Wytyczne 2/2023 w sprawie technicznego zakresu stosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej

Wersja 2.0

Przyjęte 7 października 2024 r.

Historia wersji

Wersja 1.0	14 listopada 2023 r.	Przyjęcie wytycznych do konsultacji publicznych
Wersja 2.0	7 października 2024 r.	Przyjęcie wytycznych po konsultacjach publicznych

Streszczenie

W niniejszych wytycznych EROD odnosi się do zastosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej do różnych rozwiązań technicznych. Niniejsze wytyczne stanowią rozwinięcie opinii 9/2014 Grupy Roboczej Art. 29 w sprawie zastosowania dyrektywy o prywatności i łączności elektronicznej do pobierania cyfrowych „odcisków palców" urządzeń i mają na celu zapewnienie jasnego zrozumienia operacji technicznych objętych art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

Pojawienie się nowych metod śledzenia, które mają zastąpić istniejące narzędzia śledzące (na przykład pliki cookie z powodu zaprzestania obsługi plików cookie stron trzecich przez niektórych dostawców przeglądarek) i stworzyć nowe modele biznesowe, stało się kluczowym problemem dotyczącym ochrony danych. Chociaż stosowanie art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej jest dobrze ugruntowane i wdrożone w przypadku niektórych technologii śledzenia, takich jak pliki cookie, istnieje potrzeba rozwiania niejasności związanych ze stosowaniem tego przepisu do nowych narzędzi śledzących.

Wytyczne określają trzy kluczowe elementy zastosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej (sekcja 2.1), a mianowicie „informacje", „wyposażenie urządzenia końcowego abonenta lub użytkownika", „przechowywanie i uzyskiwanie dostępu do informacji" oraz „przechowywanie informacji". Wytyczne zawierają ponadto szczegółową analizę każdego elementu (sekcja 2.2–2.6).

W sekcji 3 analiza ta jest stosowana do niewyczerpującej listy przypadków użycia reprezentujących powszechne techniki, a mianowicie:

- śledzenie adresów URL i pikseli;
- lokalne przetwarzanie danych;
- śledzenie wyłącznie na podstawie adresu IP;
- okresowe i pośrednie raportowanie internetu rzeczy (IoT);
- niepowtarzalny identyfikator.

Spis treści

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. e) 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 (zwanego dalej „RODO”),

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 15 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, zmienionej dyrektywą 2009/136/WE (zwanej dalej „dyrektywą o prywatności i łączności elektronicznej”

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZE WYTYCZNE:

1 WPROWADZENIE

1. Zgodnie z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej *przechowywanie informacji lub uzyskanie dostępu do informacji przechowanej na urządzeniu końcowym abonenta lub użytkownika* jest dozwolone wyłącznie na podstawie zgody lub konieczności w określonych celach, o których mowa w tym artykule. Jak przypomniano w motywie 24 dyrektywy o prywatności i łączności elektronicznej[2], celem tego przepisu jest ochrona urządzeń końcowych użytkowników, ponieważ są one częścią ich sfery prywatnej. Z brzmienia tego artykułu wynika, że art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej ma zastosowanie nie tylko do plików cookie, lecz również do „podobnych technologii”. Obecnie nie istnieje jednak kompleksowy wykaz operacji technicznych objętych zakresem art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

2. W opinii 9/2014 Grupa Robocza Art. 29 w sprawie zastosowania dyrektywy o prywatności i łączności elektronicznej do pobierania cyfrowych „odcisków palców” urządzeń (zwanej dalej „opinią 9/2014 Grupy Roboczej Art. 29”) wyjaśniła już, że pobieranie odcisków palców wchodzi w zakres techniczny art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej[3], ale ze względu na nowe postępy technologiczne potrzebne są dalsze wytyczne w odniesieniu do obecnie stosowanych technik śledzenia. W ciągu ostatnich dziesięciu lat krajobraz techniczny ulegał zmianom wraz z coraz częstszym

[1] Odniesienia do „państw członkowskich” w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG”.

[2] „Wyposażenie urządzeń końcowych użytkowników sieci łączności elektronicznej oraz informacje przechowywane na tych urządzeniach stanowią część prywatnej sfery użytkowników podlegającej ochronie na mocy Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Programy określane mianem spyware, błędy sieciowe, ukryte identyfikatory i inne podobne narzędzia mogą się znaleźć w terminalu użytkownika bez jego wiedzy w celu uzyskania dostępu do informacji, przechowania ukrytych informacji lub śledzenia czynności użytkownika i mogą w poważny sposób naruszyć jego prywatność. Stosowanie takich narzędzi powinno być dozwolone wyłącznie dla uzasadnionych celów, po powiadomieniu zainteresowanych użytkowników.”

[3] Opinia 9/2014 Grupy Roboczej Art. 29, s. 11.

korzystaniem z identyfikatorów wbudowanych w systemy operacyjne, a także tworzeniem nowych narzędzi umożliwiających przechowywanie informacji na urządzeniach końcowych.

3. Niejasności dotyczące zakresu stosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej zachęcają do wdrażania alternatywnych rozwiązań umożliwiających śledzenie użytkowników internetu i tworzą tendencje do omijania obowiązków prawnych przewidzianych w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Wszystkie takie sytuacje budzą obawy i wymagają dodatkowej analizy w celu uzupełnienia wcześniejszych wytycznych EROD.

