



Maastricht University

KNOWLEDGE IN ACTION

Faculteit Rechten

master in de rechten

Masterthesis

Vanuit gebruikte zoektermen op zoek gaan naar onbekende daders als onderzoeksmethode in strafzaken: wettelijke basis en beperkingen

Amelie Oosterbos

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Frank VERBRUGGEN

De transnationale Universiteit Limburg is een uniek samenwerkingsverband van twee universiteiten in twee landen: de Universiteit Hasselt en Maastricht University.



KNOWLEDGE IN ACTION

www.uhasselt.be
Universiteit Hasselt
Campus Hasselt:
Martelarenlaan 42 | 3500 Hasselt
Campus Diepenbeek:
Agoralaan Gebouw D | 3590 Diepenbeek

2024
2025



Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

Vanuit gebruikte zoektermen op zoek gaan naar onbekende daders als onderzoeksmethode in strafzaken: wettelijke basis en beperkingen

Amelie Oosterbos

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Frank VERBRUGGEN



Faculteit Rechten

Master in de rechten

Masterscriptie 2024-2025

Vanuit gebruikte zoektermen op zoek gaan naar onbekende daders als onderzoeksmethode in strafzaken: wettelijke basis en beperkingen.

Amelie Oosterbos

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR:

Prof. dr. Frank Verbruggen

BEGELEIDER:

Nele Obbels

Samenvatting

Heeft u ooit wel eens iets op internet opgezocht waarvan u zich afvroeg: "Wat ik nu zoek, zou wel eens vreemd kunnen overkomen als de politie dit ziet"? In de toekomst zou dit gevoel misschien werkelijkheid kunnen worden. In de Verenigde Staten is deze bezorgdheid al realiteit. Daar beschikken opsporingsautoriteiten over een onderzoeksmethode waarmee ze bij zoekmachinebedrijven gegevens kunnen opvragen van personen die naar bepaalde zoektermen hebben gezocht die in verband staan met een misdrijf. Deze methode speelt een cruciale rol in onderzoeken waarbij politionele instanties geen enkel aanknopingspunt hebben om een verdachte te identificeren. Ze stelt opsporingsautoriteiten in staat om op grote schaal gegevens te verzamelen van personen die verdachte zoektermen hebben ingevoerd, en hen mogelijk als verdachten te beschouwen.

In België bestaat een dergelijke onderzoeksmethode (nog) niet. Gezien de voortdurende digitalisering en de evoluerende maatschappij rijst echter de vraag of een vergelijkbare methode ook in België van waarde zou kunnen zijn, met name in het kader van 'cold cases'. Immers, de overvloed aan informatie die online beschikbaar is, biedt potentieel waardevolle aanknopingspunten die als bewijs kunnen dienen in strafrechtelijke onderzoeken.

Een dergelijke onderzoeksmethode, die in principe hoofdzakelijk onschuldige personen treft, roept echter fundamentele vragen op met betrekking tot het recht op privacy en de bescherming van persoonsgegevens. In een democratische samenleving, zoals België, worden strikte grenzen gesteld aan het gebruik van onderzoeksmethoden om willekeur en misbruik te voorkomen. Op Europees niveau zijn diverse regelgevende instrumenten geïmplementeerd om deze twee fundamentele rechten te waarborgen. Om een balans te vinden tussen het recht op privacy en de veiligheid van de samenleving, moeten er duidelijke grenzen worden gesteld waaraan onderzoeksmethoden moeten voldoen om rechtmatig te zijn. Deze grenzen en beperkingen krijgen verder vorm in de rechtspraak van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens.

Aan de hand van de grenzen die voortvloeien uit het recht op privacy en gegevensbescherming, die het normatieve kader vormen, kan worden beoordeeld in welke mate een onderzoeksmethode waarbij onbekende daders worden opgespoord op basis van gebruikte zoektermen juridisch mogelijk is in België. Binnen dit kader kan worden geconcludeerd dat dergelijke zoektermbevelen mogelijk zijn binnen het Belgisch strafrecht, mits aan strikte voorwaarden wordt voldaan. Deze voorwaarden beperken echter de inzetbaarheid van de methode zodanig, dat toepassing slechts in uitzonderlijke gevallen aangewezen is.

Met een grondige evaluatie van de juridische, technische en praktische aspecten beoogt deze scriptie beleidsmakers, juristen en rechtsgeleerden te voorzien van inzichten omtrent toekomstige online opsporingsmethoden, in het bijzonder met betrekking tot een methode waarbij onbekende daders worden geïdentificeerd aan de hand van gebruikte zoektermen.

Dankwoord

Deze masterscriptie vormt de afronding van mijn studie rechten aan de Universiteit Hasselt en markeert tevens het einde van mijn academische reis. Het afgelopen jaar was gevuld met intensief onderzoek, schrijfwerk en talrijke herschrijvingen. Het resultaat is een werk waar ik met trots op terugkijk. In dit proces heb ik veel steun ontvangen, en ik wil graag enkele mensen bedanken voor hun waardevolle bijdrage, tijd en inzichten die dit onderzoek hebben verrijkt.

Allereerst wil ik graag prof. dr. Frank VERBRUGGEN bedanken voor het aandragen van dit boeiende onderwerp, waarmee ik de vrijheid kreeg om mijn eigen onderzoek te voeren.

Verder wil ik in het bijzonder mevrouw Nele OBBELS hartelijk bedanken. Haar waardevolle feedback, geruststellende woorden en nieuwe inzichten hebben mij telkens verder geholpen in dit proces. Onderzoek doen naar een technisch complexe thematiek waar je niet vertrouwd mee bent, is niet eenvoudig, maar dankzij haar heb ik steeds waardevolle en constructieve feedback ontvangen, waarmee ik verder kon bouwen en mijn werk kon verbeteren. Haar bijdrage aan het realiseren van deze masterscriptie was dan ook essentieel, en ik ben haar zeer dankbaar voor de aangename samenwerking en het vertrouwen dat ze in mij stelde.

Mijn dank gaat tevens uit naar de Universiteit Hasselt, voor de kansen die ze mij geboden heeft, maar ook voor het creëren van een inspirerende en ondersteunende academische sfeer, die een belangrijke rol heeft gespeeld in mijn ontwikkeling en het behalen van mijn doelen.

Ik wil ook graag mijn vrienden en medestudenten bedanken. Gedurende de jaren stonden ze altijd voor me klaar, in goede en minder goede tijden. Wanneer ik het even moeilijk had, boden ze een luisterend oor, een schouder om op uit te huilen en bemoedigende woorden die me telkens weer de kracht gaven om verder te gaan.

Tot slot wil ik een persoonlijke boodschap richten aan mijn ouders, Luc en Patricia. Alles wat ik heb bereikt, is te danken aan jullie onvoorwaardelijke steun en liefde. Jullie hebben me alle kansen geboden die ik nodig had, en ik kan enkel hopen dat jullie trots zijn op wat ik tot nu toe heb verwezenlijkt. Zonder jullie voortdurende aanmoediging en steun zou dit pad veel zwaarder zijn geweest.

Amelie Oosterbos

Opoeteren, 15 mei 2025

Inhoudsopgave

Samenvatting	I
Dankwoord	II
Inhoudsopgave	III
Lijst met bijlagen	VI
Inleiding.....	1
§ 1: Onderzoekscontext	1
Afdeling 1: Onderwerp en probleemstelling	1
§ 2: Onderzoeksmethode	2
Afdeling 1: Onderzoeksvragen- en methodologie	2
Afdeling 2: Opbouw	4
§ 3: Relevantie.....	6
§ 4: Afbakening en toepassingsgebied.....	6
Hoofdstuk I. Opsporen via zoekgedrag: een Amerikaanse onderzoeksdaad onder de loep.....	8
§ 1: Een sprong in het onbekende: keyword warrants	8
§ 2: Constitutionele twijfels	11
Hoofdstuk II. Een uitstap naar het Belgisch strafrechtelijk landschap van online onderzoeksdaden14	
§ 1: Online onderzoeksmethoden	14
Afdeling 1: (Openlijke) zoeking in informaticasystemen of delen ervan – Artikel 39bis Juncto 88ter Sv.	15
A. Informaticazoeking.....	15
B. Netwerkzoeking	16
C. Restcategorie	17
Afdeling 2: Identificatie van gebruikers van een elektronische communicatiedienst – Artikel 46bis Sv.	17
Afdeling 3: Opsporen en lokaliseren van elektronische communicatie – Artikel 88bis Sv.	19
Afdeling 4: De inkijkoperatie in een informaticasysteem – Artikel 46quinquies Juncto 89ter Sv.	23
Afdeling 5: Het onderscheppen, kennis nemen, doorzoeken en opnemen van communicatie of gegevens van een informaticasysteem – Artikel 90ter Sv.....	24
§ 2: Tussenconclusie.....	26
Hoofdstuk III. Gezocht op Google, gevolgd door justitie? De juridische knelpunten van gegevensbescherming in de EU	28
§ 1: Algemene Verordening Gegevensbescherming	28

Afdeling 1: Zoekmachinebedrijven binnen AVG.....	29
A. Toepassingsgebied	29
B. Verwerkingsgronden.....	31
C. Beginselen inzake verwerking	35
§ 2: Wettelijke bewaarplicht	38
Afdeling 1: Voorwaarden	39
Afdeling 2: Dataretentiewet	43
Afdeling 3: Een bewaarplicht voor zoekmachinebedrijven?	48
§ 3: Toegang tot bewaarde gegevens.....	52
Afdeling 1: Voorwaarden	53
Afdeling 2: Dataretentiewet	54
Afdeling 3: Toegang door opsporingsautoriteiten bij zoektermbevelen	56
§ 4: Tussenconclusie.....	60
Hoofdstuk IV. Van zoekbalk naar bewijsstuk: artikel 8 EVRM en de grenzen van privacy en gegevensbescherming in strafonderzoek	62
§ 1: Reikwijdte artikel 8 EVRM	62
§ 2: Grenzen van toelaatbare inmenging	64
Afdeling 1: Bij wet voorzien	65
A. Gerichte geheime surveillancemethoden	66
B. Bulkinterceptie.....	69
Afdeling 2: Legitieme doelstelling.....	72
Afdeling 3: Noodzakelijk in democratische samenleving	73
§ 3: Zoektermbevelen in het licht van artikel 8 EVRM.....	74
Afdeling 1: Reikwijdte	74
Afdeling 2: Grenzen van toelaatbare inmenging.....	75
A. Bij wet voorzien	75
B. Legitieme doelstelling	78
C. Noodzakelijk in democratische samenleving	79
§ 4: Tussenconclusie.....	79
Conclusie	81
Lijst van geraadpleegde werken	85
§ 1: Wetgeving	85
§ 2: Rechtspraak.....	88

§ 3: Rechtsleer.....	93
Bijlagen	99
Bijlage 1.....	99
Bijlage 2.....	101
Bijlage 3.....	102
Bijlage 4.....	103
Bijlage 5.....	105

Lijst met bijlagen

Bijlage 1	Schematisch overzicht van de huidige wetsbepalingen en voorwaarden inzake online onderzoeksmethoden
Bijlage 2	Schematisch overzicht inzake bewaarplicht volgens het Hof van Justitie
Bijlage 3	Schematisch overzicht inzake toegang tot bewaarde gegevens volgens het Hof van Justitie
Bijlage 4	Schematisch overzicht inzake surveillancemethoden in het licht van artikel 8 Europees Verdrag voor de Rechten van de Mens
Bijlage 5	Voorstel inzake de wettelijke regeling van zoektermbevelen in het Belgisch strafrecht

Inleiding

§ 1: Onderzoekscontext

Afdeling 1: Onderwerp en probleemstelling

1. Stel u voor, het is zaterdagavond en na een drukke werkweek wil u rust en met uw partner naar een spannende misdaadserie kijken. In deze serie ziet u hoe personen worden opgelost in zuur. Vol verbazing over de werkwijze, begeeft u zich naar het internet en zoekt u op of het oplossen van een lichaam in zuur wel degelijk zo gemakkelijk is als weergegeven in de serie. Enkele weken later staat plots de politie voor uw deur met de mededeling dat u als verdachte wordt beschouwd in een lopend onderzoek aangaande een moord, waarbij het lichaam is opgelost in zuur. Tijdens het verhoor komt u er achter dat uw verdenking louter gebaseerd is op uw opzoeken omtrent het oplossen van een lichaam in zuur. In de huidige digitale samenleving verzamelen bedrijven grote hoeveelheden gebruikersgegevens met als doel gerichte reclame te maken en in te spelen op individuele voorkeuren.¹ Deze gegevens kunnen ook een waardevol instrument vormen bij de opsporing en oplossing van misdrijven, met name bij de identificatie van onbekende daders.² Opsporingsautoriteiten blijven dan ook niet achter en proberen op innovatieve wijze onderzoeksmethoden te ontwikkelen die gebruikmaken van de omvangrijke online beschikbare datagegevens om verdachten te identificeren en strafbare feiten op te helderen. Dat roept een fundamentele juridische vraag op: wanneer is het juridisch toelaatbaar dat opsporingsinstanties van zoekmachinebedrijven gegevens ontvangen over individuen die zoektermen hebben ingevoerd die mogelijk in verband staan met een gepleegd misdrijf?

2. In de Verenigde Staten is deze praktijk reeds realiteit. Op 16 oktober 2023 erkende het Supreme Court van Colorado in de zaak 'People tegen Seymour' dat het gebruik van een zogenaamde 'keyword warrant' aanzienlijke privacyzorgen oproept en mogelijk strijdig is met het Vierde Amendement, maar stond het gebruik van het verkregen bewijs toch toe op basis van de 'good faith'-uitzondering.³ De zaak betrof een brandstichting waarbij vijf familieleden omkwamen.⁴ Omdat de politie geen verdachten kon aanwijzen met behulp van traditionele onderzoekspraktijken diende ze een bevel in bij Google om na te gaan welke gebruikers het adres van de slachtoffers hadden opgezocht.⁵ De opsporingsautoriteiten onderzochten een lijst met IP-adressen van apparaten die hadden gezocht naar het adres van het huis in de 15 dagen voordat het in brand werd gestoken. Met behulp van deze informatie konden de onderzoekers drie tieners opsporen en uiteindelijk vervolgen.⁶

¹ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Texas Law Review* (102 Tex. L. Rev.) 2024/5, (877) 877.

² *Ibid*, 890, 934.

³ Supreme Court Colorado 16 oktober 2023, nr. 23SA12, 'People/Seymour'; STENDER S., 'Circumventing the fourth amendment: the unconstitutional nature of geofence warrants', *Utah Law Review* (U. L. Rev.) 2024/3, (733) 754.

⁴ Supreme Court Colorado 16 oktober 2023, nr. 23SA12, 'People/Seymour', § 5; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Tex. L. Rev.* 2024/5, (877) 879.

⁵ Supreme Court Colorado 16 oktober 2023, nr. 23SA12, 'People/Seymour', § 7; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Tex. L. Rev.* 2024/5, (877) 881-882; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', *97 Washington Law Review* (Wash. L. Rev.) 2022/4, (977) 977-978.

⁶ Supreme Court Colorado 16 oktober 2023, nr. 23SA12, 'People/Seymour', §12; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Tex. L. Rev.* 2024/5, (877) 882.

Een ander voorbeeld met betrekking tot een dergelijke onderzoeksmethode in de Verenigde Staten betreft het onderzoek naar seriepijpbomaanslagen in Austin, Texas, in maart 2018, waarbij twee mensen omkwamen toen ze pakketjes openmaakten die aan hun deur waren achtergelaten.⁷ Om de onbekende dader te vinden deed de politie beroep op meerdere 'keyword warrants' waarbij ze de drie grootste zoekmachineproviders, Google, Microsoft en Yahoo, opdracht gaven om te doorzoeken welke gebruikers het huisadres hadden opgezocht.⁸ Eén van 'keyword warrants' vroeg Google daarnaast om alle gebruikers bekend te maken die naar één van de adressen van het slachtoffer zochten via Google Maps of Waze. Bovendien werd ook een 'keyword warrant' uitgestuurd dat Google vroeg naar gebruikers die zochten naar verschillende combinaties van termen die te maken hebben met het maken van bommen, zoals 'bomb', 'pipe bomb' of 'PCV bomb'. Op basis van deze gegevens vond de politie de 23-jarige dader.⁹

3. Door globalisering en de groeiende digitalisering van opsporingsmethoden kunnen ontwikkelingen in de Verenigde Staten, zoals het gebruik van 'keyword warrants', de vraag oproepen in hoeverre dergelijke praktijken ook in België juridisch en maatschappelijk mogelijk of toelaatbaar kunnen zijn. In België bestaan reeds verschillende vormen van online onderzoeksmethoden, waarbij informaticasystemen kunnen worden geanalyseerd, identificatie-, locatie- en verkeersgegevens kunnen worden opgevraagd en zelfs de inhoud van communicatie kan worden onderschept. Een onderzoeksmethode waarbij opsporingsautoriteiten zoekmachinebedrijven verzoeken om informatie over personen die specifieke zoektermen hebben ingevoerd, maakt echter (vooralsnog) geen deel uit van het Belgische strafrechtelijke kader. Een dergelijke methode roept aanzienlijke bezwaren op met betrekking tot het recht op privacy en gegevensbescherming. Het idee dat het openbaar ministerie en/of de onderzoeksrechter de zoekgeschiedenis van alle Belgische burgers zou kunnen inzien en als grondslag voor verdenking zou kunnen gebruiken, lijkt moeilijk te verzoenen met deze fundamentele rechten. Ook de bewaring van de zoekgeschiedenis van een gehele bevolking is niet onproblematisch, in het bijzonder in het licht van de rechtspraak van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens. Dit roept de vraag op of, en zo ja, onder welke strikte voorwaarden en beperkingen, het in België juridisch mogelijk is om een afzonderlijke wettelijke bepaling in te voeren die deze specifieke onderzoeksmaatregel regelt.

§ 2: Onderzoeksmethode

Afdeling 1: Onderzoeksvragen- en methodologie

4. De centrale onderzoeksvraag luidt als volgt: *"In welke mate is een onderzoeksdaad waarbij onbekende daders worden opgespoord op basis van gebruikte zoektermen juridisch mogelijk binnen het Belgisch wetgevend kader, vanuit Europees (Unie)rechtelijk perspectief?"*.

⁷ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 Tex. L. Rev. 2024/5, (877) 894; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 Wash. L. Rev. 2022/4, (977) 986; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 Cardozo Law Review (Cardozo L. Rev.) 2023/1, (271) 285.

⁸ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 Tex. L. Rev. 2024/5, (877) 894.

⁹ Ibid, 895.

