Richtsnoeren

Richtsnoeren 2/2023 over het technische topassingsgebied van artikel 5, lid 3, van de e-privacyrichtlijn

Versie 2.0

Aangenomen op 7 oktober 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Versiegeschiedenis

Versie 1.0	16 november 2023	Vaststelling van de richtsnoeren voor openbare raadpleging
Versie 2.0	3 oktober 2024	Vaststelling van de richtsnoeren na openbare raadpleging

Samenvatting

In deze richtsnoeren besteedt het EDPB aandacht aan de toepasselijkheid van artikel 5, lid 3, van de e-privacy-richtlijn op verschillende technische oplossingen. Deze richtsnoeren vormen een aanvulling op Advies 9/2014 van de Artikel 29-werkgroep over de toepassing van de e-privacyrichtlijn op device fingerprinting en hebben tot doel te verduidelijken welke technische verrichtingen onder artikel 5, lid 3, van de e-privacyrichtlijn vallen.

De opkomst van nieuwe trackingmethoden om zowel bestaande trackingtools te vervangen (bijvoorbeeld cookies, omdat sommige browserleveranciers cookies van derden niet langer ondersteunen) als nieuwe bedrijfsmodellen te creëren, is een belangrijk punt van zorg geworden op het gebied van gegevensbescherming. Hoewel de toepassing van artikel 5, lid 3, van de e-privacyrichtlijn sinds geruime tijd is afgebakend en algemene praktijk is voor bepaalde trackingtechnologieën zoals cookies, moeten onduidelijkheden in verband met de toepassing van de genoemde bepaling op nieuwe trackinginstrumenten worden opgehelderd.

In de richtsnoeren worden drie kernelementen genoemd voor de toepasselijkheid van artikel 5, lid 3, van de e-privacyrichtlijn (deel 2.1), namelijk “informatie”, “eindapparatuur van een abonnee of gebruiker” en “ het verkrijgen van toegang tot informatie”, “opslag van informatie” en “opgeslagen informatie”. De richtsnoeren bevatten voorts een gedetailleerde analyse van elk van deze elementen (afdeling 2.2-2.6).

In deel 3 wordt die analyse toegepast op een niet-uitputtende lijst van praktijksituaties die gemeenschappelijke technieken vertegenwoordigen, namelijk:

- URL- en pixeltracking
- Lokale verwerking
- Uitsluitend IP-gebaseerde tracking
- Verslaglegging over intermitterend en gemedieerd internet der dingen (IoT)
- Unieke identificatiecode

Inhoudsopgave

Het Europees Comité voor gegevensbescherming,

Gezien artikel 70, lid 1, punt e), van Verordening (EU) 2016/679/EU van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "AVG");

Gezien de EER-overeenkomst en met name bijlage XI en protocol 37 daarbij, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1];

Gezien artikel 15, lid 3, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, zoals gewijzigd bij Richtlijn 2009/136/EG (hierna "e-privacyrichtlijn" of "ePD"),

Gezien de artikelen 12 en 22 van zijn reglement van orde,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD.

1 INLEIDING

1. Volgens artikel 5, lid 3, ePD is *"de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker"* alleen toegestaan op voorwaarde van toestemming of noodzaak voor specifieke doeleinden die in dat artikel worden genoemd. Zoals in overweging 24 van de ePD[2] in herinnering wordt gebracht, heeft deze bepaling tot doel de eindapparatuur van de gebruikers te beschermen, aangezien zij deel uitmaken van de privésfeer van de gebruikers. Uit de bewoordingen van het artikel volgt dat artikel 5, lid 3, ePD niet uitsluitend van toepassing is op cookies, maar ook op soortgelijke technologieën. Momenteel bestaat er echter geen volledige lijst van de technische verrichtingen die onder artikel 5, lid 3, ePD vallen.

2. In Advies 9/2014 van de Groep gegevensbescherming artikel 29 (hierna "Werkgroep artikel 29" genoemd) over de toepassing van de e-privacyrichtlijn op device fingerprinting (hierna "Advies 9/2014 van de Werkgroep artikel 29" genoemd) is reeds verduidelijkt dat het nemen van digitale vingerafdrukken binnen het technische toepassingsgebied van artikel5, lid 3, ePD[3] valt, maar dat vanwege de nieuwe technologische vooruitgang verdere sturing nodig is met betrekking tot de momenteel waargenomen trackingtechnieken. Het technische landschap is het afgelopen decennium

[1] Alle verwijzingen in dit document naar "lidstaten" moeten worden gelezen als verwijzingen naar "EER-lidstaten",

[2] "Eindapparatuur van gebruikers van netwerken voor elektronische communicatie en in die apparatuur bewaarde informatie maken deel uit van de persoonlijke levenssfeer van de gebruikers die op grond van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden bescherming vereist. Zogeheten spionagesoftware, webtaps, verborgen identificatoren en andere soortgelijke programmatuur kunnen de terminal van de gebruiker zonder diens medeweten binnenkomen teneinde toegang tot informatie te krijgen, verborgen informatie op te slaan of de activiteiten van de gebruiker te traceren en kunnen ernstig inbreuk maken op de persoonlijke levenssfeer van die gebruikers. Het gebruik van die programmatuur dient alleen te worden toegestaan voor legitieme doeleinden met medeweten van de betrokken gebruikers."

[3] Advies 9/2014 van de Werkgroep artikel 29, blz. 12.

geëvolueerd, door het toenemende gebruik van in besturingssystemen ingebedde identificatoren en de creatie van nieuwe tools die de opslag van informatie in eindapparatuur mogelijk maken.