4. Celem niniejszych wytycznych jest przeprowadzenie analizy technicznej zakresu stosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, a mianowicie wyjaśnienie, co pod względem technicznym obejmuje wyrażenie *w celu przechowywania informacji lub uzyskania dostępu do informacji przechowanej na urządzeniu końcowym abonenta lub użytkownika*. Niniejsze wytyczne nie odnoszą się do okoliczności, w których operacja przetwarzania może podlegać wyłączeniom z wymogu uzyskania zgody przewidzianym w dyrektywie o prywatności i łączności elektronicznej[4], ponieważ okoliczności te powinny być analizowane indywidualnie dla każdego przypadku, biorąc pod uwagę transpozycje w odpowiednich państwach członkowskich oraz wytyczne wydane przez właściwe organy krajowe.

5. Niewyczerpujący wykaz konkretnych przypadków użycia zostanie przeanalizowany w ostatniej części niniejszych wytycznych.

2 ANALIZA

2.1 Kluczowe elementy stosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej

6. Art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej ma zastosowanie, jeżeli:

   a. **KRYTERIUM A:** przeprowadzane operacje dotyczą *informacji*. Należy zauważyć, że użytym terminem nie są „dane osobowe", lecz „informacje".

   b. **KRYTERIUM B:** wykonywane operacje obejmują *urządzenie końcowe* abonenta lub użytkownika (B.1), co oznacza konieczność oceny pojęcia *publicznej sieci łączności* (B.2).

   c. **KRYTERIUM C** przeprowadzone operacje rzeczywiście stanowią *przechowywanie* (C.1) lub *uzyskanie dostępu* (C.2). Te dwa pojęcia można badać niezależnie, jak przypomniano w opinii 9/2014 Grupy Roboczej Art. 29: *Zastosowanie słów „przechowanie lub uzyskanie dostępu" wskazuje na to, że przechowywanie i uzyskanie dostępu nie musi odbywać się w ramach tego samego komunikatu i nie musi go wykonywać ta sama osoba*[5].

W celu ułatwienia czytelności podmiot uzyskujący dostęp do informacji przechowywanych na urządzeniu końcowym użytkownika będzie dalej określany jako „podmiot uzyskujący dostęp".

[4] Zgodnie z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej: *Nie stanowi to przeszkody dla technicznego przechowywania danych lub dostępu do danych jedynie w celu wykonania lub ułatwiania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub gdy jest to szczególnie niezbędne w celu dostarczania usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika.*

[5] Opinia 9/2014 Grupy Roboczej Art. 29, s. 8.

2.2 Pojęcie „informacji” – Kryterium A

7. Jak określono w KRYTERIUM A, niniejsza sekcja zawiera szczegółowe informacje na temat tego, co obejmuje pojęcie „informacji”. Wybór terminu „informacje”, obejmującego szerszą kategorię niż samo pojęcie danych osobowych, wiąże się z zakresem dyrektywy o prywatności i łączności elektronicznej.

8. Celem art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej jest ochrona sfery prywatnej użytkowników, jak stwierdzono w motywie 24: *Wyposażenie urządzeń końcowych użytkowników sieci łączności elektronicznej oraz informacje przechowywane na tych urządzeniach stanowią część prywatnej sfery użytkowników podlegającej ochronie na mocy Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*. Jest ona również chroniona przez art. 7 Karty praw podstawowych Unii Europejskiej.

9. W rzeczywistości scenariusze, które naruszają tę sferę prywatną nawet bez angażowania jakichkolwiek danych osobowych, są wyraźnie objęte brzmieniem art. 5 ust. 3 i motywu 24 dyrektywy o prywatności i łączności elektronicznej, np. przechowywanie wirusów na urządzeniu końcowym użytkownika. Pokazuje to, że definicja terminu „informacja” nie powinna ograniczać się do właściwości bycia powiązaną ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną.

10. Zostało to potwierdzone przez Trybunał Sprawiedliwości UE: *Ochrona ta ma zastosowanie do wszelkich informacji przechowywanych w takich urządzeniach końcowych, niezależnie od tego, czy są to dane osobowe, i ma na celu w szczególności, jak stwierdzono w tym samym motywie, ochronę użytkowników przed ryzykiem wprowadzenia ukrytych identyfikatorów lub innych podobnych narzędzi do urządzeń końcowych użytkowników bez ich wiedzy*[6].

11. Kwestie dotyczące tego, czy pochodzenie tych informacji i powody, dla których są one przechowywane na urządzeniu końcowym, powinny być brane pod uwagę przy ocenie możliwości zastosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, zostały wcześniej wyjaśnione. Na przykład w opinii 9/2014 Grupy Roboczej Art. 29: *Niewłaściwa jest interpretacja, zgodnie z którą oznacza to, że osoba trzecia nie potrzebuje zgody na uzyskanie dostępu do tych informacji tylko dlatego, że ich nie przechowywała. Wymóg uzyskania zgody ma zastosowanie również w przypadku, gdy uzyskuje się dostęp do wartości tylko do odczytu (np. żądanie adresu MAC interfejsu sieciowego za pośrednictwem systemu operacyjnego interfejsu programowania aplikacji)*[7].

12. Podsumowując, pojęcie informacji obejmuje zarówno dane nieosobowe, jak i dane osobowe, niezależnie od tego, w jaki sposób dane te zostały zapisane i przez kogo, tj. czy przez podmiot zewnętrzny (również inne podmioty niż ten, który ma do nich dostęp), przez użytkownika, przez producenta, czy w jakimkolwiek innym scenariuszu.