5. We zullen in dit onderzoek naar deze onderzoeksdaad verwijzen met de term 'zoektermbevel'. Deze aanbevelende onderzoeksvraag heeft tot doel een voorstel te doen over hoe een bepaling betreffende zoektermbevelen zou moeten worden vormgegeven zodat deze binnen het Belgische wetgevend kader past. Het normatieve criterium waarop deze aanbeveling is gebaseerd is het Europees (Unie)rechtelijk kader, met name het recht op privacy en gegevensbescherming. Om hiertoe te besluiten, moeten volgende vier subonderzoeksvragen worden beantwoord:

- **Hoe krijgen zoektermbevelen vorm in de Verenigde Staten van Amerika en wat zijn de kritieken hierop? (beschrijvend)**

6. Ter beantwoording analyseren we op een systematische maar bevattelijke wijze hoe deze onderzoeksdaad vormt krijgt binnen de Amerikaanse rechtspraak en welke kritieken hierop zijn geformuleerd.¹⁰

7. Aangezien de onderzochte methode haar oorsprong vindt in de Amerikaanse wetshandavingspraktijk, wordt ter beantwoording van de onderzoeksvraag in hoofdzaak beroep gedaan op rechtspraak en rechtsleer. In het Amerikaanse common law-systeem vormen deze bronnen de primaire juridische basis, daar expliciete wettelijke verankering veelal ontbreekt.

- **Hoe is het Belgische strafrechtelijk kader met betrekking tot online onderzoeksdaaden geregeld, en welke voorwaarden en grenzen worden daarbij gesteld? (beschrijvend)**

8. Deze beschrijvende onderzoeksvraag heeft tot doel het bestaande strafprocesrechtelijke kader waarbinnen de beschreven onderzoeksdaad moet inpassen, op een systematische en gestructureerde wijze uiteen te zetten en inzichtelijk weer te geven.¹¹ We zullen analyseren welke online onderzoeksdaaden reeds binnen het Belgische strafrechtelijke kader bestaan en aan welke precieze wettelijke voorwaarden voldaan moet worden om de legitimiteit ervan te waarborgen.

9. Ter beantwoording wordt uitgegaan van de wettelijke bepalingen betreffende online onderzoeksdaaden, zoals vastgelegd in het Wetboek van Strafvordering. Deze juridische kaders worden verder toegelicht en verdiept met inzichten uit de rechtsleer.

- **Welke beperkingen en voorwaarden stelt de wetgeving en rechtspraak met betrekking tot dataretentie en toegang tot bewaarde gegevens op Europees Unierechtelijk niveau, in het licht van het recht op privacy en gegevensbescherming? (beschrijvend)**
- **Welke beperkingen en voorwaarden stelt de wetgeving en rechtspraak met betrekking tot dataretentie en toegang tot bewaarde gegevens onder het Europees**

¹⁰ KESTEMONT L., SCHOUKENS P., HENDRICKX K. en TERRY E. (red.), *Rechtswetenschappelijk schrijven*, Acco, 2017, 30.

¹¹ KESTEMONT L., SCHOUKENS P., HENDRICKX K. en TERRY E. (red.), *Rechtswetenschappelijk schrijven*, Acco, 2017, 30.

Verdrag voor de Rechten van de Mens, rekening houdend met het recht op privacy en gegevensbescherming? (beschrijvend)

10. De derde en vierde onderzoeksvraag vertonen sterke gelijkenissen. Beide onderzoeksvragen zijn beschrijvend van aard en hebben tot doel het recht op privacy en gegevensbescherming systematisch in kaart te brengen, evenals de daaruit voortvloeiende juridische voorwaarden en grenzen met betrekking tot dataretentie en de toegang tot de bewaarde gegevens. De derde onderzoeksvraag richt zich op de voorwaarden die voortvloeien uit het Europees Unierecht en de interpretatie daarvan door het Hof van Justitie van de Europese Unie. De vierde onderzoeksvraag behandelt hetzelfde onderwerp in het licht van de jurisprudentie van het Europees Hof voor de Rechten van de Mens en de normen die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens. Deze analyse vormt een essentieel fundament voor het verdere onderzoek naar de toelaatbaarheid van het gebruik van online bewaarde gegevens voor strafrechtelijke doeleinden, en fungeert tevens als normatief toetsingskader bij de beantwoording van de centrale onderzoeksvraag.

11. De onderzoeksvragen worden beantwoord op basis van de relevante wettelijke bepalingen inzake het recht op privacy en gegevensbescherming. Binnen het Europees Unierecht nemen met name artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie, de Algemene Verordening Gegevensbescherming en de Richtlijn betreffende privacy en elektronische communicatie een centrale plaats in.¹² In het kader van de vierde onderzoeksvraag komt artikel 8 van het Europees Verdrag voor de Rechten van de Mens prominent aan bod.¹³ Deze bepalingen worden nader toegelicht en geïnterpreteerd aan de hand van relevante jurisprudentie. Daarnaast wordt gebruikgemaakt van rechtsleer en annotaties die deze rechtspraak verder analyseren en duiden.

Afdeling 2: Opbouw

12. Deze masterscriptie is opgebouwd uit vijf hoofdstukken. In het eerste hoofdstuk wordt een noodzakelijk kader geschetst waarin het onderzoeksbevel wordt afgebakend en verduidelijkt. Aangezien deze methode binnen het Belgische rechtskader ontbreekt, wordt aansluiting gezocht bij de Amerikaanse rechtspraak, waar 'keyword warrants' reeds enkele jaren worden toegepast. Voor de nadere concretisering van de vooropgestelde onderzoeksmethode wordt dan ook inspiratie geput uit de Amerikaanse rechtspraak, waarvan de gehanteerde benadering als uitgangspunt dient voor het verdere verloop van dit onderzoek. Er bestaat evenwel geen unanieme consensus over de rechtmatigheid ervan in de Verenigde Staten: critici stellen dat dergelijke praktijken strijdig zijn met het Vierde Amendement van de Amerikaanse Grondwet. Deze kritische beschouwingen worden

¹² Handvest van de grondrechten van de Europese Unie, *Pb.C.* 83, 30 maart 2010 (hierna: EU-Handvest); Verordening 2016/679 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, *Pb.L.* 4 mei 2016 (hierna: AVG); 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, *Pb.L.* 31 juli 2002 (hierna: E-Privacyrichtlijn).

¹³ Art. 8.1 Europees Verdrag voor de Rechten van de Mens, *BS* 4 november 1950 (hierna: EVRM).

meegenomen in het verdere onderzoek om tot een genuanceerde evaluatie van de voorgestelde opsporingsmethode te komen.

13. Het tweede hoofdstuk behandelt de bestaande online onderzoeksdaden binnen het Belgische strafrechtelijke kader. De digitalisering zorgde voor de implementatie van diverse online onderzoeksdaden: politiediensten kunnen informaticasystemen doorzoeken, identificatiegegevens opvragen bij online dienstverleners en communicatieverkeer traceren, en in bepaalde gevallen zelfs de inhoud van communicatie onderscheppen. Gezien het ingrijpende karakter van deze methoden is een duidelijke omkadering geboden. Hoe verregaander de maatregel, hoe strenger de voorwaarden die de Belgische wetgever oplegt. In het kader van dit onderzoek, is een analyse van deze voorwaarden onmisbaar. Het kan immers inspiratie bieden voor de eventuele voorwaarden die van toepassing moeten zijn bij de zoektermbevelen.

14. Het derde hoofdstuk richt zich op dataretentie en toegang tot bewaarde gegevens in het licht van het recht op privacy en gegevensbescherming vanuit een Europees Unierechtelijk perspectief. Binnen het kader van gegevensverwerking vormt de Algemene Verordening Gegevensbescherming het centrale juridische instrument, gericht op de bescherming van persoonsgegevens en het waarborgen van de privacy binnen de Europese Unie. De verordening legt verwerkingsverantwoordelijken stringente verplichtingen op ten aanzien van de verwerking, opslag en beveiliging van persoonsgegevens. Ook wanneer opsporingsautoriteiten in het kader van strafrechtelijk onderzoek bewaarde online gegevens wensen te raadplegen, dienen deze Unierechtelijke normen te worden nageleefd. Het Hof van Justitie van de Europese Unie heeft op dit terrein een omvangrijke en richtinggevende jurisprudentie ontwikkeld. In dit hoofdstuk wordt geanalyseerd welke juridische voorwaarden en beperkingen, voortvloeiend uit het recht op privacy en gegevensbescherming, gelden voor de bewaring van gegevens en de toegang daartoe door opsporingsinstanties. Daarbij wordt in het bijzonder aandacht besteed aan de vraag hoe deze waarborgen dienen te worden geïnterpreteerd en toegepast in het kader van de bewaring van zoekgeschiedenissen en aanverwante gegevens, en de toegang daartoe door rechtshandavingsinstanties, in het kader van zoektermbevelen. Op basis van deze analyse volgt een aanbeveling voor de juridische toepassing van zoektermbevelen, rekening houdend met de normen en grenzen gesteld in de rechtspraak.

15. Het recht op privacy en gegevensbescherming wordt niet enkel beschermd door het Unierecht, maar vindt tevens verankering in het Europees Verdrag voor de Rechten van de Mens. Dit vierde en laatste hoofdstuk behandelt hoe het Europees Hof voor de Rechten van de Mens oordeelt over online onderzoeksmethoden in het licht van deze grondrechten. Het Hof erkent dat online opsporingsmaatregelen een inmenging in het recht op privacy vormen, maar wijst tevens op de noodzaak tot een evenwichtige afweging met legitieme doelen zoals misdaadbestrijding. Dergelijke maatregelen vergen strikte naleving van grenzen en waarborgen om willekeur en machtsmisbruik te voorkomen. Wanneer gegevens op grote schaal worden verzameld en toegankelijk gemaakt in het kader van strafrechtelijk onderzoek, past het Hof bovendien een verscherpte toetsing toe. Dit laatste hoofdstuk onderzoekt welke materiële en procedurele voorwaarden het Hof stelt aan ingrijpende

onderzoeksmaatregelen en formuleert op basis van dat normatieve kader een aanbeveling over hoe zoektermbevelen vorm zouden moeten krijgen.

§ 3: Relevantie

16. Dit onderzoek heeft zowel theoretische als praktische relevantie. Theoretisch draagt het onderzoek bij aan de rechtswetenschappelijke literatuur door een inhoudelijke aanvulling te bieden op de bestaande kennis. Het reikt een kader aan waarbinnen deze onderzoeksmethode eventueel kan worden geïntegreerd in het Belgische strafrecht, en verkent op welke wijze een dergelijke onderzoeksdaad juridisch vorm zou kunnen krijgen binnen de Belgische wetgeving.

17. Praktisch gezien is het onderzoek van grote waarde, omdat het de grens aftast van wat vandaag mogelijk is in de strafprocedure, en tegelijkertijd reflecteert op toekomstige evoluties in digitale opsporing. De bevindingen kunnen richtinggevend zijn voor beleidsmakers en rechtspractici, in het bijzonder voor magistraten en politiediensten die worden geconfronteerd met steeds complexere cyber- en misdaadpatronen waarin klassieke opsporingstechnieken tekortschieten. Door te analyseren of en onder welke voorwaarden zoektermbevelen toelaatbaar zijn, kan dit onderzoek bijdragen aan de ontwikkeling van een praktijkgericht kader waarin rechtsbescherming en technologische mogelijkheden op een evenwichtige manier worden afgewogen.

§ 4: Afbakening en toepassingsgebied

18. Dit onderzoek richt zich voornamelijk op de grenzen die worden gesteld door de rechtspraak van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens met betrekking tot dataretentie en de toegang tot deze gegevens, in het bijzonder in het licht van het recht op privacy en gegevensbescherming. Het onderzoek richt zich derhalve niet op de verwerking van persoonsgegevens door bevoegde autoriteiten zelf, maar op de voorwaarden waaronder zoekmachinebedrijven gegevens kunnen bewaren en opsporingsautoriteiten toegang kunnen verkrijgen tot deze gegevens. De wijze waarop deze autoriteiten vervolgens met de verwerking van persoonsgegevens omgaan, valt buiten het bestek van dit onderzoek. De Richtlijn (EU) 2016/680 betreffende de verwerking van persoonsgegevens door politie- en justitiediensten, evenals de daarbij horende bepalingen, worden derhalve buiten beschouwing gelaten.¹⁴ Tot slot blijft, gezien de beperkte omvang en duur van dit onderzoek, de impact van versleutelingstechnieken buiten beschouwing.¹⁵

¹⁴ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad, *Pb.L.* 4 mei 2016; afdeling 12, hoofdstuk IV, "informatiebeheer" Wet van 5 augustus 1992 op het politieambt, *BS* 22 december 1992.

¹⁵ VAN DAALLEN O., 'De verplichting die er in de praktijk op neer komt dat encryptietechnologie wordt verzwakt, is in strijd met artikel 8 EVRM (noot onder EHRM 13 februari 2024)', *Computerrecht* 2024/98, (184) 184-185; ROYER S., 'Hof van Cassatie cryptisch over verbod op encryptie', *Juristenkrant* 2025/505, (1) 1-2; ROYER S., 'Cassatie verwerpt procedurele bezwaren tegen Sky ECC-onderzoek (noot onder cass. 27 juni 2023)', *T.Strafr.* 2024/2, (99) 100-101; STEPPE R., 'Prijdiscriminatie in het digitale tijdperk: beschouwingen over de nieuwe Algemene Verordening Gegevensbescherming' in STORME M.E. en HELSEN F. (eds.), *Innovatie en disruptie in het economisch recht*, Intersentia, 2017, (105) 117.

Hoofdstuk I. Opsporen via zoekgedrag: een Amerikaanse onderzoeksdaad onder de loep

19. In tegenstelling tot België kent de Verenigde Staten van Amerika (hierna: VSA) wel het concept van zoektermbevelen en worden deze ook frequent aangewend door opsporingsdiensten wanneer zij geen concrete verdachte in beeld hebben. Daarom is het interessant om terug te koppelen op de Amerikaanse toepassing en interpretatie van zoektermbevelen. De Amerikaanse toepassing kan als voorbeeld dienen voor een conceptuele en operationele invulling van zoektermbevelen in België.

§ 1: Een sprong in het onbekende: keyword warrants

20. De VSA kent 'reverse search warrants' als brede categorie van onderzoeksdaaden. Hierbij vertrekt de politie niet vanuit het doorzoeken van een plaats of het eigendom van een persoon die als verdachte wordt aangemerkt, maar wordt gebruik gemaakt van brede parameters om elke persoon te identificeren die mogelijk een verband heeft met bewijsmateriaal.¹⁶ De 'reverse search warrants' zijn belangrijke onderzoekstechnieken ingeval van onbekende daders, waarbij de politie een grote groep mensen onderzoekt, waarvan de meeste onschuldig zijn, om zo slechts een paar actoren eruit te halen als verdachte.¹⁷ Deze verschillen van de traditionele bevelschriften waarvan gebruik wordt gemaakt wanneer rechtshandhavers vermoedelijke redenen hebben om aan te nemen dat een bepaald individu een bepaald misdrijf heeft gepleegd.¹⁸

21. Tot de categorie van 'reverse search warrants' behoren onder meer de 'keyword warrants' en de 'geofence warrants'. Deze laatste onderzoekstechniek betreft de mogelijkheid om aan een bedrijf, zoals Google, gegevens op te vragen over gebruikers die zich in een bepaald gebied op een bepaald moment bevonden.¹⁹ De 'Keyword warrants', ook wel vertaald naar zoektermbevelen, betreft een onderzoeksdaad waarbij zoekmachinebedrijven zoals Google, Microsoft en Yahoo, verplicht

¹⁶ FRANKSON, J.P., 'Reverse Search Warrants: Economically Beneficial?', 18 *Journal of Law, Economics & Policy* (18 J.L. Econ. & Pol'y) 2023/2, (355) 355; LONG-KELLOUGH A., 'IF I DIE, DELETE MY BROWSER HISTORY: THE FOURTH AMENDMENT IMPLICATIONS OF REVERSE KEYWORD SEARCH WARRANTS', 52 *Capital University Law Review* (52 Cap. U. L. Rev.) 2024/1, (1) 42; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 907-908; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minnesota Law Review* (107 Minn. L. Rev.) 2023/3, (1369) 1370, 1372; SHAMONA J., 'The Unconstitutionality of Geofence Warrants', 6 *University of Central Florida Department of Legal Studies Law Journal* (6 U. Cent. Fla. Dep't Legal Stud. L.J.) 2023, (71) 76.

¹⁷ Dit fenomeen wordt ook wel 'dragnet policing' of 'filtered dragnet' genoemd; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 978-979; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 907-908; BAMBAUER J.R., 'Filtered dragnets and the anti-authoritarian Fourth Amendment', 97 *Southern California Law Review* (97 S. Cal. L. Rev.) 2024/3, (571) 579-587.

¹⁸ CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 273; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1385.

¹⁹ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 897; FAN M.D., 'Suspecting with Data', 109 *Minnesota Law Review* (109 Minn. L. Rev.) 2024, (1) 19; LONG-KELLOUGH A., 'IF I DIE, DELETE MY BROWSER HISTORY: THE FOURTH AMENDMENT IMPLICATIONS OF REVERSE KEYWORD SEARCH WARRANTS', 52 *Cap. U. L. Rev.* 2024/1, (1) 42; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1370, 1373; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 995-996; SINHA M., 'The automated fourth amendment', 73 *Emory Law Journal* (73 Emory L.J.) 2024/3, (589) 610.

worden gegevens vrij te geven over gebruikers die naar specifieke zoektermen hebben gezocht.²⁰ Bevelen op basis van trefwoorden vereisen niet de zoekgeschiedenis van een specifiek persoon, maar informatie van personen die hebben gezocht naar één of meerdere trefwoorden.²¹ Meer specifiek verplicht een dergelijk soort bevel bedrijven ertoe accountinformatie en IP-adressen te onthullen van gebruikers die hebben gezocht naar termen die gerelateerd zijn aan een misdrijf gedurende een bepaalde periode.²² De tijdsperiode voor zoekopdrachten naar trefwoorden kan verschillen, maar zal hoofdzakelijk betrekking hebben op zoektermen voorafgaand aan het misdrijf, namelijk in de planningsfase.²³ De 'keyword warrant' is een zeer verregaande maatregel aangezien een persoon als verdachte kan worden aangemerkt louter op basis van wat ze in een bepaalde periode toevallig hebben opgezocht.²⁴

22. Zoektermbevelen zijn meestal gericht op Big Tech bedrijven die de meest gebruikte zoekmachines aanbieden: Google, Microsoft en Yahoo.²⁵ Wanneer een gebruiker een zoekopdracht uitvoert, bewaren deze zoekmachinebedrijven belangrijke gegevens: de zoekopdracht, de tijd en datum waarop de zoekopdracht werd uitgevoerd, het IP-adres en de cookie van de computer waarop de zoekopdracht werd uitgevoerd en het browsertype en besturingssysteem.²⁶ Wanneer de gebruiker is ingelogd op haar account, beschikken de bedrijven daarnaast over ruime persoonlijke gegevens, zoals de naam, telefoonnummers, fysieke adressen, e-mailadressen, de duur van online sessies, ...²⁷ Ook wanneer een gebruiker niet is ingelogd op zijn account, bewaren de bedrijven de IP-adressen en de Browser Cookie ID's, van apparaten waarop gebruikers zoektermen opzoeken.²⁸ Google is hierbij de grootste, en wordt het meest verzocht om gegevens over te brengen gezien het bedrijf ook de apps Google Maps en Waze aanbiedt, die daders kunnen gebruiken om de weg te zoeken naar het adres van het beoogde misdrijf.²⁹

²⁰ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 880; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 984; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1385.