3. De onduidelijkheden over het toepassingsgebied van artikel 5, lid 3, ePD hebben stimulansen gecreëerd om alternatieve oplossingen voor tracking van internetgebruikers toe te passen en hebben geleid tot een tendens om de wettelijke verplichtingen van artikel 5, lid 3, ePD te omzeilen. Al deze situaties geven aanleiding tot bezorgdheid en vereisen een aanvullende analyse om de eerdere richtsnoeren van het EDPB aan te vullen.

4. Het doel van deze richtsnoeren is een technische analyse uit te voeren van het toepassingsgebied van artikel 5, lid 3, ePD, met name om te verduidelijken wat technisch gezien valt onder de zinsnede "*de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker*". In deze richtsnoeren wordt niet ingegaan op de omstandigheden waarin een verwerking kan vallen onder de uitzonderingen op het toestemmingsvereiste waarin de e-privacyrichtlijnvoorziet[4], aangezien deze omstandigheden per geval moeten worden geanalyseerd, rekening houdend met de relevante omzetting van de richtlijn in de lidstaten en de richtsnoeren van de nationale bevoegde autoriteiten.

5. In het laatste deel van deze richtsnoeren zal een niet-uitputtende lijst van specifieke praktijksituaties worden geanalyseerd.

2 ANALYSE

2.1 Kernelementen van de toepasselijkheid van artikel 5, lid 3, van de e-privacyrichtlijn

6. Artikel 5, lid 3, ePD is van toepassing indien:

   a. **CRITERIUM A:** de uitgevoerde verrichtingen hebben betrekking op "*informatie*". Opgemerkt moet worden dat de gebruikte term niet "persoonsgegevens" is, maar "informatie".

   b. **CRITERIUM B:** de uitgevoerde verrichtingen hebben betrekking op "*eindapparatuur*" van een abonnee of gebruiker (B.1), hetgeen impliceert dat het begrip *"openbaar communicatienetwerk*" (B.2) moet worden beoordeeld.

   c. **CRITERIUM C** de uitgevoerde verrichtingen bestaan inderdaad in "*opslag*" (C.1) of "*verkrijgen van toegang*" (C.2). Deze twee begrippen kunnen onafhankelijk van elkaar worden onderzocht, zoals in Advies 9/2014 van de Werkgroep artikel 29 in herinnering is gebracht: *"De termen ['opslag' en 'verkrijgen van toegang'] geven aan dat de opslag en toegang niet noodzakelijkerwijs binnen dezelfde communicatiestroom moeten plaatsvinden of door dezelfde partij moeten worden uitgevoerd"*[5].

   Met het oog op de leesbaarheid wordt de entiteit die toegang verkrijgt tot informatie die is opgeslagen in de eindapparatuur van de gebruiker hierna aangeduid als "toegang verkrijgende entiteit".

[4] Zoals vermeld in artikel 5, lid 3, ePD: "*Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert.*"

[5] Advies 9/2014 van de Werkgroep artikel 29, blz. 9.

2.2 Begrip "informatie" – Criterium A

7. Zoals is aangegeven in criterium A, wordt in dit deel nader toegelicht wat onder het begrip "informatie" valt. De keuze voor de term "informatie", die een ruimere categorie omvat dan het loutere begrip persoonsgegevens, houdt verband met het toepassingsgebied van de e-privacyrichtlijn.

8. Het doel van artikel 5, lid 3, ePD is de bescherming van de persoonlijke levenssfeer van de gebruikers, zoals vermeld in overweging 24 van de ePD: "*Eindapparatuur van gebruikers van netwerken voor elektronische communicatie en in die apparatuur bewaarde informatie maken deel uit van de persoonlijke levenssfeer van de gebruikers die op grond van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden bescherming vereist.*" De persoonlijke levenssfeer wordt ook beschermd door artikel 7 van het Handvest van de grondrechten van de Europese Unie.

9. Scenario's waarbij inbreuk wordt gemaakt op deze privésfeer, zelfs zonder dat het om persoonsgegevens gaat, vallen uitdrukkelijk onder de formulering van artikel 5, lid 3, en overweging 24 van de ePD, men denke bijvoorbeeld aan de opslag van virussen op de eindapparatuur van de gebruiker. Hieruit blijkt dat de definitie van de term "informatie" niet beperkt mag worden tot informatie die verband houdt met een geïdentificeerde of identificeerbare natuurlijke persoon.

10. Dit heeft het Hof van Justitie van de EU bevestigd: "*Deze bescherming is van toepassing op alle informatie die is opgeslagen op deze eindapparatuur, ongeacht of het gaat om persoonsgegevens, en beoogt met name, zoals uit dezelfde overweging blijkt, de gebruikers te beschermen tegen het risico dat verborgen identificatoren en andere soortgelijke programmatuur zonder hun medeweten binnenkomen in hun eindapparatuur.*"[6].

11. De vraag of de herkomst van deze informatie en de redenen waarom deze informatie in de eindapparatuur wordt opgeslagen in aanmerking moeten worden genomen bij de beoordeling van de toepasselijkheid van artikel 5, lid 3, van de richtlijn, is al eerder beantwoord. Zo stelt de Werkgroep artikel 29 bijvoorbeeld in zijn Advies 9/2014: "*Het is niet juist om basis hiervan af te leiden dat de derde partij geen toestemming nodig heeft om zich toegang te verschaffen tot deze informatie, omdat zij niet verantwoordelijk was voor de opslag ervan. De toestemmingsverplichting geldt ook wanneer toegang wordt verschaft tot een 'Alleen lezen'-waarde (bijv. het [opvragen van] het MAC-adres van een netwerkinterface via de OS-API).*"[7].

