooku, który dotyczy różnych opcji światopoglądowych i ideowych. Mimo odmiennych poglądów dyskutanci zgodzili się, że procedury usuwania treści, czy blokowania lub usuwania kont są niewystarczające. Rozważano m.in. stosowanie ostrzeżeń, trybu odwoławczego i włączenia w procedurę wymiaru sprawiedliwości (z wykorzystaniem przepisów karnych).

Ówczesna minister cyfryzacji Anna Streżyńska spotkała się wtedy z reprezentantami Facebooka w Europie. Trociuk zwrócił się do MC o informacje o tym spotkaniu, zwłaszcza co do ustaleń dotyczących polityki blokowania kont i profili użytkowników na Facebooku .

Ze strony internetowej Ministerstwa Cyfryzacji wynika, że rozmowy w celu wypracowania szczegółowych rozwiązań ma koordynować Rada ds. Cyfryzacji, ciało doradcze ministra. Wchodzący w skład Rady eksperci wspólnie z przedstawicielami Facebooka mają analizować politykę serwisu oraz przedstawić ministrowi swe rekomendacje. Trociuk zwrócił się do resortu o informacje w sprawie ewentualnych rezultatów tych działań.

„Jednocześnie proszę uprzejmie Pana Ministra o przedstawienie propozycji rozwiązania problemów wskazywanych we wnioskach obywateli" - zaznaczył Trociuk.

VII.562.1.2018

PODPISY POD OBYWATELSKIMI PROJEKTAMI USTAW - TAKŻE DROGĄ ELEKTRONICZNĄ

data: 2018-03-06

- **Rzecznik Praw Obywatelskich opowiada się za możliwością zbierania podpisów pod obywatelskimi projektami ustaw drogą elektroniczną. RPO zwrócił się w tej sprawie do Ministerstwa Cyfryzacji.**

W swym wystąpieniu RPO powołał się m.in. na postulaty ekspertów, organizacji społecznych oraz na sygnały od obywateli. Zdaniem RPO potrzebę taką dostrzegają od dłuższego czasu niezależne ośrodki badawcze.

Według ekspertów, procedura mogłaby polegać np. na przesłaniu podpisanej elektronicznie treści proponowanego aktu prawnego drogą elektroniczną do organizatora. Innym rozwiązaniem może być zaprojektowanie w ramach którejś z instytucji państwowych elektronicznej platformy bądź serwisu internetowego lub też uruchomienie usługi w ramach serwisu ePUAP.

RPO argumentuje, że wykorzystywanie nowoczesnych technologii mogłoby zwiększyć udział obywateli w życiu publicznym. „Każda forma ułatwienia obywatelom udziału w bezpośrednim uczestnictwie kształtowania państwa, w moim przekonaniu, jest warta szerszej analizy" - dodał. Przypomniał, że jest już możliwość złożenia petycji drogą elektroniczną.

Kwestia ta była już podnoszona przez RPO w piśmie z 2016 r. do Prezesa Rady Ministrów. W odpowiedzi Minister Cyfryzacji podkreślała wtedy, że inicjatywa ta jest możliwa do realizacji i zasługuje na poparcie. Wskazała zarazem na konieczność szczególnej analizy pod kątem procesów związanych z przygotowaniem projektu ustawy, jego rozpowszechnianiem, kampanią promocyjną i techniczną organizacją zbierania podpisów - które wymagają informatyzacji.

Kolejne wystąpienia RPO do Ministra Cyfryzacji w tej kwestii pozostały bez odpowiedzi.

VII.600.9.2015

OBYWATEL POWINIEN SAM DECYDOWAĆ, NA JAKIE STRONY WCHODZI. RZECZNIK PISZE DO MINISTER FINANSÓW W SPRAWIE BLOKOWANIA STRON INTERNETOWYCH

data: 2018-02-1 9

- **Możliwość blokowania stron internetowych, przewidziana w nowelizacji ustawy o grach hazardowych jest rozwiązaniem zbyt daleko idącym – alarmuje po raz kolejny RPO.**

- **Rzecznik przedstawił swoje wątpliwości Minister Finansów.**

Rzecznik Praw Obywatelskich zwrócił uwagę, że środek, przewidziany w ustawie o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw, polegający na blokowaniu stron internetowych jest rozwiązaniem najdalej idącym i rygorystycznym, stwarzającym ryzyko dla wolności słowa i dostępu do informacji, zaś jego zastosowanie powinno mieć szczególne uzasadnienie poparte rzetelną analizą skutków takiej regulacji, a także powinno być poprzedzone wnikliwym rozpatrzeniem innych możliwych instrumentów o mniej dolegliwym charakterze.

Obszerne wyjaśnienia, przedstawione dotychczas w stanowisku Ministra Rozwoju i Finansów, potwierdzające, że gry hazardowe stwarzają zagrożenie dla pewnych istotnych wartości, takich jak sytuacja ekonomiczna, polityczna, społeczna i rodzinna oraz że mogą one zwiększać ryzyko uzależnienia od narkotyków i alkoholu nie uzasadniają, w ocenie Rzecznika, ograniczania swobód obywatelskich w imię eliminacji tego typu zjawisk.

Zgodnie z treścią uzasadnienia wyroku Europejskiego Trybunału Praw Człowieka w sprawie Kalda przeciwko Estonii (skarga nr 17429/10), ograniczenie dostępu do witryny w sieci Internet może nastąpić wyłącznie w sytuacji realnego zagrożenia. A

contrario, zagrożenie potencjalne lub hipotetyczne nie jest wystarczającym powodem do blokowania dostępu do witryny.

Alternatywnym środkiem, którego prawodawca zdaje się nie dostrzegać, jest ograniczenie się do nałożenia na przedsiębiorcę świadczącego usługi telekomunikacyjne obowiązku informowania użytkownika – poprzez wyświetlenie stosownego komunikatu – że znalazł się on na stronie o podwyższonym ryzyku przestępstw i oszustw, oferującej nielegalne usługi, i powinien rozważyć opuszczenie tej strony. Kontynuacja przebywania na takiej witrynie internetowej o podwyższonym ryzyku powinna być uzależniona od decyzji samego konsumenta, należycie poinformowanego o negatywnych konsekwencjach takiej decyzji. Odbieranie mu jednak takiej swobody decydowania o sobie, w opinii Rzecznika, zdaje się być zbyt daleko idącym rozwiązaniem, ingerującym w wolność jednostki i odmawiającym jej prawa o podjęcia świadomego wyboru. Takie rozwiązanie cechuje się brakiem zaufania do obywatela i umiejętności podjęcia przez niego świadomej decyzji w okolicznościach, gdy został on należycie poinformowany o istniejących zagrożeniach.

Prawodawca zdecydował ponadto o zastosowaniu arbitralnego środka w postaci decyzji Ministra Finansów o wpisie do Rejestru, zamiast środka w postaci postanowienia sądu. Następcza kontrola sądowo-administracyjna wydaje się być rozwiązaniem nieadekwatnym do omawianego problemu. Zdaniem Rzecznika ograniczenie wolności słowa i dostępu do informacji powinno być uwarunkowane orzeczeniem sądu już na wstępie, a nie dopiero po zaistniałym fakcie ograniczenia.

Rzecznik zwrócił się do Minister z prośbą o ustosunkowanie się do powyższych wątpliwości.

KASACJA RZECZNIKA NA NIEKORZYŚĆ LIDERA STOWARZYSZENIA DUMA I NOWOCZESNOŚĆ. INTERNET JEST MIEJSCEM PUBLICZNYM.

data: 2018-01-24

Już 27 lipca 2017 r. Rzecznik zaskarżył do Sądu Najwyższego prawomocne postanowienie Sądu Rejonowego w Wodzisławiu Śląskim z 26 kwietnia 2017 r. (sygn. akt II W 33/17). Sąd umorzył wtedy sprawę o wykroczenie przeciwko Mateuszowi S. z ruchu Duma i Nowoczesność.

Pod koniec 2016 r. DiN opublikowało w internecie serię naklejek z nieprzyzwoitymi i obraźliwymi napisami stylizowanymi na znaki zakazu. Obrazki przedstawiały m.in. dwa „ludziki" w pozycji sugerującej seks analny i były opatrzone napisem: „Zakaz pedałowania, homoseksualiści wszystkich krajów, leczcie się". Policjanci z Wodzisławia ustalili, że naklejki opublikował lider DiN. Przedstawiono mu więc zarzut umieszczania w miejscu publicznym nieprzyzwoitych napisów oraz rysunków. To wykroczenie, za które grozi grzywna lub ograniczenie wolności.

Sąd w Wodzisławiu Śląskim przyznał, że rysunki „przez część odbiorców mogą zostać uznane za nieprzyzwoite", ale umieszczenie ich w internecie nie wypełnia znamion wykroczenia.

Zdaniem Rzecznika sąd błędnie przyjął, że: „internet nie jest miejscem publicznym" i w konsekwencji, że czyn zarzucony obwinionemu nie jest wykroczeniem. Skutkiem tego było niezasadne umorzenie postępowania przeciwko Mateuszowi S.

Strona internetowa jest miejscem publicznym w rozumieniu art. 141 k.w. Działanie „w miejscu publicznym" musi być podjęte w przestrzeni dostępnej dla ogółu, do której nieograniczony dostęp ma bliżej nieokreślona liczba ludzi. Oznacza to, że w internecie nie można bezkarnie publikować wszystkiego, co się chce. Właściciele stron internetowych i wydawcy portali odpowiadają za pojawiające się tam treści.

BPK.511.37.2017

DYREKTYWA POLICYJNA - SZANSA DLA OBYWATELI CZY LEGISLACYJNY PUSTY PRZEBIEG?

data: 2017-12-09

Od wielu lat mierzymy się z problemem braku zewnętrznej kontroli nad zdobywaniem przez służby informacji o obywatelach. Tymczasem na skutek przepisów unijnych w maju 2018 r. czeka nas rewolucja w sposobie ochrony danych osobowych. Przyjęte w 2017 r. w Unii Europejskiej nowe przepisy to nie tylko rozporządzenie ogólne o ochronie danych osobowych (tzw. RODO[1]), ale także tzw. dyrektywa policyjna, która dotyczy przetwarzania danych osobowych przez organy ścigania[2]. Dyrektywa stanowi próbę pogodzenia dwóch wartości. Z jednej strony ułatwienie wymiany danych między państwami członkowskimi, z drugiej – wzmocnieniu praw osób, których dane dotyczą. Dyrektywa przyznaje m.in. jednostce uprawnienie do złożenia skargi do organu nadzorczego czy uzyskania informacji, czy dotyczące jej dane są przetwarzane.

O szansach wzmocnienia ochrony prawa do prywatności obywateli, rozmawiali uczestnicy panelu: dr hab. Agnieszka Grzelak prof. nadzw. ALK, zastępca Dyrektora Zespołu Prawa Konstytucyjnego, Europejskiego i Międzynarodowego w Biurze Rzecznika Praw Obywatelskich; dr hab. Paweł Waszkiewicz specjalizujący się w tematach prewencji kryminalnej, monitoringu wizyjnego, biometrii, pracy operacyjnej czy metod inwigilacji; dr Barbara Grabowska-Moroz ekspertka Helsińskiej Fundacji Praw Człowieka. Moderatorem panelu był Wojciech Klicki związany z fundacją Panoptykon.

Relacja na gorąco:

Dr Barbara Grabowska-Moroz wskazywała, że takie wartości jak bezpieczeństwo publiczne i prywatność nie stoją ze sobą w konflikcie. Przyjmuje się jednak narrację o nadzwyczajnym charakterze zagrożeń jakie występują. Należy jednak zastanowić się czy te zagrożenia mają ciągle charakter nadzwyczajny. Takie spojrzenie ma wpływ na debatę w Polsce. Podstawowym punktem wyjścia jest kwestia określenia przesłanek, na podstawie których służby mogą podejmować określone działania.

„Przedstawianie bezpieczeństwa i wolności jako alternatywy rozłącznej jest nieprawdziwe".

Dr Paweł Waszkiewicz odpowiadając na pytanie dotyczące tego w jaki sposób powinniśmy myśleć o kontroli aby była ona skuteczna i jednocześnie nie blokowała realizacji zadań służb zwracał uwagę, że „przedstawianie bezpieczeństwa i wolności jako alternatywy rozłącznej jest nieprawdziwe". Stwierdził, że pozbywanie się wolności za obietnice bezpiecznego życia nigdzie do tej pory się nie sprawdziło. Polska nie jest wyjątkowa, dlatego ograniczając wolność nie wzmocnimy bezpieczeństwa. Potrzeby funkcjonowania służb nikt nie kwestionuje. Diabeł tkwi w szczegółach. Zwracał uwagę na specyfikę pracy w służbach. Sytuacją idealną jest kontrola służb przez niezależny organ.

Na konieczne zmiany z punktu widzenia Rzecznika Praw Obywatelskich wskazywała prof. Agnieszka Grzelak. Podkreślała, że kwestia kontroli służb nie jest nowym problemem, w tym kontekście wskazywała na wyrok TK w sprawie K 23/11 (z wniosku RPO), który był pretekstem do przyjęcia przepisów ustawy inwigilacyjnej. Tymczasem w ocenie RPO ten wyrok TK nie tyko nie jest wykonany, ale zawiera regulacje które budzą wątpliwości konstytucyjne. Problem nadzoru jest przedmiotem wniosku RPO do TK w sprawie ustawy inwigilacyjnej i ustawy antyterrorystycznej. W tym kontekście wskazywała również na opinię Komisji Weneckiej, w której również został poruszony problem braku niezależnej kontroli. Rzecznik przedstawiając swoje stanowiska w tym zakresie, m.in. występując do MSWiA, a także MC, podkreślał, że musi istnieć organ który te służby kontroluje. Każda osoba zainteresowana ochroną swoich praw musi mieć możliwość zwrócenia się do organu, który jest organem niezależnym. Prof. Grzelak wskazywała także, że mamy wyznaczony standard europejski, problemem jest jak przekonać władze do tego aby ten standard stosować.

Dr Barbara Grabowska-Moroz wskazywała, patrząc z perspektywy przedstawiciela organizacji pozarządowej, że argument z prawa Unii Europejskiej działa jak dźwignia. Jesteśmy lepiej słyszalni wykorzystując argumenty UE. W ustawie implementacyjnej stworzenie skutecznych mechanizmów będzie problematyczne, ale również trudne może okazać się wytoczenie granicy między bezpieczeństwem publicznym, a porządkiem publicznym.

Dr Waszkiewicz wskazywał, że Dyrektywa jest szansą nie tylko dla obywateli, ale także wszystkich osób fizycznych, a także dla pracy służb policyjnych. Jeżeli chodzi o szanse to należy wskazać na preambułę Dyrektywy. Dyrektywa ma ułatwić pracę służbom, a nie być kagańcem dla nich (np. umożliwia korzystanie z baz danych).

Prof. Agnieszka Grzelak podkreślała, że Dyrektywa reguluje standard ochrony danych. Wskazywała przy tym na termin implementacji Dyrektywy (6 maja 2018 r.). Przypominała również stanowisko RPO dotyczące niezależności organu nadzorczego, które prezentował w swoim wystąpieniu do MC i MSWiA. Wskazywała na szansę jaką daje art. 17 Dyrektywy, tj. na wykonywanie praw osoby, której dane dotyczą za pośrednictwem organu nadzorczego. Ważne jest również to, że Dyrektywa przewiduje, przyjęcie przepisów określających sankcje za naruszenie przepisów przyjętych na podstawie Dyrektywy. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające (art. 57 Dyrektywy). Poza wdrożeniem dyrektywy konieczne jest dokonanie przeglądu bieżącego ustawodawstwa, trzeba sprawdzić czy te przepisy, które obowiązują są zgodne z prawem unii europejskie.

Podczas dyskusji podkreślano, że istnieje poważne niebezpieczeństwo związane z brakiem kontroli działań służb. Uczestnicy dyskusji wskazywali również na potrzebę kompleksowego podejścia od reformy ochrony danych osobowych (związanej z

przyjęciem RODO i Dyrektywy), gdyż mamy do czynienia z pakietem ustaw. Sygnalizowano także, że dzisiaj mamy jedynie kontrolę formalną, a nie merytoryczną ocenę sądów nad działalnością służb.

Podsumowując dyskusję Wojciech Klicki wskazywał, że istnieje ryzyko, że Dyrektywa może okazać się tylko „pustym przebiegiem". Dlatego aktualnie, ważna jest rola instytucji takich jak GIODO i RPO, które powinny podejmować działania ukierunkowane na to aby dyrektywa została implementowana do prawa polskiego.