2.3 Pojęcie „urządzenia końcowego abonenta lub użytkownika” – Kryterium B.1

13. Podstawę niniejszej sekcji stanowi definicja zastosowana w dyrektywie 2008/63/WE i przywołana w art. 2 dyrektywy (UE) 2018/1972, gdzie „urządzenie końcowe” zdefiniowano jako: *urządzenie bezpośrednio lub pośrednio podłączone do interfejsu publicznej sieci telekomunikacyjnej w celu przesyłania, przetwarzania lub odbierania informacji; w obydwu przypadkach (połączenia bezpośredniego lub pośredniego), połączenie może być dokonane za pomocą przewodu, światłowodu*

[6] Wyrok Trybunału Sprawiedliwości z dnia 1 października 2019 r., Planet 49, sprawa C-673/17, ECLI:EU:C:2019:801, pkt 70.
[7] Opinia 9/2014 Grupy Roboczej Art. 29, s. 8.

lub elektromagnetycznie; połączenie jest pośrednie, jeżeli urządzenie jest umieszczone między końcowym urządzeniem telekomunikacyjnym a interfejsem sieci[8].

14. Motyw 24 dyrektywy o prywatności i łączności elektronicznej zapewnia jasne zrozumienie roli urządzeń końcowych w zakresie ochrony oferowanej przez art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Dyrektywa o prywatności i łączności elektronicznej chroni prywatność użytkowników nie tylko w odniesieniu do poufności ich informacji, ale również poprzez zabezpieczenie integralności urządzenia końcowego użytkownika. Takie rozumienie będzie stanowiło podstawę interpretacji pojęcia urządzenia końcowego w niniejszych wytycznych.

15. Art. 3 dyrektywy o prywatności i łączności elektronicznej stanowi, że dyrektywę tę stosuje się do przetwarzania danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności. Oznacza to, że urządzenie powinno nadawać się do użytku w związku z taką usługą i że, aby mogło zostać uznane za urządzenie końcowe, powinno być podłączone lub możliwe do podłączenia[9] do interfejsu publicznej sieci łączności. EROD zauważa, że zmiany wprowadzone w 2009 r.[10] w tekście art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej rozszerzyły ochronę urządzeń końcowych poprzez usunięcie odniesienia do „korzystania z sieci łączności elektronicznej" jako sposobu przechowywania informacji lub uzyskiwania dostępu do informacji przechowywanych na urządzeniach końcowych. W związku z tym, o ile urządzenie posiada interfejs sieciowy, który umożliwia mu połączenie (nawet jeśli takie połączenie nie istnieje), art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej ma zastosowanie do każdego podmiotu, który będzie przechowywał i uzyskiwał dostęp do informacji już przechowywanych na urządzeniu końcowym, niezależnie od sposobu dostępu do urządzenia końcowego oraz od tego, czy jest on podłączony do sieci, czy też od niej odłączony.

16. Urządzenia stanowiące część publicznej sieci łączności elektronicznej nie będą uznawane za urządzenie końcowe na mocy art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej[11].

17. Urządzenie końcowe może składać się z dowolnej liczby pojedynczych elementów sprzętowych, które razem tworzą urządzenie końcowe. Może to przybrać postać fizycznie zamkniętego urządzenia, w którym znajdują się wszystkie monitory, urządzenia przetwarzające, urządzenia pamięci masowej i sprzęt peryferyjny (na przykład: smartfony, laptopy, przyłączone do sieci urządzenie pamięciowe, samochody podłączone do sieci lub telewizory podłączone do sieci, inteligentne okulary).

18. Dyrektywa o prywatności i łączności elektronicznej uznaje, że ochrona poufności informacji przechowywanych na urządzeniu końcowym użytkownika i integralności urządzenia końcowego użytkownika nie ogranicza się do ochrony sfery prywatnej osób fizycznych, ale dotyczy również prawa

[8] Dyrektywa Komisji 2008/63/WE z dnia 20 czerwca 2008 r. w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych (wersja skodyfikowana) art. 1 ust. 1.

[9] Oznacza to posiadanie technicznych możliwości połączenia z siecią, nawet jeśli to połączenie nie jest obecnie dostępne.

[10] Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Tekst mający znaczenie dla EOG), Dz.U. L 337 z 18.12.2009, art. 2 ust. 5 i motyw 65.

[11] Aby określić ograniczenia sieci w różnych kontekstach, należy zapoznać się z wytycznymi BEREC dotyczącymi wspólnych podejść do identyfikacji punktu końcowego sieci w różnych topologiach sieci (BoR (20) 46).

do poszanowania ich korespondencji lub prawnie uzasadnionych interesów osób prawnych[12]. W związku z tym urządzenie końcowe, który umożliwia prowadzenie tej korespondencji i prawnie uzasadnionych interesów osób prawnych, jest chronione na mocy art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

19. Użytkownik lub abonent może być właścicielem lub najemcą urządzenia końcowego lub w inny sposób może być w niego wyposażony. Z tego samego urządzenia końcowego może korzystać wielu użytkowników lub abonentów.

20. Ochronę tę gwarantuje urządzeniu końcowemu użytkownika lub abonenta dyrektywa o prywatności i łączności elektronicznej, a ocena ta nie jest ona zależna od tego, czy użytkownik skonfigurował środek dostępu (np. czy to on zainicjował łączność elektroniczną), ani nawet od tego, czy użytkownik jest świadomy istnienia takiego środka dostępu.