²¹ EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 984.

²² FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 893; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 272.

²³ In 'people/Seymour' werd bijvoorbeeld gekeken naar zoektermen tot twee weken voor de brandstichting. In het onderzoek naar de pijpbomaanslagen in Austin Texas, werd zelfs een maand teruggegaan in de zoekgeschiedenis; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 893.

²⁴ EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 1002.

²⁵ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024, (877) 892; FAN M.D., 'Suspecting with Data', 109 *Minn. L. Rev.* 2024/5, (1) 14.

²⁶ WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1388.

²⁷ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 893; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 980-983; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 284-285.

²⁸ WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1387; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 288.

²⁹ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 893; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 979.

23. Over het algemeen verloopt een 'keyword warrant' in drie stappen.³⁰ In eerste instantie vraagt de overheid providers om hun databases te doorzoeken om zo een lijst te produceren van IP-adressen die op de gevraagde zoektermen hebben gezocht.³¹ Het zoekmachinebedrijf geeft de opsporingsinstanties daarbij een lijst met de datum en tijd waarop de zoekopdracht werd uitgevoerd, de informatie over de locatie, de zoekopdracht van de gebruiker, ... Deze gegevens worden echter wel geanonimiseerd.³² Vervolgens bekijken de onderzoekers de lijst en sluiten ze de personen uit die onwaarschijnlijke verdachte zijn, bijvoorbeeld omdat hun IP-adres laat zien dat ze zich ten tijde van het misdrijf in een ander land bevonden.³³ De rechtshandavingsinstanties kunnen dan eventueel een tweede bevelschrift uitvaardigen met betrekking tot toegang tot persoonlijke identificatiegegevens. In tegenstelling tot de eerste fase kan de toevoeging van accountgerelateerde informatie de opsporingsautoriteiten voorzien van namen, adressen, telefoongegevens, gegevens over sessietijden- en duur, identificatienummers van het apparaat, ...³⁴ Tenslotte kan de politie een persoonsgebonden bevel uitvaardigen voor degene die geïdentificeerd zijn door de informatie van de providers.³⁵ Zo kan er dan bijvoorbeeld een huiszoekingsbevel worden verkregen om gegevens te onderzoeken die zijn gekoppeld aan de apparaten van de verdachte.³⁶

24. Wat houdt zo'n 'keyword warrant' nu in in de praktijk? Stel dat je recent verhuisd bent naar een nieuwe stad en je bent uitgenodigd op een verjaardagsfeest. Als cadeau wilt u graag een brief afgeven met cash. U zoekt via Waze de route op tot de dichtstbijzijnde bank en rijdt hiernaartoe. Nog geen dag later wordt de bank toevallig overvallen en, aangezien de politie geen aanwijzingen kan vinden op basis van getuigenissen en camerabeelden, vragen de onderzoekers aan Google om op te zoeken welke gebruikers het adres van de bank hebben opgezocht en welke gebruikers het adres ingaven via Google Maps of Waze. Uw IP-adres, naam, thuisadres en andere belangrijke informatie worden doorgegeven aan de politie-eenheden en enkele dagen later staan deze aan uw deur met een huiszoekingsbevel en delen ze u mee dat u verdachte bent in het onderzoek naar de overval van de desbetreffende bank.³⁷

25. De 'keyword warrants' tonen aan hoe ver politionele instanties kunnen gaan in het onderzoeken van digitale gegevens van burgers in het kader van het zoeken naar een dader van een misdrijf. Deze onderzoeksmaatregel is echter niet onproblematisch. Zo kunnen zoektermbevelen sterk variëren in reikwijdte wat aanleiding kan geven tot rechtsonzekerheid. Om verzoeken van wethandhavers effectief te analyseren en aan te vechten, is het daarbij van belang om te weten wat de onderzoekers precies zoeken.³⁸ Ook met betrekking tot de potentiële kosten en baten van het

³⁰ FAN M.D., 'Suspecting with Data', *109 Minn. L. Rev.* 2024, (1) 14-15.

³¹ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Tex. L. Rev.* 2024/5, (877) 896; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', *107 Minn. L. Rev.* 2023/3, (1369) 1371, 1387.

³² CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', *45 Cardozo L. Rev.* 2023/1, (271) 287.

³³ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Tex. L. Rev.* 2024/5, (877) 896; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', *107 Minn. L. Rev.* 2023/3, (1369) 1371, 1389.

³⁴ WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', *107 Minn. L. Rev.* 2023/3, (1369) 1371, 1402.

³⁵ *Ibid*, 1371.

³⁶ *Ibid*.

³⁷ FRANKSON, J.P., 'Reverse Search Warrants: Economically Beneficial?', *18 J.L Econ. & Pol'y* 2023/2, (355) 355.

³⁸ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Tex. L. Rev.* 2024/5, (877) 897.

onderzoek is het belangrijk om te weten hoeveel zoekgeschiedenis van mensen wordt onthuld uit een trefwoord en welke resultaten onderzoekers daaruit verkrijgen.³⁹ Het grootste probleem in het kader van deze onderzoekstactiek betreft echter het recht op privacy, zowel van de dader als van de niet-betrokken derden.⁴⁰ Door een 'keyword warrant' kunnen namelijk duizenden of miljoenen individuen beïnvloed worden door één enkele zoekopdracht, waarvan slechts één of enkele, de effectieve dader zal zijn.⁴¹ De autoriteiten hebben toegang tot hun persoonlijke gegevens, terwijl daarvoor geen toestemming werd gegeven en zelfs terwijl de betrokkene zich niet bewust is van het feit dat de persoonlijke gegevens worden verzameld.⁴² Zoeken op trefwoorden is een gemakkelijk hulpmiddel om potentiële daders eruit te vissen, maar de gemakkelijkste manier is daarom niet altijd de correcte.

§ 2: Constitutionele twijfels

26. Gezien het ingrijpende karakter van zoektermbevelen is het niet verrassend dat zij vanuit verschillende hoeken kritiek ontvangen. Een veelgehoord bezwaar is dat deze zogeheten 'keyword warrants' in strijd zouden zijn met het Vierde Amendement van de Amerikaanse Grondwet en het daarmee gepaard gaande recht op privacy.⁴³ Dit amendement verbiedt huiszoekingen en inbeslagnames die onredelijk zijn of zonder verdenking plaatsvinden.⁴⁴ De 'keyword warrants' vallen onder de bescherming van het Vierde Amendement, aangezien er een 'reasonable expectation' geldt in het kader van online surveillance, en het verkrijgen van zoekgeschiedenisgegevens door de overheid aldus beschouwd kan worden als een zoeking in de zin van het amendement.⁴⁵

³⁹ FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 897.

⁴⁰ *Ibid*, 877, 897, 914-916, 922; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1370, 1373-1374.

⁴¹ EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 987, 1001; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 284; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1372.

⁴² BAJPAI A., GUPTA A. en SHAH M.G., 'Search and seizure of electronic devices in India: time for a change?', 28 *International Journal of Evidence & Proof* (28 E. & P.) 2024/4, (298) 300-301; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 978.

⁴³ EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 995; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 925-931; WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1389-1390; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 274; zie ook voor geofence warrants waar een gelijkaardige problematiek heerst: U.S. Court of Appeal for the Fourth Circuit 9 juli 2024, nr. 22-4489, 'United States/Chatrie'; DRANA D., 'Why it's time to ban geofence searches in light of united states v. chatrrie', 38 *Berkeley Technology Law Journal* (38 *Berkeley Tech. L.J.*) 2023/4, (1307).

⁴⁴ CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 276; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 990; DRANA D., 'Why it's time to ban geofence searches in light of united states v. chatrrie', 38 *Berkeley Tech. L.J.* 2023/4, (1307) 1316; RADFORD M., 'Back to the future: revisiting state constitutions to protect against new technological intrusions', 81 *Washington and Lee Law Review* (81 *Wash. & Lee L. Rev.*) 2024/4, (1641) 1651-1652; TURSI R., 'Gone Fishing: Casting a Wide Net Using Geofence Warrants', 98 *Washington Law Review* (98 *Wash. L. Rev.*) 2023/1, (323) 335-336.

⁴⁵ U.S. Supreme Court 22 juni 2018, 138 S. Ct. 2206, 'Carpenter/United States'; U.S. Supreme Court Colorado 16 oktober 2023, nr. 23SA12, 'People/Seymour', §32; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 290; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 999; zie meer over 'reasonable expectation' onder Fourth Amendment; U.S. Supreme Court 18 december 1967, 389 U.S. 347; 'Katz/United States'; U.S. Supreme Court 21 april 1976, 425 U.S. 435, 'United States/Miller'; U.S. Supreme Court 20 juni 1979, 442 U.S. 735, 'Smith/Maryland'; U.S. Supreme Court 2 januari 2012, 615 F. 3d 544, 'United States/Jones'; U.S. Court of Appeal for the Third Circuit 11 december 2014, 806 F.3d 125, 'In re Google Inc.

27. Volgens het Vierde Amendement moet een (huis)zoekingsbevel gebaseerd zijn op een 'probable cause', ondersteund door een eed, en voldoen aan de eis van 'particularity'.⁴⁶ Er is sprake van 'probable cause' wanneer er een redelijke grond bestaat om aan te nemen dat bewijs van een misdrijf aanwezig zal zijn op de plaats die doorzocht moet worden.⁴⁷ 'Keyword warrants' kunnen niet voldoen aan deze voorwaarde, aangezien de enige basis voor het bevel de veronderstelling van een wetshandhaver is dat de verdachte mogelijk heeft gezocht naar een zoekterm dat gerelateerd is aan het vermeende misdrijf. Bovendien kunnen wetshandhavers niet met redelijke overtuiging, op basis van de feiten die zij kennen, vaststellen dat de verdachte gebruik heeft gemaakt van Google of een andere zoekmachine, waardoor niet met redelijke waarschijnlijkheid kan worden aangenomen dat bewijs zal worden gevonden in de zoekgeschiedenis van de onderzochte personen.⁴⁸

28. De eis van 'particularity' houdt in dat het bevel specifiek en afgebakend moet zijn.⁴⁹ Een bevel kan niet worden uitgevaardigd als het gebied te breed is of wanneer er geen specifieke personen worden geïdentificeerd.⁵⁰ 'Keyword warrants' voldoen niet aan deze eis, omdat ze geen specifieke persoon omschrijven, maar in plaats daarvan een breed digitaal net werpen dat onschuldige individuen kan omvatten die toevallig naar bepaalde termen zochten.⁵¹ Deze warrants hebben een ongerichte en brede reikwijdte, omdat zij niet gebaseerd zijn op een geïndividualiseerde verdenking. Pas na de uitvoering van het bevel kunnen personen worden geïdentificeerd, wat het gebrek aan voorafgaande verdenking benadrukt en aantoont dat de noodzakelijke precisie ontbreekt die het amendement vereist.⁵² Bevelen moeten specifiek zijn en gericht op de persoon die doorzocht

Cookie Placement Consumer Priv. Litig.'; U.S. Court of Appeal for the Ninth Circuit 9 april 2020, 956 F.3d 589, 'In re Facebook, Inc. Internet Tracking Litig.'; U.S. District Court for the Northern District of Illinois Eastern Division 24 augustus 2020, 481 F. Supp. 3d 730, 'In re Search of Info. Stored at Premises Controlled by Google'; FOLEY J., 'Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases', 22 *Berkeley Technology Law Journal* (22 *Berkeley Tech. L.J.*) 2007/1, (447) 465, 468.

⁴⁶ EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 992; FRANKSON, J.P., 'Reverse Search Warrants: Economically Beneficial?', 18 *J.L. Econ. & Pol'y* 2023/2, (355) 359-360; SINHA M., 'The automated fourth amendment', 73 *Emory L.J.* 2024/3, (589) 593.

⁴⁷ CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 277.

⁴⁸ MÁRQUEZ J., 'Dissenting opinion bij U.S. Supreme Court Colorado 16 oktober 2023', nr. 23SA12, 'People/Seymour', §§ 81-88; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 299; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 933.

⁴⁹ WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', 107 *Minn. L. Rev.* 2023/3, (1369) 1370, 1375-1376.

⁵⁰ U.S. Supreme Court 8 juni 1983, 462 U.S. 213, 'Illinois/Gates'; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 992; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 930; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 277; STENDER S., 'Circumventing the fourth amendment: the unconstitutional nature of geofence warrants', *U. L. Rev.* 2024/3, (733) 751; SHAMONA J., 'The Unconstitutionality of Geofence Warrants', 6 *U. Cent. Fla. Dep't Legal Stud. L.J.* 2023, (71) 78-80.

⁵¹ EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 1001; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 925-926.

⁵² U.S. Supreme Court Colorado 16 oktober 2023, nr. 23SA12, 'People/Seymour'; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 1001; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 274-275, 299; zie analogie met geofence warrants in STENDER S., 'Circumventing the fourth amendment: the unconstitutional nature of geofence warrants', *U. L. Rev.* 2024/3, (733) 750-754; SHAMONA J., 'The Unconstitutionality of Geofence Warrants', 6 *U. Cent. Fla. Dep't Legal Stud. L.J.* 2023, (71) 83-85.

wordt.⁵³ Dit is echter niet mogelijk bij zoekbevelen op basis van trefwoorden, aangezien wetshandhavers deze bevelen gebruiken om verdachten te identificeren, in plaats van reeds geïdentificeerde personen te doorzoeken.⁵⁴

29. Critici vanuit de VSA stellen dan ook dat 'keyword warrants' een vorm van algemene surveillance vormen en in feite neerkomen op een zogenaamde 'fishing expedition': een brede, willekeurige zoekactie waarbij opsporingsinstanties hopen dat relevante verdachten of bewijzen naar boven komen. Om deze reden wordt bepleit dat rechtbanken dergelijke bevelschriften als ongrondwettelijk moeten beschouwen.⁵⁵

⁵³ U.S. Supreme Court 28 november 1979, 444 U.S. 88, 'Ybarra/Illinois'; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 281, 303.

⁵⁴ CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 303; FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', 102 *Tex. L. Rev.* 2024/5, (877) 908.

⁵⁵ Assembly Bill A84A van State of New York van 6 januari 2021; Electronic Keyword and Location Amendments HB0251 van State of Utah van 26 januari 2021; U.S. Supreme Court Colorado 16 oktober 2023, nr. 23SA12, 'People/Seymour'; EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 999-1002; CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', 45 *Cardozo L. Rev.* 2023/1, (271) 299-307; STENDER S., 'Circumventing the fourth amendment: the unconstitutional nature of geofence warrants', *U. L. Rev.* 2024/3, (733) 753; SHAMONA J., 'The Unconstitutionality of Geofence Warrants', 6 *U. Cent. Fla. Dep't Legal Stud. L.J.* 2023, (71) 96-101.

Hoofdstuk II. Een uitstap naar het Belgisch strafrechtelijk landschap van online onderzoeksdaden

30. Hoewel zoektermbevelen momenteel geen deel uitmaken van het bestaande repertoire aan Belgische digitale opsporingsmethoden, is een grondige analyse van het huidige juridische kader noodzakelijk, aangezien een eventuele toekomstige regeling omtrent zoektermbevelen noodgedwongen moet aansluiten bij het reeds bestaande kader van digitale strafvorderlijke bevoegdheden.

§ 1: Online onderzoeksmethoden⁵⁶

31. Door de voortschrijdende digitalisering zijn communicatie, informatievergaring en sociale interactie steeds meer verplaatst naar digitale kanalen, waarbij vrijwel elke handeling digitaal wordt geregistreerd. Ook criminelen maken steeds vaker gebruik van technologische middelen, wat heeft geleid tot een fundamentele verschuiving in het strafrechtelijk onderzoek. Elektronische gegevens vormen vandaag een essentiële bron van informatie, en het onderzoek steunt dan ook in toenemende mate op digitale opsporingsmethoden.⁵⁷ Om deze digitale realiteit het hoofd te bieden, is er de afgelopen decennia steeds meer aandacht besteed aan het wettelijk verankeren van onderzoeksbevoegdheden gericht op het verkrijgen en analyseren van digitale gegevens.⁵⁸ Deze bevoegdheden vormen een cruciaal instrumentarium voor een effectief en toekomstgericht strafrechtelijk optreden. Ze omvatten onder meer het openlijk of heimelijk doorzoeken van informaticasystemen, het opvragen van identificatie-, verkeers- en lokalisatiegegevens, en het onderscheppen van communicatie-inhoud in real-time of met terugwerkende kracht.

32. De ontwikkeling van digitale opsporingsmethoden gaat gepaard met aanzienlijke juridische en ethische uitdagingen, aangezien zij onvermijdelijk inbreuk maken op het recht op privacy en gegevensbescherming. In de rechtspraak en rechtsleer is daardoor een fundamenteel spanningsveld

⁵⁶ Bijlage 1.

⁵⁷ DE KEERSMAECKER R. en VAN DE HEYNING C., 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *T.Strafr.* 2021/4, (171) 171-172; VAN DE HEYNING C., 'Overzicht van rechtspraak – Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog (noot onder GwH 19 juli 2018)', *T.Strafr.* 2019/1, (38) 38-39; CONINGS C., 'Speuren op sociale media: de nieuwigheden op een rij', *P&R* 2020/1, (3) 3; VAN LINTHOUT P. en KERKHOFS J., 'Actuele uitdagingen in cybercrime voor de advocatuur en de magistratuur: vervolgen en verdedigen met een bot scalpel?' in LIEVENS A., VALCKE P., DUMORTIER J., GRAUX H., KERKHOFS J., LEFEVER K., SOMERS G., VAN LINTHOUT P. en WAUTERS E. (eds.), *Themis 81 - ICT- en mediarecht*, die Keure, 2013, (27) 27-29.