12. Concluderend kan worden gesteld dat het begrip informatie zowel niet-persoonsgebonden gegevens als persoonsgegevens omvat, ongeacht de wijze waarop deze gegevens zijn opgeslagen en door wie, d.w.z. of deze zijn opgeslagen door een externe entiteit (met inbegrip van andere entiteiten dan die welke toegang hebben), door de gebruiker, door een fabrikant, of een ander scenario.

2.3 Het begrip "eindapparatuur van een abonnee of gebruiker" – criterium B.1

13. Dit deel bouwt voort op de in Richtlijn 2008/63/EG gebruikte definitie waarnaar wordt verwezen in artikel 2 van Richtlijn (EU) 2018/1972, volgens welke onder "eindapparatuur" wordt worden verstaan: "*de apparaten die voor overbrenging, verwerking of ontvangst van informatie direct of indirect op de interface van een openbaar telecommunicatienet zijn aangesloten; in beide gevallen, direct of indirect, kan de aansluiting geschieden per draad, per optische vezel of via elektromagnetische golven; een*

[6] Arrest van het Hof van Justitie van 1 oktober 2019, Planet 49, zaak C-673/17, ECLI:EU:C:2019:801, punt 70.
[7] Advies 9/2014 van de Werkgroep artikel 29, blz. 9.

aansluiting is indirect wanneer een apparaat geplaatst is tussen het eindapparaat en de interface van het net"[8].

14. Overweging 24 van de ePD bevat een duidelijke uitleg van de rol van eindapparatuur voor de bescherming die wordt geboden door artikel 5, lid 3, van de richtlijn. De ePD beschermt de privacy van gebruikers niet alleen met betrekking tot de vertrouwelijkheid van hun informatie, maar ook door de integriteit van de eindapparatuur van de gebruiker te waarborgen. Deze uitleg dient in deze richtsnoeren als leidraad voor de interpretatie van het begrip "eindapparatuur".

15. In artikel 3 ePD is bepaald dat de e-privacyrichtlijn van toepassing is op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken. Dit houdt in dat een apparaat geschikt moet zijn voor gebruik in verband met een dergelijke dienst en dat het, om te worden aangemerkt als eindapparatuur, aangesloten moet zijn op of verbinding moet kunnen maken[9] met de interface van een openbaar communicatienetwerk. Het EDPB merkt op dat de in 2009 aangebrachte wijzigingen[10] in de tekst van artikel 5, lid 3, ePD de bescherming van eindapparatuur hebben uitgebreid door de verwijzing te schrappen naar "het gebruik van elektronische-communicatienetwerken" als middel om informatie op te slaan of om toegang te verkrijgen tot informatie die is opgeslagen in de eindapparatuur. Zolang een apparaat een netwerkinterface heeft waardoor het in staat is verbinding te maken (ook al is er geen verbinding gemaakt), is artikel 5, lid 3, ePD daarom van toepassing op elke entiteit die informatie opslaat die reeds in de eindapparatuur is opgeslagen of toegang verkrijgt tot dergelijke informatie, ongeacht de wijze van toegang tot de eindapparatuur en ongeacht of deze is aangesloten op of losgekoppeld van een netwerk.

16. Apparatuur die deel uitmaakt van het openbare elektronische-communicatienetwerk zelf zou niet worden beschouwd als eindapparatuur in de zin van artikel 5, lid 3, ePD[11].

17. Een eindapparaat kan bestaan uit een willekeurig aantal afzonderlijke hardwareonderdelen, die samen het eindapparaat vormen. Dit kan al dan niet de vorm aannemen van een fysiek omsloten apparaat dat alle weergave-, verwerkings-, opslag- en randapparatuur bevat (bijvoorbeeld smartphones, laptops, netwerkopslagapparaten, verbonden auto's of verbonden tv's, slimme brillen).

18. In de e-rpivacyrichtlijn is aangegeven dat de bescherming van de vertrouwelijkheid van de informatie die is opgeslagen op de eindapparatuur van de gebruiker en de integriteit van de eindapparatuur van de gebruiker niet beperkt zijn tot de bescherming van de persoonlijke levenssfeer van natuurlijke personen, maar zich ook uitstrekt tot het recht op eerbiediging van hun correspondentie of de

[8] Richtlijn 2008/63/EG van de Commissie van 20 juni 2008 betreffende de mededinging op de markten van telecommunicatie-eindapparatuur (PB L 162 van 21.6.2008, blz. 20).

[9] Dat wil zeggen dat het de technische mogelijkheden heeft om te worden verbonden met het netwerk, zelfs als er actueel geen verbinding is gemaakt.

[10] Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (Voor de EER relevante tekst) (PB L 337 van 18.12.2009, blz. 11), artikel 2, lid 5, en overweging 65.

[11] Meer over het bepalen van de grenzen van het netwerk in verschillende contexten vast te stellen is te vinden in de Berec-richtsnoeren inzake de gemeenschappelijke aanpak van de identificatie van het netwerkeindpunt in verschillende netwerktopologieën ("Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies", BoR (20) 46).

rechtmatige belangen van rechtspersonen[12]. Als zodanig is eindapparatuur die deze correspondentie en de behartiging van gerechtvaardigde belangen van de rechtspersonen mogelijk maakt, beschermd op grond van artikel 5, lid 3, ePD.

19. De gebruiker of abonnee kan de eindapparatuur bezitten of huren of op een andere wijze ter beschikking gesteld krijgen. Meerdere gebruikers of abonnees kunnen dezelfde eindapparatuur delen.

20. Deze door de e-privacyrichtlijn gewaarborgde bescherming heeft betrekking op de eindapparatuur waarvan de gebruiker of abonnee gebruikmaakt, ongeacht of de gebruiker de toegangsmiddelen zelf heeft ingesteld (bijvoorbeeld of hij of zij de elektronische communicatie heeft geïnitieerd) en zelfs ongeacht of de gebruiker zich bewust is van de bedoelde toegangsmiddelen).