[1] rozporządzenie 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 o dyrektywy 95/46/WE

[2] dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW

WYKORZYSTANIE INTERNETU W SZKOLE - ODPOWIEDŹ MINISTERSTWA EDUKACJI NARODOWEJ

data: 2017-10-10

Raport Instytutu Badawczego NASK „Nastolatki 3.0", zgodnie z sugestiami RPO, został przeanalizowany i przekazany wszystkim kuratorom oświaty z prośbą o jego upowszechnienie w szkołach tak, aby przedstawione w nim wyniki badań i rekomendacje mogły być pomocne, między innymi, w przygotowywaniu szkolnych programów wychowawczo-profilaktycznych – poinformowała w swoim liście do Rzecznika Minister Edukacji Narodowej. Minister podzieliła również pogląd RPO, że z uwagi na wskazane m.in. w raporcie problemy korzystania z urządzeń mobilnych przez uczniów konieczne wydaje się określenie w statucie szkoły zasad używania telefonów komórkowych i innych urządzeń elektronicznych na terenie szkoły.

Minister poinformowała ponadto, że nowa podstawa programowa kształcenia ogólnego uwzględnia wyzwania, jakie stawia we współczesnym świecie wzrost aktywności dzieci i młodzieży w internecie. W zakresie zajęć z informatyki wprowadzono naukę programowania i rozwiązywania problemów z wykorzystaniem narzędzi ICT. Wszystkie szkoły i placówki mają obowiązek upowszechniania wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowania właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem technologii informacyjno-komunikacyjnych, i sytuacji nadzwyczajnych. Zadaniem szkół jest również kształtowanie u uczniów umiejętności sprawnego posługiwania się technologiami informacyjno-komunikacyjnymi. Wszyscy kuratorzy oświaty wyznaczyli osoby odpowiedzialne za wdrażanie najnowszych technologii w szkołach tzw. wojewódzkich koordynatorów do spraw innowacji. W podstawowych kierunkach realizacji polityki oświatowej państwa na rok szkolny 2017/2018 Minister Edukacji Narodowej, wśród priorytetów wskazał: Bezpieczeństwo w Internecie. Odpowiedzialne korzystanie z mediów społecznych.

POLSKIE PRAWO W ZAKRESIE RETENCJI DANYCH TELEKOMUNIKACYJNYCH POWINNO BYĆ DOSTOSOWANE DO WYMOGÓW PRAWA UE. RPO PISZE W TEJ SPRAWIE DO MINISTRA SPRAW ZAGRANICZNYCH

data: 2017-09-14

W związku z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej z dnia 21 grudnia 2016 r. w sprawie Tele2 Sverige AB, dotyczącej problemu przepisów krajowych implementujących unijną dyrektywę retencyjną (2006/24/WE), której nieważność stwierdził Trybunał Sprawiedliwości UE w 2014 r. w wyroku w sprawie DRI, powstała konieczność dostosowania prawa polskiego do wymogów prawa Unii Europejskiej w zakresie tzw. retencji danych telekomunikacyjnych i dostępu właściwych organów do tych danych dla potrzeb zwalczania przestępczości.

W ocenie resortu cyfryzacji nie ma potrzeby wprowadzania zmian w przepisach pozostających we właściwości Ministra Cyfryzacji, natomiast otwartą kwestią pozostaje konieczność dokonania zmian w przepisach odrębnych zawierających upoważnienie do dostępu do danych telekomunikacyjnych. Z kolei Ministerstwo Spraw Wewnętrznych i Administracji wyraziło opinię, że nieodzownym do ostatecznej oceny przedmiotowej sprawy wydaje się stanowisko Trybunału Konstytucyjnego.

Tymczasem w przekonaniu Rzecznika Praw Obywatelskich oczekiwanie na wyrok TK nie może przesłonić obowiązków wynikających z faktu członkostwa Polski w Unii Europejskiej, w szczególności płynących z zasady lojalnej współpracy i obowiązku zapewnienia zgodności prawa polskiego z prawem UE.

Obowiązujące przepisy Prawa telekomunikacyjnego oraz ustaw regulujących dostęp służb do danych budzą także zastrzeżenia z punktu widzenia zgodności ze standardem wynikających z Konwencji o ochronie praw człowieka i podstawowych wolności.

Stanowiska zarówno Ministra Spraw Wewnętrznych i Administracji, jak również Ministra Cyfryzacji nie wyjaśniają podnoszonych wcześniej przez Rzecznika wątpliwości.

W związku z powyższym Rzecznik zwrócił się do Ministra z prośbą o przedstawienie stosownych wyjaśnień w sprawie.

MONITOROWANIE KORESPONDENCJI ELEKTRONICZNEJ PRACOWNIKA STANOWIŁO NARUSZENIE JEGO PRAWA DO POSZANOWANIA ŻYCIA PRYWATNEGO I KORESPONDENCJI

data: 2017-09-07

- **5 września 2017 r. Europejski Trybunał Praw Człowieka - Wielka Izba - wydał wyrok w sprawie Bărbulescu przeciwko Rumunii (61496/08)**

Fakty

Sprawa dotyczy zwolnienia skarżącego z pracy w prywatnym przedsiębiorstwie po skontrolowaniu prywatnej korespondencji mailowej oraz poznaniu jej treści przez pracodawcę. Chodziło o używanie w pracy internetu do celów niezwiązanych z pracą w czasie godzin pracy. Skarżący zarzucał, że decyzja pracodawcy o zakończeniu z nim współpracy wynikała z wcześniejszego naruszenia jego prawa do poszanowania życia prywatnego.

Wyrok Izby Trybunału z 12 stycznia 2016 r.

Rok temu Trybunał w składzie 7-osobowym, stwierdzając brak naruszenia Artykułu 8, nie uznał za nieusprawiedliwione działania pracodawcy polegającego na sprawdzeniu, czy pracownicy wypełniali swoje obowiązki w czasie godzin pracy oraz wejściu na konto pracownika w przekonaniu, że zawiera jedynie korespondencję zawodową z klientami.

Wskazał dodatkowo, że skarżący mógł podnieść zarzuty odnośnie naruszenia jego prawa do życia prywatnego oraz korespondencji przed sądami krajowymi i nie wspomniano w żadnej z decyzji o treści wiadomości. Ponadto w ocenie Trybunału, sądy krajowe użyły transkrypcji z korespondencji skarżącego jedynie w zakresie zmierzającym do udowodnienia, że używał firmowego komputera do prywatnych celów w czasie godzin pracy oraz że tożsamość osób, z którymi się komunikował nie został ujawniona.

W związku z tym rok temu Trybunał uznał, iż sądy krajowe odpowiednio wyważyły z jednej strony prawo skarżącego do poszanowania jego życia prywatnego, a z drugiej interesy pracodawcy. W związku z tym nie doszło do naruszenia Artykułu 8 Konwencji.

Wyrok Wielkiej Izby Trybunału

Wielka Izba Trybunału zajęła odmienne stanowisko. Trybunał uznał, że władze krajowe nie zagwarantowały skarżącemu odpowiedniej ochrony prawa do poszanowania życia prywatnego i korespondencji. W konsekwencji nie wyważyły w sposób odpowiedni konkurujących interesów.

W szczególności, sądy krajowe nie ustaliły, czy pan Bărbulescu został uprzednio zawiadomiony przez pracodawcę o możliwości monitorowania jego korespondencji. Sądy nie wzięły również pod uwagę okoliczności, że skarżący nie został poinformowany ani o charakterze, ani o zakresie monitoringu, czy też o stopniu ingerencji w jego życie prywatne i korespondencję. Dodatkowo, sądy krajowe nie ustaliły, po pierwsze, szczególnych przyczyn uzasadniających zastosowanie monitoringu; po drugie, czy pracodawca mógł użyć środków mniej inwazyjnych w prywatne życie i korespondencję skarżącego; po trzecie, czy dostęp do jego korespondencji mógł zostać zrealizowany bez jego wiedzy.

Dlatego 11 głosami do 6 Trybunał stwierdził naruszenie Artykułu 8 (prawo do poszanowania życia prywatnego, rodzinnego, mieszkania i korespondencji) Konwencji.

MINISTER CYFRYZACJI O KONIECZNOŚCI ZMIANY PRZEPISÓW W SPRAWIE RETENCJI DANYCH TELEKOMUNIKACYJNYCH

data: 2017-09-06

W lutym 2017 r. Rzecznik Praw Obywatelskich zwrócił się do Ministra Cyfryzacji z pytaniem dotyczącym konieczności dostosowania polskiego prawa do stanowiska Trybunału Sprawiedliwości Unii Europejskiej, wyrażonego w wyroku w sprawie Tele2 (C-203/15 i C-698/15 z 21 grudnia 2016 r.)

Dla przypomnienia należy wskazać, że w wyroku tym - analizując przypadki szwedzki i brytyjski - TSUE uznał, że nie jest zgodne z prawem Unii Europejskiej wprowadzenie przepisów w prawie państw członkowskich, przewidujących uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej, z uwagi na prewencyjny charakter zapobiegania przestępstwom. W dalszych tezach wyjaśnił, że dopuszczalne jest ustanowienie obowiązku indywidualnego zatrzymywania danych w celu zwalczania poważnej przestępczości pod warunkiem, że takie zatrzymywanie nie będzie wykraczać poza to, co jest absolutnie konieczne jeśli chodzi o zakres danych, stosowane środki łączności, podmioty zaangażowane w tej proces, jak i przyjęty okres przechowywania tych danych.

Oznacza to, że TSUE zakwestionował możliwość nałożenia na przedsiębiorców telekomunikacyjnych obowiązków gromadzenia i przechowywania informacji o tym, kto, kiedy i do kogo dzwonił, jeżeli nie jest to uzasadnione koniecznością zwalczania poważnej przestępczości, w konkretnych przypadkach i wtedy wyłącznie, gdy jest to absolutnie niezbędne. W ocenie RPO przepisy ustawy - Prawo telekomunikacyjne, a w szczególności art. 180a budzą wątpliwości, czy faktycznie polskie prawo nakłada ten obowiązek wyłącznie w niezbędnym zakresie.

W odpowiedzi przekazanej do Rzecznika w dniu 30 sierpnia 2017 r. Minister Cyfryzacji stwierdziła, że w ocenie Ministerstwa Cyfryzacji obowiązujące przepisy ustawy - Prawo telekomunikacyjne regulujące tę problematykę nie wymagają zmian. Otwartą kwestią pozostaje natomiast ocena konieczności zmiany przepisów zawierających upoważnienie do dostępu do danych telekomunikacyjnych.

Przedstawionej odpowiedzi nie można uznać za satysfakcjonującą, ponieważ analiza orzeczenia sądów międzynarodowych (TSUE i ETPCz) prowadzi jednak do wyraźnie odmiennych wniosków, niż przedstawione w piśmie Ministerstwa. RPO będzie zatem dalej prowadził działania, których efektem powinno być dostosowania prawa polskiego do prawa UE.

W tym kontekście należy przypomnieć stanowisko Generalnego Inspektora Ochrony Danych Osobowych wyrażonego w piśmie z 25 stycznia 2017 r., skierowanym do MSZ, w którym wskazano na konieczność dokonania zmian w przepisach ustawy - Prawo telekomunikacyjne (a zatem inaczej, niż obecnie twierdzi Minister Cyfryzacji).

Warto również dodać, że w sprawie dostosowania przepisów regulujących dostęp do danych telekomunikacyjnych RPO występował też do Ministra Spraw Wewnętrznych i Administracji. W dniu 16 marca 2017 r. MSWiA poinformowało RPO o konieczności pozyskania dodatkowych informacji. Odpowiedź wpłynęła w kwietniu br. i jest przedmiotem analizy RPO.

Należy też wskazać, że w dniu dzisiejszym ukazał się raport organizacji Privacy International, w którym wyraźnie odnotowano, że w Polsce nie podjęto dotąd żadnych działań zmierzających do dostosowania prawa krajowego do wymagań prawa UE po wyroku w sprawie Tele2. Wskazano, że poczynione zmiany mają charakter wręcz bardziej restrykcyjny.

PRZED ROZPOCZĘCIEM ROKU SZKOLNEGO RPO PYTA: JAK UCZNIOWIE WYKORZYSTUJĄ INTERNET W SZKOLE?

data: 2017-09-01

Rzecznik Praw Obywatelskich zapoznał się z zawartymi w raporcie Instytutu Badawczego NASK pt. Nastolatki 3.01, wynikami badań dotyczącymi różnych aspektów aktywności uczniów szkół gimnazjalnych i ponadgimnazjalnych w internecie. W raporcie zawarto informacje dotyczące zarówno zagrożeń, z którymi spotyka się młodzież w sieci, jak i sposobów korzystania z internetu w życiu codziennym nastolatków, ze szczególnym uwzględnieniem wykorzystania internetu w procesie nauczania w szkole i w domu.

Zebrane w tym raporcie dane oraz sformułowane na ich podstawie rekomendacje mogą być w ocenie Rzecznika niezwykle przydatne dla realizacji celów, jakie stawia sobie MEN w zakresie zwiększenia poziomu bezpieczeństwa dzieci i młodzieży w cyberprzestrzeni oraz usprawnienia stosowanych metod nauczania.

W raporcie zwrócono uwagę m.in. na problemy korzystania z urządzeń mobilnych na terenie szkoły. Z przeprowadzonych badań wynika bowiem, że w co piątej szkole brak jest jakichkolwiek regulacji dotyczących zasad korzystania z urządzeń mobilnych mających dostęp do internetu. Ponadto 78% badanych uczniów zadeklarowało, że potrafi korzystać z takich urządzeń mobilnych podczas przeprowadzanych w szkole sprawdzianów i klasówek. **Zdaniem Rzecznika zasadne wydaje się ujednolicenie regulacji dotyczących korzystania z takich urządzeń w polskich szkołach tak, aby zapobiegać niewłaściwym zachowaniom uczniów, z jednoczesnym poszanowaniem ich godności i prawa własności.**

Raport NASK zawiera również dane dotyczące wykorzystywania przez uczniów internetu w samodzielnym zdobywaniu wiedzy oraz w wypełnianiu szkolnych obowiązków.

Z przedstawionych w tym zakresie informacji wynika, że szkoła w niewystarczającym stopniu wspiera tę formę poszerzania wiedzy i umiejętności przez dzieci i młodzież. Uczniowie najczęściej korzystają z serwisów oferujących gotowe materiały potrzebne do wykonywania prac domowych, bardzo rzadko korzystają zaś z profesjonalnych portali edukacyjnych umożliwiających samodzielne i aktywne rozwijanie wiedzy. Z raportu wynika ponadto, że nauczyciele bardzo rzadko korzystają z internetu podczas zajęć lekcyjnych i posługują się konwencjonalnymi źródłami, takimi jak filmy i zdjęcia, które w niewielki sposób aktywizują uczniów. Wobec powyższego zasadnym wydaje się podejmowanie dalszych działań na rzecz włączenia internetu w system edukacji.

W kontekście informacji zawartych w omawianym raporcie konieczne wydaje się również poszerzanie świadomości rodziców o znaczeniu mediów społecznościowych oraz formach korzystania z nich. Zasadne jest też zachęcanie rodziców do

współuczestniczenia w tej sferze życia ich dzieci.

Rzecznik zwrócił się do Minister z prośbą o rozważenie uwzględnienia zawartych w raporcie NASK rekomendacji w działalności resortu edukacji narodowej i poinformowanie o działaniach mających na celu upowszechnienie informacji na temat tego raportu wśród pracowników systemu oświaty i rodziców.

ODPOWIEDŹ MINISTRA ROZWOJU I FINANSÓW NA WĄTPLIWOŚCI RZECZNIKA DOTYCZĄCE BLOKOWANIA TREŚCI W INTERNECIE

data: 2017-08-30

Do Rzecznika Praw Obywatelskich wpłynęło stanowisko Ministra Rozwoju i Finansów sporządzone w odpowiedzi na wystąpienie Rzecznika z dnia 5 lipca 2017 r. RPO w swoim wystąpieniu podkreślał konstytucyjne i międzynarodowoprawne wątpliwości na temat uchwalonej ustawy o zmianie ustawy o grach hazardowych, w tym te dotyczące niewystarczającego uzasadnienia dla jej przyjęcia, niezbędności i efektywności wprowadzonych rozwiązań.

Minister Rozwoju i Finansów odniósł się do większości zastrzeżeń Rzecznika. Wskazał na wnioski pokontrolne Najwyższej Izby Kontroli dotyczące unikania odpowiedzialności podmiotów niezarejestrowanych na terenie Polski świadczących nielegalne usługi hazardowe. Według Ministra wprowadzone uregulowania są odpowiedzią na wnioski NIK oraz opierają się na szerokiej analizie rynku nielegalnego hazardu wykonanej przez Służbę Celną.

Minister wskazuje, że wprowadzone rozwiązanie blokowania dostępu do nielegalnych stron hazardowych jest oparte na dobrych przykładach regulacji z innych państw m.in. Francji, Danii, Słowacji czy Włoch. W opinii Ministra prawa i wolności obywatela gwarantowane przez Konstytucję i Konwencję o ochronie praw człowieka i podstawowych wolności są chronione w sposób wystarczający, w szczególności za pośrednictwem wprowadzenia sądowej kontroli mechanizmu blokowania stron. Ustawa została notyfikowana Komisji Europejskiej, która nie zgłosiła uwag i zarzutów naruszenia prawa europejskiego.