2.4 Pojęcie „publicznej sieci łączności" – Kryterium B.2

21. Ponieważ sytuacja regulowana przez dyrektywę o prywatności i łączności elektronicznej jest związana z *dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności we Wspólnocie*[13], a definicja urządzenia końcowego wyraźnie wymienia pojęcie *publicznej sieci łączności*, kluczowe jest wyjaśnienie tego pojęcia w celu określenia kontekstu, w którym stosuje się art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

22. Pojęcie sieci łączności elektronicznej nie jest zdefiniowane w samej dyrektywie o prywatności i łączności elektronicznej. Do tej koncepcji odniesiono się pierwotnie w dyrektywie 2002/21/WE (dyrektywa ramowa) w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej[14], zastąpionej następnie art. 2 ust. 1 dyrektywy 2018/1972 (Europejski kodeks łączności elektronicznej). Teraz brzmi ona następująco:

> *„sieć łączności elektronicznej" oznacza systemy transmisyjne, niezależnie do tego, czy opierają się na stałej infrastrukturze lub scentralizowanym zarządzaniu zasobami, oraz, w stosownych przypadkach, urządzenia przełączające lub routingowe oraz inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają przekazywanie sygnałów przewodowo, za pomocą radia, środków optycznych lub innych rozwiązań wykorzystujących fale, w tym sieci satelitarnych, stacjonarnych (komutowanych i pakietowych, w tym internetu) i sieci ruchomych, elektroenergetycznych systemów kablowych, w zakresie, w jakim są one wykorzystywane do przekazywania sygnałów, w sieciach nadawania radiowego i telewizyjnego oraz sieciach telewizji kablowej, niezależnie od rodzaju przekazywanej informacji.*[15]

23. Definicja ta jest neutralna w odniesieniu do technologii transmisji. Zgodnie z tą definicją sieć łączności elektronicznej, to dowolny system sieciowy umożliwiający transmisję sygnałów elektronicznych pomiędzy swoimi węzłami, niezależnie od używanego sprzętu i protokołów.

[12] W rzeczy samej, jak przypomniano w art. 2 ust. 13 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej, użytkownikiem może być osoba fizyczna lub prawna.

[13] Art. 3 dyrektywy o prywatności i łączności elektronicznej.

[14] Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa)

[15] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Tekst mający znaczenie dla EOG), art. 2 ust. 1.

24. Pojęcie sieci łączności elektronicznej w rozumieniu dyrektywy 2018/1972 nie zależy od publicznego lub prywatnego charakteru infrastruktury ani od sposobu, w jaki sieć jest wdrażana lub zarządzana (*niezależnie do tego, czy opiera się na stałej infrastrukturze lub scentralizowanym zarządzaniu zasobami*[16]). W związku z tym definicja sieci łączności elektronicznej w art. 2 dyrektywy 2018/1972 jest na tyle szeroka, że obejmuje każdy rodzaj infrastruktury. Obejmuje to sieci zarządzane lub nie zarządzane przez operatora, sieci współzarządzane przez grupę operatorów, a nawet sieci ad-hoc, w których urządzenie końcowe może dynamicznie łączyć się z siecią innych urządzeń końcowych lub odłączać się od niej, korzystając z protokołów transmisji krótkiego zasięgu.

25. Ta definicja sieci nie nakłada żadnych ograniczeń na liczbę urządzeń końcowych obecnych w sieci w dowolnym momencie. Niektóre schematy sieciowe opierają się na węzłach przekazujących informacje w sposób ad-hoc do węzłów obecnie połączonych[17] a w pewnym momencie może się zdarzyć, że komunikują się ze sobą tylko dwa węzły równorzędne. Takie przypadki mieszczą się w ogólnym zakresie dyrektywy o prywatności i łączności elektronicznej, pod warunkiem, że protokół sieciowy pozwala na dalsze włączanie elementów równorzędnych.

26. Publiczna dostępność sieci łączności jest konieczna, aby urządzenie można było uznać za urządzenie końcowe, a w konsekwencji, aby można było zastosować art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Należy zauważyć, że fakt, iż sieć jest udostępniana ograniczonej grupie odbiorców (na przykład abonentom, niezależnie od tego, czy uiszczają opłaty, czy nie, z zastrzeżeniem warunków kwalifikowalności), nie czyni takiej sieci prywatną[18].

2.5 Pojęcie „uzyskania dostępu” – kryterium C.1

27. Aby poprawnie sformułować pojęcie „uzyskania dostępu”, należy wziąć pod uwagę zakres stosowania dyrektywy o prywatności i łączności elektronicznej, o którym mowa w jej art. 1: *zapewnienie równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej*.

28. W skrócie, dyrektywa o prywatności i łączności elektronicznej jest instrumentem prawnym chroniącym prywatność, mającym na celu ochronę poufności komunikacji i integralności urządzeń. W motywie 24 dyrektywy o prywatności i łączności elektronicznej wyjaśniono, że w przypadku osób fizycznych urządzenia końcowe użytkowników stanowią część ich sfery prywatnej oraz że dostęp do przechowywanych na nich informacji bez ich wiedzy może poważnie naruszyć ich prywatność.

29. Osoby prawne są również chronione przez dyrektywę o prywatności i łączności elektronicznej[19]. Dlatego też pojęcie „uzyskania dostępu” w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej należy interpretować w sposób chroniący te prawa przed naruszeniem przez osoby trzecie.

30. Przechowywanie informacji lub uzyskiwanie dostępu mogą być niezależnymi operacjami i mogą być wykonywane przez niezależne podmioty. Przechowywanie informacji i dostęp do informacji już

[16] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Tekst mający znaczenie dla EOG), art. 2 ust. 1.

[17] Na przykład w kontekście schematu sieciowego odpornego na opóźnienia, który wdraża „techniki przechowywania i przekazywania”, takie jak projekt open source Briar.