2.4 Begrip "openbaar communicatienetwerk" – Criterium B.2

21. Aangezien de door de e-privacyrichtlijn geregelde situatie verband houdt met "*de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Gemeenschap*"[13] en in de definitie van eindapparatuur specifiek het begrip "*openbaar communicatienetwerk*" wordt vermeld, is het van cruciaal belang om dit begrip te verduidelijken om te bepalen binnen welke context artikel 5, lid 3, ePD van toepassing is.

22. Het begrip elektronische-communicatienetwerk wordt in de e-privacyrichtlijn zelf niet gedefinieerd. Een definitie van begrip was oorspronkelijk opgenomen in Richtlijn 2002/21/EG (de kaderrichtlijn) inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten[14] en is vervolgens vervangen door artikel 2, punt 1, van richtlijn 2018/1972 (het Europees wetboek voor elektronische communicatie). De definitie luidt thans:

> *"'elektronischecommunicatienetwerk': de transmissiesystemen, al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit, en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen, waaronder netwerkelementen die niet actief zijn, die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakketgeschakelde, met inbegrip van internet) en mobiele netwerken, elektriciteitsnetten voor zover deze voor overdracht van signalen worden gebruikt, netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie."*[15]

23. Deze definitie is neutraal met betrekking tot de transmissietechnologieën. Een elektronisch communicatienetwerk is volgens deze definitie elk netwerksysteem dat de overdracht van elektronische signalen tussen de nodes ervan mogelijk maakt, ongeacht de gebruikte apparatuur en protocollen.

24. Het begrip elektronische-communicatienetwerk in de zin van Richtlijn 2018/1972 gaat niet uit van het openbare of particuliere karakter van de infrastructuur, noch van de wijze waarop het netwerk wordt

[12] Zoals vermeld in artikel 2, punt 13, van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie kan de gebruiker een natuurlijke persoon of een rechtspersoon zijn.

[13] Artikel 3 EPD.

[14] Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (Kaderrichtlijn)

[15] Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking) (Voor de EER relevante tekst), artikel 2, punt 1.

uitgerold of beheerd ("*al dan niet gebaseerd op een permanente infrastructuur of gecentraliseerde beheercapaciteit*")[16]. Als gevolg daarvan is de definitie van elektronische-communicatienetwerk in artikel 2 van Richtlijn 2018/1972 ruim genoeg om elk type infrastructuur te omvatten. Zij omvat netwerken die al dan niet worden beheerd door een exploitant, netwerken die gezamenlijk worden beheerd door een groep exploitanten, en zelfs ad-hocnetwerken waarin eindapparatuur dynamisch kan worden verbonden met of kan worden losgekoppeld van een net van andere eindapparatuur met behulp van protocollen voor korteafstandstransmissie.

25. Deze definitie van netwerk behelst geen enkele beperking ten aanzien van het aantal eindapparaten dat op enig moment in het netwerk aanwezig is. Sommige netwerksstructuren maken gebruik van nodes die ad hoc informatie doorgeven aan nodes waarmee verbinding is gemaakt[17] en omvatten op een bepaald tijdstip soms slechts twee peers die met elkaar communiceren. Dergelijke gevallen zouden binnen het algemene toepassingsgebied van de e-privacyrichtlijn vallen, zolang het netwerkprotocol voorziet de deelname van meer peers.

26. De openbare beschikbaarheid van het communicatienetwerk is noodzakelijk om het apparaat te kunnen beschouwen als eindapparatuur waarop artikel 5, lid 3, ePD van toepassing is. Het feit dat het netwerk beschikbaar wordt gesteld voor een beperkt deel van het publiek (bijvoorbeeld abonnees, al dan niet tegen betaling, mits zij aan de toegangsvoorwaarden voldoen) maakt niet dat een dergelijk netwerk een privénetwerk is[18].

2.5 Het begrip "verkrijgen van toegang" – Criterium C.1

27. Om het begrip "verkrijgen van toegang" in de juiste context te plaatsen, is het belangrijk om het toepassingsgebied van de e-privacyrichtlijn, zoals vermeld in artikel 1, in aanmerking te nemen: "*[het waarborgen van] een gelijk niveau van bescherming van fundamentele rechten en vrijheden – met name het recht op een persoonlijke levenssfeer en vertrouwelijkheid – bij de verwerking van persoonsgegevens in de sector elektronische communicatie [...] en [...] zorgen voor het vrij verkeer van dergelijke gegevens en van elektronischecommunicatieapparatuur en -diensten in de Gemeenschap*".

28. Kort samengevat is de e-privacyrichtlijn een rechtsinstrument ter bescherming van de persoonlijke levenssfeer dat gericht is op de bescherming van de vertrouwelijkheid van communicatie en de integriteit van apparaten. In overweging 24 van de e-privacyrichtlijn wordt verduidelijkt dat, in het geval van natuurlijke personen, de eindapparatuur van de gebruiker deel uitmaakt van hun persoonlijke levenssfeer en dat toegang tot daarop opgeslagen informatie zonder hun medeweten een ernstige inbreuk kan vormen op hun privacy.

29. Rechtspersonen genieten eveneens bescherming door de e-privacyrichtlijn[19]. Bijgevolg moet het begrip "verkrijgen van toegang" in artikel 5, lid 3, ePD zodanig worden geïnterpreteerd dat het recht op een persoonlijke levenssfeer en vertrouwelijkheid wordt beschermd tegen schending door derden.

[16] Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking) (Voor de EER relevante tekst), artikel 2, punt 1.