⁵⁸ Wet van 11 februari 1991 tot invoeging van een artikel 88bis in het Wetboek van Strafvordering, *BS* 16 maart 1991; Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privécommunicatie en -telecommunicatie, *BS* 24 januari 1995; Wet tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *BS* 22 september 1998; Wet van 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001; Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 mei 2003; Wet van 27 december 2005 houdende diverse bepalingen, *BS* 30 december 2005; Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016; Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrucken, *BS* 17 januari 2017; Wet van 5 mei 2019 houdende diverse bepalingen in strafzaken en inzake erediensten, en tot wijziging van de wet van 28 mei 2002 betreffende de euthanasie en van het Sociaal Strafwetboek, *BS* 24 mei 2019.

ontstaan tussen privacybescherming en veiligheid (Cf. *supra*, hoofdstukken 3 en 4). Zowel het Europees Hof van Justitie als het Europees Hof voor de Rechten van de Mens hebben grenzen gesteld aan de inzet van dergelijke methoden, wat de Belgische wetgever ertoe heeft aangezet om deze beperkingen te verankeren in nationale regelgeving. Daarbij geldt een duidelijke proportionaliteitsbenadering: hoe ingrijpender de maatregel, des te strikter de toepasselijke voorwaarden en waarborgen.

33. Vanuit het onderzoeksopzet rijst de vraag hoe een bepaling omtrent zoektermbevelen zou kunnen worden geïntegreerd in het bestaande wettelijk kader voor online onderzoeksmaatregelen. Een dergelijke bepaling zal namelijk een eigen invulling vereisen, met bijbehorende voorwaarden en grenzen. Het is dan ook van cruciaal belang om te onderzoeken welke voorwaarden reeds opgelegd worden voor de bestaande onderzoeksmethoden, aangezien de concretisering van zoektermbevelen binnen de reeds gevestigde kaders en de daarmee samenhangende beperkingen moet worden ingepast.

Afdeling 1: (Openlijke) zoeking in informaticasystemen of delen ervan – Artikel 39bis Juncto 88ter Sv.

34. Een eerste categorie van digitale onderzoeksdaten betreft de openlijke zoekingen in een informaticasysteem. Openlijk betekent dat de procureur des Konings (hierna: PdK) of de onderzoeksrechter de verantwoordelijke van het informaticasysteem zo spoedig mogelijk op de hoogte stelt van de zoeking of de uitbreiding daarvan, tenzij diens identiteit of woonplaats redelijkerwijs niet kan worden vastgesteld.⁵⁹

In het licht van artikel 39bis juncto artikel 88ter Wetboek van Strafvordering (hierna: Sv.) kunnen drie verscheidene zoekingen worden onderscheiden: (i) de informaticazoeeking, (ii) de netwerkzoeeking en (iii) een restcategorie. Afhankelijk van de categorie van zoeking in een informaticasysteem gelden andere regels omtrent de bevoegde instantie, de vorm en de voorwaarden opdat een zoeking kan plaatsvinden.⁶⁰

A. Informaticazoeeking

35. De informaticazoeeking heeft betrekking op informaticasystemen die in beslag zijn genomen, dan wel in beslag kunnen worden genomen.⁶¹ Op deze informaticasystemen kunnen relevante gegevens opgeslagen zijn die het bewijs kunnen leveren van een bepaald misdrijf.⁶² De zoeking dient weliswaar steeds beperkt te zijn tot het aangetroffen systeem en de gegevens die zich daarop bevinden, waardoor elke externe verbinding (gsm-verbinding, wifi-connectie, ...) van het

⁵⁹ Art. 39bis, §7 Wetboek van Strafvordering, BS 17 november 1808 (hierna: Sv.).

⁶⁰ CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, (99) 102-109.

⁶¹ Art. 39bis, §2, lid 1 Sv.

⁶² CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, (99) 102.

informaticasysteem uitgezet moet worden, alvorens de zoeking kan worden aangevat.⁶³ Een voorbeeld van een informaticazoeking betreft de situatie waarbij tijdens een huiszoeking verschillende computers en geheugenkaarten in beslaggenomen worden. Deze kunnen dan door gespecialiseerde computer crime units onderzocht worden.⁶⁴

36. Gezien het minder ingrijpende karakter van deze onderzoekshandeling gelden er relatief milde voorwaarden voor de uitvoering ervan. Wat betreft de bevoegdheid tot het overgaan van een dergelijke zoeking, wordt gewerkt met een getrapt systeem.⁶⁵ Zo bepaalt art. 39bis, §2, eerste lid Sv. dat de officier van de gerechtelijke politie bevoegd is voor zoekingen in een informaticasysteem of een deel ervan dat in beslag is genomen. Indien het systeem weliswaar in beslag kan worden genomen, maar dit niet wenselijk of noodzakelijk wordt geacht, is een bevel van de PdK vereist.⁶⁶ In de praktijk betekent dit dat indien een officier van gerechtelijke politie tijdens een huiszoeking een informaticasysteem aantreft, en enkel ter plaatste wil doorzoeken, hij voorafgaand een machtiging van de PdK nodig heeft, terwijl dat niet het geval is wanneer besloten wordt het systeem in beslag te nemen.⁶⁷

De wet stelt verder geen specifieke inhoudelijke voorwaarden. Niettemin geldt, overeenkomstig het fundamentele recht op eerbiediging van het privéleven, dat dergelijke onderzoekshandelingen enkel mogen plaatsvinden indien zij noodzakelijk zijn in een democratische samenleving. Het gebruik van deze bevoegdheid moet in dat verband relevant, proportioneel en evenredig zijn.⁶⁸

B. Netwerkzoeking

37. De netwerkzoeking betreft een uitbreiding van de informaticazoeking naar informaticasystemen, of delen daarvan, die zich op een andere plaats bevinden dan daar waar de zoeking plaatsvindt.⁶⁹ Gezien het omvangrijke karakter van de netwerkzoeking heeft deze een beperkt toepassingsgebied en heeft ze enkel betrekking op het doorzoeken van informaticasystemen op afstand, die niet voor publiek toegankelijk zijn en die een gefundeerde link vertonen met het initieel onderzochte informaticasysteem.⁷⁰

⁶³ Art. 39bis, §2, lid 3, tweede zin Sv.; Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001, 16-17.

⁶⁴ Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001, 16.

⁶⁵ CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, (99) 102-109.

⁶⁶ Art. 39bis, §2, lid 2 Sv.; Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001, 16; VAN LINTHOUT P. en KERKHOF J., 'Actuele uitdagingen in cybercrime voor de advocatuur en de magistratuur: vervolgen en verdedigen met een bot scalpel?' in LIEVENS A., VALCKE P., DUMORTIER J., GRAUX H., KERKHOF J., LEFEVER K., SOMERS G., VAN LINTHOUT P. en WAUTERS E. (eds.), *Themis 81 - ICT- en mediarecht*, die Keure, 2013, (27) 49-50.

⁶⁷ CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, (99) 103.

⁶⁸ *Ibid*, 104.

⁶⁹ Art. 88ter, lid 1 Sv.

⁷⁰ Art. 88ter, lid 2 Sv.; Wetsontwerp inzake informaticacriminaliteit, KAMER, 1999-2000, 3 november 1999, nr. 50K0213/001, 23; Wetsontwerp inzake informaticacriminaliteit, KAMER, 1999-2000, 24 maart 2000, nr. 50K0213/004, 91; CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, (99) 106.

38. In de oorspronkelijke bepaling kon de netwerkzoeking uitsluitend worden bevolen door de onderzoeksrechter.⁷¹ Bij de wet van 25 december 2016 werd deze bevoegdheid echter overgedragen aan de PdK.⁷² Deze wijziging werd echter vernietigd door het Grondwettelijk Hof, dat oordeelde dat, gezien de ernst van de inmenging in het privéleven, een dergelijke verregaande maatregel enkel door een onderzoeksrechter kan worden toegestaan.⁷³ Ook inhoudelijk worden er strengere grenzen gesteld. Zo kan een netwerkzoeking slechts plaatsvinden indien dit noodzakelijk is om de waarheid aan het licht te brengen en andere maatregelen disproportioneel blijken, of er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.⁷⁴ Ten slotte vereist de wet in principe een schriftelijke vorm voor het bevel van de onderzoeksrechter. In geval van dringende noodzakelijkheid kan de zoeking mondeling worden bevolen, mits het bevel vervolgens zo spoedig mogelijk schriftelijk wordt bevestigd.⁷⁵

C. Restcategorie

39. Ten slotte introduceerde de wetgever een restcategorie, waarin zoekingen kunnen plaatsvinden in een informaticasysteem of delen daarvan die niet onder de informaticazoeking en netwerkzoeking vallen.⁷⁶ Het betreft hoofdzakelijk het rechtstreeks uitvoeren van een zoeking in een systeem op afstand vanaf de computers van de overheid.⁷⁷ Dezelfde bevoegdheids-, inhouds- en vormvereisten als bij de netwerkzoeking dienen te worden nageleefd.⁷⁸

Afdeling 2: Identificatie van gebruikers van een elektronische communicatiedienst – Artikel 46bis Sv.

40. Onder bepaalde omstandigheden kunnen opsporingsinstanties zich toegang verschaffen tot identificatiegegevens (in het kader van elektronische communicatie) die zich bij bepaalde tussenpersonen bevinden.⁷⁹ Een onderscheid kan worden gemaakt tussen twee soorten identificatiegegevens. Ten eerste de gegevens van de abonnee of gebruiker van een communicatiedienst, zoals een (dynamisch of vast) IP-adres, IMEI-nummer van een gsm of de

⁷¹ Art. 88ter Sv.

⁷² Wet houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecomcommunicaties en tot oprichting van een gegevensbank stemafdrucken, *BS* 17 januari 2017.

⁷³ GwH. 6 december 2018, 174/2018; art. 11 Wet houdende diverse bepalingen in strafzaken en inzake erediensten, en tot wijziging van de wet van 28 mei 2002 betreffende de euthanasie en van het Sociaal Strafwetboek, *BS* 24 mei 2019.

⁷⁴ Art. 88ter, lid 1 Sv.; Wetsontwerp inzake informaticacriminaliteit, KAMER, 1999-2000, 3 november 1999, nr. 50K0213/001, 22-23.

⁷⁵ Art. 88ter, lid 5 Sv.

⁷⁶ Art. 39bis, §4 Sv.

⁷⁷ Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomcommunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001, 21; CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, (99) 108.

⁷⁸ Art. 39bis, §4, lid 1 en lid 2 Sv.; Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomcommunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001, 21.

⁷⁹ Art. 46bis Sv.; CONINGS C., *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 118.

houder van een telefoonnummer.⁸⁰ Ten tweede de gegevens van de diensten waarop een bepaald persoon geabonneerd is of die door een bepaald persoon gewoonlijk worden gebruikt, zoals geheime nummers of de internetdiensten die een persoon gebruikt.⁸¹ Deze onderzoeksmethode maakt het aldus mogelijk om zowel te achterhalen wie geabonneerd is op welk communicatiemiddel als welk middel door een specifieke persoon wordt gebruikt.⁸²

41. De bevoegdheid tot identificatie van gebruikers van een elektronische communicatiedienst is enkel toepasselijk voor het verkrijgen van gegevens die zich bij een operator van een elektronisch communicatienetwerk of bij de vestrekker van een elektronische communicatiedienst *sensu lato* bevinden.⁸³ Het gaat dan bijvoorbeeld over Telenet, Orange, Proximus, Jim Mobile, ...⁸⁴

42. Er dient een onderscheid gemaakt te worden tussen het verkrijgen van toegang tot gegevens en het bevel tot medewerking.⁸⁵ Artikel 46bis bepaalt: "*Bij het opsporen van misdrijven en wanbedrijven kan de procureur overgaan of doen overgaan ...*". In eerste instantie kan directe toegang tot gezochte identificatiegegevens worden verkregen via de klantenbestanden van operatoren, door tussenkomst van de Centrale Technische Interceptiefaciliteit (CTIF).⁸⁶ Daarnaast zijn opsporingsinstanties vaak afhankelijk van de medewerking van de operator of dienstverlener.⁸⁷ Deze zijn verplicht gehoor te geven aan het bevel, aangezien een weigering kan leiden tot

⁸⁰ Art. 46bis, §1, 1° Sv.; Wetsontwerp tot wijziging van artikel 46bis van het Wetboek van strafvordering, SENAAT, 2005-2006, 31 juli 2006, nr. 3-1824/1, 3 -5, 7; Zie voor begrip 'gewoonlijke gebruiker of abonnee': Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het af luisteren, kennismaken en opnemen van privécommunicatie en -telecommunicatie, KAMER, 1996-1997, 12 november 1997, nr. 49K1075/007, 3.

⁸¹ Art. 46bis, §1, 2° Sv.; Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het af luisteren, kennismaken en opnemen van privécommunicatie en -telecommunicatie, KAMER, 1996-1997, 12 november 1997, nr. 49K1075/001, 3; Wetsontwerp tot wijziging van artikel 46bis van het Wetboek van strafvordering, SENAAT, 2005-2006, 31 juli 2006, nr. 3-1824/1, 4-5.

⁸² Wetsontwerp tot wijziging van artikel 46bis van het Wetboek van strafvordering, SENAAT, 2005-2006, 31 juli 2006, nr. 3-1824/1, 4: "*Indien de procureur wil weten wie een welbepaald telefoonnummer gebruikt, dan kan de procureur dit doen op basis van artikel 46bis, §1, 1°. Wanneer de procureur echter wil weten over welke telefoonnummers een welbepaalde persoon beschikt, dan kan hij dit vragen op grond van artikel 46bis, §1, 2°. Ook is het mogelijk om te achterhalen naar welke nummers werd gebeld vanaf een welbepaald toestel of waar iemand zich bevond toen hij op een bepaald moment werd gebeld of zelf naar iemand belde. Deze onderzoekshandelingen vallen echter niet onder artikel 46bis, maar vallen onder artikel 88bis.*"; DAENINCK P, *Telefonieonderzoek in het strafrecht. Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.*, die Keure, 2020, 14-15.

⁸³ Art. 46bis, §1, lid 2, eerste en tweede gedachtestreepje Sv.; art. 2, 3°, 5° en 11° juncto artikel 9 Wet van 13 juni 2005 betreffende de elektronische communicatie, BS 20 juni 2005 (hierna: WEC); Cass. 18 januari 2011, P.10.1347.N, ECLI:BE:CASS:2011:CONC.20110118.1; DE SCHEPPER K. en VERBRUGGEN F., 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', *T.Strafr.* 2013/3, (143) 153; CONINGS C., *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 186-189; DERUYCK F., BEERNAERT M-A, BERKMOES S. e.a., *Het Strafrecht bedreven. Liber Amicorum Alain De Nauw*, die Keure, 2011, 295-297.

⁸⁴ DE SWAEF M., 'Conclusie bij Cass. 18 januari 2011', NC 2011, ECLI:BE:CASS:2011:CONC.20110118.1, (84) 84; VANDEZANDE N., 'Yahoo! Als operator of verstrekker (noot onder cass. 18 januari 2011)', *AM* 2011/2, (220) 222; DE SCHEPPER K. en VERBRUGGEN F., 'Ontsnappen *space invaders* aan onze *pacmannen*? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', *T.Strafr.* 2013/3, (143) 153.

⁸⁵ Art. 46bis, §1, lid 1 en lid 2 Sv.

⁸⁶ Art. 46bis, §1, lid 1 Sv.; Wetsontwerp tot wijziging van artikel 46bis van het Wetboek van strafvordering, SENAAT, 2005-2006, 31 juli 2006, nr. 3-1824/1, 6-7; Koninklijk besluit van 8 februari 2011 tot wijziging van het koninklijk besluit van 9 januari 2003 tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88bis, § 2, eerste en derde lid en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109terE, § 2 van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, BS 23 februari 2011; DERUYCK F., BEERNAERT M-A, BERKMOES S. e.a., *Het Strafrecht bedreven. Liber Amicorum Alain De Nauw*, die Keure, 2011, 299.

⁸⁷ Art. 46bis, §1, lid 2 Sv.; CONINGS C., *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 189-190.

strafrechtelijke sancties.⁸⁸ De medewerkingsplicht omvat zowel het verstrekken van feitelijke gegevens als het bieden van technische ondersteuning.⁸⁹ Wat betreft de termijn voor het verlenen van medewerking, dient deze te gebeuren "*in werkelijke tijd, of, indien van toepassing, op het tijdstip zoals bepaald in de vordering*".⁹⁰

43. De maatregel kan worden bevolen door de PdK, maar enkel indien aan bepaalde voorwaarden is voldaan. Zo moeten de beginselen van proportionaliteit en subsidiariteit in acht worden genomen, en dient de vordering tot identificatiegegevens te worden opgenomen in een gemotiveerde, schriftelijke beslissing.⁹¹ Proportionaliteit verwijst naar de afweging tussen het recht op privacy van de gebruiker en het belang van misdrijfdetectie.⁹² Bovendien kan de maatregel alleen worden toegepast indien blijkt dat minder ingrijpende onderzoeksdaden niet effectief zijn om de waarheid te achterhalen.⁹³ Om de balans met het recht op privacy en gegevensbescherming te waarborgen, geldt dat voor misdrijven die geen correctionele hoofdgevangenisstraf van een jaar of meer met zich meebrengen, de identificatiegegevens slechts voor een periode van zes maanden voorafgaand aan de beslissing gevorderd kunnen worden.⁹⁴

44. De mogelijkheid tot toegang tot identificatiegegevens speelt een cruciale rol binnen het kader van zoektermbevelen. Zoals eerder toegelicht, verloopt een dergelijk bevel in de VSA in drie fasen (Cf. *supra*, nr. 23). In eerste instantie ontvangen de autoriteiten van het zoekmachinebedrijf een lijst met gegevens omtrent de datum en het tijdstip van de uitgevoerde zoekopdracht, de locatiegegevens en de ingegeven zoektermen, zij het in geanonimiseerde vorm. Vervolgens kan, via het tweede bevel, toegang worden verkregen tot concrete identificerende gegevens, zoals namen, adressen, telefoonnummers, alsook unieke identificatoren van gebruikte apparaten. De tweede fase in de uitvoering van zoektermbevelen is aldus reeds voldoende uitgewerkt en verankerd in de Belgische praktijk. Niettemin dient het toepassingsgebied uitgebreid te worden naar zoekmachine-exploitanten die zoekplatforms aanbieden, aangezien de huidige regelgeving enkel van toepassing is op operatoren en dienstverleners binnen het domein van elektronische communicatie.

Afdeling 3: Opsporen en lokaliseren van elektronische communicatie – Artikel 88bis Sv.

45. In het kader van strafrechtelijk onderzoek kunnen opsporingsinstanties, naast identificatiegegevens, tevens toegang verkrijgen tot verkeers- en locatiegegevens met betrekking tot elektronische communicatie, voor zover deze gegevens worden bewaard door dienstverleners die

⁸⁸ Art. 46bis, §2, lid 4 Sv.; Koninklijk besluit van 8 februari 2011 tot wijziging van het koninklijk besluit van 9 januari 2003 tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88bis, § 2, eerste en derde lid en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109terE, § 2 van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *BS* 23 februari 2011.

⁸⁹ HvB Antwerpen 15 november 2017, nr. 2016/CO/1006, *Juristenkrant* 2017/359.

⁹⁰ Art. 46bis, §2, lid 1 Sv.; Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomunicaties, KAMER, 2015-2016, 8 juli 2016, 54K1966/001, 34.