[18] Dalsze analizy dotyczące identyfikacji publicznych sieci łączności można znaleźć w wytycznych BEREC w sprawie wdrożenia rozporządzenia w sprawie otwartego internetu (BoR (20) 112).

[19] Motyw 26 dyrektywy o prywatności i łączności elektronicznej, zob. pkt 17 powyżej.

przechowywanych nie muszą występować jednocześnie, aby art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej miał zastosowanie.

31. Jak zauważono w opinii 9/2014 Grupy Roboczej Art. 29: *Zastosowanie słów „przechowywanie lub uzyskanie dostępu" wskazuje na to, że przechowywanie i uzyskanie dostępu nie musi odbywać się w ramach tego samego komunikatu i nie musi go wykonywać ta sama osoba. Informacje przechowywane przez jedną osobę (w tym dane przechowywane przez użytkownika lub producenta urządzenia), do których później uzyskuje dostęp inna osoba są zatem objęte zakresem art. 5 ust. 3*[20]. W związku z tym nie wprowadzono żadnych ograniczeń co do pochodzenia informacji na temat urządzenia końcowego użytkownika, aby miało zastosowanie pojęcie dostępu.

32. W każdym przypadku, gdy podmiot podejmuje działania mające na celu uzyskanie dostępu do informacji przechowywanych na urządzeniu końcowym, zastosowanie ma art.5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Zwykle wiąże się to z koniecznością proaktywnego wysłania przez podmiot uzyskujący dostęp określonych instrukcji do urządzenia końcowego w celu otrzymania z powrotem żądanych docelowych informacji. Dotyczy to na przykład plików cookie, w przypadku których podmiot uzyskujący dostęp wydaje urządzeniu końcowemu polecenie proaktywnego wysyłania informacji przy każdym kolejnym wywołaniu protokołu Hypertext Transfer Protocol (HTTP).

33. Podobnie jest w przypadku, gdy podmiot uzyskujący dostęp dystrybuuje oprogramowanie na urządzeniu końcowym użytkownika, które jest przechowywane, a następnie proaktywnie wywołuje punkt końcowy interfejsu programowania aplikacji („API") za pośrednictwem sieci. Dodatkowymi przykładami mogą być kod JavaScript, w którym podmiot uzyskujący dostęp wydaje przeglądarce użytkownika polecenie wysłania asynchronicznych żądań zawierających określone informacje. Taki dostęp wyraźnie wchodzi w zakres art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, ponieważ podmiot uzyskujący dostęp wyraźnie nakazuje urządzeniu końcowemu przesłanie informacji.

34. W niektórych przypadkach podmiot wydający urządzeniu końcowemu polecenie odesłania żądanych danych i podmiot odbierający informacje mogą nie być tym samym podmiotem. Może to wynikać z udostępnienia lub wykorzystania wspólnego mechanizmu pomiędzy tymi dwoma podmiotami. Polecenie urządzeniu wysłania już zapisanych informacji (np. za pomocą protokołu lub zestawu SDK[21], które zakładają proaktywne wysyłanie informacji przez urządzenie końcowe) umożliwia włamanie się do urządzenia końcowego, dlatego taki dostęp powoduje zastosowanie art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Jak zauważono w opinii 09/2014 Grupy Roboczej Art. 29 może to mieć miejsce, gdy strona internetowa nakazuje urządzeniu końcowemu wysyłanie informacji do zewnętrznych usług reklamowych poprzez włączenie piksela śledzącego[22]. Ten przypadek użycia omówiono bardziej szczegółowo w sekcji 3.1.

2.6 Pojęcia „przechowywania informacji" i „przechowywanych informacji" – kryterium C.2

35. Przechowywanie informacji w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej odnosi się do umieszczenia informacji na fizycznym elektronicznym nośniku danych, który jest częścią urządzenia końcowego użytkownika lub abonenta[23].

[20] Opinia 9/2014 Grupy Roboczej Art. 29, s. 8.
[21] SDK („zestaw oprogramowania") to zestaw narzędzi do opracowywania oprogramowania udostępnianych w celu ułatwienia tworzenia oprogramowania aplikacyjnego.
[22] Opinia 9/2014 Grupy Roboczej Art. 29, s. 9.
[23] Jak określono w sekcji 2.3 niniejszych wytycznych.

36. Z reguły informacje nie są przechowywane na urządzeniu końcowym użytkownika lub abonenta poprzez bezpośredni dostęp do pamięci urządzenia przez osobę trzecią, lecz poprzez instrukcje dla oprogramowania na urządzeniu końcowym w celu wygenerowania określonych informacji. Przechowywanie realizowane na podstawie takich instrukcji uważa się za zainicjowane bezpośrednio przez drugą stronę. Obejmuje to korzystanie z ustalonych protokołów, takich jak przechowywanie plików cookie przeglądarki, jak również z dedykowanego oprogramowania, niezależnie od tego, kto stworzył lub zainstalował protokoły lub oprogramowanie na urządzeniu końcowym.

37. Dyrektywa o prywatności i łączności elektronicznej nie nakłada żadnego górnego ani dolnego limitu na czas, przez jaki informacje muszą znajdować się na nośniku pamięci, aby można je było uznać za przechowywane, ani nie ma górnego ani dolnego limitu na ilość przechowywanych informacji.