Stanowisko Ministra Rozwoju i Finansów nie daje jednak pełnej odpowiedzi na zastrzeżenia Rzecznika co do proporcjonalności i adekwatności wprowadzonych rozwiązań. Wątpliwości budzi również brak konsultacji społecznych w procesie stanowienia prawa oraz możliwe trudności kadrowe ministerstwa w związku z nowymi ustawowymi obowiązkami. Rzecznik Praw Obywatelskich jest w trakcie analizowania stanowiska i sporządzania kolejnego wystąpienia do Ministra w omawianej sprawie.

RPO PRZESTRZEGA: PRZEPISY USTAWY O GRACH HAZARDOWYCH MOGĄ ZOSTAĆ WYKORZYSTANE DO BLOKOWANIA RÓŻNYCH TREŚCI W INTERNECIE

data: 2017-07-05

Do Rzecznika Praw Obywatelskich wpływają skargi dotyczące ustawy o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw, która w części dotyczącej blokowania stron internetowych weszła w życie dnia 1 lipca 2017 r. Skarżący wskazują na wątpliwości dotyczące zgodności z Konstytucją uchwalonych przepisów i obawiają się, że mechanizm blokowania stron internetowych będzie wykorzystywany w przyszłości również do innych celów.

Blokowanie dostępu do stron internetowych to środek, który ma uniemożliwić dostęp do określonej treści końcowemu użytkownikowi internetu. Ustawodawca w przypadku omawianej ustawy wybrał mechanizm blokowania, który ma być wykonywany przez przedsiębiorcę telekomunikacyjnego świadczącego usługi dostępu do sieci Internet. Tak ukształtowany mechanizm blokowania stron w internecie jest bez wątpienia rozwiązaniem, które stwarza poważne ryzyko dla wolności słowa i dostępu do informacji. Konstytucyjnie gwarantowana wolność słowa oznacza nie tylko możliwość swobodnego otrzymywania i przekazywania informacji, ale również jej aktywne poszukiwanie i zdobywanie. W art. 54 ust. 2 Konstytucji wprowadza się zaś zakaz cenzury prewencyjnej. Każde ograniczenie wolności słowa musi być zatem uzasadnione w sposób szczególny.

Rzecznik zauważył, że uchwalona ustawa o zmianie ustawy o grach hazardowych może budzić konstytucyjne i międzynarodowoprawne wątpliwości i zastrzeżenia, dotyczące przyjętych rozwiązań, w szczególności w kontekście uzasadnienia dla jej przyjęcia, niezbędności i proporcjonalności. W uzasadnieniu do ustawy nie odniesiono się do już istniejących mechanizmów walki z nielegalnymi treściami w internecie, nie wykazano zatem, że zakładany cel, jakim jest walka z hazardem, realizowany jest spójnie i systematycznie.

Problematyczna jest również kwestia tego, czy w istocie rejestr będzie narzędziem efektywnym zwłaszcza w związku z obiektywnymi trudnościami związanymi z blokowaniem nielegalnych treści znajdujących się na zagranicznych serwerach. Nie ma zatem pewności, że rozwiązanie osiągnie w istocie zamierzony przez ustawodawcę cel, polegający na ograniczeniu dostępu do treści szkodliwych.

Ponadto, ustawodawca poprzestał na wybraniu środka, jakim jest decyzja organu administracyjnego o wpisie do rejestru. Nie podążył zatem drogą ustawy o działaniach antyterrorystycznych, która do zablokowania dostępu do treści znajdujących się na stronie wymaga postanowienia sądu. Proponowany mechanizm prewencyjnego blokowania dostępu do stron oferujących

nielegalny hazard na mocy decyzji podejmowanej przez urzędnika państwowego może budzić sprzeciw. Istnieje bowiem zbyt duże ryzyko, że będzie to instrument nadużywany i będący poza kontrolą.

Rzecznik zwrócił się do Ministra z prośbą o ustosunkowanie się do powyższych wątpliwości dotyczących nowelizacji ustawy o grach hazardowych. Poprosił również o informację na temat pierwszych wniosków dotyczących jej stosowania oraz informację na temat ilości zablokowanych stron internetowych w trybie z niej wynikającym.

MINISTERSTWO CYFRYZACJI PO INTERWENCJI RPO PRZYPOMINA RESORTOWI SPRAWIEDLIWOŚCI: SERWISY INTERNETOWE PODMIOTÓW PUBLICZNYCH POWINNY BYĆ DOSTOSOWANE DO POTRZEB OSÓB Z NIEPEŁNOSPRAWNOŚCIAMI JUŻ OD 30 MAJA 2015 R.

data: 2017-07-05

Po interwencji Rzecznika Praw Obywatelskich Minister Cyfryzacji zwraca uwagę w piśmie do Ministra Sprawiedliwości, że systemy teleinformatyczne podmiotów realizujących zadania publiczne powinny zostać dostosowane do międzynarodowego standardu Web Content Accessibility Guidelines (WCAG 2.0) do dnia 30 maja 2015 r.

RPO skierował wystąpienie do Ministra Sprawiedliwości w związku z sygnałami o niedostosowaniu bazy internetowej Krajowego Rejestru Sądowego do potrzeb osób niewidzących.

RPO przypomniał, że przepisy o dostępności (w tym wymóg dotyczący WCAG 2.0) zawarte są w z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności … (Dz. U. z 2016 r. poz. 113). Weszło ono w życie 30 maja 2012 r., zaś serwisy internetowe podmiotów realizujących zadania publiczne dostały trzy lata na dostosowanie się do wymagań - te regulacje zaczęły obowiązywać 30 maja 2015 r.

Minister Sprawiedliwości nie podzielił jednak tej interpretacji. Uznał, że skoro baza Krajowego Rejestru Sądowego jest modernizowana, to wymóg dostępności dotyczyć jej będzie dopiero po zakończeniu tych prac – czyli w marcu 2018 r. Ministerstwo Cyfryzacji przypomina jednak, że czas na to był do 30 maja 2015 r.

Stanowisko Ministra Cyfryzacji może przyczynić się do szybszej realizacji obowiązku dostosowania portalu administrowanego przez Ministra Sprawiedliwości do potrzeb wszystkich użytkowników, w tym osób z niepełnosprawnością wzroku.

Czym jest dostępność i komu służy?

Istotą wymagań dotyczących dostępności jest to, by z serwisu powstałego z publicznych środków mógł korzystać każdy, w tym także osoba z dysfunkcją wzroku czy ruchu. Aby tak się stało, twórcy i redaktorzy stron muszą przestrzegać kilku podstawowych zasad, dzięki którym m.in.:

- z serwisu można korzystać także bez myszki (przy pomocy klawisza Tab, co jest ważne w przypadku kłopotów z ręką);
- zdjęcia i grafiki zaopatrywane są w alternatywne opisy tak, aby ich treść była dostępna dla osób niewidomych (ale także osób, które nie wyświetlają grafiki na przykład na urządzeniach mobilnych);
- informacje o strukturze tekstu (co jest tytułem, co śródtytułem) przekazywane są nie przy pomocy wielkości czy grubości czcionki (bo do tego trzeba mieć sprawny wzrok), ale dzięki wzorcowym tytułom podstron, porządkującej funkcji nagłówków oraz innym udogodnieniom wprowadzonym pod kątem czytników ekranów (w ten sposób osoba korzystająca z czytnika łatwo może poruszać się po serwisie).

Jedną z zasad wywodzących się z kultury dostępności (choć w Polsce nie obwarowana prawne) jest zasada, by teksty pisać w sposób zrozumiały dla jak najszerszej rzeszy odbiorców – w tym osób bez wykształcenia specjalistycznego, starszych czy znających język polski w stopniu ograniczonym (cudzoziemców, ale też Polaków z dysfunkcją słuchu, dla których język polski jest drugim po migowym językiem).

WYSTĄPIENIE DO MINISTER CYFRYZACJI W SPRAWIE NOWYCH UNIJNYCH PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

data: 2017-06-20

Rzecznik Praw Obywatelskich z uwagą obserwuje proces przygotowywania oraz wdrażania reformy systemu ochrony danych osobowych w UE od 2012 r., czyli od przedstawienia pierwszych wersji projektów aktów prawnych Unii Europejskiej w tym zakresie.

Reforma - rozporządzenie unijne - wejdzie w życie w przyszłym roku, została wypracowana wspólnie przez wszystkie państwa Unii, w tym Polskę, która w tym procesie brała bardzo aktywny udział. Istotą zmiany jest to, że nie tylko uwzględnia ona zmiany związane z rozwojem technologii cyfrowych, ale także wprowadza jednolite zasady dla całej Unii Europejskiej (dotychczas każdy kraj, a nawet land miał swoje odrębne regulacje).

Ze względu na wagę reformy RPO na bieżąco analizuje wszystkie informacje, raporty ze spotkań, czy doniesienia medialne dotyczące prac przygotowawczych do stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia o dyrektywy 95/46/WE (dalej jako: rodo).

Publicznie informacje, m.in. na stronach internetowych Ministerstwa Cyfryzacji oraz Generalnego Inspektora Ochrony Danych Osobowych, nie usuwają jednak wszystkich wątpliwości, jakie w tej sprawie się pojawiają.

Z udostępnionego przez resort cyfryzacji projektu ustawy o ochronie danych osobowych wynika jasno, że w planach jest utworzenie nowego organu ochrony danych osobowych. Projekt przewiduje zmianę nazwy organu – z dotychczasowego Generalnego Inspektora Ochrony Danych Osobowych – na Prezesa Urzędu Ochrony Danych Osobowych, lecz nie zawiera propozycji przepisów ustrojowych, dotyczących przyszłej instytucji odpowiedzialnej za ochronę danych osobowych.

Oprócz kwestii praw podmiotów danych, całego systemu dochodzenia praw przez jednostkę, szczególne znaczenie – ze względu na konieczność zapewnienia efektywnego systemu ochrony danych osobowych – Rzecznik przywiązuje do kwestii funkcjonowania niezależnego organu ochrony danych osobowych. Przepisy ustrojowe w powyższym zakresie powinny być zatem przygotowane jak najszybciej. Państwo zobowiązane jest zagwarantować organowi prawną możliwość wykonywania określonych zadań w sposób wolny od ingerencji ze strony innych podmiotów. Niezależne organy ochrony danych osobowych są strażnikami prawa do ochrony danych osobowych, a ich funkcjonowanie w państwach członkowskich UE jest niezbędnym ogniwem systemu ochrony jednostek w związku z przetwarzaniem ich danych.

Należy przy tym zaznaczyć, że nawet potencjalny polityczny wpływ innych organów może skutkować zaistnieniem po stronie organu ochrony danych osobowych tzw. „przewidywanego posłuszeństwa" (ang. prior compliance). Brak pewności co do przyszłości organu i obsługującego go urzędu może wywoływać skutki, które wiązać się będą z ograniczeniem jego niezależności. Sytuacja, w której sam organ nie ma jasności co do przyszłości, a przepisy tworzone są bez odpowiednich konsultacji, nie może być oceniona jako prawidłowa w kontekście przepisów zarówno obowiązującej nadal dyrektywy 95/46/WE, jak i przepisów rodo. Konieczne jest, by organ ochrony danych osobowych miał możliwość wywarcia wpływu na proponowane rozwiązania, a także by mógł podjąć działania, które umożliwią mu prawidłowe funkcjonowanie w momencie rozpoczęcia stosowania nowych przepisów.

Rzecznik zwrócił się do Minister z prośbą o dodatkowe informacje w sprawie planów co do pozycji ustrojowej organu ochrony danych osobowych w związku z wejściem w życie rodo, stosowaniem rodo do kościołów i związków wyznaniowych oraz koniecznością wdrożenia dyrektywy policyjnej.

NIŻSZY VAT NA E-BOOKI JUŻ WKRÓTCE? PARLAMENT EUROPEJSKI PRZEGŁOSOWAŁ NOWELIZACJĘ DYREKTYWY

data: 2017-06-06

W niedawnym wyroku Trybunał Sprawiedliwości UE potwierdził, że w świetle obowiązujących przepisów prawa UE nie ma możliwości zastosowania obniżonej stawki VAT na publikacje elektroniczne (sprawa C-390/15 RPO). Obowiązuje bowiem dyrektywa 2006/112/WE, która w tym zakresie pozostawia prawodawcy UE szeroki margines uznania, dopuszczając zróżnicowanie stawek na publikacje tradycyjne i elektroniczne. Zgodnie z obowiązującym brzmieniem dyrektywy sprzedaż książek elektronicznych jest usługą, a sprzedaż książek papierowych regulowana jest jak sprzedaż towarów, stąd zróżnicowanie stawek VAT, także w Polsce, gdzie książki papierowe oraz audiobooki (tzw. książki na nośnikach fizycznych) obłożone są w Polsce stawką obniżoną (5%), a książki elektroniczne (e-booki) – stawką podstawową wynoszącą 23%.

To jednak nie wyklucza zmian w prawie wtórnym UE, które zostały podjęte przez Komisję Europejską. Już od początku 2016 roku w Komisji Europejskiej trwały prace nad nowelizacją dyrektywy dotyczącej VAT (2006/112/WE) i m.in. zrównaniem stawek VAT dla książek na nośnikach fizycznych i e-booków.

Wniosek w sprawie zmiany dyrektywy 2006/112/WE w odniesieniu do stawek podatku od wartości dodanej stosowanego do książek, gazet i czasopism (COM (2016) 758 final) został przyjęty przez Komisję Europejską dnia 1 grudnia 2016 roku i następnie skierowany do uzgodnień w Radzie i Parlamencie Europejskim. W maju 2017 r. projekt zaakceptowała Komisja Gospodarcza i Monetarna Parlamentu Europejskiego. W I czytaniu, które odbyło się 1 czerwca 2017 roku, Parlament Europejski przyjął propozycję nowelizacji dyrektywy z nielicznymi poprawkami stosunkiem głosów: 590 za, 8 przeciw i 10 wstrzymujących. Parlament Europejski zauważył, że obniżonej stawki podatku VAT nie można stosować do publikacji dostarczanych drogą elektroniczną, które podlegają podstawowej stawce VAT, co stawia publikacje dostarczane drogą elektroniczną w niekorzystnej sytuacji oraz hamuje rozwój tego rynku. Ta niekorzystna sytuacja może z kolei utrudnić rozwój gospodarki cyfrowej w Unii. Zgodnie ze strategią jednolitego rynku cyfrowego oraz z określonym w niej celem, aby Europa była konkurencyjna w kontekście globalnym i by była światowym liderem gospodarki cyfrowej, należy umożliwić państwom członkowskim dostosowanie stawek

VAT na publikacje dostarczane drogą elektroniczną do niższych stawek VAT na publikacje dostarczane na wszystkich nośnikach fizycznych, a tym samym pobudzić innowacje, zachęcić do tworzenia i produkowania nowych treści oraz inwestowania w nie, a także wesprzeć cyfrowe uczenie się, transfer wiedzy oraz dostęp do kultury w środowisku cyfrowym oraz jej promocję. Możliwość zastosowania przez państwa członkowskie obniżonej, nadzwyczajnie obniżonej lub zerowej stawki podatkowej w odniesieniu do publikacji drukowanych i publikacji elektronicznych powinna doprowadzić do transferu korzyści ekonomicznych na konsumentów, a tym samym promocji czytelnictwa, a także na wydawców, których zachęci do inwestycji w nowe treści, a w przypadku gazet i czasopism – zmniejszy zależność od reklamodawców.

To nie oznacza jeszcze końca procesu legislacyjnego, bowiem projekt powinien jeszcze zostać przyjęty przez ministrów zasiadających w Radzie Unii Europejskiej. Wydaje się jednak, że wkrótce do tego dojdzie i na forum UE może zostać ostatecznie przyjęta dyrektywa zmieniająca dyrektywę 2006/112/WE. To będzie oznaczać, że państwa członkowskie będą mogły obłożyć publikacje elektroniczne preferencyjnymi stawkami: 5% lub 0%. Tym samym nowelizacja dyrektywy umożliwi państwom członkowskim wyeliminowanie nierównego traktowania, nie likwiduje ona jednak potrzeby zapewnienia bardziej skoordynowanego, efektywnego i prostszego systemu obniżonych stawek VAT, przewidującego mniejszą liczbę wyjątków.