[17] Bijvoorbeeld in de context van "delay-tolerant" netwerkstructuren die "store and forward"-technieken implementeren, zoals het Briar open source project.

[18] Zie de Berec-richtsnoeren voor de tenuitvoerlegging van de verordening inzake open internettoegang ("BEREC Guidelines on the Implementation of the Open Internet Regulation", BoR (20) 112) voor een nadere analyse van de identificatie van openbare communicatienetwerken.

[19] Overweging 26 van de ePD, zie punt 17 hierboven.

30. Het opslaan van informatie of het verkrijgen van toegang kunnen onafhankelijke verrichtingen zijn en worden uitgevoerd door onafhankelijke entiteiten. Er hoeft niet tegelijkertijd sprake te zijn van zowel opslag van informatie als toegang tot reeds opgeslagen informatie om artikel 5, lid 3, e-PD te kunnen toepassen.

31. Zo merkt de Werkgroep artikel 29 in zijn Advies 9/2014 op: "*De termen ['opslag' en 'verkrijgen van toegang'] geven aan dat de opslag en toegang niet noodzakelijkerwijs binnen dezelfde communicatiestroom moeten plaatsvinden of door dezelfde partij moeten worden uitgevoerd. Informatie die is opgeslagen door een partij (waaronder informatie die is opgeslagen door de gebruiker of de fabrikant van het apparaat), en die vervolgens wordt geraadpleegd door een andere partij, valt dan ook binnen de werkingssfeer van artikel 5, lid 3.*"[20]. Bijgevolg zijn er geen beperkingen gesteld aan de oorsprong van op de eindapparatuur opgeslagen informatie opdat het begrip "verkrijgen van toegang" van toepassing is.

32. Altijd wanneer een entiteit stappen onderneemt om toegang te krijgen tot informatie die is opgeslagen in de eindapparatuur, is artikel 5, lid 3, ePD van toepassing. Gewoonlijk betekent dit dat de toegang verkrijgende entiteit proactief specifieke instructies naar de eindapparatuur moet sturen om de te verkrijgen informatie te ontvangen. Dit is bijvoorbeeld het geval voor cookies, waarbij de toegang verkrijgende entiteit de eindapparatuur instrueert om proactief informatie te verzenden bij elke volgende Hypertext Transfer Protocol (HTTP)-oproep.

33. Dat is ook het geval wanneer de toegang verkrijgende entiteit software distribueert die op de eindapparatuur van de gebruiker wordt opgeslagen en vervolgens via het netwerk proactief verbinding maakt met een API-eindpunt. Andere voorbeelden zijn JavaScript-code, waarbij de toegang verkrijgende entiteit de browser van de gebruiker opdraagt om asynchrone verzoeken met de te verkrijgen informatie te verzenden. Dergelijke toegang valt duidelijk binnen de werkingssfeer van artikel 5, lid 3, ePD, aangezien de toegang verkrijgende entiteit de eindapparatuur expliciet opdracht geeft om de informatie te verzenden.

34. In sommige gevallen is de entiteit die de eindapparatuur instrueert om de te verkrijgen gegevens te verzenden, niet identiek met de entiteit die de informatie ontvangt. Dit kan het gevolg zijn van de onderlinge levering en/of het gebruik van een gemeenschappelijk mechanisme door de twee entiteiten. Wanneer het apparaat wordt opgedragen reeds opgeslagen informatie te verzenden (bijvoorbeeld door gebruik te maken van een protocol of een SDK[21] dat de proactieve verzending van informatie door de eindapparatuur initieert) kan er een inbreuk op de eindapparatuur plaatsvinden, zodat een dergelijke toegang leidt tot de toepasselijkheid van artikel 5, lid 3, ePD. Zoals opgemerkt in Advies 09/2014 van de Werkgroep artikel 29, kan dit het geval zijn wanneer een website de eindapparatuur door middel van een trackingpixel instrueert om informatie door te geven aan advertentiediensten van derden[22]. Dze praktijksituatie wordt verder uitgewerkt in afdeling 3.1.

[20] Advies 9/2014 van de Werkgroep artikel 29, blz. 9.
[21] Een SDK ("software development kit") is een bundel softwareontwikkelingstools die beschikbaar wordt gesteld om het maken van applicatiesoftware te vergemakkelijken.
[22] Advies 9/2014 van de Werkgroep artikel 29, blz. 10.

2.6 Begrippen "opslag van informatie" en "opgeslagen informatie" – Criterium C.2

35. Onder opslag van informatie in de zin van artikel 5, lid 3, ePD wordt verstaan het plaatsen van informatie op een fysiek elektronisch opslagmedium dat deel uitmaakt van de eindapparatuur van een gebruiker of abonnee[23].

36. Informatie wordt doorgaans niet in de eindapparatuur van een gebruiker of abonnee opgeslagen doordat een andere partij zich rechtstreeks toegang verschaft tot het geheugen van het apparaat, maar doordat software op de eindapparatuur wordt geïnstrueerd om specifieke informatie te genereren. Opslag die plaatsvindt door middel van dergelijke instructies wordt geacht rechtstreeks door de andere partij te worden geïnitieerd. Dit houdt onder meer in dat gebruik moet worden gemaakt van vaste protocollen zoals opslag van browsercookies en gepersonaliseerde software, ongeacht wie de protocollen of software op de eindapparatuur heeft aangemaakt of geïnstalleerd.

37. De e-privacyrichtlijn stelt geen boven- of ondergrens aan de tijdspanne gedurende welke informatie op een opslagmedium moet blijven staan om te worden beschouwd als opgeslagen, noch is er een boven- of ondergrens gesteld aan de hoeveelheid informatie die moet zijn opgeslagen.