38. Pojęcie przechowywania nie zależy także od rodzaju nośnika, na którym przechowywane są informacje. Typowymi przykładami są dyski twarde („HDD"), dyski półprzewodnikowe („SSD"), elektrycznie kasowalna i programowalna pamięć tylko do odczytu („EEPROM") i pamięć o swobodnym dostępie („RAM"), ale mniej typowe scenariusze obejmujące nośniki, takie jak taśma magnetyczna lub pamięć podręczna procesora („CPU"), nie są wyłączone z zakresu stosowania. Nośnik pamięci masowej może być podłączony wewnętrznie (np. przez złącze SATA), zewnętrznie (np. przez złącze USB).

39. „Przechowywane informacje" oznaczają informacje już istniejące w urządzeniu końcowym, niezależnie od źródła lub charakteru tych informacji. Obejmuje to wszelkie wyniki przechowywania informacji w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, jak opisano powyżej (zarówno przez tę samą stronę, która później uzyska dostęp, jak i przez inną stronę trzecią). Ponadto są to też wyniki procesów przechowywania informacji wykraczające poza zakres art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, takie jak: przechowywanie na urządzeniu końcowym przez samego użytkownika lub abonenta lub przez producenta sprzętu (takie jak adresy MAC kontrolerów interfejsu sieciowego), czujniki zintegrowane z urządzeniem końcowym lub procesy i programy wykonywane na urządzeniu końcowym, które mogą, ale nie muszą, generować informacje zależne od przechowywanych informacji lub z nich pochodzące.

3 PRZYPADKI UŻYCIA

40. Jak wskazano we wstępie do niniejszych wytycznych[24], nie analizują one stosowania wyłączeń obowiązku uzyskania zgody przewidzianych w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. EROD przypomina, że we wszystkich przypadkach, w których dochodzi do przechowywania informacji lub uzyskiwania dostępu do informacji już przechowywanych, należy ocenić, czy potrzebna jest zgoda, czy też może mieć zastosowanie wyłączenie na mocy art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Należy zatem wziąć pod uwagę wyłączenia w przypadku ich zastosowania, w powiązaniu z niniejszą analizą techniczną.

41. Bez uszczerbku dla konkretnego kontekstu, w którym można stosować kategorie techniczne niezbędne do zakwalifikowania, czy art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej ma zastosowanie, możliwe jest określenie, w sposób niewyczerpujący, szerokich kategorii identyfikatorów i informacji, które są powszechnie używane i mogą podlegać stosowaniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

42. Łączność sieciowa zazwyczaj opiera się na modelu warstwowym, który wymaga użycia identyfikatorów, aby umożliwić prawidłowe ustanowienie i przeprowadzenie łączności. Przekazywanie

[24] Zob. pkt 4 powyżej.

tych identyfikatorów zdalnym podmiotom odbywa się za pośrednictwem oprogramowania zgodnie z ustalonymi protokołami komunikacyjnymi. Jak wskazano powyżej, fakt, że podmiot odbierający może nie być podmiotem zlecającym przesłanie informacji, nie wyklucza zastosowania art. art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Może to dotyczyć identyfikatorów routingu, takich jak adres MAC lub IP urządzenia końcowego, ale także identyfikatorów sesji (SSRC, identyfikator Websocket) lub tokenów uwierzytelniających.

43. Podobnie protokół aplikacji może obejmować kilka mechanizmów dostarczających dane kontekstowe (takich jak nagłówek HTTP zawierający pole „accept" lub agent użytkownika), mechanizm buforowania (taki jak ETag[25]) lub inne funkcjonalności (jedną z nich są pliki cookie lub HSTS[26]). Poleganie na tych mechanizmach w celu gromadzenia informacji (na przykład w kontekście pobierania „odcisków palców"[27] lub śledzenia identyfikatorów zasobów) może również skutkować zastosowaniem art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

44. Z drugiej strony istnieją pewne konteksty, w których lokalne aplikacje zainstalowane na urządzeniu końcowym wykorzystują pewne informacje ściśle wewnątrz urządzenia końcowego, jak może mieć to miejsce w przypadku interfejsów API systemu smartfona (dostęp do kamery, mikrofonu, czujnika GPS, układu akceleratora, układu radiowego, dostęp do plików lokalnych, listy kontaktów, dostęp do identyfikatorów itp.). Może to dotyczyć również przeglądarek internetowych, które przetwarzają informacje przechowywane lub generowane w urządzeniu (takie jak pliki cookie, pamięć lokalna, WebSQL, a nawet informacje dostarczane przez samych użytkowników). Wykorzystanie takich informacji przez aplikację nie stanowiłoby „uzyskania dostępu do przechowywanych informacji" w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, o ile informacje nie opuszczają urządzenia, ale w przypadku uzyskania dostępu do tych informacji lub jakichkolwiek pochodnych tych informacji zastosowanie miałby art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

45. Ponadto w niektórych przypadkach elementy złośliwego oprogramowania są dystrybuowane przez podmioty, na przykład oprogramowanie do wydobywania kryptowalut lub, bardziej ogólnie, złośliwe oprogramowanie, wykorzystujące możliwości przetwarzania urządzenia końcowego z korzyścią dla podmiotu dystrybuującego. Dystrybucja wspomnianego złośliwego oprogramowania na urządzeniu końcowym użytkownika stanowiłaby „przechowywanie" w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Ponadto, gdyby oprogramowanie ustanowiło połączenie sieciowe w celu przesłania informacji na późniejszym etapie, stanowiłoby to „uzyskanie dostępu" w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

46. Poniżej przedstawiono szczegółową analizę dotyczącą podzbioru tych kategorii, które budzą szczególne zainteresowanie, czy to ze względu na ich powszechne stosowanie, czy też dlatego, że uzasadnione jest przeprowadzenie konkretnego badania dotyczącego okoliczności ich stosowania.