Należy podkreślić, że Rzecznik Praw Obywatelskich był inicjatorem postępowania przed Trybunałem Konstytucyjnym (sprawa K 61/13), w sprawie obniżenia stawki VAT na e-booki w świetle możliwego charakteru dyskryminującego obecnie funkcjonujących przepisów, dlatego tym bardziej z satysfakcją przyjął wiadomość o postępujących pracach legislacyjnych w tej materii na szczeblu unijnym. RPO wyraził głęboką nadzieję, że zmiany te zostaną szybko i sprawnie implementowane do krajowych porządków prawnych, a tym samym, biorąc pod uwagę fakt, że prace prawodawcze w Unii Europejskiej mające na celu zrównanie stawek VAT dla książek na nośnikach fizycznych i e-booków są w toku, zdecydował się wnieść o umorzenie postępowania w sprawie K 61/13, co nastąpiło postanowieniem Trybunału Konstytucyjnego z 17 maja 2017 r.

WDRAŻANIE KODEKSU POSTĘPOWANIA DOTYCZĄCEGO NIELEGALNEGO NAWOŁYWANIA DO NIENAWIŚCI W INTERNECIE. USUWANIE MOWY NIENAWIŚCI Z INTERNETU MOŻE BYĆ SKUTECZNIEJSZE

data: 2017-06-01

Rzecznik Praw Obywatelskich z zadowoleniem odnotowuje pozytywne efekty wdrażania Kodeksu postępowania dotyczącego nielegalnego nawoływania do nienawiści w internecie z 31 maja 2016 r.

W świetle najnowszych danych, 59% zawiadomień skierowanych do największych platform społecznościowych spowodowało usunięcie nienawistnych treści, przy 28% skuteczności stwierdzonej w poprzednim badaniu. Wciąż migranci i uchodźcy stanowią najczęstszy cel ataku:

- **17,8%** **zawiadomień dotyczyło wypowiedzi o charakterze ksenofobicznym,**
- **17,7%** **- muzułmanów**
- **15,8%** **- pochodzenia etnicznego.**

Dodatkowo, dosyć wysoki wskaźnik odnosi się do mowy nienawiści motywowanej uprzedzeniami wobec osób LGBT (12,7% zawiadomień).

Połowa (51,4%) zgłoszeń była oceniona w terminie przyjętym w Kodeksie, czyli w ciągu 24 godzin, co wciąż jest wskaźnikiem poniżej oczekiwań.

W Biurze Rzecznika Praw Obywatelskich 27 stycznia 2017 r. odbyła się konferencja mająca na celu upowszechnienie w Polsce ww. Kodeksu.

Komisja Europejska przedstawiła 1 czerwca 2017 r. raport z drugiej rundy monitoringu realizacji Kodeksu postępowania dotyczącego nielegalnego nawoływania do nienawiści w internecie, który wskazuje na pozytywne zmiany w porównaniu do stanu przedstawionego w podobnym raporcie z grudnia 2016 r.

Według badań przeprowadzonych wiosną 2017 r. w 24 państwach członkowskich Unii Europejskiej, tym razem także w Polsce, nastąpiła znacząca poprawa w zakresie sposobu i tempa reagowania przez największe platformy społecznościowe – Facebook, Twitter, YouTube – na zgłoszenia dotyczące nielegalnej mowy nienawiści.

Ten rezultat osiągnięty został dzięki wzmocnieniu wewnętrznych procedur, szkoleniom pracowników oraz lepszej współpracy z organizacjami pozarządowymi, w szczególności posiadającymi status zaufanego podmiotu zgłaszającego.

Komisja Europejska zaznaczyła, że pomimo poprawy konieczne jest dalsze doskonalenie rozwiązań dotyczących zawiadamiania i reagowania przez pośredników internetowych na zgłoszenia, na co wskazuje także raport z przeglądu unijnej Strategii na rzecz Jednolitego Rynku Cyfrowego.

Wskazane jest określenie minimalnych wymogów dotyczących zawartości tego rodzaju zgłoszeń, trybu wnoszenia do nich zastrzeżeń, obowiązków sprawozdawczych, mechanizmów konsultacji z podmiotami trzecimi oraz systemów rozwiązywania sporów.

Niezwykle istotne jest ponadto zapewnienie współpracy pomiędzy przedsiębiorstwami z branży IT a organami państwowymi. Dlatego zalecono utworzenie odpowiedniego punktu kontaktowego. Rzecznik zwracał się do Ministra Cyfryzacji oraz Ministra Spraw Wewnętrznych i Administracji o podjęcie działań m.in. w tym zakresie.

Świadomość rosnącej odpowiedzialności portali internetowych za udostępniane treści o charakterze nielegalnej mowy nienawiści, potwierdzanej w orzecznictwie sądowym (zob. wyrok Wielkiej Izby ETPCz w sprawie Delfi przeciwko Estonii, czy wyrok SN w sprawie o sygn. akt I CSK 598/15), przyczynia się do większej aktywności w zakresie reagowania przez nie na to negatywne zjawisko.

Rzecznik Praw Obywatelskich apeluje do wszystkich użytkowników internetu nie tylko o kierowanie zawiadomień o treściach, które należy usunąć, ale także o wzmocnienie pozytywnego przekazu dotyczącego różnych grup mniejszościowych, w celu eliminowania dotyczących ich stereotypów i uprzedzeń będących źródłem mowy nienawiści.

MINISTERSTWO EDUKACJI NARODOWEJ ODPOWIADA RZECZNIKOWI W SPRAWIE BEZPIECZEŃSTWA CYFROWEGO DZIECI I MŁODZIEŻY

data: 2017-05-23

Ministerstwo Edukacji Narodowej skierowało pismo do dyrektorów szkół i nauczycieli w związku z doniesieniami medialnymi dotyczącymi niebezpiecznej gry internetowej Niebieski Wieloryb. W piśmie tym sformułowano prośbę o zorganizowanie spotkań z rodzicami i uczniami, podczas których możliwe będzie omówienie kwestii dotyczących bezpiecznego korzystania z zasobów internetu przez uczniów. Takie spotkania niewątpliwie należy uznać za potrzebne. Rzecznik skierował do MEN wystąpienie, w którym wskazał, że podczas takich spotkań warto też podnieść kwestię bardzo szczególnej formy aktywności internetowej, jaką są media społecznościowe, takie jak Facebook, Instagram, czy Snapchat, które stanowią coraz istotniejszy element codziennego życia dzieci i młodzieży. Korzystanie z nich wiąże się także ze specyficznymi rodzajami zagrożeń, np. kontaktem z mową nienawiści, czy rozprzestrzenianiem się niebezpiecznych zachowań, takich jak te związane z uczestnictwem w grach-wyzwaniach, których przykładem jest Niebieski Wieloryb.

Za bardzo istotny należy uznać również podniesiony w piśmie MEN wątek gier komputerowych i wiążącego się z nimi systemu kategoryzacji wiekowej PEGI. Z treści raportu „Branża rozrywki elektronicznej" w Polsce opublikowanego przez Krajową Izbę Gospodarki Cyfrowej w 2015 roku wynika, że znajomość tego systemu wśród rodziców nie jest duża. Dane opublikowane w raporcie wskazują, że rodzice co do zasady mają świadomość istnienia tego systemu i poszczególnych kategorii wiekowych. Znacznie mniejsza jest jednak znajomość poszczególnych oznaczeń piktograficznych odnoszących się do treści zawartych w grach. Należy mieć na uwadze, że rodzice często mają znacznie mniejszą wiedzę o rodzajach gier komputerowych i zawartych w nich treściach niż ich dzieci. Dlatego bardzo pozytywnie należy ocenić zawarty w piśmie MEN postulat upowszechniania wśród rodziców wiedzy o systemie PEGI. W ocenie Rzecznika warto byłoby położyć większy nacisk na upowszechnienie tego systemu i udzielać rodzicom możliwie szczegółowych informacji na jego temat.

Ministerstwo Edukacji Narodowej przedstawiło Rzecznikowi szczegółowe informacje o działaniach podejmowanych na rzecz zwiększenia poziomu bezpieczeństwa dzieci i młodzieży w internecie. Warto zwrócić uwagę na zrealizowany pod patronatem MEN projekt pn. „Działania na rzecz bezpiecznego korzystania z Internetu", w ramach którego powstało opracowanie „Standard bezpieczeństwa online placówek oświatowych". Publikacja ta zawiera, m.in. wytyczne w zakresie postępowania z agresją występującą w internecie. Materiał jest dostępny na stronach internetowych programu „Bezpieczna i przyjazna szkoła" i może być nieodpłatnie pobierany przez wszystkich zainteresowanych.

W świetle wyników badań wskazujących na niewystarczający poziom kompetencji cyfrowych rodziców uczniów kierowanie do nich działań o charakterze edukacyjno-informacyjnym poświęconych bezpieczeństwu w cyberprzestrzeni powinno stanowić integralny element statutowej działalności szkoły. Istotne wsparcie dla szkół w tym zakresie zapewnia „Rządowy program wspomagania w latach 2015-2018 organów prowadzących szkoły w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w szkołach Bezpieczna+". Jednym z celów tego programu jest poprawa kompetencji pracowników szkoły, uczniów i ich rodziców w zakresie bezpiecznego korzystania z przestrzeni internetowej oraz reagowania na zagrożenia.

Rzecznik pozytywnie ocenia działania podejmowane przez MEN i w dalszym ciągu monitoruje stan bezpieczeństwa cyfrowego dzieci i młodzieży.

DOSTĘP POLICJI DO DANYCH TELEKOMUNIKACYJNYCH I INTERNETOWYCH. JAK POLSKA ZAREAGUJE NA WAŻNY WYROK TRYBUNAŁU SPRAWIEDLIWOŚCI UE? – ODPOWIEDŹ MSWIA

data: 2017-05-05

Z ewentualną zmianą przepisów ustawy inwigilacyjnej MSWiA poczeka na orzeczenie Trybunału Konstytucyjnego w sprawie K 9/16 – wynika z odpowiedzi udzielonej przez resort Rzecznikowi Praw Obywatelskich

Rzecznik pytał się o zmianę przepisów o retencji, bowiem 21 grudnia 2016 r. Trybunał Sprawiedliwości UE wydał wyrok w tzw. sprawie Tele 2, który - w ocenie Rzecznika Praw Obywatelskich - powinien mieć znaczenie dla wykładni przepisów krajowych członkowskich państw takich jak Polska, które po wyroku TSUE z 2014 r. w tzw. sprawie DRI (C-293/12 i C-594/12) nie zmieniły swoich przepisów o retencji danych. Już w 2014 r. TSUE stwierdził nieważność tzw. dyrektywy retencyjnej, która regulowała te zagadnienia na poziomie całej Unii Europejskiej. Chodzi o przepisy, które nakładają na operatorów telekomunikacyjnych obowiązek przechowywania danych abonentów i udostępniania ich właściwym służbom na potrzeby prowadzonych postępowań (to m.in. o bilingi i dane lokalizacyjne, które w Polsce trzeba przechowywać przez rok od chwili połączenia). W 2016 r. w sprawie Tele 2 TSUE doprecyzował, że przedmiotem oceny pod kątem zgodności z prawem UE muszą być nie tylko przepisy nakładające na operatorów telekomunikacyjnych obowiązki związane z retencją danych, ale również te przepisy, które regulują dostęp właściwych służb do tych danych, takie jak np. ustawa inwigilacyjna.

W związku z wyrokiem w sprawach połączonych C-203/15 i C-698/15 w sprawie Tele2, RPO wystąpił 1 lutego 2017 r. z pytaniem m.in. do Ministra Spraw Wewnętrznych i Administracji o stanowisko w sprawie zgodności ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (tzw. ustawy inwigilacyjnej) z przepisami Karty Praw Podstawowych.

5 kwietnia RPO dostał odpowiedź, w której sekretarz stanu Jarosław Zieliński informuje, że trudno jest obecnie przesądzić o konieczności i konkretnym kierunku ewentualnych prac legislacyjnych. Zagadnienie pozyskiwania danych telekomunikacyjnych przez właściwe służby „nie wydaje się bowiem jednoznaczne nie tylko w ujęciu faktycznym (wpływ na bezpieczeństwo publiczne i możliwość realizacji podstawowych funkcji państwa w tym zakresie)”.

MSWiA wskazuje zatem na konieczność oczekiwania na stanowisko Trybunału Konstytucyjnego w sprawie K 9/16, zainicjowanej m.in. wnioskiem RPO (wniosek dotyczący tzw. ustawy inwigilacyjnej), również w związku z tym, że - zdaniem MSWiA - Trybunał Konstytucyjny dotychczas dopuszczał tzw. następczą kontrolę gromadzonych danych (sprawa K 23/11).

MSWiA poinformowało również o przedstawieniu do uzgodnień międzyresortowych projektu ustawy o zmianie ustawy o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do sprawę wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra oraz niektórych innych ustaw.

Zdaniem MSWiA projekt ten zakłada urealnienie standardu cywilnego nadzoru nad umundurowanymi służbami porządku publicznego.

W załączeniu do odpowiedzi przekazano również kopię Wytycznych w sprawie realizacji przez Policję i Straż Graniczną obowiązków dotyczących przekazywania do sądu sprawozdania w zakresie uzyskiwania danych telekomunikacyjnych, pocztowych i internetowych oraz prowadzenia elektronicznego rejestru.

RPO PYTA MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI O ZMIANY W USTAWIE O POLICJI

data: 2016-10-10

Na posiedzeniu plenarnym w dniach 10-11 czerwca 2016 r. Europejska Komisja na rzecz Demokracji przez Prawo (tzw. Komisja Wenecka) przyjęła opinię w sprawie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw. Analiza dotyczyła przede wszystkim: zasad dostępu Policji do danych telekomunikacyjnych, pocztowych i internetowych, podmiotów, których dane mogą być zbierane zgodnie z ustawą, a także gwarancji proceduralnych zabezpieczających przed nadużyciami, a w szczególności kwestii nadzoru nad zbieraniem i przetwarzaniem danych w związku ze zwalczaniem przestępczości w kraju.

Według Komisji Weneckiej wspomniana ustawa w znacznym stopniu realizuje rekomendacje i zalecenia płynące z wyroku Trybunału Konstytucyjnego, jednocześnie jednak Komisja wykazała szereg braków, które ustawodawca powinien naprawić.

Chodzi tu m.in. o sprecyzowanie i ograniczenie bardzo szerokiego dostępu do danych telekomunikacyjnych, pocztowych i internetowych, który nie spełnia wymogu przewidywalności ingerencji w prawo do prywatności chronione przez Europejską Konwencję Praw Człowieka. Ponadto przepisy powinny doprecyzować, w jakich sytuacjach możliwe jest korzystanie z tych danych, gdy istnieją inne, mniej inwazyjne środki. Zdaniem Komisji mechanizm kontroli pozyskiwania informacji oparty o sądy jest niewystarczający. W analizie znalazła się propozycja wprowadzenia do polskiego prawa instytucji niezależnego od organów ścigania pełnomocnika, którego zadaniem będzie obrona interesów osoby inwigilowanej. Podobne rozwiązania funkcjonują w różnych państwach Europy. Komisja wskazała też, że w polskich przepisach brakuje mechanizmu informowania osoby poddanej inwigilacji – po jej zakończeniu - o fakcie jej prowadzenia. Prawo powinno również przewidywać jakąś formę następczej kontroli legalności przeprowadzonej kontroli np. poprzez możliwość złożenia skargi. Podobne wnioski dotyczące nadzoru nad organami zbierającymi dane o osobach w ramach zwalczania przestępczości tj. służbami działającymi w kraju oraz poza jego granicami, płyną z raportu Agencji Praw Podstawowych Unii Europejskiej (FRA). W opracowaniu szczególny nacisk położono na mechanizmy kontroli i środki odwoławcze przysługujące jednostkom, których prawo do prywatności zostało naruszone. Ma to zapobiec nadużywaniu uprawnień przez służby i zwiększyć zakres odpowiedzialności za podejmowane działania. Rzecznik zwrócił się z prośbą o informacje dotyczące działań podjętych w związku z opinią Komisji Weneckiej oraz wskazanie, czy rozważana jest możliwość dokonania zmian ustawowych w zakresie nadzoru nad służbami policyjnymi, czy służbami ochrony państwa.

SKARGA KASACYJNA RPO DOTYCZĄCA ODPOWIEDZIALNOŚCI OSOBY PROWADZĄCEJ PORTAL INTERNETOWY ZA WPISY NARUSZAJĄCE DOBRA OSOBISTE

data: 2016-08-02

Rzecznik wniósł do Sądu Najwyższego skargę kasacyjną w sprawie o naruszenie dóbr osobistych przez wpis na portalu założonym i prowadzonym przez osobę fizyczną w ramach jednego z serwisów społecznościowych.

Sądy przypisały prowadzącemu portal odpowiedzialność za wpisy, wskazując jako podstawę prawną przepisy o naruszeniu dóbr osobistych oraz ustawę o świadczeniu usług drogą elektroniczną.