⁹¹ Art. 46bis, §1, lid 3 en 4 Sv.

⁹² DAENINCK P, *Telefonieonderzoek in het strafrecht. Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.*, die Keure, 2020, 17.

⁹³ *Ibid.*

⁹⁴ Art. 46bis, §1, lid 5 Sv.; Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennismaken en opnemen van privécommunicatie en -telecommunicatie, SENAAT, 1997-1998, 25 maart 1998, nr. 1-828/3, 21-23.

als tussenpersonen optreden in het communicatieproces.⁹⁵ Er wordt aldus voorzien in een dubbele bevoegdheid, met name enerzijds de registratie van telecommunicatie (verkeersgegevens), en anderzijds de lokalisering van telecommunicatie (lokalisatiegegevens). Dit betekent dat aan de hand van deze onderzoeksdaad kan worden onderzocht met wie werd gecommuniceerd, waar, wanneer en hoe lang.⁹⁶

Een eerste categorie van bevoegdheden betreft het opsporen van verkeersgegevens van elektronische communicatiemiddelen, met als doel na te gaan welke toestellen of elektronische adressen met elkaar in verbinding stonden, en op welk moment.⁹⁷ Dit omvat onder meer het onderzoeken naar welke nummers er werd gebeld vanaf een welbepaald toestel⁹⁸, telefoonnummers via welke een faxbericht werd verstuurd⁹⁹, het moment waarop een bepaald informaticasysteem contact had met andere IT-systemen¹⁰⁰, ...

De tweede categorie van bevoegdheden betreft het lokaliseren van de oorsprong of bestemming van elektronische communicatie.¹⁰¹ Hiermee kan worden onderzocht waar een persoon zich bevond op het moment van verzenden of ontvangen van communicatie, bijvoorbeeld bij een inkomend of uitgaand telefoongesprek.¹⁰²

46. Net zoals bij de identificatiegegevens dienen de verkeers- en lokalisatiegegevens zich te bevinden bij een operator van een elektronische communicatienetwerk of een verstrekker van een elektronische communicatiedienst *sensu lato*. Voor de uitoefening van registratie- en lokalisatiebevoegdheden wordt in de regel beroep gedaan op de medewerking van deze operatoren of dienstverstrekkers.¹⁰³ Hoewel de wet geen expliciete rechtstreekse toegang tot gegevensbestanden voorziet, zoals bij identificatiegegevens, suggereert de term 'zo nodig' in de wettekst dat de wetgever nieuwe technische mogelijkheden niet uitsluit.¹⁰⁴ Niettemin blijft de tussenkomst van de operator of dienstverstrekker aangewezen.¹⁰⁵

⁹⁵ Art. 88bis Sv.

⁹⁶ DAENINCK P, *Telefonieonderzoek in het strafrecht. Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.*, die Keure, 2020, 5.

⁹⁷ Art. 88bis, §1, lid 1, 1° Sv.; DAENINCK P, *Telefonieonderzoek in het strafrecht. Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.*, die Keure, 2020, 30; CONINGS C, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 195.

⁹⁸ Wetsontwerp tot wijziging van artikel 46bis van het Wetboek van strafvordering, SENAAT, 2005-2006, 31 juli 2006, nr. 3-1824/1, 4.

⁹⁹ Ontwerp van wet tot invoeging van een artikel 90bis in het Wetboek van Strafvordering, SENAAT, 1990-1991, 20 november 1990, nr. 1118/2, 13.

¹⁰⁰ Wetsontwerp tot wijziging van artikel 46bis van het Wetboek van strafvordering, SENAAT, 2005-2006, 31 juli 2006, nr. 3-1824/1, 5.

¹⁰¹ Art. 88bis, §1, lid 1, 2° Sv.

¹⁰² DAENINCK P, *Telefonieonderzoek in het strafrecht. Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.*, die Keure, 2020, 30; Wetsontwerp tot wijziging van artikel 46bis van het Wetboek van strafvordering, SENAAT, 2005-2006, 31 juli 2006, nr. 3-1824/1, 4.

¹⁰³ Art. 88bis, §1, lid 2 Sv.; Wetsontwerp tot invoeging van een artikel 90bis in het Wetboek van Strafvordering, KAMER, 1984-1985, 28 juni 1985, nr. 45K1234/002, 3.

¹⁰⁴ Ontwerp van wet tot invoeging van een artikel 90bis in het Wetboek van Strafvordering, SENAAT, 1990-1991, 20 november 1990, nr. 1118/2, 9.

¹⁰⁵ De verplichtingen tot medewerking zijn opgenomen in: Koninklijk besluit van 8 februari 2011 tot wijziging van het koninklijk besluit van 9 januari 2003 tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88bis, § 2, eerste en derde lid en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109terE, § 2 van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, BS 23 februari 2011.

47. Aangezien de registratie en lokalisatie van elektronische communicatie een bijzonder ingrijpende onderzoeksmaatregel vormt, en duidelijk verder reikt dan het opvragen van identificatiegegevens, die op zichzelf geen directe informatie verschaffen over het privéleven van een persoon (Cf. *infra*, nr. 104), heeft de wetgever strikte grenzen en waarborgen vastgelegd. De bevoegdheid om registratie- of lokalisatiemaatregelen toe te staan is in eerste instantie toegekend aan de onderzoeksrechter.¹⁰⁶ De medewerking van een operator of verstrekker kan echter rechtstreeks of via de tussenkomst van een door de Koning aangewezen politiedienst worden gevraagd.¹⁰⁷ Ook de PdK kan in bepaalde gevallen dergelijke maatregelen toestaan.¹⁰⁸

48. Zoals bij alle bijzondere opsporingsmethoden moeten de beginselen van proportionaliteit, subsidiariteit en noodzakelijkheid worden gerespecteerd: de maatregel moet noodzakelijk zijn voor waarheidsvinding, evenredig zijn met de inmenging in de persoonlijke levenssfeer en niet vervangen kunnen worden door een minder ingrijpende onderzoeksdaad.¹⁰⁹ De maatregel vereist daarnaast steeds een met redenen omkleed bevelschrift.¹¹⁰ Gezien het ingrijpende karakter van de maatregel heeft de wetgever bijkomend voorzien in een strafdrempel. De maatregel kan slechts worden toegepast wanneer er ernstige aanwijzingen bestaan van strafbare feiten die een correctionele hoofdgevangenisstraf van minstens één jaar of een zwaardere straf kunnen opleveren.¹¹¹ In de toekomst zal de wetgever evenwel de nodige aandacht moeten besteden aan de strafdrempel die aan deze onderzoeksmethode wordt gekoppeld. In het kader van de herziening van het Strafwetboek wordt immers gewerkt met verschillende niveaus van toepasselijke straffen.¹¹² Het is aan de wetgever om, met inachtneming van de hoe ingrijpend deze maatregel is, het gepaste strafniveau vast te stellen teneinde een evenwichtige afweging te maken tussen de effectiviteit van het strafrechtelijk onderzoek en de waarborging van het recht op privacy en gegevensbescherming.

49. Om de inmenging in het recht op privacy te minimaliseren, wordt een tijdslimiet opgelegd. Er wordt onderscheid gemaakt tussen realtime-observatie, waarbij toekomstig elektronisch communicatiegedrag wordt gemonitord, en retrobevraging, waarbij communicatiegegevens uit het verleden wordt opgespoord.¹¹³ De wetgever heeft een maximale duur van twee maanden gekoppeld aan de realtime-maatregel, te rekenen vanaf het bevelschrift.¹¹⁴ Een retrobevraging is niet gebonden aan deze limiet, maar de wet voorziet in een trapsgewijs systeem voor de terugwerkende tijd.¹¹⁵

¹⁰⁶ Art. 88bis, §1 lid 1 Sv.

¹⁰⁷ Art. 88bis, §1, lid 2 Sv.; VAN DE HEYNING C., 'Noot onder cass. 19 februari 2019', *T.Strafr.* 2019/6, (349) 351-352; VERBRUGGEN F. en ROYER S., 'Veroordeling Skype niet verboden, vele vragen blijven onbeantwoord', *RW* 2018-2019/37, (1442) 1442.

¹⁰⁸ Art. 88bis, §1, lid 6-9 Sv.; art. 28septies, lid 1 Sv.

¹⁰⁹ Art. 88bis, §1, lid 1 en lid 4 Sv.

¹¹⁰ Art. 88bis, §1, lid 4 Sv.; zie voor realtime-observatie: Cass. 19 januari 2005, P.04.1383.F, ECLI:BE:CASS:2005:ARR.20050119.6; DEWANDELEER D., 'Misdrijven en strafonderzoek in de IT-context' in VERSTRAETEN R. en VERBRUGGEN F. (eds.), *Straf- en strafprocesrecht*, die Keure, 2010, (125) 137; KENNES L., 'Le repérage téléphonique relatif à une période révolue (noot onder Cass. 16 april 2003 en Cass. 21 april 2004)', *JT* 2004/6155, (820) 821; HERBOTS P., 'Rol van onderzoeksrechter bij retroactieve lokalisatie telefoongesprekken', *Juristenkrant* 2004/89, (9) 9.

¹¹¹ Art. 88bis, §1, lid 1 Sv.

¹¹² Art. 36 wet van 29 februari 2024 tot invoering van boek I van het Strafwetboek, *BS* 8 april 2024.

¹¹³ CONINGS C., *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 196.

¹¹⁴ Art. 88bis, §1, lid 5 Sv.

¹¹⁵ Cass. 23 juni 1999, P.99.0663.F, ECLI:BE:CASS:1999:ARR.19990623.13; DE SMET B., 'Registratie en lokalisatie van telecommunicatie' in X. (ed.), *Strafrecht en strafvordering. Artikelsgewijze commentaar van rechtspraak (Comm.Straf.)*, Kluwer, 2018, (1) 19; KENNES L., 'Le repérage téléphonique relatif à une période révolue (noot onder Cass. 16 april 2003 en Cass. 21 april 2004)', *JT* 2004/6155, (820) 821.

Voor terroristische misdrijven kan de onderzoeksrechter gegevens opvragen tot twaalf maanden voor het bevelschrift. Voor strafbare feiten volgens artikel 90ter, paragraaf 2-4 Sv., misdrijven gerelateerd aan criminele organisaties, of misdrijven met een straf van vijf jaar of meer, kan dit tot negen maanden terug.¹¹⁶ Voor andere strafbare feiten geldt een limiet van zes maanden voorafgaand aan het bevelschrift.¹¹⁷

50. Een bijzondere toepassing van artikel 88bis Sv. betreft de toegang tot verkeers- en lokalisatiegegevens door middel van zendmastbepalingen.¹¹⁸ Deze bepaling is met name relevant in het kader van onderzoek naar onbekende daders. Wanneer de opsporingsdiensten de locatie van een verdacht persoon op een bepaald tijdstip kunnen vaststellen, bijvoorbeeld door de aanwezigheid van de dader op de plaats delict op het moment dat het misdrijf plaatsvond, kan er informatie worden opgevraagd over de elektronische communicatie die via een specifieke zendmast in een bepaalde periode tot stand is gekomen. Dit kan gebeuren zonder dat vooraf kennis bestaat over de identiteit van de gebruiker of het specifieke oproepnummer.¹¹⁹ Zo kan nagegaan worden via welke oproepnummers oproepen en sms-berichten werden uitgestuurd of ontvangen in een welbepaald geografisch gebied.¹²⁰ Tevens kan de zendmastbepaling in gevallen zoals dreig telefoons, inzicht verschaffen in de geografische locatie van de oproep.¹²¹ In combinatie met artikel 46bis Sv. kan dit leiden tot identificatie van de verdachte.

Ook wanneer er geen telecommunicatie heeft plaatsgevonden is het mogelijk om een verdachte te lokaliseren. Het Belgisch Instituut voor Postdiensten en Telecommunicatie (hierna: BIPT) heeft namelijk de bevoegdheid tot het onderscheppen van signalen naar de dichtsbijzijnde zendmast van een ingeschakelde gsm, op basis waarvan kan worden overgegaan tot een nauwkeurige lokalisatie.¹²² De BIPT kan namelijk de locatie van een gsm-toestel nauwkeurig bepalen op basis van signalen die het toestel uitzendt, ook al is er geen inkomende of uitgaande telecommunicatie. Een ingeschakelde gsm zendt namelijk meerdere malen per minuut signalen uit naar de nabijgelegen zendmast ter

¹¹⁶ Art. 88bis, §2, lid 1 eerste en tweede gedachtestreepje Sv.

¹¹⁷ Art. 88bis, §2, lid 1 derde gedachtestreepje Sv.

¹¹⁸ DE SMET B., 'Opvangen van signalen van gsm-toestellen als onderzoeksdaad (noot onder Cass. 10 november 2009)', *RW* 2010-2011/31, (1302) 1303; VAN LINTHOUT P. en KERKHOFS J., 'Actuele uitdagingen in cybercrime voor de advocatuur en de magistratuur: vervolgen en verdedigen met een bot scalpel?' in LIEVENS A., VALCKE P., DUMORTIER J., GRAUX H., KERKHOFS J., LEFEVER K., SOMERS G., VAN LINTHOUT P. en WAUTERS E. (eds.), *Themis 81 - ICT- en mediarecht*, die Keure, 2013, (27) 53.

¹¹⁹ CONINGS C., *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 193.

¹²⁰ DE SMET B., 'Registratie en lokalisatie van telecommunicatie' in X. (ed.), *Strafrecht en strafvordering. Artikelsgewijze commentaar van rechtspraak (Comm.Straf.)*, Kluwer, 2018, (1) 13; DE SMET B., 'Opvangen van signalen van gsm-toestellen als onderzoeksdaad (noot onder Cass. 10 november 2009)', *RW* 2010-2011/31, (1302) 1303; KERKHOFS J. en VAN LINTHOUT P., *Cybercrime*, Politeia, 2013, 258.

¹²¹ DE SMET B., 'Registratie en lokalisatie van telecommunicatie' in X. (ed.), *Strafrecht en strafvordering. Artikelsgewijze commentaar van rechtspraak (Comm.Straf.)*, Kluwer, 2018, (1) 12-13.

¹²² In 2009 oordeelde het Hof van Cassatie dat de lokalisatie door het BIPT niet onder artikel 88bis Sv. viel, aangezien de lokalisatie niet plaatsvond aan de hand van inkomende of uitgaande gesprekken of sms-berichten; Cass. 10 november 2009, P.09.1584.F, ECLI:BE:CASS:2009:ARR.20091110.3. In 2011 keert het Hof om en bepaalt dat deze lokalisatietechniek wel onder artikel 88bis valt; Cass. 24 mei 2011, P.11.0909.N, ECLI:BE:CASS:2011:ARR.20110524.10. Zie hierover meer: DERUYCK F., BEERNAERT M-A, BERKMOES S. e.a., *Het Strafrecht bedreven. Liber Amicorum Alain De Nauw*, Die Keure, 2011, 302-303; DE SMET B., 'Registratie en lokalisatie van telecommunicatie' in X. (ed.), *Strafrecht en strafvordering. Artikelsgewijze commentaar van rechtspraak (Comm.Straf.)*, Kluwer, 2018, (1) 13.

bepaling van locatie om mobiele communicatie mogelijk te maken, waardoor het gsm-toestel noodzakelijkerwijze verbinding maakt met het netwerk van de operator.¹²³

51. De bijzondere toepassing van de zendmastbepaling kan, net als zoektermbevelen, worden ingezet in gevallen van onbekende daders. Aangezien zoektermbevelen op dit moment (nog) niet zijn geïmplementeerd, biedt de toepassing van zendmastbepalingen waardevolle inzichten voor een toekomstige ontwikkeling van een dergelijke onderzoeksmethode. De zendmastbepaling maakt het mogelijk om gegevens te verzamelen over potentieel duizenden personen van wie de mobiele telefoon tijdens het misdrijf verbinding maakte met een zendmast in de nabijheid van de plaats delict. Deze methode vertoont gelijkenissen met zoektermbevelen, waarbij eveneens gegevens van een brede groep personen worden onderzocht om na te gaan of iemand in een bepaalde periode een specifieke zoekopdracht heeft ingevoerd.

Afdeling 4: De inijkoperatie in een informaticasysteem – Artikel 46quinquies Juncto 89ter Sv.

52. De inijkoperatie in een informaticasysteem is opgenomen in het kader van de klassieke inijkoperatie.¹²⁴ Deze inijkoperatie betreft de mogelijkheid voor de politiediensten om buiten medeweten van de eigenaar, bezitter of de gebruiker en zonder hun toestemming, zich toegang te verschaffen tot een informaticasysteem en het te doorzoeken.¹²⁵ Ze laat aldus toe om zich heimelijk toegang te verschaffen tot private informaticasystemen.¹²⁶

53. Ondanks het feit dat kan worden aangenomen dat een informaticasysteem een private plaats is, die geen woning betreft, wordt de inijkoperatie in een informaticasysteem bewust onder artikel 89ter Sv. geplaatst en niet onder artikel 46quinquies Sv.¹²⁷ Vanwege de omvangrijke en gevoelige informatie, gecombineerd met het feit dat deze privacy heimelijk wordt onderzocht, vond de wetgever dat de IT-inijkoperatie onder de controle van de onderzoeksrechter dient te ressorteren.¹²⁸ De IT-inijkoperatie is bovendien uitgesloten van het toepassingsgebied van de mini-instructie.¹²⁹ Het binnendringen van een informaticasysteem om een technisch hulpmiddel te plaatsen, te herstellen of terug te nemen in het kader van een observatie is echter wel weggelegd voor de PdK.¹³⁰

¹²³ VANDROMME S., 'Ook louter lokaliseren van gsm in werking vereist bevelschrift onderzoeksrechter', *Juristenkrant* 2011/231, (3) 3; VERSTRAETEN R., *Handboek Strafvordering*, Maklu, 2012, 515.

¹²⁴ Art. 46quinquies juncto art. 89ter Sv.

¹²⁵ Art. 89ter, lid 1, gedachtestreepje 2 Sv.

¹²⁶ CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, (99) 110.

¹²⁷ In het kader van private plaatsen die niet de woning uitmaken, geen door een woning omsloten aanhorigheid in de zin van artikelen 479 tot 480 van het Strafwetboek zijn en geen lokaal aangewend voor beroepsdoeleinden of de woonplaats van een advocaat of arts is, is de inijkoperatie in principe mogelijk in het kader van een opsporingsonderzoek; art. 46quinquies, §1, lid 1 en 2 Sv.

¹²⁸ Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomcommunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001, 52.

¹²⁹ Art. 28septies, lid 1 Sv.

¹³⁰ Art. 46quinquies, §6 en §2, 3° Sv.