3.1 Śledzenie adresów URL i pikseli

47. Piksel śledzący to hiperłącze do zasobu, zazwyczaj pliku graficznego, osadzonego w treści, takiej jak strona internetowa lub wiadomość e-mail. Zazwyczaj piksel ten nie spełnia żadnego celu związanego z

[25] HTTP ETag to identyfikator umożliwiający wykonywanie żądań warunkowych w oparciu o poprawność danych klienta przechowywanych w pamięci podręcznej.
[26] Mechanizm HSTS (HTTP Strict Transport Security) umożliwia serwerom określenie, które zasoby zawsze powinny być żądane za pomocą połączeń HTTPS.
[27] Jak zauważono we wprowadzeniu, zob. opinia 9/2014 Grupy Roboczej Art. 29 w sprawie stosowania dyrektywy o prywatności i łączności elektronicznej do pobierania cyfrowych „odcisków palców" urządzeń

żądaną treścią; jego jedynym zadaniem jest automatyczne nawiązanie łączności pomiędzy klientem a hostem piksela, co w przeciwnym razie nie miałoby miejsca. Nie jest to jednak rozwiązanie systematyczne. Piksele śledzące można również tworzyć, dodając dodatkowe informacje do obrazów ładujących hiperłącza, które są istotne dla treści wyświetlanych użytkownikowi. Nawiązanie komunikacji powoduje przesłanie różnych informacji do hosta piksela, zależnie od konkretnego przypadku użycia.

48. W przypadku wiadomości e-mail nadawca może dodać piksel śledzący, aby wykryć, kiedy odbiorca przeczytał wiadomość. Piksele śledzące na stronach internetowych mogą łączyć się z podmiotem gromadzącym wiele takich żądań i w ten sposób umożliwiającym śledzenie zachowań użytkowników. Takie piksele śledzące mogą również zawierać dodatkowe identyfikatory, metadane lub treść stanowiącą część łącza. Właściciel strony internetowej może dodać te dane, prawdopodobnie związane z aktywnością użytkownika na tej stronie internetowej, co umożliwi generowanie raportów analitycznych dotyczących korzystania ze strony internetowej. Mogą być one również generowane dynamicznie poprzez logikę aplikacyjną po stronie klienta dostarczaną przez jednostkę.

49. Linki śledzące mogą działać w ten sam sposób, ale identyfikator jest dołączany do adresu strony internetowej. Gdy użytkownik odwiedza Uniform Resource Locator („URL"), docelowa strona internetowa ładuje żądany zasób, ale zbiera również identyfikator, który nie jest istotny w kontekście identyfikacji zasobu. Są one bardzo powszechnie wykorzystywane przez strony internetowe handlu elektronicznego w celu identyfikacji źródła ruchu przychodzącego. Na przykład takie strony internetowe mogą udostępniać partnerom śledzone linki do wykorzystania w ich domenach, dzięki czemu strona internetowa e-commerce wie, który z jej partnerów odpowiada za sprzedaż i wypłaca prowizję — praktyka ta znana jest jako marketing afiliacyjny.

50. Zarówno linki śledzące, jak i piksele śledzące można rozpowszechniać za pośrednictwem wielu kanałów, na przykład za pośrednictwem wiadomości e-mail, stron internetowych lub, w przypadku linków śledzących, nawet za pośrednictwem dowolnego systemu wiadomości tekstowych. Dystrybucja do urządzenia końcowego użytkownika stanowi przechowywanie, przynajmniej poprzez mechanizm buforowania oprogramowania po stronie klienta. W związku z tym zastosowanie ma art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, nawet jeżeli takie przechowywanie nie jest trwałe.

51. Dodanie informacji śledzących do adresów URL lub obrazów (pikseli) wysyłanych do użytkownika stanowi instrukcję dla urządzenia końcowego nakazującą odesłanie docelowych informacji (określonego identyfikatora). W przypadku pikseli śledzących tworzonych dynamicznie, instrukcję stanowi rozkład logiki aplikacyjnej (zwykle kodu JavaScript). W konsekwencji można uznać, że gromadzenie identyfikatorów dostarczonych za pośrednictwem takich mechanizmów śledzenia stanowi „uzyskanie dostępu" w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, a zatem ma zastosowanie również do tego kroku.

3.2 Lokalne przetwarzanie danych;

52. Niektóre technologie opierają się na lokalnym przetwarzaniu, które jest wykonywane za pomocą oprogramowania dystrybuowanego na urządzeniu końcowym użytkowników, gdzie informacje wygenerowane w wyniku lokalnego przetwarzania są następnie udostępniane wybranym podmiotom za pośrednictwem interfejsu API po stronie klienta. Może tak być na przykład w przypadku interfejsu API udostępnianego przez przeglądarkę internetową, gdzie lokalnie wygenerowane wyniki mogą być dostępne zdalnie.

53. Jeżeli w dowolnym momencie, na przykład w kodzie po stronie klienta, przetworzone informacje zostaną udostępnione osobie trzeciej, na przykład przesłane z powrotem przez sieć do serwera, taka

operacja (zlecona przez podmiot wytwarzający kod po stronie klienta rozpowszechniany na urządzeniu końcowym użytkownika) będzie stanowić „uzyskanie dostępu do informacji już przechowywanych". Fakt, że informacje te są opracowywane lokalnie, nie wyklucza stosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

3.3 Śledzenie wyłącznie na podstawie adresu IP

54. Niektórzy dostawcy opracowują rozwiązania, które polegają tylko na gromadzeniu jednego elementu, a mianowicie adresu IP, w celu śledzenia nawigacji[28] użytkownika, w niektórych przypadkach w wielu domenach. W tym kontekście art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej mógłby mieć zastosowanie, nawet jeśli polecenie udostępnienia adresu IP zostało wydane przez inny podmiot niż podmiot otrzymujący.