Tymczasem zdaniem Rzecznika podstawa prawna w tego typu przypadkach (gdy administratorem strony jest osoba fizyczna nie będąca przedsiębiorcą) nie jest jednoznaczna. Dlatego też w skardze kasacyjnej Rzecznik wskazał na istotne zagadnienie prawne:

Czy osoba fizyczna, niebędąca przedsiębiorcą w rozumieniu Kodeksu cywilnego, a udostępniająca innym w sieci miejsce do wyrażania poglądów, w ramach założonego portalu społecznościowego, jest:

- usługodawcą w rozumieniu ustawy o świadczeniu usług drogą elektroniczną (art. 2 ust. 1, Dz. U. z 2013 r., poz. 1422 ze zm.) i odpowiada za treści umieszczone na prowadzonej przez nią stronie na podstawie przepisów Kodeksu cywilnego o naruszeniu dóbr osobistych (art. 24 K.c).
- czy osobą pośredniczącą w przekazywaniu postów, albo pomagającą w ich rozpowszechnieniu i odpowiada za treści umieszczone na prowadzonym przez siebie portalu w związku z obowiązkiem naprawienia szkody wynikającym z przepisów Kodeksu cywilnego (art. 415 lub 422 K.c.)?

KOMENDANT GŁÓWNY POLICJI ODPOWIADA W SPRAWIE UCIĄŻLIWOŚCI ZWIĄZANYCH Z ZABEZPIECZANIEM SPRZĘTU KOMPUTEROWEGO NA POTRZEBY POSTĘPOWANIA

data: 2016-07-29

Osoby zwracające się do Rzecznika wskazują na uciążliwości związane z zabezpieczeniem przez Policję urządzeń zawierających dane informatyczne na potrzeby postępowania karnego. RPO zwrócił się w sprawie tego problemu do Komendanta Głównego Policji i Ministra Sprawiedliwości.

Dotyczy to zwłaszcza postępowań prowadzonych w sprawach o przestępstwa z art. 116 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (j.t. Dz.U.2006.90.631 z późniejszymi zmianami), polegające na nieuprawnionym udostępnianiu za pośrednictwem internetu cudzych utworów np. w postaci filmów.

Ludzie piszą do RPO, że w związku z postępowaniami przygotowawczymi dotyczącymi przestępstw w cyberprzestrzeni zabezpieczany jest cały sprzęt komputerowy wraz z zawartymi w nim nośnikami danych. Zatrzymanie sprzętu komputerowego najdującego się w domu (np. laptopa, komputera, telefonu komórkowego) powoduje, że m.in. nie mogą wykonywać pracy, nie mają dostępu do kont bankowych, nie mogą utrzymywać kontaktu z innymi osobami. Ponadto, pozbawieni są dostępu do swoich prywatnych dokumentów, zdjęć, plików – stanowiących często dane wrażliwe. Sprzęt ten niejednokrotnie służy także dzieciom do nauki. Jako szczególnie uciążliwe wskazywane jest to, że w wyniku zatrzymania omawianych urządzeń niedogodności takie trwają kilka miesięcy a nawet dłużej.

W odpowiedzi nadinsp. dr Jarosław Szymczyk wskazał, że zgodnie z przepisami Kodeksu postępowania karnego celem postępowania przygotowawczego jest m.in. zebranie, zabezpieczenie i w niezbędnym zakresie utrwalenie dowodów dla sądu, co może się wiązać z koniecznością zatrzymania sprzętu komputerowego. Podkreślił, że ustawodawca nie przewiduje odrębnych procedur wobec zabezpieczenia urządzeń zawierających dane informatyczne.

Odnosząc się do kwestii uciążliwości związanych z zabezpieczaniem sprzętu komputerowego, Komendant zaznaczył, że Policja stara się korzystać z możliwości wykonywania kopii danych zawartych na informatycznych nośnikach. Jednakże każdy przypadek należy rozpatrywać indywidualnie, a poszczególne decyzje o sposobie zabezpieczania dowodów są konsultowane z nadzorującymi czynności prokuratorami.

Natomiast sama ocena sposobu, w jaki dane informatyczne zostaną zabezpieczone zależy zwykle od kilku czynników:

- możliwości technicznych osób realizujących zabezpieczenie,
- parametrów technicznych nośników danych znajdujących się w miejscu prowadzenia czynności procesowych (wzrost pojemności nośników postępuje zdecydowanie szybciej niż możliwe do osiągnięcia prędkości ich kopiowania za pomocą odpowiednich narzędzi. W konsekwencji wykonanie procesowych kopii kilku nośników o dużej pojemności może trwać nawet dziesiątki godzin, a w przypadku ich uszkodzeń, nawet kilka dni),
- sposobu zabezpieczenia dostępu do danych zawartych na nośnikach (niektóre rozwiązania wykorzystują do szyfrowania zawartości dysków moduł sprzętowy, umiejscowiony na płycie głównej komputera – poza nośnikiem danych. Odszyfrowanie danych jest możliwe tylko za pomocą modułu, który je zaszyfrował, więc zabezpieczony musi zostać cały komputer).

Jednocześnie nadinsp. dr Jarosław Szymczyk zadeklarował, że Policja będzie starała się, aby czynności zabezpieczania cyfrowego materiału dowodowego były jak najmniej uciążliwe.

MOŻLIWOŚĆ SKŁADANIA PODPISÓW POD OBYWATELSKĄ INICJATYWĄ LEGISLACYJNĄ DROGĄ ELEKTRONICZNĄ – MINISTER CYFRYZACJI POPIERA POSTULAT RPO

data: 2016-07-20

Od wielu lat Rzecznik Praw Obywatelskich w swoich działaniach zwraca szczególną uwagę na właściwe funkcjonowanie obywatelskiej inicjatywy ustawodawczej. Jest to bardzo ważny mechanizm demokratycznego państwa prawnego. Prawo do obywatelskiej inicjatywy ustawodawczej jest przyznane obywatelom przez art. 118 ust. 2 Konstytucji RP oraz regulowane przez ustawę z dnia 24 czerwca 1999 r. o wykonywaniu inicjatywy ustawodawczej przez obywateli (Dz.U. nr 62, poz. 688 ze zm.).

31 maja 2016 roku Rzecznik Praw Obywatelskich skierował wystąpienie do Prezesa Rady Ministrów, w którym wskazał potrzebę rozważenia wprowadzenia przepisów, które umożliwiałyby obywatelom składanie podpisów pod obywatelską inicjatywą legislacyjną - drogą elektroniczną.

Rzecznik podkreślił, że wykorzystanie nowoczesnych technologii, jako mechanizmu elektronicznego zbierania poparcia pod

inicjatywą, mogłoby wpłynąć na wzrost udziału obywateli w życiu publicznym. Zdaniem Rzecznika każda forma ułatwienia obywatelom udziału w bezpośrednim kształtowaniu państwa, jest warta analizy.

W odpowiedzi udzielonej Rzecznikowi 4 lipca 2016 r., Minister Cyfryzacji – Anna Streżyńska stwierdziła, że „inicjatywa, zmierzająca do zapewnienia możliwości składania podpisów drogą elektroniczną w ramach obywatelskiej inicjatywy legislacyjnej, jest możliwa do realizacji i zasługuje na poparcie".

Jednocześnie zauważyła, że „waga oraz charakter podejmowanego zagadnienia są nad wyraz istotne i wymagają szczególnej analizy pod kątem procesów składających się na realizację czynności związanych z przygotowaniem projektu ustawy, jego rozpowszechnianiem, kampanią promocyjną, a także techniczną organizacją zbierania podpisów obywateli popierających projekt, które wymagają informatyzacji w świetle postulatu Rzecznika".

RPO będzie kontynuował działania mające na celu wprowadzenie ułatwień w procedurach wykonywania inicjatywy ustawodawczej przez obywateli.

dr Jarosław Zbieranek, Zespół Prawa Konstytucyjnego, Międzynarodowego i Europejskiego BRPO:

Rzecznik monitoruje sposób funkcjonowania prawa do obywatelskiej inicjatywy ustawodawczej. Podejmuje w tym zakresie badania i analizy. Zwraca szczególną uwagę, by usunąć wszelkie bariery, jakie mogą napotkać obywatele w realizowaniu swoich praw. Stara się również wspierać wprowadzenie nowych rozwiązań, które mogą przyczynić się do ich bardziej efektywnego stosowania, czego przykładem jest postulat umożliwienia obywatelom składania podpisów pod obywatelską inicjatywą legislacyjną drogą elektroniczną. Warto podkreślić, że koncepcja ta została wypracowana przez organizacje społeczne, a wiodącą rolę odegrał Instytut Spraw Obywatelskich.

RZECZNIK PRAW OBYWATELSKICH SKARŻY USTAWĘ ANTYTERRORYSTYCZNĄ DO TRYBUNAŁU KONSTYTUCYJNEGO

data: 2016-07-11

Ustawa antyterrorystyczna jest sprzeczna z Konstytucją, Kartą Praw Podstawowych Unii Europejskiej oraz Konwencją o ochronie praw człowieka i podstawowych wolności – 11 lipca Rzecznik Praw Obywatelskich zaskarżył ustawę do Trybunału Konstytucyjnego.

100-stronicowy dokument Rzecznika przedstawia argumenty za ułomnością poszczególnych przepisów. Pokazuje, że choć ustawa miała szczytny cel - uporządkowanie przepisów i wzmocnienie bezpieczeństwa w kraju, to napisana została tak nieprecyzyjnie i ogólnie, że służby specjalne otrzymały ogromne i niekontrolowane uprawnienia, a ludzie nie mogą mieć pewności, że nie będą na tej podstawie ścigani. Ustawa nie pozwala bowiem zrozumieć np., o kim i z jakiego powodu można zbierać informacje, kogo i za co można aresztować, czy kiedy można odciąć internet.

Rzecznik podkreśla, że jednym z powodów tego stanu był pośpieszny tryb prac i nieuwzględnienie istotnych uwag zgłaszanych przez ekspertów i organizacje społeczne.

„Tryb procedowania ustawy nie był adekwatny do powagi celu ustawy. Zagwarantowanie fundamentalnej wartości, jaką jest bezpieczeństwo publiczne, powinno wiązać się bowiem z szeroką dyskusją na temat kierunków zmian, konkretnych zagrożeń i sposobu reagowania na nie" – stwierdza Adam Bodnar.

To dlatego Rzecznik Praw Obywatelskich alarmował Prezydenta RP, by przed podpisaniem tej ustawy skierował ją do sprawdzenia do Trybunału Konstytucyjnego. Tak się jednak nie stało i ustawa weszła już w życie. A 11 lipca Rzecznik otrzymał odpowiedź z Kancelarii Prezydenta podpisaną przez podsekretarz stanu Annę Surówkę-Pasek, że „wskutek niekwestionowanych zagrożeń międzynarodowym terroryzmem poprawa stanu bezpieczeństwa Polski (…) stała się niezbędna i z tego powodu Prezydent RP podpisał ustawę".

RPO: Cele ustawy są słuszne

Rzecznik Praw Obywatelskich wielokrotnie podkreślał, że efektywność działania państwa w zakresie nie tylko reagowania, ale także przeciwdziałania zagrożeniom jest szczególnie istotna w warunkach globalizacji przestępczości. Demokratyczne państwo prawne nie może ignorować rosnącego znaczenia nowych technologii, skali ich wykorzystywania, niekiedy również w celu naruszania prawa.

Dlatego służby muszą być wyposażone w stosowne uprawnienia, muszą mieć warunki finansowe i organizacyjne do efektywnej walki z naruszeniami prawa.

Jak chronić bezpieczeństwo nie grożąc wolności?

Ponieważ jednak działania organów ścigania oraz służb specjalnych, zwłaszcza te, które realizowane są w warunkach niejawności, pozostają w naturalnym konflikcie z niektórymi prawami podstawowymi człowieka (prawem do prywatności, wolnością komunikowania się, ochroną autonomii informacyjnej, a także konstytucyjną gwarancją sądowej ochrony praw

jednostki), problem, jak to dobrze uregulować prawnie, jest przedmiotem prac prawników w całym demokratycznym świecie.

Dlatego jest wiele wzorów, w tym dokumentów międzynarodowych, które mogą być w tym względzie inspiracją – przypomina RPO.

Chodzi bowiem nie tylko o to, by państwo zapewniło bezpieczeństwo, lecz by hasłem walki z terroryzmem nie ingerowało w prawa i wolności człowieka w sposób nieproporcjonalny i nadmierny. Wtedy bowiem środki ochrony bezpieczeństwa publicznego w postaci legalnie dopuszczalnej działalności organów ścigania oraz służb specjalnych same w sobie stwarzają zagrożenie dla tych wolności.

W przypadku ustawy antyterrorystycznej zagrożenia te stwarza już sama definicja zdarzenia, przed którym mamy być chronieni - „Zdarzenia o charakterze terrorystycznym". Obywatele nie wiedzą też, czy i z powodu jakiej ich aktywności (skoro nie wiadomo, czym jest „zdarzenie…") ich dane będą zbierane przez służby, kto będzie miał do nich dostęp, i co będzie, jeśli służby zbiorą informacje nieprawdziwe, a potem podejmą na ich podstawie działania. Nieprecyzyjne są przepisy o tymczasowym aresztowaniu i o blokowaniu internetu. – To dlatego regulacje ustawy o działaniach antyterrorystycznych w wielu miejscach budzą istotne wątpliwości – stwierdza rzecznik praw obywatelskich Adam Bodnar we wniosku do Trybunału Konstytucyjnego.

Co jest we wniosku RPO?

„Zdarzenia o charakterze terrorystycznym" – co to jest i przed czym chroni ustawa?

Rozważania na temat zgodności zaskarżonych przepisów ustawy Rzecznik zaczyna od analizy podstawowego pojęcia, jakim jest definicja „zdarzenia o charakterze terrorystycznym". Zostało ono określone jako sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 ze zm.), lub zagrożenia zaistnienia takiego przestępstwa.

Pojęcie to wykorzystywane jest przede wszystkim do zdefiniowania „działań antyterrorystycznych", a ustawa odsyła do niego po wielekroć w swych kluczowych punktach.

Problem w tym, że pojęcie jest niejasne, a - jak podkreślił TK - „ustawodawca nie może poprzez niejasne formułowanie tekstu przepisów pozostawiać organom mającym je stosować nadmiernej swobody przy ustalaniu w praktyce zakresu podmiotowego i przedmiotowego ograniczeń konstytucyjnych wolności i praw jednostki" (zob. wyrok z 22 maja 2002 r. w sprawie K 6/02 albo wyrok z 14 czerwca 2000 r. w sprawie P 3/00).

Wymóg jasności oznacza nakaz tworzenia przepisów klarownych i zrozumiałych dla ich adresatów - człowiek ma prawo, by decydować o swoim postępowaniu na podstawie pełnej znajomości przesłanek działania organów państwowych oraz konsekwencji prawnych, jakie jego działania mogą pociągnąć za sobą (por. wyrok TK z 14 czerwca 2000 r. w sprawie P 3/00).

Tymczasem pozbawiona precyzji definicja „zdarzenia o charakterze terrorystycznym" pozwala na bardzo szeroką interpretację, zwłaszcza w sytuacji „zagrożenie zaistnienia" przestępstwa o charakterze terrorystycznym.

Na etapie prac parlamentarnych wskazywano, że podejrzenie powinno przynajmniej mieć charakter „uzasadniony", tak aby ograniczyć zakres oddziaływania tego przepisu – ustawodawca takiej zmiany jednak nie wprowadził. Wydaje się to istotne zwłaszcza w kontekście „działań antyterrorystycznych", które obejmują działania organów publicznych polegające na zapobieganiu zdarzeniom o charakterze terrorystycznym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć, reagowaniu w przypadku wystąpienia takich zdarzeń oraz usuwaniu ich skutków, w tym odtwarzaniu zasobów wykorzystywanych do reagowania na nie.

Pojęcie to jest przesłanką do wprowadzenia określonych stopni alarmowych (art. 15 ustawy), zaś wprowadzenie trzeciego lub czwartego stopnia alarmowego oznaczać może ograniczenie prawa do zgromadzeń (art. 21 ustawy).

Kto może trafić do rejestru Szefa ABW

Szef Agencji Bezpieczeństwa Wewnętrznego dostał zadanie prowadzenia wykazu osób, które – ujmując ogólnie – mogły mieć związek ze „zdarzeniem o charakterze terrorystycznym". W wykazie gromadzone są zatem dane osobowe, a prowadzony on jest w bardzo ogólnie określonym celu.

We współczesnych realiach walki z terroryzmem możliwość szybkiej identyfikacji osoby mającej związek ze zdarzeniem terrorystycznym stanowi istotę sukcesu. Umożliwia również wymianę danych ze służbami państw trzecich, co przy zniesionych kontrolach granicznych w ramach porozumienia z Schengen wydaje się być w pełni uzasadnione.

Jednak żeby zrozumieć, czyje dane gromadzi teraz Szef ABW, trzeba sobie uświadomić, że przy konstrukcji jego uprawnień znowu posłużono się pojęciem „zdarzenia o charakterze terrorystycznym". Do tego ustawodawca wskazuje, że zbieranie danych może być odpowiedzią na „uzasadnione podejrzenie możliwości prowadzenia" przez określone osoby działań zmierzających do popełnienia przestępstwa o charakterze terrorystycznym, a nie chociażby „uzasadnionego podejrzenia prowadzenia" przez określone osoby takiej działalności.