54. De inijkoperatie in een informaticasysteem is onderworpen aan de voorwaarden zoals bepaald in artikel 46quinquies Sv.¹³¹ Deze operatie mag slechts plaatsvinden om vast te stellen of er gegevens aanwezig zijn die verband houden met het misdrijf, zoals zaken die zijn gebruikt of bestemd voor het misdrijf, voortkomen uit het misdrijf, of direct of indirect vermogensvoordelen opleveren, of om bewijzen te verzamelen van de aanwezigheid van de opgesomde zaken.¹³² In zo'n geval kan enkel worden beslist tot een inijkoperatie indien men op basis van precieze aanwijzingen vermoedt dat deze zaken er zich bevinden, dat er bewijzen van kunnen worden verzameld, of dat ze gebruikt worden door personen op wie een verdenking rust.¹³³ De derde finaliteit, namelijk de installatie, het herstel en de verwijdering van een technisch hulpmiddel in het kader van een observatie, is niet relevant bij de IT-inijkoperatie.¹³⁴ Naast de vereiste finaliteit moet de inijkoperatie voldoen aan de proportionaliteits- en subsidiariteitsvereiste. De inijkoperatie is enkel toegestaan bij ernstige aanwijzingen dat de strafbare feiten vallen onder artikel 90ter, §2-4 Sv. of verband houden met een criminele organisatie, en wanneer andere onderzoeksmiddelen onvoldoende zijn om de waarheid te achterhalen.¹³⁵ De inijkoperatie kan daarnaast slechts plaatsvinden bij een schriftelijke en met rede omklede beslissing.¹³⁶

Afdeling 5: Het onderscheppen, kennis nemen, doorzoeken en opnemen van communicatie of gegevens van een informaticasysteem – Artikel 90ter Sv.

55. Een tweede heimelijke IT-doorzoeking betreft het heimelijk onderscheppen, kennisnemen, doorzoeken en opnemen van niet voor het publiek toegankelijke communicatie of gegevens van een informaticasysteem, met behulp van technische hulpmiddelen, ook wel de tapmaatregel genoemd.¹³⁷ Deze maatregel wordt beschouwd als een van de ingrijpendste, aangezien hiermee de inhoud van communicatie kan worden onderschept.¹³⁸ De maatregel is zowel gericht op het real-time monitoren van communicatie als het toegang verschaffen tot bestaande communicatie-inhoud, maar betreft geen proactieve af luistermaatregel.¹³⁹

¹³¹ Art. 89ter juncto art. 46quinquies Sv.

¹³² Art. 89ter juncto art. 46quinquies, §2, 1° en 2° Sv.; Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001, 51.

¹³³ Art. 89ter juncto art. 46quinquies, §3 Sv.

¹³⁴ Art. 89ter juncto art. 46quinquies, §2, 3° Sv.; CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, (99) 110; CONINGS C., 'Speuren op sociale media: de nieuwigheden op een rij', *P&R* 2020/1, (3) 12.

¹³⁵ Art. 89ter juncto art. 46quinquies, § 1, lid 1 Sv.

¹³⁶ Art. 46quinquies, §1, lid 1 Sv.

¹³⁷ Art. 90ter, §1, lid 1 Sv.

¹³⁸ DAENINCK P, *Telefonieonderzoek in het strafrecht. Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.*, die Keure, 2020, 5.

¹³⁹ CONINGS C., *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 207; zie voor historische schets: Wet 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het af luisteren, kennisnemen en openen van privé-communicatie en -telecommunicatie, *BS* 24 januari 1995; art. 17 Wet houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrucken, *BS* 17 januari 2017; Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001, 53; DAENINCK P, *Telefonieonderzoek in het strafrecht. Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv.*, die Keure, 2020, 42; 56.

56. Gezien de ingrijpende aard van de tapmaatregel, stelt de wetgever strikte voorwaarden, de strengste regels voor online onderzoeksdaten. Zo is de bevoegdheid tot het heimelijk onderzoeken van private (tele)communicatie primair toevertrouwd aan de onderzoeksrechter.¹⁴⁰ Ook is het uitgesloten van het toepassingsgebied van de mini-instructie, al kan de PdK ze onder zeer uitzonderlijke voorwaarden toestaan.¹⁴¹

57. Er dient steeds een verband te bestaan met de verdachte vooraleer de communicatie het voorwerp kan uitmaken van de tapmaatregel. Ten aanzien van personen moet er concrete aanwijzing zijn dat zij verdacht worden van een strafbaar feit uit de taplijst. De maatregel mag enkel worden toegepast op communicatiemiddelen en informaticasystemen die de verdachte regelmatig gebruikt, en op locaties waar hij vermoedelijk verblijft.¹⁴² Daarnaast kan de maatregel ook gericht zijn op derden, wanneer er aanwijzingen zijn dat zij regelmatig in contact staan met de verdachte en dat die communicatie bijdraagt aan de waarheidsvinding.¹⁴³

58. Opnieuw dient de maatregel steeds verantwoord te worden in het licht van de proportionaliteit, subsidiariteit en het uitzonderlijk karakter.¹⁴⁴ Om te voorzien in de proportionaliteit van een dergelijke verregaande maatregel laat de wetgever de tapmaatregel slechts toe ten aanzien van zware misdrijven, die aangeduid worden als misdrijven uit de taplijst (art. 90ter, §§ 2-4 Sv.).¹⁴⁵ Het gaat onder andere over genocide, terroristische misdrijven, gijzeling, verkrachting, kinderpornografie, moord, ...¹⁴⁶ De meeste van deze misdrijven zijn opgenomen vanwege hun ernstig karakter, al werden sommige, zoals informaticamisdrijven, toegevoegd omdat ze zonder tapmaatregel moeilijk te bewijzen zijn.¹⁴⁷ De maatregel kan dan ook slechts bevolen worden wanneer er ernstige aanwijzingen zijn dat het feit een strafbaar feit uitmaakt dat in die lijst is opgenomen, en bovendien enkel met het oog op het opsporen van gegevens die kunnen bijdragen tot de waarheidsvinding.¹⁴⁸ De subsidiariteitstoets vereist opnieuw dat de onderzoeksrechter slechts kan opteren voor de maatregel wanneer de andere middelen van onderzoek ondoeltreffend blijken om de waarheid aan het licht te brengen.¹⁴⁹ Tot slot kan de onderzoeksmaatregel slechts worden aangewend in zeer uitzonderlijke omstandigheden, namelijk wanneer het onderzoek dat vereist.¹⁵⁰

59. Om de inmenging in het recht op privacy te minimaliseren, wordt opnieuw een tijdslimiet opgelegd. De maatregel kan slechts één maand duren.¹⁵¹ De onderzoeksrechter kan de maatregel

¹⁴⁰ Art. 90ter, §1 Sv.

¹⁴¹ Art. 28septies Sv.; art. 90ter, §5 Sv.

¹⁴² Art. 90ter, §1, lid 4 Sv.

¹⁴³ Ontwerp van wet ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie, SENAAT, 1992-1993, 18 mei 1994, nr. 843/2, 92.

¹⁴⁴ Art. 90ter, §1, lid 2 en lid 4 Sv.

¹⁴⁵ Art. 90ter, §2 Sv.

¹⁴⁶ Art. 90ter, §2, 2°, 3°, 14°, 15°, 19° Sv.

¹⁴⁷ CONINGS C., *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 214.

¹⁴⁸ Art. 90ter, §1, lid 2 en lid 4 Sv.

¹⁴⁹ Art. 90ter, §1, lid 2 Sv.; Cass. 28 december 2004, P.04.1647.F, ECLI:BE:CASS:2004:ARR.20041228.1; VERSTRAETEN R., *Handboek Strafvordering*, Maklu, 2012, 522.

¹⁵⁰ Art. 90ter, §1, lid 2 Sv.

¹⁵¹ Art. 90quater, §1, lid 2, 4° Sv.; KERKHOFS J., 'Het onderscheppen van communicatie in de praktijk: wie, wat, waar en wanneer? (noot onder Cass. 16 december 2014)', *T.Strafr.* 2015/4-5, (235) 240.

telkens met één maand verlengen via een met redenen omklede machtiging, mits de totale duur niet langer wordt dan zes maanden.¹⁵²

§ 2: Tussenconclusie

60. Naarmate een onderzoeksmethode ingrijpender is en dieper ingrijpt in het recht op privacy en gegevensbescherming, voorziet de wetgever in meer waarborgen tegen willekeur en ter bescherming van de betrokkene. Voor openlijke doorzoeking in informaticasystemen of het verkrijgen van identificatiegegevens volstaat de tussenkomst van de PdK, terwijl bij ernstigere inbreuken doorgaans de onderzoeksrechter bevoegd is. Slechts uitzonderlijk kan ook de PdK dergelijke maatregelen bevelen. De tussenkomst van de onderzoeksrechter geldt als bijkomende waarborg, aangezien hij, in tegenstelling tot de als partij optredende PdK, een onafhankelijke en onpartijdige beoordeling garandeert.¹⁵³ Dit versterkt het vertrouwen in een objectieve beoordeling van de wettigheid van ingrijpende onderzoeksmaatregelen.

61. Bij elke onderzoeksdaad moeten de beginselen van proportionaliteit en subsidiariteit worden gerespecteerd. In het geval van minder ingrijpende methoden volstaan deze algemene toetsingscriteria vaak als enige waarborgen, terwijl voor verregaandere maatregelen aanvullende voorwaarden, zoals een minimale strafdrempel, het bestaan van ernstige aanwijzingen met betrekking tot misdrijven die op de zogeheten 'taplijst' staan, of het uitzonderlijke karakter van de maatregel, opgelegd worden. In die gevallen gelden vaak ook bijkomende vereisten met betrekking tot de noodzakelijkheid of finaliteit van de inzet van de betrokken opsporingsmethode.

62. Volgens ons vertoont de eerste fase van een zoektermbevel (Cf. *supra*, nr. 23) sterke gelijkenissen met het bevel tot het verkrijgen van verkeers- en lokalisatiegegevens, zoals geregeld in artikel 88bis Sv. Verkeers- en lokalisatiegegevens geven immers inzicht in welke apparaten met elkaar communiceren, op welk tijdstip en voor welke duur dat gebeurt, alsook de locatie van de betrokken communicatie. Evenzo beoogt een zoektermbevel, in zijn initiële fase, het bekomen van een geanonimiseerde lijst van welke apparaten een specifieke zoekterm hebben ingevoerd, met vermelding van het tijdstip, de locatie en de gebruikte zoekopdracht. Het voornaamste onderscheid ligt in de aard van de beoogde gegevens en de gerichtheid van onderzoek. Een onderzoeksmaatregel uit artikel 88bis Sv. richt zich op de verkrijging van verkeers- en lokalisatiegegevens van elektronische communicatie tussen apparaten, vaak met betrekking tot een specifiek doel of een reeds verdachte persoon. Een zoektermbevel daarentegen beoogt in zekere zin het verkrijgen van gelijkaardige gegevens, zij het in relatie tot een zoekterm die mogelijk door duizenden gebruikers werd ingevoerd. Daardoor wordt het onderzoek aanzienlijk breder van opzet en minder individueel gericht.

63. Hoewel zoektermbevelen gelijkenissen vertonen met de bevelen uit artikel 88bis Sv., zijn zij potentieel ingrijpender vanwege het type gegevens waarop zij betrekking hebben. Terwijl artikel

¹⁵² Art. 90quinquies, lid 1 Sv.

¹⁵³ VERSTRAETEN R. en VERBRUGGEN F., *Strafrecht en strafprocesrecht voor bachelors*, Intersentia, 2020, 154.

88bis Sv. fysieke en objectieve verkeers- en locatiegegevens oplevert, gebonden aan tijd en plaats, dringen zoektermbevelen binnen in de persoonlijke denkwereld van gebruikers. Ze verschaffen geen informatie over de fysieke aanwezigheid van een persoon op of nabij de plaats delict of communicatiegedrag, maar kunnen leiden tot verdenking louter op basis van ingevoerde zoektermen. De enige link met de gebruiker is de inhoud van diens zoekopdracht, die minder exact is dan het vaststellen van de fysieke aanwezigheid op een misdrijfplaats of communicatiegedrag.¹⁵⁴ O.i. overstijgen zoektermbevelen aldus de toelaatbare reikwijdte van de bevelen op basis van artikel 88bis Sv.

64. Volgens ons kan worden gesteld dat een zoektermbevel minder ver strekt dan een tapmaatregel of IT-inkijkoperatie. Deze maatregelen verkrijgen heimelijk diepgaande informatie over het privéleven van een persoon, zoals de inhoud van berichten, bestanden en communicatie. In tegenstelling tot deze ingrijpende maatregelen, betreft een zoektermbevel slechts onderzoek naar een specifieke zoekterm, zonder de gehele zoekgeschiedenis of een compleet IT-systeem te onderzoeken. Dit maakt een zoektermbevel naar onze mening een minder ingrijpende maatregel dan het onderzoeken van de inhoud van communicatie of het doorzoeken van een volledig IT-systeem.

65. Naar onze mening vormen zoektermbevelen een hybride categorie tussen enerzijds verkeers- en locatiegegevens, en anderzijds de tapmaatregel en inkijkoperatie. Wij zijn van oordeel dat de in de wet vastgestelde voorwaarden en grenzen voor het verkrijgen van verkeers- en locatiegegevens van elektronische communicatie in de context van zoektermbevelen ten minste dienen te worden gehandhaafd, met mogelijke aanvulling van extra waarborgen. Dit zou echter niet in dezelfde mate moeten zijn als de strengere eisen die gelden voor de tapmaatregel of de inkijkoperatie.

¹⁵⁴ EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', 97 *Wash. L. Rev.* 2022/4, (977) 1001-1002.

Hoofdstuk III. Gezocht op Google, gevolgd door justitie? De juridische knelpunten van gegevensbescherming in de EU

66. In het voorgaande hoofdstuk is aangetoond dat online onderzoeksmethoden duidelijk moeten worden afgebakend en voorzien zijn van voldoende waarborgen, gezien het spanningsveld met het recht op privacy en gegevensbescherming. Ter bescherming daarvan bestaan op supranationaal niveau diverse rechtsinstrumenten, zowel van de Europese Unie als van de Raad van Europa. Omdat beide instanties verschillende benaderingen hanteren, worden zij afzonderlijk besproken. Dit hoofdstuk behandelt het juridische kader van de Europese Unie.

67. Binnen de Europese context wordt gegevensbescherming vrijwel automatisch geassocieerd met de Algemene Verordening Gegevensbescherming, die concrete grenzen stelt aan de verwerking van persoonsgegevens, en daarmee het recht op privacy en gegevensbescherming versterkt. Dit rechtsinstrument is van direct belang bij online opsporingsmethoden waarbij autoriteiten bewaarde gegevens willen raadplegen in strafrechtelijke onderzoeken. Het Hof van Justitie van de Europese Unie heeft in dit kader belangrijke rechtspraak ontwikkeld over de bewaring en toegang tot online gegevens. De toelaatbaarheid van zoektermbevelen hangt nauw samen met deze EU-regelgeving en jurisprudentie. Dergelijke bevelen, die brede toegang tot opgeslagen gegevens op basis van zoektermen mogelijk maken, moeten in overeenstemming zijn met het Unierecht. Een grondige analyse van de voorwaarden die het Hof van Justitie stelt in het licht van het recht op privacy en gegevensbescherming is essentieel, aangezien deze de juridische haalbaarheid en reikwijdte van dergelijke bevelen bepalen.

§ 1: Algemene Verordening Gegevensbescherming

68. Het recht op gegevensbescherming is verankerd in artikel 8 van het Handvest van de grondrechten van de Europese Unie, dat luidt als volgt: *"Eenieder heeft recht op bescherming van zijn persoonsgegevens. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming (...)".*¹⁵⁵ De Europese Algemene Verordening Gegevensbescherming (hierna: AVG), die in de internationale context beter bekend is onder de Engelse afkorting GDPR (General Data Protection Regulation), versterkt en concretiseert dit grondrecht.¹⁵⁶ De AVG heeft tot doel het bestaande Europese en nationale wetgevend kader betreffende de verwerking van persoonsgegevens te harmoniseren en af te stemmen op de gewijzigde maatschappelijke en technologische ontwikkelingen.¹⁵⁷ De AVG is echter niet geheel nieuw, maar introduceert een vernieuwd wetgevend kader voor gegevensbescherming. Ze vervangt namelijk de Richtlijn van 1995¹⁵⁸, die destijds het

¹⁵⁵ Art. 8 EU-Handvest.

¹⁵⁶ Verordening 2016/679 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, *Pb.L.* 4 mei 2016 (hierna: AVG).

¹⁵⁷ Overw. 6-7 AVG; WAEM H. en VAN EECKE P., '3 - Verwerking van persoonsgegevens' in VAN EECKE P. (ed), *Recht en elektronische handel*, Intersentia, 2021, (259) 260.

¹⁵⁸ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.L.* 23 november 1995.

eerste instrument was om het gegevensbeschermingsrecht te harmoniseren en het vrije verkeer van persoonsgegevens binnen de EU te waarborgen.

69. Hoewel harmonisatie één van de belangrijkste doelstellingen is, laat de Europese wetgever de lidstaten toe om bepaalde regels (de zgn. open clausules) uit de AVG verder te verduidelijken in nationaal recht.¹⁵⁹ In België worden deze "open clausules" ingevuld door de gegevensbeschermingswet.¹⁶⁰

Afdeling 1: Zoekmachinebedrijven binnen AVG

A. Toepassingsgebied

70. De AVG is van toepassing op *"de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen"*.¹⁶¹ Het materieel toepassingsgebied wordt aldus afgebakend aan de hand van twee basisbegrippen in de AVG, zijnde 'persoonsgegevens' en 'verwerking'.

71. Het begrip persoonsgegevens dekt een brede lading.¹⁶² Het heeft betrekking op *"alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon"*.¹⁶³ Daarbij verduidelijkt de AVG dat een natuurlijke persoon als identificeerbaar wordt beschouwd wanneer hij of zij *"direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier, zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon"*.¹⁶⁴ Zodra gegevens informatie over een geïdentificeerde persoon verstrekken, of wanneer de informatie toelaat om een persoon te identificeren, wordt de kwalificatie aldus als persoonsgegeven weerhouden. Anonieme gegevens, zoals gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is, vallen aldus niet onder de term.¹⁶⁵

72. Om onder de toepassing te vallen van de AVG dienen de persoonsgegevens te worden verwerkt. Er is sprake van verwerking ingeval van *"een bewerking of een geheel van bewerkingen*

¹⁵⁹ Overw. 10 AVG; WAEM H. en VAN EECKE P., '3 - Verwerking van persoonsgegevens' in VAN EECKE P. (ed.), *Recht en elektronische handel*, Intersentia, 2021, (259) 260; DE POORTER I., 'De GDPR of Algemene Verordening Gegevensbescherming (AVG) – Een algemene inleiding' in Instituut Financieel Recht (ed.), *Financiële regulering: een dwarsdoorsnede*, Intersentia, 2019, (449) 453.

¹⁶⁰ Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, BS 5 september 2018 (hierna: gegevensbeschermingswet).