38. Evenmin is het begrip "opslag" afhankelijk van het soort medium waarop de informatie wordt opgeslagen. Typische voorbeelden zijn harde schijven (HDD), solid-state drives (SSD), elektrisch wisbaar programmeerbaar alleen-lezen geheugen (EEPROM) en geheugen met willekeurige toegang (RAM), maar minder typische scenario's met een medium zoals magnetische tape of een cachegeheugen van een centrale verwerkingseenheid (CPU) zijn niet uitgesloten van het toepassingsgebied. Het opslagmedium kan intern (bijv. via een SATA-aansluiting), extern (bijv. via een USB-aansluiting) zijn aangesloten.

39. Onder "opgeslagen informatie" wordt informatie verstaan die zich reeds in de eindapparatuur bevindt, ongeacht de bron of aard van deze informatie. Dit omvat elk resultaat van informatieopslag in de zin van artikel 5, lid 3, ePD zoals hierboven beschreven (hetzij door dezelfde partij die later toegang verkrijgt of door een andere derde partij). Tevens omvat dit resultaten van informatieopslagprocessen die buiten het toepassingsgebied van artikel 5, lid 3, ePD vallen, zoals opslag op de eindapparatuur door de gebruiker of abonnee zelf of door een hardwarefabrikant (zoals de MAC-adressen van netwerkinterfacecontrollers), sensoren die zijn geïntegreerd in de eindapparatuur, of processen en programma's die worden uitgevoerd op de eindapparatuur, die al dan niet informatie kunnen produceren die afhankelijk is van of afgeleid is van opgeslagen informatie.

3 PRAKTIJKSITUATIES

40. Zoals aangegeven in de inleiding van deze richtsnoeren[24], bevatten deze geen analyse van de toepassing van de uitzonderingen op de in artikel 5, lid 3, ePD vastgelegde verplichting om toestemming te verkrijgen. Het EDPB herinnert eraan dat voor alle gevallen waarin informatie wordt opgeslagen of toegang wordt verkregen tot reeds opgeslagen informatie, moet worden beoordeeld of toestemming nodig is dan wel of een uitzondering op grond van artikel 5, lid 3, ePD van toepassing kan zijn. De lezer moet daarom naast deze technische analyse rekening houden met de uitzonderingen die in de betrokken praktijksituatie kunnen gelden.

[23] Zoals gedefinieerd in deel 2.3 van deze richtsnoeren.
[24] Zie punt 44 hierboven.

41. Onverminderd de specifieke context waarin die technische categorieën kunnen worden gebruikt die nodig zijn om te bepalen of artikel 5, lid 3, ePD van toepassing is, is het mogelijk om op niet-uitputtende wijze brede categorieën identificatoren en informatie in kaart te brengen die op grote schaal worden gebruikt en die binnen het toepassingsgebied van artikel 5, lid 3, ePD kunnen vallen.

42. Netwerkcommunicatie werkt gewoonlijk volgens op een gelaagd model dat het gebruik van identificatoren noodzakelijk maakt om een goede totstandbrenging en uitvoering van de communicatie mogelijk te maken. De mededeling van deze identificatoren aan actoren op afstand wordt door software ingeleid volgens overeengekomen communicatieprotocollen. Zoals hierboven uiteengezet, sluit het feit dat de ontvangende entiteit mogelijk niet de entiteit is die opdracht geeft tot het verzenden van informatie, de toepasselijkheid van artikel 5, lid 3, ePD niet uit. Het kan hierbij gaan om routing-identificatoren zoals het MAC- of IP-adres van de eindapparatuur, maar ook om sessie-identificatoren (SSRC, Websocket identifier) of authenticatietokens.

43. Ook kan het applicatieprotocol voorzien in verschillende mechanismen voor het verschaffen van contextgegevens (zoals een HTTP-header met onder meer "Aaanvaarden"-veld of user-agent), een caching-mechanisme (zoals ETag[25]) of andere functies (bijv. cookies of HST[26]). Nogmaals: het gebruik van dergelijke mechanismen om informatie te verzamelen (bijvoorbeeld in de context van fingerprinting[27] of het tracken van bronidentificatoren) kan inhouden dat artikel 5, lid 3, ePD van toepassing is.

44. Anderzijds zijn er sommige contexten waarin op de eindapparatuur geïnstalleerde lokale toepassingen gebruik maken van bepaalde informatie die zich strikt binnen het eindapparaat bevindt, zoals het geval kan zijn voor API's van smartphone-systemen (toegang tot camera, microfoon, GPS-sensor, acceleratorchip, radiochip, toegang tot lokale bestanden, contactenlijst, toegang tot identificatoren, enz.). Dit kan ook het geval zijn voor webbrowsers die opgeslagen of gegenereerde informatie binnen het apparaat verwerken (zoals cookies, lokale opslag, WebSQL of zelfs door de gebruikers zelf verstrekte informatie). Het gebruik van dergelijke informatie door een toepassing zou niet worden beschouwd als "het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur" in de zin van artikel 5, lid 3, ePD zolang de informatie het apparaat niet verlaat, maar indien toegang wordt verkregen tot deze informatie of hiervan afgeleide informatie, zou artikel 5, lid 3, ePD wel van toepassing zijn.

45. Tot slot worden in sommige gevallen door bepaalde actoren kwaadaardige software-elementen verspreid, bijvoorbeeld cryptomining-software of meer in het algemeen malware, waarbij de verwerkingsmogelijkheden van de eindapparatuur worden uitgebuit voor doeleinden van die actoren. De verspreiding van deze kwaadaardige software op de eindapparatuur van de gebruiker zou "opslag" vormen in de zin van artikel 5, lid 3, ePD. Mocht de software bovendien een netwerkverbinding tot stand brengen om in een later stadium informatie te verzenden, zou dit "verkrijgen van toegang" zijn in de zin van artikel 5, lid 3, ePD.