Żaden organ państwowy nie będzie też odpowiedzialny za weryfikację prawidłowości ustaleń Szefa ABW. Żaden przepis nie przewiduje, by Szef ABW zobowiązany był do dokonywania weryfikacji potrzeby dalszego przetwarzania zebranych danych osobowych. Ustawa nie tylko nie wprowadziła żadnej możliwości zapoznania się przez podmiot, którego dane znalazły się w wykazie, z tym faktem, nie przyznała żadnych uprawnień do żądania sprostowania czy usunięcia informacji nieprawdziwych, niepełnych czy zebranych w sposób sprzeczny z ustawą. Nie przewidziała też żadnej innej możliwości kontroli – nawet bez wiedzy podmiotu zainteresowanego.

Do tego ustawa przewiduje, że Szef ABW w zarządzeniu zdecyduje, jaki będzie zakres informacji gromadzonych w wykazie i na jakich zasadach będzie je przekazywał innym służbom. Rozwiązania tego nie sposób pogodzić z Konstytucją, która wskazuje, że zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa, oraz że zarządzenie nie może stanowić podstawy decyzji wobec obywateli, osób prawnych oraz innych podmiotów.

Kto ty jesteś? Polak czy nie-Polak?

Zaskarżony przepis art. 9 ust. 1 ustawy o działaniach antyterrorystycznych przewiduje możliwość stosowania czynności operacyjno-rozpoznawczych wobec osób niebędących obywatelami Rzeczypospolitej Polskiej, ustanawiając regulację o charakterze szczególnym w stosunku do ogólnych mechanizmów – dotyczących także obywateli polskich – przewidzianych m.in. w ustawie o Policji. Zarządzenie kontroli operacyjnej wobec cudzoziemców nie wymaga więc zgody żadnego organu zewnętrznego w stosunku do Szefa Agencji Bezpieczeństwa Wewnętrznego.

Rzecznik Praw Obywatelskich podziela stanowisko, że niejawne pozyskiwanie informacji może stanowić skuteczny i zarazem konieczny do zwalczania masowych niebezpieczeństw współczesności środek, a zwłaszcza do zwalczania szczególnie niebezpiecznej działalności terrorystycznej. Rzecznik wielokrotnie zwracał uwagę, że tego typu środki nie tylko mogą być uznane za dopuszczalne w określonych układach sytuacyjno-prawnych, ale czasami nawet mogą okazać się wręcz konieczne do zapewnienia pełniejszej realizacji praw i wolności jednostki. Niemniej tego typu ingerencjom zawsze powinny towarzyszyć odpowiednie zabezpieczenia praw i wolności jednostki, które mogą zostać potencjalnie naruszone.

Zatem skoro ustawodawca zdecydował się na pozbawienie pewnych grup jednostek fundamentalnego prawa do prywatności, to jego konstytucyjnym obowiązkiem w demokratycznym państwie prawa jest zapewnienie minimalnego standardu ochrony w postaci ustanowienia chociażby następczej kontroli sądowej w tym zakresie. Brak takiego rozwiązania należy uznać za sprzeczny z podstawowymi założeniami ustroju prawnego Rzeczypospolitej Polskiej.

W art. 10 ust. 1 ustawy uregulowano przesłanki uzasadniające dopuszczalność pobierania danych biometrycznych (obrazu linii papilarnych, wizerunku twarzy lub nieinwazyjnego pobierania materiału biologicznego w celu oznaczenia profilu DNA osoby niebędącej obywatelem Rzeczypospolitej Polskiej).

Warto pamiętać, że ustawa antyterrorystyczna nie wprowadza tych rozwiązań niejako od początku, bo są one – tyle że bardziej precyzyjnie sformułowane – w ustawie o Straży Granicznej i w ustawie o ABW. Co prawda, przepisy te nie przewidują uprawnienia do pobierania materiału biologicznego w celu oznaczenia DNA, jednak ta możliwość została dodana do ustawy antyterrorystycznej dopiero na etapie prac sejmowych, a zatem widac, że art. 10 ust. 1 ustawy został przyjęty w celu odstąpienia od wymogów związanych z gwarancjami proceduralnymi dla osób, których dane mają zostać pobrane i którym – w przypadku zastosowania trybu wynikającego z ustawy o działaniach antyterrorystycznych – nie będą w związku z tym przysługiwały żadne środki prawne.

W tym kontekście warto zwrócić uwagę na jedną rzecz – choć przepisy mają dotyczyć „osoby niebędącej obywatelem Rzeczypospolitej Polskiej", to ponieważ można je stosować m.in. „gdy istnieje wątpliwość co do tożsamości osoby", to de facto mogą być tej procedurze poddani także obywatele polscy.

Istotne jest także to, że przepis ten nie tylko nie posługuje się żadną kategorią kodeksową, co umożliwiłoby zastosowanie gwarancji proceduralnych, lecz odwołuje się do bardzo ogólnych i nieprecyzyjnych pojęć „istnienia podejrzenia" lub „istnienia wątpliwości". Już samo to – w świetle przywołanego już stwierdzenia dotyczącego wymogu precyzyjności przepisów ograniczających prawa i wolności człowieka – stanowi naruszenie zasady zaufania do państwa i zasady przyzwoitej legislacji, wywodzonych z art. 2 Konstytucji. Użycie podwójnie nieprecyzyjnych i ocennych pojęć (np. w przypadku art. 10 ust. 1 pkt 4 ustawy – „podejrzenia" związku osoby ze „zdarzeniem o charakterze terrorystycznym") uzasadnia stwierdzenie, że przepis art. 10 ust. 1 ustawy o działaniach antyterrorystycznych narusza art. 2 Konstytucji.

Wątpliwa jest też konieczność koncentrowania się przez ustawodawcę wyłącznie na danych osobowych osób, które nie posiadają polskiego obywatelstwa. Całkowicie pomija się bowiem w ten sposób zagrożenie, jakie może wynikać z działań obywateli Polski. Tym samym, wprowadzone rozróżnienie, które dodatkowo łączy się z szerokimi i nieostrymi przesłankami może być uznane za mające charakter arbitralny i nieuzasadniony w świetle art. 31 ust. 3 w zw. z art. 37 Konstytucji. Nie ma powodów, by prawo osób, które nie posiadają polskiego obywatelstwa, do ochrony danych osobowych, czy prawa do prywatności, było ograniczone w sposób dalej idący niż prawa obywateli polskich.

Gdzie może zajrzeć Szef ABW?

Artykuł 11 ustawy upoważnia Szefa ABW do nieodpłatnego dostępu do danych i informacji zgromadzonych w rejestrach publicznych i ewidencjach prowadzonych przez w zasadzie wszystkie podmioty publiczne na szczeblu centralnym, które prowadzą jakiekolwiek rejestry oraz ewidencje, oraz przez jednostki organizacyjne podległe i nadzorowane. Dostaje też prawo do wglądu do wszelkich rejestratorów obrazu umieszczonych w obiektach użyteczności publicznej, przy drogach publicznych i innych miejscach publicznych

To również oznacza szeroką ingerencję w prawo do prywatności osób, wobec których ustawa nie przewiduje żadnych uprawnień informacyjnych. Trzeba podkreślić, że – według informacji uzyskanych z Ministerstwa Spraw Wewnętrznych i Administracji przez Rzecznika Praw Obywatelskich – prace nad ustawą regulującą ogólne zasady stosowania monitoringu wizyjnego trwają, ale nie wiadomo, czy i kiedy się zakończą oraz jakie będą jej efekty. 24 maja 2016 r. Rzecznik otrzymał odpowiedź z MSWiA, że projekt założeń do projektu ustawy o monitoringu wizyjnym został wycofany spod obrad Zespołu do spraw Programowania Prac Rządu.

Warto dodać, że podobne przepisy istnieją w ustawie o Policji, tyle że dużo bardziej precyzyjnie określają cel, w jakim dane są pozyskiwane, a także sposób posługiwania się nimi.

Kogo można tymczasowo aresztować?

W ocenie Rzecznika Praw Obywatelskich przewidziana w art. 26 ust. 2 ustawy możliwość stosowania tymczasowego aresztowania na podstawie jedynie uprawdopodobnienia popełnienia, usiłowania lub przygotowania do popełnienia przestępstwa o charakterze terrorystycznym, pozostaje w sprzeczności z fundamentalnymi zasadami demokratycznego państwa prawnego. Ten przepis, posługując się pojęciami wyjątkowo nieostrymi, stwarza podstawę do daleko idącej ingerencji w sferę praw i wolności, w szczególności w sferę nietykalności osobistej jednostki.

W ocenie Rzecznika Praw Obywatelskich „uprawdopobnienie" dokonania, usiłowania lub przygotowania czynu o charakterze terrorystycznym nie może w sposób wystarczający legitymizować tak daleko idącej ingerencji w wolność jednostki.

Jak można dziś zablokować internet?

W art. 38 pkt 6 ustawy wprowadza się zmiany w ustawie o ABW polegające m.in. na dodaniu art. 32c, dopuszczającego blokadę dostępności w „systemie teleinformatycznym" określonych „danych informatycznych", mających związek ze zdarzeniem terrorystycznym lub „usług teleinformatycznych" służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym.

I znowu przepis ten posługuje się albo określeniami, które nie mają definicji legalnej i w związku z tym będą powodowały trudności z ich interpretacją (jak np. „dane informatyczne"), albo przewiduje odwołanie do pojęcia „zdarzenia o charakterze terrorystycznym", które także precyzyjne nie jest.

Można zatem wyobrazić sobie, że blokada będzie dotyczyła zarówno pojedynczych komentarzy, jak też całych portali społecznościowych, czy elektronicznych wydań gazet. Nie jest też jasne, czy zakaz blokowania ma dotyczyć tylko uniemożliwienia dostępu do określonych informacji na konkretnej stronie internetowej, blokowania całej witryny, czy też całej domeny internetowej, a może nawet aplikacji internetowych, skoro blokowanie dotyczyć ma nie tylko danych, ale również usług teleinformatycznych.

Użycie niejasnych, nieprecyzyjnych i ocennych pojęć, które w istocie są wykorzystywane przy ograniczeniu praw i wolności jednostki, musi być uznane – z tych samych powodów, o których była mowa we wcześniejszych punktach wniosku – za niezgodne z art. 2 Konstytucji.

- Zwalczanie terroryzmu i prawidłowe rozpoznawanie zagrożenia terrorystycznego niewątpliwie stanowi istotne zadanie państwa, którego obowiązkiem jest stanie na straży bezpieczeństwa osób pozostających w jego jurysdykcji. Wobec tego pozytywnie należy ocenić podjęcie inicjatywy ustawodawczej w tym obszarze. Jednak wszelkie środki prawne służące do osiągnięcia tego celu muszą być proporcjonalne i ingerować w prawa człowieka jedynie wówczas i jedynie w takim zakresie, jaki jest konieczny i niezbędny. Regulacje ustawy o działaniach antyterrorystycznych w wielu miejscach budzą istotne wątpliwości, co do ich zgodności ze standardem konstytucyjnym oraz wynikającym z EKPCz i KPP UE – stwierdza rzecznik praw obywatelskich Adam Bodnar we wniosku do Trybunału Konstytucyjnego.

WYSTĄPIENIA DO MINISTRA CYFRYZACJI ORAZ PEŁNOMOCNIKA RZĄDU DS. SPOŁECZEŃSTWA OBYWATELSKIEGO I RÓWNEGO TRAKTOWANIA W SPRAWIE PRZECIWDZIAŁANIA MOWIE NIENAWIŚCI I INNYM AKTOM NIETOLERANCJI

data: 2016-06-30

Rzecznik Praw Obywatelskich zwrócił w piśmie z 30 czerwca 2016 r. do Pełnomocnika Rządu ds. Społeczeństwa Obywatelskiego i Równego Traktowania z prośbą o zajecie stanowiska w odniesieniu do potrzeby przyjęcia mechanizmu koordynującego działania rządu i innych organów władzy publicznej i służb, we współpracy z organizacjami społecznymi. Tego rodzaju platformą współpracy była do 1 czerwca 2016 r. Rada do spraw Przeciwdziałania Dyskryminacji Rasowej, Ksenofobii i związanej z nimi Nietolerancji, działająca przy Ministerstwie Cyfryzacji. W związku z likwidacją Rady Rzecznik podzielił opinię Ministra Cyfryzacji że szczególną rolę w tym zakresie może wypełniać Pełnomocnik Rządu ds. Równego Traktowania (obecnie Pełnomocnik Rządu ds. Społeczeństwa Obywatelskiego i Równego Traktowania), jako organ odpowiedzialny za realizowanie polityki rządu w zakresie równego traktowania. Ustawa z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania wskazuje bowiem szereg zadań Pełnomocnika, które powinny być wykonywane we współpracy z różnymi podmiotami: organami publicznymi i organizacjami społecznymi. Pełnomocnik, wyposażony w odpowiednie zasoby finansowe i organizacyjne, z powodzeniem mógłby zatem przejąć funkcje uprzednio przypisane Radzie. Rzecznik zwrócił się do Pełnomocnika Rządu ds. Społeczeństwa Obywatelskiego i Równego Traktowania z prośbą o zajęcie stanowiska w przedstawionej sprawie.

APEL RPO DO PREZYDENTA W SPRAWIE USTAWY ANTYTERRORYSTYCZNEJ

data: 2016-06-21

Rzecznik Praw Obywatelskich zaapelował do Prezydenta RP, aby przed podpisaniem ustawy antyterrorystycznej wysłał ją do Trybunału Konstytucyjnego

- Zwracam się do Pana Prezydenta o wystąpienie z wnioskiem do Trybunału Konstytucyjnego o zbadanie zgodności ustawy o działaniach antyterrorystycznych z Konstytucją przed jej podpisaniem – napisał rzecznik praw obywatelskich Adam Bodnar w liście z 21 czerwca 2016 r. do prezydenta RP Andrzeja Dudy.

Ustawa o działaniach antyterrorystycznych będzie miała wpływ na stan przestrzegania praw i wolności człowieka i obywatela, na straży których, stoi Rzecznik Praw Obywatelskich.

Projekt został przyjęty przez rząd 10 maja, uchwaloną przez Sejm ustawę Prezydent otrzymał 17 czerwca. Nowe przepisy mają wejść w życie w ciągu 7 dni od ogłoszenia. Tymczasem budzą one bardzo poważne wątpliwości.

Rzecznik Praw Obywatelskich podkreśla, że przyznanie właściwych uprawnień służbom odpowiedzialnym za walkę z terroryzmem jest obowiązkiem państwa. Jednak pod hasłem walki z terroryzmem nie można ingerować w prawa i wolności człowieka w sposób nieproporcjonalny.

- Dlatego, mając na uwadze to, że Pan Prezydent jest strażnikiem Konstytucji, zwracam się do Pana Prezydenta o skorzystanie z uprawnienia określonego w art. 122 ust. 3 Konstytucji RP – pisze RPO.

Zarzuty dotyczące niezgodności z Konstytucją projektowanych przepisów zgłaszane były na etapie prac rządu, i później – w parlamencie. Szereg uwag zgłoszono także w trakcie obywatelskiego wysłuchania publicznego 6 czerwca na Uniwersytecie Warszawskim Nie zostały rozpatrzone. Dlatego tak ważne jest, by zajął się nimi Prezydent.

Najistotniejsze wątpliwości, które powinny być starannie zbadane, dotyczą czterech kwestii:

1) Przyznanie nowych uprawnień ABW, przy jednoczesnym braku jakiejkolwiek kontroli nad jej działaniami

Szef ABW ma prowadzić wykaz osób podejrzewanych o działalność terrorystyczną. To, kogo ten wykaz ma dotyczyć, opisane jest tak nieprecyzyjnie. Nie ma żadnych procedur kontroli i sprawdzenia, czy ABW się nie pomyliła wpisując kogoś do wykazu.

Szef ABW może zarządzić podsłuch wobec osoby niebędącej obywatelem RP, jeśli są wobec niej podejrzenia, że może prowadzić działalność terrorystyczną. Nie podlega to kontroli sądu. Jeżeli rozpatrzy się ten problem w kontekście innych zmienionych ostatnio przepisów, można dojść do przekonania, że wykorzystanie dowodów zdobytych przy okazji tych czynności nie będzie podlegało żadnej kontroli,

2) Nieproporcjonalne ograniczenie praw i wolności człowieka i obywatela, w szczególności prawa do prywatności i prawa do zgromadzeń publicznych

Zasadnicze wątpliwości budzi przepis pozwalający na blokowanie internetu

Można będzie zakazać zgromadzeń i imprez masowych w przypadku trzeciego lub czwartego stopnia alarmowego. Sam zakaz nie budziłby wątpliwości, ale nie jest jasne, jak i kiedy wprowadza się poszczególne stopnie alarmowe i co to jest „zdarzenie o charakterze terrorystycznym”.