¹⁶¹ Art. 2.1 AVG.

¹⁶² DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSgegevens (hierna: GROEP GEGEVENSbescherming ARTIKEL 29), Advies 4/2007 over het begrip persoonsgegeven, 20 juni 2007, nr. 01248/07/NL, WP 136.

¹⁶³ Art. 4.1 AVG.

¹⁶⁴ *Ibid.*

¹⁶⁵ Overw. 26 AVG; CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I., 'hoofdstuk 1 – Overkoepelende principes' in CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I. (eds.), *Werk & Privacy*, Intersentia, 2019, (3) 9; FOCQUET A. en DECLERCK E., 'Hoofdstuk 1 – Verwerking van persoonsgegevens' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, (5) 12.

met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens”.¹⁶⁶ Opnieuw wordt een zeer breed begrip gehanteerd, waardoor als het ware steeds sprake zal zijn van een verwerking in een online context, aangezien dit per definitie altijd het gebruik van geautomatiseerde procedés impliceert.¹⁶⁷

73. Bij het gebruik van zoekmachines worden grote hoeveelheden gegevens verwerkt. Deze gegevens variëren van IP-adressen en cookies van individuele gebruikers tot uitgebreide zoekgeschiedenissen en persoonlijke informatie die gebruikers zelf verstrekken bij het aanmelden voor gepersonaliseerde diensten.¹⁶⁸

74. De zoekgeschiedenis van een persoon wordt als een persoonsgegeven beschouwd wanneer de betreffende persoon identificeerbaar is.¹⁶⁹ Dat is mogelijk op basis van cookies, gebruikersID's en IP-adressen. Hoewel zoekmachines (dynamische) IP-adressen doorgaans niet direct kunnen herleiden tot een individu, kunnen internetproviders deze adressen wel bewaren en koppelen aan specifieke gebruikers, waardoor indirecte identificatie mogelijk wordt.¹⁷⁰ Daarnaast kunnen cookies, met name wanneer ze een unieke gebruikers-ID bevatten, worden beschouwd als persoonsgegevens. Het gebruik van permanente cookies of soortgelijke technologieën maakt het mogelijk om gebruikers te volgen, zelfs bij dynamische IP-adressen. Hierdoor kunnen zoekmachines gedetailleerde gedragsgegevens verzamelen, wat hen in staat stelt om een steeds nauwkeuriger beeld te vormen van de persoonlijke kenmerken en voorkeuren van een gebruiker.¹⁷¹ Zowel het opslaan van dergelijke gegevens als het verlenen van toegang daartoe aan opsporingsautoriteiten kwalificeert als een verwerking in de zin van de AVG.

75. Niet elke verwerking van persoonsgegevens valt onder de reikwijdte van de AVG. Het is een Europees rechtsinstrument waardoor er rekening dient te worden gehouden met het territoriale

¹⁶⁶ Art. 4.2 AVG.

¹⁶⁷ FEYS M. en MOREL C., 'De nieuwe Verordening Gegevensbescherming: een algemeen overzicht van de (nieuwe) verplichtingen rond gegevensbescherming' in Orde van Advocaten bij de balie te Gent (ed.), *De advocaat als generalist*, Intersentia, 2018, (125) 133; FOCQUET A. en DECLERCK E., 'Hoofdstuk 1 – Verwerking van persoonsgegevens' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, (5) 14-15; WAEM H. en VAN EECKE P., '3 - Verwerking van persoonsgegevens' in VAN EECKE P. (ed.), *Recht en elektronische handel*, Intersentia, 2021, (259) 271.

¹⁶⁸ GROEP GEGEVENSBEscherMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 4-5.

¹⁶⁹ *Ibid*, 8.

¹⁷⁰ Overw. 26 AVG; HvJ 24 november 2011, C-70/10, ECLI:EU:C:2011:771, 'Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs', §51; HvJ 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779, 'Patrick Breyer/Bondsrepubliek Duitsland', §§ 39-49; CAMPOS SÁNCHEZ-BORDONA M., 'conclusie 12 mei 2016 bij HvJ, C-582/14, 'Patrick Breyer/Bondsrepubliek Duitsland', ECLI:EU:C:2016:339, §§ 52-78; DE POORTER I., 'De GDPR of Algemene Verordening Gegevensbescherming (AVG) – Een algemene inleiding' in Instituut Financieel Recht (ed.), *Financiële regulering: een dwarsdoorsnede*, Intersentia, 2019, (449) 455, GROEP GEGEVENSBEscherMING ARTIKEL 29, Working Document Privacy on the Internet - An integrated EU Approach to Online Data Protection, 21 november 2000, nr. 5063/00/EN/FINAL, WP 37, 21; GROEP GEGEVENSBEscherMING ARTIKEL 29, Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, 30 mei 2002, nr. 10750/02/EN/Final, WP 58, 3; WAEM H. en VAN EECKE P., '3 - Verwerking van persoonsgegevens' in VAN EECKE P. (ed.), *Recht en elektronische handel*, Intersentia, 2021, (259) 265.

¹⁷¹ Overw. 30 AVG; GROEP GEGEVENSBEscherMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 6-7 en 8-9.

toepassingsgebied. Omwille van de globalisering heeft de Europese wetgever erkent dat gegevensverwerking binnen de EU niet beperkt kan blijven tot intra-Europese actoren.¹⁷² De AVG is namelijk zowel van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, alsook op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker.¹⁷³ De verwerking dient dan wel verband te houden met het aanbieden van goederen of diensten aan deze betrokkenen in de Unie of het monitoren van hun gedrag. De Europese wetgever heeft bij het bepalen van het territoriaal toepassingsgebied zijn doorwerking aldus tot buiten de grenzen van de Europese Unie gebracht.¹⁷⁴

76. Daardoor vallen de meest prominente zoekmachinebedrijven, waaronder Google, Yahoo en Microsoft, binnen dit toepassingsgebied. Hun hoofdkantoor bevindt zich dan wel in de VSA, ze beschikken over vestigingen binnen de Europese Unie (Londen, Dublin, Brussel).¹⁷⁵ Zij zijn daarom onderworpen aan de verplichtingen en reguleringen van de AVG.¹⁷⁶

77. Wanneer zoekmachinebedrijven de zoekgeschiedenis van gebruikers verwerken op basis van IP-adressen, cookies of gebruikers-ID's, valt deze verwerking aldus binnen het toepassingsgebied van de AVG, aangezien de zoekgeschiedenissen vaak direct of indirect herleidbaar zijn tot een individueel persoon. Dit betekent dat zij verplicht zijn de strenge regels omtrent de verwerking van persoonsgegevens na te leven. Zo kunnen zij de zoekgeschiedenis van gebruikers slechts verzamelen wanneer daar een specifieke rechtsgrond toe bestaat, en dienen ze de beginselen inzake de verwerking van persoonsgegevens in acht te nemen.

B. Verwerkingsgronden

78. De verwerking van persoonsgegevens dient altijd te steunen op een rechtmatige rechtsgrond. De AVG somt limitatief de rechtsgronden op waarop een verwerking kan berusten, teneinde de rechtmatigheid van de verwerking te waarborgen. De rechtsgronden betreffen: (i) toestemming van de betrokkene, (ii) uitvoering van een overeenkomst, (iii) wettelijke verplichting, (iv) noodzakelijk voor vitale belangen, (v) noodzakelijk voor vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag en (vi) noodzakelijk voor de behartiging van gerechtvaardigde belangen.¹⁷⁷

¹⁷² FEYS M. en MOREL C., 'De nieuwe Verordening Gegevensbescherming: een algemeen overzicht van de (nieuwe) verplichtingen rond gegevensbescherming' in Orde van Advocaten bij de balie te Gent (ed.), *De advocaat als generalist*, Intersentia, 2018, (125) 140-141; VANDE VORST C., 'Algemene verordening gegevensbescherming: vijf nieuwigheden van dichtbij bekeken', *CJ* 2016/4, (75) 76.

¹⁷³ Art. 3.1 en 3.2 AVG; overw. 23-24 AVG; art. 4, §§ 1-2 gegevensbeschermingswet; HvJ 1 oktober 2015, C-230/14, ECLI:EU:C:2015:639, 'Weltimmo s.r.o./Nemzeti Adatvédelmi és Információszabadság Hatóság', §§ 29, 31; EUROPEAN DATA PROTECTION BOARD (hierna: EDPB), Richtsnoeren 3/2018 over het territoriale toepassingsgebied van de AVG (art. 3), 12 november 2019, 6.

¹⁷⁴ FEYS M. en MOREL C., 'De nieuwe Verordening Gegevensbescherming: een algemeen overzicht van de (nieuwe) verplichtingen rond gegevensbescherming' in Orde van Advocaten bij de balie te Gent (ed.), *De advocaat als generalist*, Intersentia, 2018, (125) 140-144.

¹⁷⁵ HvJ 13 mei 2014, C-131/12, ECLI:EU:C:2014:317, 'Google Spain en Google Inc./Agencia Española de Protección de Datos en Mario Costeja González', §§ 43, 48-56; HvJ 24 september 2019, C-507/19, ECLI:EU:C:2019:772, 'Google LLC/Commission nationale de l'informatique et des libertés', §§ 49-52.

¹⁷⁶ GROEP GEGEVENS BESCHERMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 10-11.

¹⁷⁷ Art. 6.1 AVG.

79. Zoekmachinebedrijven verwerken de zoekgeschiedenis van gebruikers doorgaans op basis van volgende rechtsgronden: toestemming, uitvoering van een overeenkomst en noodzakelijk in het kader van een gerechtvaardigd belang.¹⁷⁸

80. De belangrijkste rechtsgrond betreft de toestemming die wordt gegeven door de betrokkene voor de verwerking van zijn persoonsgegevens.¹⁷⁹ Toestemming betreft *"elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt"*.¹⁸⁰ Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.¹⁸¹ Daarnaast is het van belang dat de betrokkene zich er steeds van bewust is dat hij toestemming geeft en hoever deze toestemming reikt.¹⁸² Opdat aanvaarding met kennis van zaken wordt gegeven, moet de betrokkene ten minste bekend zijn met de identiteit van de verwerkingsverantwoordelijke, de doeleinden van de verwerking, welke soort gegevens worden verzameld en gebruikt, het bestaan van het recht om toestemming in te trekken, informatie over het gebruik van de gegevens voor geautomatiseerde besluitvorming en de risico's bij doorgifte naar derde landen.¹⁸³

De toestemming dient daarnaast steeds ingegeven te zijn door middel van een duidelijke actieve handeling, zoals een schriftelijke of mondelinge verklaring, eventueel verricht met elektronische middelen. Hieronder kan het klikken van een vakje bij een bezoek aan een internetwebsite vallen. Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit sluiten daarentegen de toestemming uit.¹⁸⁴ Tot slot is het van belang dat de betrokkene het recht heeft zijn toestemming te allen tijde terug in te trekken. Het intrekken van de toestemming heeft alleen gevolgen voor toekomstige verwerkingen, terwijl eerdere verwerkingen op basis van geldige toestemming rechtmatig blijven. Alvorens toestemming wordt gegeven dient de betrokkene in kennis te zijn gesteld van diens recht om de toestemming in te trekken.¹⁸⁵

81. In veel gevallen verstrekken gebruikers van zoekmachines expliciete toestemming voor het bijhouden van hun zoekgeschiedenis bij het aanmaken van een specifiek gebruikersaccount.¹⁸⁶ Dit

¹⁷⁸ GROEP GEGEVENS BESCHERMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 16-18.

¹⁷⁹ Artikel 6.1, a) AVG; EDPB, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, 4 mei 2020, 6-7; FOCQUET A. en DECLERCK E., 'Hoofdstuk 3 – Verwerkingsgronden' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, (47) 48.

¹⁸⁰ Art. 4.11 AVG.

¹⁸¹ Overw. 42 AVG; EDPB, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, 4 mei 2020, 8.

¹⁸² Overw. 42 AVG; FOCQUET A. en DECLERCK E., 'Hoofdstuk 3 – Verwerkingsgronden' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, (47) 53.

¹⁸³ Overw. 42 AVG; EDPB, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, 4 mei 2020, 17.

¹⁸⁴ Overw. 32 AVG.

¹⁸⁵ Art. 7.3 AVG; CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I., 'hoofdstuk 1 – Overkoepelende principes' in CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I. (eds.), *Werk & Privacy*, Intersentia, 2019, (3) 19.

¹⁸⁶ GROEP GEGEVENS BESCHERMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 16-17.

gebeurt wanneer zij akkoord gaan met de gebruiksvoorwaarden en het privacybeleid van de desbetreffende zoekmachine. Hierin wordt doorgaans vermeld dat zoekopdrachten worden geregistreerd als onderdeel van de instellingen voor "web- en app-activiteit" of "gepersonaliseerde ervaringen". Belangrijk is dat gebruikers de toestemming te allen tijde kunnen intrekken via hun accountinstellingen.

Bovendien verstrekken gebruikers vaak hun toestemming, hetzij expliciet, hetzij impliciet door het accepteren van het privacybeleid, voor het bewaren en delen van gegevens aan wetshandhavingsautoriteiten in het kader van politionele doeleinden. In dergelijke gevallen gaat het om een mogelijke doorgifte van gegevens naar aanleiding van juridische verzoeken, zoals een gerechtelijk bevel.¹⁸⁷ Deze opt-in mogelijkheid dient te worden onderscheiden van de wettelijke bewaarplicht die aan zoekmachinebedrijven kan worden opgelegd (Cf. *infra*, nr. 88).¹⁸⁸ Ondanks het feit dat sommige zoekmachinebedrijven in hun privacybeleid voorzien in de mogelijkheid tot medewerking aan juridische verzoeken van autoriteiten, ontbreekt in België momenteel een specifieke wettelijke grondslag die dergelijke medewerking afdwingbaar maakt ten aanzien van zoekgeschiedenissen via een gerechtelijk bevel.

82. Eveneens wordt toestemming verleend wanneer een gebruiker bij het eerste gebruik van de zoekmachine een cookiebanner accepteert, waarin expliciet wordt vermeld dat zoekopdrachten worden opgeslagen ten behoeve van personalisatie, of wanneer de gebruiker instemt met gepersonaliseerde advertenties, waarbij zoekopdrachten worden gebruikt voor de opbouw van advertentieprofielen.¹⁸⁹

83. Zoekmachine-aanbieders bieden niet alleen toegang tot hun diensten voor geregistreerde gebruikers, maar ook voor ongeregistreerde gebruikers, waarbij zoekopdrachten kunnen worden uitgevoerd zonder dat een account noodzakelijk is. In het geval van anonieme gebruikers wordt er geen expliciete toestemming verstrekt, zoals dit het geval is bij het aanmaken van een account.¹⁹⁰ Desondanks kan een zoekmachine, zelfs zonder dat er een account bestaat, het zoekgedrag van de gebruiker koppelen aan het gebruikte apparaat via technieken zoals cookies, tijdelijke IP-adressen of browser-fingerprinting. Wanneer een gebruiker bijvoorbeeld geen account heeft, kan hij/zij toch toestemming geven door een cookiebanner te accepteren.¹⁹¹

84. Naast de toestemming kan de verwerking van persoonsgegevens ook rechtmatig zijn in het kader van een overeenkomst.¹⁹² Wanneer de betrokkene partij is in een overeenkomst, is het soms belangrijk om bepaalde gegevens te verwerken die noodzakelijk zijn voor de uitvoering ervan. Een voorbeeld hiervan is de verwerking van identificatie- en adresgegevens van een klant met als doel

¹⁸⁷ *Ibid*, 16, 18.

¹⁸⁸ *Ibid*, 18.

¹⁸⁹ *Ibid*, 7, 16, 20; GROEP GEGEVENSBECHERMING ARTIKEL 29, Working Document Privacy on the Internet - An integrated EU Approach to Online Data Protection, 21 november 2000, nr. 5063/00/EN/FINAL, WP 37, 16.

¹⁹⁰ GROEP GEGEVENSBECHERMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 16-17.

¹⁹¹ *Ibid*, 6-7, 20.

¹⁹² Art. 6.1, b) AVG.

de levering van een online bestelling.¹⁹³ Het blijft echter van cruciaal belang dat er een direct en objectief verband bestaat tussen de verwerking van persoonsgegevens en het beoogde doel van de overeenkomst.¹⁹⁴

85. In beginsel kunnen zoekmachinebedrijven zich niet beroepen op deze rechtsgrond, aangezien het gebruik van een zoekmachine op zichzelf geen contractuele dienst betreft. Een uitzondering op deze regel doet zich voor wanneer een gebruiker een account aanmaakt. In dat geval kunnen zoekmachines de rechtsgrond van uitvoering van een overeenkomst inroepen om persoonsgegevens te verzamelen die de gebruiker vrijwillig verstrekt tijdens de registratie voor een bepaalde dienst, zoals het aanmaken van een gebruikersaccount.¹⁹⁵ Indien de gebruiker daarnaast gebruik maakt van een dienst voor gepersonaliseerde zoekresultaten, kan het zoekmachinebedrijf betogen dat de verwerking van zoekgeschiedenis noodzakelijk is voor het leveren van een gepersonaliseerde zoekervaring. Hierbij worden eerdere zoekopdrachten geanalyseerd om relevantere zoekresultaten te genereren.¹⁹⁶

86. Ook kunnen gerechtvaardigde belangen van een verwerkingsverantwoordelijke of een derde een rechtsgrond bieden voor verwerking.¹⁹⁷ Het enkel bestaan van een gerechtvaardigd belang volstaat niet om dit als verwerkingsgrond in te roepen. Dit belang moet zwaarder wegen dan de belangen, grondrechten en fundamentele vrijheden van de betrokkenen, wat een complexe evenwichtsoefening vereist.¹⁹⁸ De AVG bespreekt enkele situaties waarin de belangen van de verwerkingsverantwoordelijke zwaarder wegen, zoals fraudevoorkoming, direct marketing en interne administratieve doeleinden.¹⁹⁹

87. In privacyverklaringen stellen zoekmachinebedrijven veelal dat de opslag van zoekgeschiedenis noodzakelijk is voor doeleinden zoals fraudebestrijding, beveiliging en verbetering van de dienstverlening en rechtshandhaving.²⁰⁰ Het bewaren en delen van gegevens met wetshandhavingsautoriteiten in het kader van politionele doeleinden kan aldus aangeduid worden als een gerechtvaardigd belang. Hierop dient echter kritisch te worden gereflecteerd, aangezien dit belang zwaarder moet wegen dan de belangen, grondrechten en fundamentele vrijheden van de betrokkenen, wat niet in alle gevallen gegarandeerd is.²⁰¹

¹⁹³ FOCQUET A. en DECLERCK E., 'Hoofdstuk 3 – Verwerkingsgronden' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, (47) 49; WAEM H. en VAN EECKE P., '3 - Verwerking van persoonsgegevens' in VAN EECKE P. (ed.), *Recht en elektronische handel*, Intersentia, 2021, (259) 278.