[25] De HTTP ETag is een identificator die het mogelijk maakt een voorwaardelijk verzoek te doen op basis van de geldigheid van de gecachete cliëntgegevens.
[26] Met HTTP Strict Transport Security (HSTS) kunnen servers aangeven welke bronnen altijd via HTTPS-verbindingen moeten worden opgevraagd.
[27] Zoals opgemerkt in de inleiding, is nadere informatie te vinden in Advies 9/2014 van de Artikel 29-werkgroep over de toepassing van de e-privacyrichtlijn op device fingerprinting.

46. Voor een aantal van deze categorieën die van een specifiek belang zijn, hetzij vanwege het wijdverbreide gebruik ervan, hetzij omdat een specifieke studie gerechtvaardigd is in het licht van de gebruiksomstandigheden ervan, wordt hieronder een specifieke analyse gegeven.

3.1 URL- en pixeltracking

47. Een trackingpixel is een hyperlink naar een resource, meestal een beeldbestand, die is ingebed in een stuk content zoals een website of e-mail. Deze pixel heeft meestal geen enkel doel in verband met de opgevraagde inhoud zelf – het enige doel is het automatisch tot stand brengen van communicatie door de client met de host van de pixel, die anders niet zou hebben plaatsgevonden. Dit is echter niet altijd het geval en trackingpixels worden soms ook gecreëerd door extra informatie toe te voegen aan via hyperlinks geladen afbeeldingen die relevant zijn voor de inhoud die voor de gebruiker wordt weergegeven. Door de aanmaak van de communicatie wordt verschillende informatie naar de host van de pixel gestuurd, afhankelijk van de specifieke praktijksituatie.

48. In het geval van een e-mail kan de afzender een trackingpixel toevoegen om vast te kunnen stellen wanneer de ontvanger de e-mail leest. Trackingpixels op websites kunnen koppelingen maken met een entiteit die veel van dergelijke verzoeken verzamelt en zo het gedrag van gebruikers kan volgen. Dergelijke trackingpixels kunnen ook aanvullende identificatoren, metagegevens of inhoud bevatten als onderdeel van de link. Deze gegevenspunten kunnen door de eigenaar van de website worden toegevoegd, eventueel in verband met de activiteit van de gebruiker op die website, zodat analytische rapporten over het gebruikersgedrag kunnen worden gegenereerd. Ze kunnen ook dynamisch worden gegenereerd via door de entiteit gedistribueerde client-side applicatielogica.

49. Trackinglinks kunnen op dezelfde manier werken, maar de identificator is dan toegevoegd aan het adres van de website. Wanneer de Uniform Resource Locator (URL) door de gebruiker wordt bezocht, laadt de website de gevraagde resource, maar haalt ook een identificator op die niet relevant is voor identificatie van de resource. Zeer vaak worden zij gebruikt door websites voor elektronische handel om de herkomst van inkomend verkeer te identificeren. Dergelijke websites kunnen bijvoorbeeld getraceerde links aanbieden aan partners om op hun domein te gebruiken zodat de e-commerce website weet wie van hun partners verantwoordelijk is voor een verkoop en een commissie betaalt, een praktijk die bekend staat als affiliate marketing.

50. Zowel trackinglinks als trackingpixels kunnen via een breed scala aan kanalen worden verspreid, bijvoorbeeld via e-mails, websites, of zelfs, in het geval van trackinglinks, via alle soorten tekstberichtensystemen. Die distributie naar de eindapparatuur van de gebruiker is wel degelijk opslag, op zijn minst via het cachingmechanisme van de client-side software. Als zodanig is artikel 5, lid 3, van de Europese Richtlijn van toepassing, zelfs als deze opslag niet permanent is.

51. De toevoeging van trackinginformatie aan URL's of afbeeldingen (pixels) die aan de gebruiker zijn toegezonden, vormt een instructie aan de eindapparatuur om de gerichte informatie (de gespecificeerde identificator) terug te sturen. In het geval van dynamisch geconstrueerde trackingpixels is het de verdeling van de toepassingslogica (gewoonlijk een JavaScript-code) die de instructie vormt. Bijgevolg kan worden gesteld dat het verzamelen van identificatoren via dergelijke traceringsmechanismen een “verkrijgen van toegang” vormt in de zin van artikel 5, lid 3, ePD, en is deze dus ook op die stap van toepassing.

3.2 Lokale verwerking

52. Sommige technologieën vertrouwen op lokale verwerking onder leiding van software die op de eindapparatuur van gebruikers wordt gedistribueerd, waarbij de informatie die door de lokale

verwerking wordt geproduceerd vervolgens via client-side API's beschikbaar wordt gemaakt voor geselecteerde actoren. Dit kan bijvoorbeeld het geval zijn voor een API die door de webbrowser wordt verstrekt, waar lokaal gegenereerde resultaten op afstand kunnen worden geraadpleegd.

53. Als op enig moment en bijvoorbeeld in de client-side code de verwerkte informatie beschikbaar wordt gemaakt voor een derde partij, bijvoorbeeld teruggestuurd over het netwerk naar een server, zou een dergelijke verrichting (opgedragen door de entiteit die de client-side code produceert die wordt gedistribueerd op de eindapparatuur van de gebruiker) een "verkrijgen van toegang tot reeds opgeslagen informatie" vormen. Het feit dat deze informatie lokaal wordt geproduceerd, sluit de toepassing van artikel 5, lid 3, van de richtlijn niet uit.