Szef ABW dostaje prawo dostępu do wszystkich danych zgromadzonych w rejestrach publicznych i ewidencjach Nie podlega to kontroli

3) Szczególne środki wobec cudzoziemców, w tym obywateli państw Unii Europejskiej

Chociaż Trybunał Konstytucyjny dopuścił możliwość różnicowania standardów wobec obywateli oraz nieobywateli, to nie może to znaczyć zupełnego odebrania cudzoziemcom praw (podsłuchy, możliwość pobierania danych biometrycznych). Przesłanki, dla których służby podejmują działania wobec tych osób, oparte są – zgodnie z ustawą – głównie na podejrzeniach i wątpliwościach. Nie ma żadnej procedury weryfikującej prawidłowość działań.

4) Przyznanie prawa do specjalnego użycia broni

W art. 23 ustawy uregulowano zasady użycia broni palnej do ratowania życia ofiar terrorysty. Znaczenie tego przepisu można poznać wyłącznie analizując kluczowe dla ustawy pojęcia „zdarzenie o charakterze terrorystycznym”, czy „działania antyterrorystyczne”. A nie są one precyzyjne.

RPO przypomina, że w podobnym trybie – i bez uwzględnienia zgłaszanych uwag – procedowana była nowelizacja ustawy o Policji z 15 stycznia 2016 r. W efekcie 10 czerwca Komisja Wenecka wydała w jej sprawie opinię, stwierdzając, że budzi zastrzeżenia co do zgodności ze standardami międzynarodowymi, zwłaszcza dlatego, że działania służb nie są poddane wystarczającej kontroli.

OBYWATELSKIE WYSŁUCHANIE PUBLICZNE WS. USTAWY ANTYTERRORYSTYCZNEJ - RPO PRZEDSTAWIA SWOJĄ OPINIĘ

data: 2016-06-06

- Hasło walki z terroryzmem nie może jednocześnie oznaczać nieuzasadnionej i nieproporcjonalnej ingerencji w prawa i wolności człowieka – zarówno obywateli RP, jak i cudzoziemców znajdujących się pod władzą Rzeczypospolitej Polskiej. I z tego punktu widzenia rządowy projekt budzi poważne wątpliwości – mówiła dr hab. Agnieszka Grzelak, zastępczyni dyrektora Zespołu Prawa Konstytucyjnego, Międzynarodowego i Europejskiego w Biurze RPO, podczas obywatelskiego wysłuchania publicznego dotyczącego ustawy o działaniach antyterrorystycznych.

Spotkanie odbyło się na Uniwersytecie Warszawskim. Wzięło w nim udział ponad 100 osób, w tym przedstawiciele organizacji pozarządowych i instytucji, które zgłaszały swoje opinie w tracie procesu legislacyjnego. Podczas prac w Sejmie posłowie komisji administracji i spraw wewnętrznych nie przyjęli jednak wniosku o wysłuchanie publiczne. Dlatego organizacje zdecydowały się same zorganizować takie spotkanie, by przedstawić na nim swoje uwagi do projektu.

Agnieszka Grzelak zaprezentowała kluczowe zastrzeżenia Rzecznika Praw Obywatelskich dotyczące przygotowywanej ustawy. Zwróciła uwagę, że wiele zawartych w niej pojęć jest nieprecyzyjnych i może w nadmierny sposób ograniczać prawa obywatelskie. Wskazywała również na daleko idącą ingerencję w prawa cudzoziemców – chodzi m.in. o możliwość ich podsłuchiwania, pobierania materiału genetycznego czy odcisków palców.

- Projekt ustawy o działaniach antyterrorystycznych zasadniczo podejmuje istotne zagadnienia z zakresu koordynacji działań służb. Dalecy jesteśmy od twierdzenia, że w ogóle nie jest potrzebny. Jednak budzi on poważne wątpliwości, co do dopuszczalnego konstytucyjnie ograniczenia praw i wolności człowieka. Z tego punktu widzenia ubolewamy nad faktem, że nad projektem nie przeprowadzono żadnej szerokiej debaty publicznej, która by pozwoliła na przedstawienie argumentacji i wypracowanie wspólnego stanowiska wraz z projektodawcą – zaznaczyła przedstawicielka RPO.

Spotkanie zostało zorganizowane przez Uniwersytet Warszawski, Fundację Panoptykon, Helsińską Fundację Praw Człowieka, Fundację ePaństwo i Amnesty International, przy wsparciu Fundacji im. Stefana Batorego i Pracownii Badań i Innowacji Społecznych „Stocznia".

PROJEKT USTAWY O DZIAŁANIACH ANTYTERRORYSTYCZNYCH – OPINIA RPO

data: 2016-05-19

Rzecznik Praw Obywatelskich przekazał Marszałkowi Sejmu RP opinię w sprawie projektu ustawy o działaniach antyterrorystycznych (druk sejmowy nr 516).

Projekt ma określać zasady prowadzenia działań antyterrorystycznych oraz współpracy w tym zakresie między właściwymi organami. Z uzasadnienia do projektu ustawy wynika, że jej podstawowym celem ma być „podniesienie efektywności polskiego systemu antyterrorystycznego, a tym samym zwiększenie bezpieczeństwa wszystkich obywateli RP".

RPO podkreślił, że samo przyznanie właściwych uprawnień służbom odpowiedzialnym za walkę z terroryzmem może wpłynąć na ograniczenie skali przestępczości i wzrost poczucia bezpieczeństwa. Jednak hasło walki z terroryzmem nie może jednocześnie oznaczać nieuzasadnionej i nieproporcjonalnej ingerencji w prawa i wolności człowieka – zarówno obywateli RP, jak i cudzoziemców znajdujących się pod władzą Rzeczypospolitej Polskiej. I z tego punktu widzenia rządowy projekt budzi poważne wątpliwości. Dlatego – zdaniem Rzecznika – konieczna jest publiczna debata na temat proponowanych rozwiązań. W żadnym razie nie wolno z niej zrezygnować, mimo że niektórzy twierdzą, iż nie mamy już na to czasu w związku ze zbliżającymi się wydarzeniami o charakterze międzynarodowym, które będą miały miejsce w Polsce.

Wątpliwości RPO wzbudziły też konkretne kwestie dotyczące:

1. Definicji pojęcia „zdarzenie o charakterze terrorystycznym", od której zależy możliwość stosowania instrumentów przyznanych ABW oraz możliwość ograniczenia prawa do zgromadzeń – pojęcie sformułowane jest w sposób bardzo szeroki, bez wskazania, kto i w jakich okolicznościach ma dokonywać oceny oraz w jakiej procedurze stwierdzać, że istnieje podejrzenie zaistnienia czynu, co powoduje, że nie można mieć pewności, że środki te będą wykorzystywane wyłącznie w razie faktycznej konieczności związanej z terroryzmem.
2. Prowadzenia przez szefa ABW wykazu zawierającego informacje m.in. o osobach, wobec których istnieje „uzasadnione podejrzenie, że mogą prowadzić działania zmierzające do popełnienia przestępstwa o charakterze terrorystycznym, w tym stanowiących zagrożenie bezpieczeństwa lotnictwa cywilnego" – przesłanka ta zawiera elementy ocenne i nieprecyzyjne, pozostawiające dużą swobodę uznania Szefowi ABW.
3. Prowadzenia czynności operacyjno-rozpoznawczych wobec osoby niebędącej obywatelem Rzeczypospolitej Polskiej – zarządzenie kontroli operacyjnej nie wymaga w tym przypadku zgody żadnego organu zewnętrznego wobec Szefa ABW. Wątpliwości budzi również brak jakiejkolwiek kontroli sądowej, choćby następczej.

4. Dopuszczalności pobierania i przetwarzania danych biometrycznych cudzoziemców (obrazu linii papilarnych lub wizerunku twarzy) przez funkcjonariuszy ABW, Policji i Straży Granicznej – wątpliwości budzi nieuzasadnione różnicowanie pozycji prawnej cudzoziemców i obywateli RP w zakresie pozyskiwania informacji o nich oraz ochrony ich danych osobowych.
5. Dostępu Szefa ABW do danych zgromadzonych w rejestrach publicznych i ewidencjach – projekt ustawy narusza podstawowe zasady ochrony danych osobowych, ponieważ nie tylko nie wyjaśnia, czy w istocie dostęp do wszystkich rejestrów jest potrzebny dla realizacji wskazanych w nim celów, ale także nie przewiduje żadnych uprawnień przysługujących podmiotowi danych, nie realizuje zasady czasowego ograniczenia przechowywania danych i nie przewiduje żadnej kontroli nad pozyskiwaniem tak szerokiego zakresu informacji.
6. Możliwości blokowania danych informatycznych – nieprecyzyjne określenie zakresu blokady oraz brak jakichkolwiek uprawnień osoby, której dane zostały zablokowane.
7. Wprowadzenia obowiązku rejestrowania telefonicznych kart przedpłaconych – brak uzasadnienia ograniczenia prawa do prywatności.
8. Możliwości wydania decyzji o natychmiastowym wydaleniu cudzoziemca (również obywatela UE), mogącego prowadzić działalność terrorystyczną lub szpiegowską albo podejrzewanego o popełnienie jednego z tych przestępstw – decyzja ma podlegać natychmiastowemu, przymusowemu wykonaniu, a ewentualne odwołanie możliwe będzie już spoza granic RP. Sytuacja ta rodzi szereg wątpliwości w kontekście prawa do sądu, prawa do prywatności czy też prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium Państw Członkowskich.
9. Wprowadzenia tzw. specjalnego użycia broni (użycie broni w celu pozbawienia człowieka życia) – wątpliwości dotyczą kryteriów wymogu legalności.
10. Wprowadzenia możliwości zastosowania tymczasowego aresztowania tylko na podstawie uprawdopodobnienia popełnienia, usiłowania lub przygotowania do popełnienia przestępstwa o charakterze terrorystycznym – takie rozwiązanie nie zapewnia odpowiedniego stopnia ochrony praw i wolności jednostek.
11. Zmian w Kodeksie karnym - wątpliwości z perspektywy zasady demokratycznego państwa prawnego i zasady proporcjonalności.

PUBLICZNE KONSULTACJE RPO NA TEMAT PROJEKTU USTAWY O DZIAŁANIACH ANTYTERRORYSTYCZNYCH

data: 2016-05-06

- **- Nie możemy sprowadzać debaty do tego, czy jesteśmy za terrorystami czy nie. Debata nad projektem ustawy antyterrorystycznej powinna być poważna, a opinia publiczna powinna dowiedzieć się, czego dotyczą zmiany. Nie możemy nie zabierać głosu - powiedział Adam Bodnar podsumowując spotkanie konsultacyjne w sprawie projektu.**

Ustawa tworzy bardzo poważne zagrożenia i nie powinna być procedowana w takim trybie - powtarzali uczestnicy spotkania. W konsultacjach uczestniczyli m.in. przedstawiciele Helsińskiej Fundacji Praw Człowieka, Krajowego Stowarzyszenie Ochrony Informacji Niejawnych, ISOC Polska, Fundamentu Społeczeństwa Informacyjnego, Fundacji Bezpieczna Cyberprzestrzeń, Związku Pracodawców Branży Internetowej IAB Polska, Polskiego Forum Migracyjnego, Amnesty International, Naczelnej Rady Adwokackiej, Collegium Civitas, Uniwersytetu Warszawskiego, Internet Society Polska, Fundacji Panoptykon.

Rząd w pośpiesznym trybie przygotowuje ustawę antyterrorystyczną. 5 maja 2016 r. Rada Ministrów ma przyjąć projekt ustawy o działaniach antyterrorystycznych. Ustawa ma wejść w życie 1 czerwca 2016 r.

Tymczasem w debacie publicznej wiele osób wskazywało na wątpliwości z nim związane dotyczące zachwiania równowagi między dwoma wartościami – bezpieczeństwem państwa i obywateli z jednej strony, a ochroną swobód i prywatności (także przebywających w RP obywateli innych państw) z drugiej strony.

Żadna ingerencja w tak podstawowe prawa nie powinna być przeprowadzana bez wyraźnego uzasadnienia i zgody obywateli. Wiedza i doświadczenie kompetentnych obywateli o różnych punktach widzenia powinna być wykorzystywana dla publicznego dobra. Dlatego rzecznik praw obywatelskich Adam Bodnar zaprosił na konsultacje ekspertów, działaczy społecznych, przedstawicieli organizacji społecznych na spotkanie konsultacyjne. Jego celem jest zebranie opinii i przygotowanie RPO stworzenia pogłębionej opinii jeszcze w trakcie prac legislacyjnych.

Co jest w projekcie? Co zapowiada rząd?

Zgodnie z uzasadnieniem, „mając na uwadze udział Polski w działaniach międzynarodowej koalicji antyterrorystycznej, jak również fakt, że terytorium RP uznawane jest w materiałach rozpowszechnianych przez organizacje terrorystyczne, jako potencjalny cel zamachów, zasadne jest podjęcie na poziomie prawa krajowego odpowiednich działań legislacyjnych, zmierzających do poprawy bezpieczeństwa w związku z tymi zagrożeniami".

Projektodawcy wskazują na podstawowe cele ustawy, którymi mają być:

- wzmocnienie mechanizmów koordynacji działań,
- doprecyzowanie zadań poszczególnych służb i organów oraz zasad współpracy między nimi,
- zapewnienie możliwości skutecznych działań w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, w tym w zakresie postępowania przygotowawczego,
- zapewnienie mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń,
- dostosowanie przepisów karnych do nowych typów zagrożeń o charakterze karnym.

Istotne pytania

Jeśli takie są cele tej ustawy, to:

1. Czy nie mamy już przepisów, które realizują postawione cele? Czy ta ustawa jest nam potrzebna?
2. Czy ta ustawa nas ochroni? Czy zaproponowane rozwiązania faktycznie zapobiegną zdarzeniom o charakterze terrorystycznym (będą efektywne)?
3. Czego ta ustawa faktycznie dotyczy (czy zakres przedmiotowy ustawy został określony prawidłowo?) Czy konieczna jest zmiana w kodeksie karnym dotycząca definicji przestępstwa o charakterze terrorystycznym?
4. Czy ograniczenie praw i wolności człowieka, przewidziane w ustawie, można uznać za dopuszczalne i zgodne z wymogami określonymi Konstytucji? (w art. 31 ust. 3)
5. Czy dopuszczalne z punktu widzenia praw człowieka inne traktowanie obywateli polskich i cudzoziemców (zasady kontroli operacyjnej, pobierania i przetwarzania danych biometrycznych)?

NIELEGALNY HANDEL BILLINGAMI – INFORMACJA KOMENDANTA GŁÓWNEGO POLICJI

data: 2016-04-19

W ostatnich miesiącach pojawiały się w mediach informacje na temat procederu nielegalnego dostępu do tzw. billingów oraz handlu nimi, w którym mogli brać udział – zdaniem dziennikarzy – również byli i obecni oficerowie Policji.

W odpowiedzi na wystąpienie Rzecznika, Zastępca Komendanta Głównego Policji poinformował o podstawach prawnych pozyskiwania przez Policję stosownych danych. Jednocześnie wskazał, że w sprawach nielegalnego pozyskiwania billingów toczyły się konkretnie dwa postępowania. Jedno z nich zakończyło się wniesieniem aktu oskarżenia przeciwko emerytowanemu funkcjonariuszowi, natomiast drugie umorzono z powodu braku wystarczających dowodów.

W kwestii działań, które mają zapobiegać tego typu nieprawidłowościom, Zastępca Komendanta Głównego Policji poinformował, że Biuro Spraw Wewnętrznych KGP regularnie sprawdza stan zagrożenia zjawiskiem bezprawnego pozyskiwania danych telekomunikacyjnych oraz informacji z policyjnych i pozapolicyjnych baz danych.

Wskazał także na akt wewnętrzny KGP (decyzja nr 98), przyjęty w celu realizacji ustawy o zmianie ustawy o Policji, uchwalonej 7 lutego 2016 r. Określa on jednostki i komórki organizacyjne Policji, których policjanci mogą być uprawnieni do bezpośredniego lub pośredniego uzyskiwania danych i ich przetwarzania. Decyzja reguluje tryb udzielania policjantom upoważnień do występowania o udostępnienie danych, jak również sposób i tryb uzyskiwania danych oraz ich niszczenia.

KGP zapewniła o szczególnym nadzorze kierownictwa Policji w tej sprawie.

OPINIA GIODO DOT. PROJEKTU USTAWY O POLICJI

data: 2016-01-13

Rzecznik Praw Obywatelskich zwrócił się do Generalnego Inspektora Ochrony Danych Osobowych z pytaniem, czy GIODO poddał analizie i zaopiniował poselski projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw.