55. Uzyskanie dostępu do adresów IP spowodowałoby jednak zastosowanie art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej tylko w przypadkach, gdy informacje te pochodzą z urządzenia końcowego abonenta lub użytkownika. Choć nie dzieje się tak systematycznie (na przykład gdy aktywowany jest protokół CGNAT[29]), statyczny adres IPv4 wychodzący z routera użytkownika mieściłby się w tym przypadku, podobnie jak adresy IPv6, ponieważ są one częściowo definiowane przez hosta. Jeżeli podmiot nie jest w stanie zagwarantować, że adres IP nie pochodzi z urządzenia końcowego użytkownika lub abonenta, musi podjąć wszelkie kroki zgodnie z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

56. Chociaż niniejsze wytyczne nie analizują stosowania wyłączeń z obowiązku uzyskania zgody przewidzianych w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, należy raz jeszcze przypomnieć, że stosowalność tego artykułu nie oznacza, że regularnie zgoda musi zostać uzyskana. EROD przypomina zatem, że należy zawsze ocenić, czy konieczna jest zgoda, czy też można zastosować wyłączenie na podstawie art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej[30].

3.4 Okresowe i pośrednie raportowanie IoT

57. Urządzenia IoT (Internet rzeczy) nieustannie generują informacje, na przykład za pomocą czujników wbudowanych w urządzenie, które mogą lecz nie muszą być lokalnie wstępnie przetworzone. W wielu przypadkach informacje są udostępniane zdalnemu serwerowi, ale sposoby ich gromadzenia mogą być różne.

58. Niektóre urządzenia IoT łączą się bezpośrednio z publiczną siecią komunikacyjną za pomocą karty SIM. Inne mogą mieć pośrednie połączenie z publiczną siecią komunikacyjną, na przykład poprzez wykorzystanie Wi-Fi lub przekazywanie informacji do innego urządzenia za pomocą połączenia typu punkt-punkt (na przykład przez Bluetooth). Drugim urządzeniem może być na przykład smartfon lub dedykowana brama, która może lecz nie musi wstępnie przetworzyć informacje przed wysłaniem ich na serwer.

[28] Jest to element dodatkowy i niezależny od wykorzystania i funkcji adresu IP w celu ustanowienia i przekazywania lub transmisji podstawowych komunikatów technicznych, ani od faktu, że mogą to być lub mogą to nie być dane osobowe (w odniesieniu do analizy e-prywatności jest to „informacja").

[29] Dostawcy usług internetowych stosują NAT klasy operatorskiej (CGNAT) w celu maksymalnego wykorzystania ograniczonej przestrzeni adresów IP. CGNAT grupuje pewną liczbę subskrybentów pod tym samym publicznym adresem IP.

[30] Opinia 9/2014 Grupy Roboczej Art. 29 zawiera kilka przykładów sytuacji, w których zgoda może nie być konieczna.

59. Urządzenia IoT mogą otrzymać od producenta instrukcję, aby zawsze przesyłały strumieniowo zebrane informacje, ale najpierw przechowywały je lokalnie w pamięci podręcznej, np. do czasu nawiązania połączenia.

60. W każdym przypadku urządzenie IoT, jeśli jest podłączone (bezpośrednio lub pośrednio) do publicznej sieci komunikacyjnej, samo w sobie będzie uważane za urządzenie końcowe. Fakt, że informacje są przesyłane strumieniowo lub buforowane w celu okresowego raportowania, nie zmienia charakteru tych informacji. W obu sytuacjach zastosowanie miałby art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, ponieważ poprzez instrukcję kodu na urządzeniu IoT dotyczącą wysłania dynamicznie przechowywanych danych do zdalnego serwera następuje „uzyskanie dostępu".

3.5 Niepowtarzalny identyfikator

61. Powszechnie stosowanym przez przedsiębiorstwa narzędziem jest pojęcie „unikalnych identyfikatorów" lub „trwałych identyfikatorów". Takie identyfikatory mogą pochodzić z trwałych danych osobowych (imię i nazwisko, adres e-mail, numer telefonu itp.), które są haszowane na urządzeniu użytkownika, zbierane i udostępniane kilku administratorom w celu jednoznacznej identyfikacji osoby w różnych zbiorach danych (dane dotyczące użytkowania zbierane za pośrednictwem strony internetowej lub aplikacji, dane dotyczące zarządzania relacjami z klientami (CRM) związane z zakupami lub subskrypcją online lub offline itp.). W przypadku stron internetowych trwałe dane osobowe są zazwyczaj pozyskiwane w kontekście uwierzytelniania lub subskrypcji newsletterów.

62. Jak wskazano wcześniej, fakt, że informacje są wprowadzane przez użytkownika, nie wyklucza zastosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej w odniesieniu do przechowywania, ponieważ informacje te są tymczasowo przechowywane na urządzeniu końcowym przed ich zebraniem.

63. W kontekście gromadzenia „unikalnych identyfikatorów" na stronach internetowych lub w aplikacjach mobilnych podmiot gromadzący wydaje przeglądarce (poprzez dystrybucję kodu po stronie klienta) instrukcje dotyczące wysłania tych informacji. W takim przypadku następuje „uzyskanie dostępu" i zastosowanie ma art. 5 ust. dyrektywy o prywatności i łączności elektronicznej.