3.3 Uitsluitend IP-gebaseerde tracking

54. Sommige aanbieders ontwikkelen oplossingen die slechts één component ophalen, namelijk het IP-adres, om de navigatie[28] van de gebruiker te volgen, in sommige gevallen verspreid over meerdere domeinen. In deze context zou artikel 5, lid 3, ePD van toepassing kunnen zijn, ook al is de instructie om het IP-adres beschikbaar te stellen verstrekt door een andere entiteit dan de ontvangende entiteit.

55. Het verkrijgen van toegang tot IP-adressen zou echter alleen leiden tot toepasselijkheid van artikel 5, lid 3, ePD in gevallen waarin deze informatie afkomstig is van de eindapparatuur van een abonnee of gebruiker. Hoewel dit niet altijd het geval is (bijvoorbeeld wanneer CGNAT[29] wordt geactiveerd), zou het statische uitgaande IPv4 dat voortkomt uit de router van een gebruiker binnen dat geval vallen, evenals IPV6-adressen, aangezien deze gedeeltelijk worden gedefinieerd door de host. Tenzij de entiteit ervoor kan zorgen dat het IP-adres niet afkomstig is van de eindapparatuur van een gebruiker of abonnee, moet zij alle maatregelen nemen overeenkomstig artikel 5, lid 3, ePD.

56. Hoewel de toepassing van de uitzonderingen van de verplichting om toestemming te verkrijgen waarin artikel 5, lid 3, ePD voorziet, in de deze richtsnoeren niet wordt geanalyseerd, is het belangrijk er nogmaals aan te herinneren dat de toepasselijkheid van dit artikel niet systematisch betekent dat toestemming moet worden verkregen. Het EDPB herinnert er dus aan dat voor elk geval moet worden beoordeeld of toestemming nodig is of dat een uitzondering krachtens artikel 5, lid 3, ePD van toepassing zou kunnen zijn[30].

3.4 Intermitterende en gemedieerde ivd-rapportage

57. IoT-apparaten (het internet der dingen) produceren continu informatie, bijvoorbeeld via sensoren die in het apparaat zijn ingebouwd en die al dan niet lokaal worden voorverwerkt. In veel gevallen wordt informatie ter beschikking gesteld van een server op afstand, maar de modaliteiten van die verzameling kunnen verschillen.

58. Sommige IoT-apparaten hebben een directe verbinding met een openbaar communicatienetwerk met een cellulaire SIM-kaart. Andere kunnen een indirecte verbinding hebben met een openbaar communicatienetwerk, bijvoorbeeld door het gebruik van WIFI of het doorgeven van informatie aan

[28] Dit is een aanvulling op en onafhankelijk van het gebruik en de functie van een IP-adres voor de vaststelling en overdracht of doorgifte van onderliggende technische communicatie, of van het feit dat het hierbij al dan niet om persoonsgegevens kan gaan (wat de analyse van e-privacy betreft, is het "informatie")

[29] Carrier-Grade NAT of CGNAT wordt door aanbieders van internetdiensten gebruikt om het gebruik van beperkte IP-adresruimte te maximaliseren. Het groepeert een aantal abonnees onder hetzelfde openbare IP-adres.

[30] Advies 9/2014 van de Werkgroep artikel 29 voorziet in een aantal voorbeelden wanneer toestemming misschien niet nodig is.

een ander apparaat via een punt-tot-puntverbinding (bijvoorbeeld via Bluetooth). Het andere apparaat kan bijvoorbeeld een smartphone of een speciale gateway zijn die de informatie al dan niet vooraf verwerkt voordat zij naar de server wordt verzonden.

59. IoT-apparaten kunnen door de fabrikant worden geïnstrueerd om de verzamelde informatie altijd te streamen, maar de informatie toch eerst lokaal te cachen, bijvoorbeeld totdat er een verbinding beschikbaar is.

60. In elk geval zou het IoT-apparaat, wanneer het (direct of indirect) verbonden is met een openbaar communicatienetwerk, zelf als eindapparatuur worden beschouwd. Het feit dat de informatie wordt gestreamd of opgeslagen voor intermitterende rapportage verandert niets aan de aard van die informatie. In beide situaties zou artikel 5, lid 3, ePD van toepassing zijn, aangezien er, door de instructie van code op het IoT-apparaat om de dynamisch opgeslagen gegevens naar de externe server te sturen, sprake is van “verkrijgen van toegang”.

3.5 Unieke identificatiecode

61. Een algemeen instrument dat door bedrijven wordt gebruikt, is de notie van “unieke identificatoren” of “permanente identificatoren”. Dergelijke identificatoren kunnen worden afgeleid van persistente persoonlijke gegevens (naam en achternaam, e-mail, telefoonnummer, enz.), die worden gehasht op het apparaat van de gebruiker, verzameld en gedeeld tussen verschillende controllers om een persoon uniek te identificeren in verschillende datasets (gebruiksgegevens verzameld door het gebruik van website of applicatie, CRM-gegevens (customer relation management) met betrekking tot online of offline aankoop of abonnement, enz.) Op websites worden de aanhoudende persoonsgegevens over het algemeen verkregen in het kader van authenticatie of bij het abonneren op nieuwsbrieven.

62. Zoals hierboven uiteengezet, zou het feit dat informatie door de gebruiker wordt ingevoerd, de toepassing van artikel 5, lid 3, ePD met betrekking tot opslag niet in de weg staan, aangezien deze informatie tijdelijk op de eindapparatuur wordt opgeslagen alvorens te worden verzameld.

63. In de context van het ophalen van “unieke identificatoren” op websites of mobiele applicaties instrueert de ophalende entiteit de browser (via de distributie van client-side code) om die informatie te verzenden. Als zodanig is er sprake van “verkrijgen van toegang” plaats en is artikel 5, lid 3, ePD van toepassing.