W odpowiedzi Generalny Inspektor przesłał kopię pisma skierowanego do Marszałka Sejmu, w którym zostały zasygnalizowane zastrzeżenia GIODO do wskazanego projektu.

ETPC WS. NIEJAWNEGO NADZOROWANIA OBYWATELI W ZWIĄZKU ZE ZWALCZANIEM TERRORYZMU

data: 2016-01-13

Europejski Trybunał Praw Człowieka (dalej ETPC) wydał wyrok w sprawie Szabó i Vissy przeciwko Węgrom. W skardze nr 37138/14 skarżący (pracujący dla węgierskiej organizacji pozarządowej) podnieśli, że doszło do naruszenia art. 8 (prawo do poszanowania życia prywatnego, mieszkania i korespondencji) oraz art. 13 (prawo do skutecznego środka odwoławczego) Europejskiej Konwencji Praw Człowieka (dalej EKPC) w rezultacie samego istnienia ustawodawstwa zezwalającego na środki niejawnego nadzoru i ich ryzyka, a nie stosowania wobec nich konkretnych środków. Trybunał – kontynuując swoje podejście w sprawach podobnych – dopuścił skargę, chociaż skarżący nie byli w stanie udowodnić, że byli przedmiotem inwigilacji.

Skarga dotyczyła węgierskich przepisów przyjętych w 2010 r., na podstawie których w strukturze policji wyodrębniono specjalną jednostkę do spraw zwalczania terroryzmu. Jednostce tej przyznano prawo do niejawnego przeszukania mieszkania, niejawnego nagrywania, otwierania paczek i listów, a także sprawdzania i nagrywania treści komunikacji elektronicznej – bez zgody osoby, której to dotyczyło. Należy dodać, że działania te odbywały się na podstawie zgody sądu (jeśli były prowadzone w konkretnej sprawie) lub Ministra Sprawiedliwości (jeśli ich celem było ogólnie zapobieżenia działaniom terrorystycznym lub węgierskiemu bezpieczeństwu narodowemu albo ratowanie obywateli węgierskich w przypadku działań wojennych za granicą lub ataków terrorystycznych).

Europejski Trybunał Praw Człowieka nie miał wątpliwości, że doszło do naruszenia prawa skarżących do poszanowania ich życia prywatnego (art. 8), jednocześnie nie stwierdził naruszenia art. 13 EKPC. Analizując przepisy węgierskie Trybunał podkreślił, że nie można zakwestionować celu, w jakim ww. uprawnienia zostały przyznane wskazanej służbie. Trybunał uznał, że naturalną odpowiedzią władz państwowych na zjawisko terroryzmu jest podejmowanie działań, również o charakterze prewencyjnym, zmierzających do jego zwalczania, w szczególności poprzez masowe monitorowanie środków komunikacji. Trybunał podniósł jednak zastrzeżenia co do tego, czy w przepisach krajowych przewidziano gwarancje, które byłyby wystarczająco precyzyjne, efektywne i zrozumiałe w odniesieniu do zarządzania, wykonywania i realizacji wskazanych uprawnień. W szczególności Trybunał dostrzegł, że przepisy węgierskie:

- nie określają kategorii osób, które mogłyby podlegać niejawnemu nadzorowi, w szczególności nie wymagają wskazania żadnego związku z zagrożeniem terrorystycznym,
- służby, które żądają zezwolenia od Ministra Sprawiedliwości na dokonanie podsłuchu, nie muszą uzasadnić w żaden szczegółowy sposób, by zbieranie takich informacji było konieczne, co – zdaniem Trybunału – może z łatwością prowadzić do nadużyć,
- niewystarczająco precyzyjnie określają maksymalny okres trwania nadzoru, co w efekcie może prowadzić do tego, że nie będzie on ograniczony czasowo w żaden sposób,
- nie przewidziano żadnych środków prawnych przysługujących osobom, których komunikacja była nadzorowana – w szczególności za właściwy środek nadzoru Trybunał nie uznał obowiązku przedstawiania raportu w odstępach półrocznych komisji parlamentarnej.

Mirosław Wróblewski – dyrektor Zespołu Prawa Konstytucyjnego, Międzynarodowego i Europejskiego w Biurze RPO:

Wyrok ETPC w sprawie Vissy i Szabó przeciwko Węgrom to kolejna sprawa, w której Trybunał zbadał przepisy krajowe dotyczącego niejawnego nadzoru i inwigilacji obywateli, wprowadzane w celu zapobiegania przestępczości, w tym przypadku terroryzmowi. Trybunał kontynuuje swoją linię orzeczniczą, wywodzoną jeszcze ze sprawy Klass przeciwko Niemcom, potwierdzoną następnie w sprawie Kennedy p. Wielkiej Brytanii, a ostatnio w grudniu 2015 r. w orzeczeniu w sprawie Zakharov p. Rosji. Trybunał konsekwentnie dopuszcza przyznanie statusu pokrzywdzonego osobom obawiającym się, że służby mogą zbierać i przechowywać informacje na ich temat. Wskazuje też ponownie, że jeżeli system krajowy nie zapewnia skutecznego środka prawnego osobie, która podejrzewa, że jest poddana tajnej inwigilacji, wówczas istnieje potrzeba większej kontroli przez Trybunał i skarga w tej sytuacji jest dopuszczalna.

Stanowisko przedstawione przez Trybunał jest kolejnym argumentem potwierdzającym pogląd reprezentowany przez Rzecznika Praw Obywatelskich w odniesieniu do wymogów, jakie muszą spełniać również polskie przepisy umożliwiające policji i innym służbom ochrony państwa pozyskiwanie, gromadzenie i przetwarzanie rozmaitego rodzaju danych, w ramach dokonywania czynności operacyjno-rozpoznawczych. W szczególności, Rzecznik Praw Obywatelskich stoi na stanowisku, że przedłożony poselski projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, który jest obecnie przedmiotem prac w Sejmie, jest sprzeczny z Konstytucją RP, a także z art. 8 EKPC. Również w trakcie prac nad zapowiadaną ustawą „antyterrorystyczną" linia orzecznicza ETPC, w której interpretuje się art. 8 EKPC w kontekście działań operacyjnych służb krajowych podejmowanych dla walki z terroryzmem i innymi rodzajami przestępczości, będzie musiała zostać uwzględniona.

DO MS WS. NIEJASNEGO BRZMIENIA PRZEPISU DOTYCZĄCEGO PRZESTĘPSTW KOMPUTEROWYCH

data: 2016-01-08

Konstrukcja art. 269b § 1 k.k. budzi wątpliwości interpretacyjne. Kwestionowany przepis zawiera pominięcie prawodawcze polegające na niedookreśleniu podmiotu przestępstwa. Nie precyzuje bowiem, że podmiotem opisanego w nim przestępstwa wytwarzania, pozyskiwania, zbywania lub udostępniania hasła komputerowego, kodu dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, jest wyłącznie osoba nieuprawniona. W obecnym brzmieniu przepis może prowadzić do pociągnięcia do odpowiedzialności karnej osoby, która, będąc uprawnioną, przekazała innej osobie hasło do systemu komputerowego. Kwestia ta była przedmiotem wystąpienia RPO w dniu 30 stycznia 2014 r. do Ministra Sprawiedliwości. Minister podzielił wówczas przedstawione zastrzeżenia. Zapowiedział ponadto, że wystąpi do Komisji Kodyfikacyjnej Prawa Karnego o zajęcie stanowiska w tej sprawie. Rzecznik Praw Obywatelskich zwrócił się o przekazanie informacji na temat ewentualnych prac legislacyjnych prowadzonych w Ministerstwie Sprawiedliwości.

DO MC ORAZ GIODO WS. DOSTĘPU SŁUŻB DO DANYCH INTERNETOWYCH W PROJEKCIE USTAWY O POLICJI

data: 2016-01-04

W ocenie Rzecznika Praw Obywatelskich poselski projekt ustawy o Policji oraz niektórych innych ustaw budzi poważne zastrzeżenia konstytucyjne w zakresie dostępu policji i innych służb do danych internetowych. Rzecznik podkreślił w wystąpieniu, że specyfika nowych technologii i ocena zagrożeń z nimi związanych uzasadnia powierzenie policji i innym służbom ochrony państwa adekwatnych uprawnień, umożliwiających zapobieganie i wykrywanie przestępstw, a także ściganie ich sprawców. Jednak wszelkie przypadki ograniczenia praw i wolności konstytucyjnych, w tym prawa do prywatności, powinny być uregulowane w przepisach w sposób jasny i precyzyjny. Zakres danych internetowych gromadzonych przez służby jest określony w projekcie w sposób niejasny, co stwarza ryzyko arbitralności działań organów państwa. Dostęp służb do szerokiego zakresu informacji będzie pozwalał na precyzyjne odtworzenie różnych aspektów życia prywatnego. Może również prowadzić do budowania profilu osobowego użytkowników Internetu. Projektowane przepisy nie gwarantują, że gromadzenie i przetwarzanie danych internetowych będzie subsydiarnym środkiem pozyskiwania informacji lub dowodów. Stwarza to możliwość wykorzystywania tych danych nie tylko w sytuacjach, gdy będzie to niezbędne do wykrywania lub zapobiegania przestępstwom, ale także wówczas, gdy będzie to najprostszym rozwiązaniem. Projekt nie przewiduje żadnego ograniczenia czasowego w zakresie gromadzenia i przetwarzania danych. Wątpliwości dotyczą także procedur kontrolnych. Ponadto nie określono żadnej procedury, w wyniku której podmiot, którego dane były przetwarzane, dowiedziałby się o pozyskiwaniu jego danych internetowych.

Rzecznik Praw Obywatelskich zwrócił się również do Generalnego Inspektora Ochrony Danych Osobowych z pytaniem, czy GIODO poddał analizie i zaopiniował poselski projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw.

2015

ODPOWIEDŹ URZĘDU KOMUNIKACJI ELEKTRONICZNEJ WS. HANDLU BILINGAMI TELEFONICZNYMI

data: 2015-11-26

Rzecznik Praw Obywatelskich wystąpił do Prezesa Urzędu Komunikacji Elektronicznej w poruszonej przez media sprawie procederu handlu bilingami telefonicznymi. W odpowiedzi Prezes UKE wskazał, że nie jest w posiadaniu żadnych informacji, które potwierdzałyby fakt naruszenia tajemnicy telekomunikacyjnej przez któregoś z dostawców usług telekomunikacyjnych lub podmiotów z nimi współpracujących. Do Prezesa UKE nie wpłynęły żadne oficjalne zgłoszenia na temat procederu handlu bilingami, zarówno ze strony abonentów usług telekomunikacyjnych, jak i samych operatorów lub innych podmiotów. W związku z tym UKE nie podjął żadnych działań. Ponadto, przedstawiony w mediach proceder może mieć charakter przestępczy, a Prezes UKE nie posiada odpowiednich kompetencji w tym zakresie.

Rzecznik Praw Obywatelskich będzie monitorował tę sprawę.

WAŻNY WYROK TRYBUNAŁU SPRAWIEDLIWOŚCI WS. OCHRONY DANYCH W INTERNECIE

data: 2015-10-06

Trybunał Sprawiedliwości UE stwierdził nieważność decyzji Komisji Europejskiej stwierdzającej, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony przekazywanych danych osobowych (wyrok w sprawie C-362/14, Maximillian Schrems)

Unijna dyrektywa o przetwarzaniu danych osobowych 95/46/WE stanowi, że przekazywanie tego rodzaju danych do państwa trzeciego może nastąpić - co do zasady – tylko wtedy, gdy dane państwo trzecie zapewni odpowiedni stopień ochrony tych danych. Zgodnie z dyrektywą Komisja Europejska może stwierdzić, że państwo trzecie – poprzez swe ustawodawstwo krajowe lub zobowiązania międzynarodowe – zapewnia odpowiedni stopień ochrony. Komisja decyzją 2000/520/WE stwierdziła, że w ramach systemu zwanego „bezpieczną przystanią" (Safe harbour) USA zapewniają odpowiedni stopień przekazywania danych.

Tymczasem Trybunał Sprawiedliwości orzekł, że system bezpiecznej przystani Stanów Zjednoczonych umożliwia ingerencję amerykańskich organów władz publicznych w prawa podstawowe i prywatności obywateli Unii Europejskiej. Z tego też powodu uznał, że irlandzki organ ochrony danych osobowych jest zobowiązany do zbadania skargi skarżącego M. Schremsa z wszelką wymaganą starannością i - po przeprowadzeniu dochodzenia - do wydania decyzji, czy należy zawiesić przekazywanie danych europejskich użytkowników Facebooka do USA z tego względu, że państwo to nie zapewnia odpowiedniego stopnia ochrony danych osobowych.

Zdaniem Mirosława Wróblewskiego, Dyrektora Zespołu Prawa Konstytucyjnego, Międzynarodowego i Europejskiego w Biurze RPO, „wyrok Trybunału Sprawiedliwości ma ogromne znaczenie dla ochrony prywatności użytkowników Internetu w całej Unii Europejskiej. Trzeba podkreślić, że Trybunał z uwagi na wiadomości o masowej inwigilacji przez amerykańskie służby specjalne uznał, że uregulowania pozwalające organom publicznym na uzyskanie dostępu do treści wiadomości elektronicznych są sprzeczne z samą istotą podstawowego prawa do poszanowania życia prywatnego. Brak możliwości skorzystania przez osoby inwigilowane z jakichkolwiek środków prawnych narusza zaś zasadniczą istotę prawa do skutecznej ochrony sądowej. Trybunał Sprawiedliwości zobowiązał zatem krajowe organy ochrony danych osobowych do badania każdego takiego przypadku przekazywania danych i wydawania stosownych decyzji. Warto także dodać, że Trybunał Sprawiedliwości oparł swoją decyzję w znacznej mierze na Karcie praw podstawowych Unii Europejskiej, która po raz kolejny wykazała w ten sposób swą skuteczność w ochronie praw podstawowych".

ZASTRZEŻENIA RPO WS. KONTROLI OPERACYJNEJ SŁUŻB

data: 2015-09-21

W związku z przygotowywaną nowelizacją przepisów dotyczących przeprowadzania kontroli operacyjnej Rzecznik Praw Obywatelskich zgłosił szereg wątpliwości i uwag. Wystąpieniu do Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych prosi o podjęcie działań mających na celu realizację wyroku Trybunału Konstytucyjnego z dnia 14 lica 2014 r. (sygn. akt K 23/11) oraz uwzględnienie wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r. i postanowień zawartych w Karcie Praw Podstawowych Unii Europejskiej. Swoje wystąpienie RPO skierował również do przewodniczących Komisji Praw Człowieka, Praworządności i Petycji oraz Komisji Ustawodawczej Senatu RP.

Zdaniem Rzecznika, projektowane rozwiązania nie gwarantują odpowiedniego przestrzegania praw i wolności człowieka i obywatela określonych we wskazanych orzeczeniach oraz aktach prawnych. W tej sprawie do RPO apelowało wiele organizacji pozarządowych, jak również Przewodniczący Naczelnej Rady Adwokackiej. Zastrzeżenia zgłaszał także Generalny Inspektor Ochrony Danych Osobowych.

W opinii Rzecznika, przygotowywana nowelizacja nie stwarza wystarczających gwarancji ochrony prywatności i tajemnicy komunikowania się. Zarzut ten dotyczy przede wszystkim braku precyzyjnego sformułowania przypadków, zakresu i sposobów ingerencji służb w konstytucyjne prawa i wolności. Ponadto, ustawodawca nie przewidział obowiązku informowania osób objętych kontrolą operacyjną – już po jej zakończeniu – że została ona przeprowadzona, choć taki obowiązek wynika z postanowienia sygnalizacyjnego Trybunału Konstytucyjnego z dnia 25 stycznia 2006 r. (sygn. akt S 2/06). Nieprecyzyjnie sformułowano również przepisy dotyczące czasu przetwarzania danych telekomunikacyjnych. Rzecznik podzielił też wątpliwości Naczelnej Rady Adwokackiej dotyczące upoważnienia funkcjonariuszy służb do dokonywania oceny, czy materiał zgromadzony w ramach kontroli operacyjnej zawiera dane objęte tajemnicą adwokacką, a także do przekazywania ich w takim przypadku prokuratorowi. Ponadto zdaniem RPO, powierzenie sądom okręgowym funkcji niezależnego organu sprawującego kontrolę nad sposobem przetwarzania przez służby np. danych telekomunikacyjnych sprawi, że mechanizm ten będzie nieefektywny. Także w opinii Krajowej Rady Sądownictwa, może mieć to negatywny wpływ na sprawność postępowania w sprawach karnych.

Jednocześnie, w związku ze zbliżającym się terminem wejścia w życie wskazanego wyroku Trybunału Konstytucyjnego, Rzecznik Praw Obywatelskich zaapelował o pilne uchwalenie przygotowywanej nowelizacji, w której uwzględnione zostaną rozwiązania zasygnalizowanych w wystąpieniach problemów.

RZECZNIK PRAW OBYWATELSKICH