¹⁹⁴ EDPB, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, 4 mei 2020, 11.

¹⁹⁵ GROEP GEGEVENSBESCHERMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 17.

¹⁹⁶ *Ibid*, 18.

¹⁹⁷ Art. 6.1, f) AVG.

¹⁹⁸ Overw. 47 AVG

¹⁹⁹ *Ibid*, 47-49; EDPB, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2020.

²⁰⁰ GROEP GEGEVENSBESCHERMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 17-18.

²⁰¹ HvJ 13 mei 2014, C-131/12, ECLI:EU:C:2014:317, 'Google Spain en Google Inc./Agencia Española de Protección de Datos en Mario Costeja González', § 76.

88. Tot slot verdient de rechtsgrond betreffende het voldoen aan een wettelijke verplichting bijzondere aandacht.²⁰² Verwerkingsverantwoordelijken kunnen bij wet worden verplicht om bepaalde gegevens gedurende een specifieke periode te bewaren en hun medewerking te verlenen aan juridische verzoeken tot toegang tot deze gegevens, in het kader van de opsporing en vervolging van strafbare feiten. Op deze wijze wordt gewaarborgd dat gegevens die van belang kunnen zijn voor strafrechtelijke onderzoeken, veilig worden bewaard en toegankelijk zijn voor bevoegde autoriteiten.

89. Een dergelijke wettelijke bewaarplicht en grondslag voor toegang is reeds vastgesteld voor aanbieders van elektronische communicatiediensten en -netwerken (Cf. *infra*, nrs. 111-124, 142-145; Cf. *supra*, nrs. 40-51). Voor zoekmachinebedrijven bestaan dergelijke wettelijke bepalingen (nog) niet. De introductie van een wettelijke verplichting voor zoekmachinebedrijven om zoekgeschiedenissen en daaraan gerelateerde gegevens (zoals identificatiegegevens, IP-adressen, gegevens betreffende het tijdstip en de duur van de activiteit, de ingevoerde zoektermen, de gebruikte browser, het apparaattype en de locatie voor politionele doeleinden te bewaren) systematisch te bewaren, met het oog op de opsporing en vervolging van strafbare feiten, evenals een wettelijke bepaling die de medewerking aan juridische verzoeken tot toegang tot deze bewaarde gegevens reguleert, zou echter een duidelijke, consistente en vooraf gedefinieerde rechtsgrond voor de verwerking van zoekgeschiedenissen kunnen creëren. Hierdoor is men niet langer afhankelijk van de toestemming van de betrokkene of de vraag of een verwerking ten behoeve van politionele doeleinden voldoende opweegt tegen het recht op privacy, hetgeen doorgaans een complexe en vaak onzekere afweging vereist. Evenmin is het nodig om te betogen dat de verwerking plaatsvindt in het kader van de uitvoering van een overeenkomst.

90. Een wettelijke verplichting tot het bewaren van zoekgeschiedenissen en het reguleren van toegang daartoe is dan ook van wezenlijk belang. Zij waarborgt dat potentieel cruciale gegevens niet verloren gaan en tijdig beschikbaar zijn voor bevoegde autoriteiten in het kader van strafrechtelijke onderzoeken. Door een duidelijke en afdwingbare rechtsgrond te creëren, wordt zowel rechtszekerheid geboden aan verwerkingsverantwoordelijken als de effectiviteit van opsporings- en vervolgingsprocedures versterkt. De bruikbaarheid van zoektermbevelen is immers afhankelijk van een adequate en duurzame opslag van, en toegang tot, zoekgegevens. In de volgende paragrafen van dit hoofdstuk wordt nader ingegaan op de praktische haalbaarheid en de juridische implicaties van een dergelijke bewaarplicht en bepaling betreffende toegang tot deze gegevens.

C. Beginselen inzake verwerking

91. Het fundamentele uitgangspunt van de AVG is dat de verwerking van persoonsgegevens tot een minimum dient te worden beperkt. Indien verwerking toch noodzakelijk is, dient deze te geschieden op een wijze die zowel veilig als transparant is. Dit principe is verder uitgewerkt in verschillende overkoepelende beginselen die de verwerking van persoonsgegevens reguleren en die

²⁰² Art. 6.1, c) AVG.

als leidraad door de AVG fungeren.²⁰³ Niet alleen de rechtsgrondslag is van cruciaal belang voor de rechtmatigheid van de verwerking, maar ook de naleving van deze beginselen dient in overweging te worden genomen bij de beoordeling van de rechtmatigheid van de verwerking.²⁰⁴

92. De beginselen inzake de verwerking van persoonsgegevens betreffen de rechtmatigheid, behoorlijkheid en transparantie, doelbinding, minimale gegevensbescherming, juistheid, integriteit en vertrouwelijkheid en de opslagbeperking.²⁰⁵

93. Persoonsgegevens dienen te worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.²⁰⁶ Dit houdt in dat persoonsgegevens op eerlijke en transparante wijze worden verkregen en verwerkt en dat hierover beknopte, duidelijke en begrijpelijke informatie wordt verstrekt.²⁰⁷ Daarnaast kunnen persoonsgegevens slechts worden verwerkt en verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.²⁰⁸ Deze doeleinden dienen nauwkeurig en specifiek te worden afgebakend en op een heldere, begrijpelijke wijze te worden geformuleerd, zodat voor de betrokkenen te allen tijde duidelijk is welk gebruik binnen de beoogde doelstellingen valt en welke niet.²⁰⁹ Hiermee hangt samen dat de geïnterpreteerde persoonsgegevens toereikend, ter zake dienend en beperkt moeten blijven tot hetgeen noodzakelijk is voor die vooropgestelde doeleinden.²¹⁰ Men is aldus verplicht om de verzameling van persoonsgegevens te herleiden tot het minimum.²¹¹

94. Bijkomend is het van belang dat de gegevens die worden verwerkt en verzameld correct zijn en zo nodig worden geactualiseerd.²¹² In de praktijk komen veel verwerkingsverantwoordelijken aan dit beginsel tegemoet door de gebruiker zelf de mogelijkheid te geven om de gegevens in een account te wijzigen.²¹³ Samenhangend aan het beginsel dat de gegevens correct moeten zijn geldt het recht op vergetelheid, wat het recht inhoudt van de betrokkene om de verwijdering van de hem betreffende persoonsgegevens te verkrijgen.²¹⁴ Dit recht kan in principe steeds toegepast worden indien de verwerking onrechtmatig is.²¹⁵ Op dit recht wordt echter een uitzondering voorzien in het kader van politieke doeleinden.²¹⁶

²⁰³ CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I., 'hoofdstuk 1 – Overkoepelende principes' in CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I. (eds.), *Werk & Privacy*, Intersentia, 2019, (3) 12.

²⁰⁴ Art. 5.1 AVG.

²⁰⁵ *Ibid.*

²⁰⁶ Art. 5.1, a) AVG.

²⁰⁷ Art. 12.1 AVG; FEYS M. en MOREL C., 'De nieuwe Verordening Gegevensbescherming: een algemeen overzicht van de (nieuwe) verplichtingen rond gegevensbescherming' in Orde van Advocaten bij de balie te Gent (ed.), *De advocaat als generalist*, Intersentia, 2018, (125) 156.

²⁰⁸ Art. 5.1, b) AVG.

²⁰⁹ FOCQUET A. en DECLERCK E., 'Hoofdstuk 1 – Verwerking van persoonsgegevens' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, (5) 17-19.

²¹⁰ Art. 5.1, c) AVG.

²¹¹ FEYS M. en MOREL C., 'De nieuwe Verordening Gegevensbescherming: een algemeen overzicht van de (nieuwe) verplichtingen rond gegevensbescherming' in Orde van Advocaten bij de balie te Gent (ed.), *De advocaat als generalist*, Intersentia, 2018, (125) 161.

²¹² Art. 5.1, d) AVG.

²¹³ WAEM H. en VAN EECKE P., '3 - Verwerking van persoonsgegevens' in VAN EECKE P. (ed.), *Recht en elektronische handel*, Intersentia, 2021, (259) 276.

²¹⁴ Art. 17 AVG.

²¹⁵ Art. 17.1, a)-f) AVG.

²¹⁶ Art. 23, lid 1, a)-j) AVG.

95. Tot slot geldt het beginsel van opslagbeperking. Dit beginsel stipuleert dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor het doel waarvoor zij zijn verzameld.²¹⁷ Na deze termijn dienen de persoonsgegevens ofwel te worden geanonimiseerd, ofwel te worden verwijderd. De verwerkingsverantwoordelijke is derhalve verplicht een retentiebeleid vast te stellen en dient erop toe te zien dat gegevens niet onbeperkt worden opgeslagen.²¹⁸ In het retentiebeleid dienen specifieke termijnen te worden vastgesteld voor de duur van het bewaren van bepaalde persoonsgegevens, evenals termijnen voor het wissen van gegevens of voor de periodieke evaluatie.²¹⁹

96. Zoekmachinebedrijven kunnen tegemoet komen aan deze beginselen via hun privacybeleid.²²⁰ Zoekmachineaanbieders geven doorgaans in hun privacybeleid de volgende doeleinden op voor het verwerken en bewaren van persoonsgegevens in hun rol als verantwoordelijken voor de verwerking: verbetering van de service, systeembeveiliging, naleving van boekhoudkundige verplichtingen, gepersonaliseerde advertenties, rechtshandhaving, en andere gerelateerde doeleinden.²²¹ Zoals eerder vermeld, geven zoekmachinebedrijven in hun privacybeleid doorgaans aan dat zij persoonsgegevens kunnen bewaren ten behoeve van rechtshandavingsdoeleinden en aan opsporingsinstanties toegang kunnen verlenen, hetzij op grond van een gerechtelijk bevel, hetzij ingevolge een wettelijke bewaarplicht (Cf. *supra*, nrs. 81 en 87).

97. In hun privacybeleid wordt doorgaans ook een regeling opgenomen met betrekking tot de bewaartermijn van persoonsgegevens. Zoekmachinebedrijven trachten te voldoen aan het beginsel van opslagbeperking door zoekgegevens na een bepaalde periode te anonimiseren of pseudonimiseren, waardoor de betrokkene niet langer identificeerbaar is.²²² Daarnaast wordt gebruikers de mogelijkheid geboden hun zoekgeschiedenis te verwijderen of zelf de bewaartermijn van hun gegevens te bepalen. Zo kan een gebruiker instellen dat zijn zoekgeschiedenis gedurende 3, 18 of 36 maanden wordt bewaard. In het kader van web- en app-activiteit hanteert Google voor nieuwe accounts standaard een bewaartermijn van 18 maanden, waarna de verzamelde gegevens automatisch en continu worden verwijderd. Volgens de Werkgroep29, op basis van de oorspronkelijke verklaringen van zoekmachineaanbieders over de doeleinden voor het verzamelen van persoonsgegevens, is een bewaartermijn van meer dan zes maanden echter niet gerechtvaardigd.²²³ Toch hanteren de zoekmachinebedrijven (te) lange bewaartermijnen.

²¹⁷ Art. 5.1, e) AVG.

²¹⁸ CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I., 'hoofdstuk 1 – Overkoepelende principes' in CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I. (eds.), *Werk & Privacy*, Intersentia, 2019, (3) 55.

²¹⁹ *Ibid*; FOCQUET A. en DECLERCK E., 'Hoofdstuk 1 – Verwerking van persoonsgegevens' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, (5) 18.

²²⁰ WAEM H. en VAN EECKE P., '3 - Verwerking van persoonsgegevens' in VAN EECKE P. (ed.), *Recht en elektronische handel*, Intersentia, 2021, (259) 275-276.

²²¹ GROEP GEGEVENS BESCHERMING ARTIKEL 29, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148, 15-16.

²²² *Ibid*, 20.

²²³ *Ibid*, 19.

§ 2: Wettelijke bewaarplicht

98. Opdat zoektermbevelen daadwerkelijk bruikbaar zijn, is het essentieel dat de zoekgeschiedenis en daarmee verband houdende gegevens, zoals identificatiegegevens, IP-adressen, gegevens betreffende het tijdstip en de duur van de activiteit, de ingevoerde zoektermen, de gebruikte browser, het apparaattype en de locatie, van gebruikers op een effectieve wijze kunnen worden opgeslagen, zodat opsporingsautoriteiten toegang kunnen krijgen tot deze gegevens bij het traceren van verdachten. Dit kan gewaarborgd worden door middel van een wettelijke bewaarplicht. Een dergelijke plicht verplicht instanties om gedurende een vooraf vastgestelde en juridisch afgebakende termijn alle relevante gegevens op te slaan, met als doel het faciliteren van opsporing en vervolging van strafbare feiten.

99. Ondanks het feit dat dataretentie en de toegang door opsporingsautoriteiten tot de bewaarde data een belangrijke bijdrage kunnen leveren in het licht van de vrijwaring van de veiligheid en criminaliteitsbestrijding, zijn er ook risico's aan verbonden. Dataretentie en de toegang tot deze data vormen immers inmengingen in verschillende grondrechten, in het bijzonder het recht op privacy en het recht op gegevensbescherming.²²⁴ Uit metadata, zijnde identificatie-²²⁵, locatie²²⁶- en verkeersgegevens²²⁷, kunnen namelijk zeer precieze gegevens worden afgeleid over het privéleven van personen.²²⁸ Het is dan ook geen verrassing dat Europese wetgevers al jarenlang worstelen met de spanningen tussen enerzijds een dataretentieplicht en anderzijds de bescherming van het recht op privacy en gegevensbescherming. In dat spanningsveld speelt ook de AVG een centrale rol. Binnen het kader van een wettelijke bewaarplicht dienen de bepalingen van de AVG namelijk onverkort nageleefd te worden. Dit creëert een fundamentele spanning, aangezien een algemene en ongedifferentieerde gegevensbewaring haaks staat op de kernbeginselen van de AVG, zoals minimale gegevensverwerking en proportionaliteit.²²⁹ Deze spanning wordt bovendien onderstreept in de rechtspraak van het HvJ, waarin duidelijke voorwaarden worden gekoppeld aan de toelaatbaarheid van dataretentie (infra, nr). Ook in België heerst(e) al geruime tijd juridische en politieke onzekerheid over de geldigheid en houdbaarheid van een algemene bewaarplicht.

²²⁴ Zoals gewaarborgd in art. 7 en 8 EU-handvest en art. 8 EVRM.

²²⁵ Art. 46bis, §1, lid 1 Sv.; Identificatiegegevens zijn de gegevens die toelaten de abonnee of gewoonlijke gebruiker van een dienst en het gebruikte elektronische communicatiemiddel te identificeren. Concreet gaat het bijvoorbeeld over de naam en het adres van de gebruiker, het e-mailadres van de gebruiker, het telefoonnummer van een gebruiker, het identificatienummer van het mobiele eindtoestel van de gebruiker, etc.

²²⁶ Art. 88bis, §1, lid 1, 2° Sv.; art. 2, 7° WEC; art. 2, lid 2, c) E-Privacyrichtlijn; Locatiegegevens zijn de gegevens waarmee de geografische positie van de eindapparatuur van een eindgebruiker wordt weergegeven. In dat geval gaat het om de technische gegevens die toelaten om de geografische locatie van de oorsprong of de bestemming van de communicatie te bepalen, bijvoorbeeld op basis van zendmastgegevens.

²²⁷ Art. 88bis, §1, lid 1, 1° Sv.; art. 2, 6° WEC; art. 2, lid 1, b) E-Privacyrichtlijn; Verkeersgegevens zijn de gegevens die worden verwerkt door het overbrengen van communicatie over een elektronisch communicatienetwerk of voor het factureren van dergelijke communicatie. Concreet gaat het bijvoorbeeld over de oorsprong en bestemming van de communicatie, de datum, het tijdstip en de duur van de communicatie en de hoeveelheid dataverkeer.

²²⁸ HvJ 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, 'Digital Rights Ireland', § 27, HvJ 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, 'Tele2 Sverige AB', § 99, HvJ 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788, 'Ministerio Fiscal', § 54; HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/premier ministre', § 117; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', § 36, HvJ 20 september 2022, C-793/19 en C-749/19, ECLI:EU:C:2022:702, 'SpaceNet en Telekom Deutschland', § 61.

²²⁹ Art. 15.1 E-Privacyrichtlijn; hierin wordt bepaald dat bij het opleggen van beperkingen — zoals een bewaarplicht — de beginselen van noodzakelijkheid, proportionaliteit en redelijkheid in acht moeten worden genomen. Bij deze beoordeling kan bovendien rekening worden gehouden met de grondbeginselen en rechten zoals vastgelegd in de AVG.

Afdeling 1: Voorwaarden²³⁰

100. Het HvJ heeft zich herhaaldelijk uitgesproken over de verenigbaarheid van een algemene bewaarplicht van elektronische communicatie, met de fundamentele rechten op privacy en gegevensbescherming, zoals gewaarborgd in artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Deze bewaarplicht verplicht aanbieders van elektronische communicatiediensten en -netwerken om door hen gegenereerde of verwerkte metadata, waaronder identificatie-, verkeers- en locatiegegevens, gedurende een bepaalde termijn te bewaren.²³¹ Het HvJ heeft geoordeeld dat een dergelijke algemene en ongedifferentieerde dataretentieplicht een bijzonder ernstige inbreuk vormt op het recht op privacy en gegevensbescherming.²³² Het uitgangspunt binnen het kader van elektronische communicatie is namelijk dat deze communicatie vertrouwelijk is en bijgevolg niet mag worden afgeluisterd, opgeslagen of onderschept.²³³ Artikel 15, lid 1 van de E-privacyrichtlijn bevat evenwel een uitzonderingsbepaling, die het de lidstaten mogelijk maakt om wetgeving in te voeren die een bewaarplicht oplegt *"indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten [...]"*. Een algemene, ongedifferentieerde bewaring van alle metadata van alle abonnees en gebruikers van elektronische communicatiemiddelen wordt in dat licht dan ook als te verstrekkend en disproportioneel beschouwd.²³⁴

101. Enkele jaren na deze rechtspraak heeft het HvJ een belangrijke en richtinggevende uitspraak gewezen in de zaak *La Quadrature du Net* (hierna: QDN), waarin de grenzen en mogelijkheden van dataretentie binnen de Europese rechtsorde nader werden afgebakend.²³⁵ In dit arrest verduidelijkte het HvJ met name onder welke voorwaarden gegevensbewaring toelaatbaar is, waarbij bijzondere aandacht werd besteed aan de aard van de te bewaren gegevens en het nagestreefde doel van de bewaring.

102. In QDN start het HvJ opnieuw met het benadrukken dat elektronische communicatie een vertrouwelijk karakter heeft, en dat het verzamelen van metagegevens steeds als uitzondering dient te gelden.²³⁶ Het HvJ benadrukt echter ook dat overheden maatregelen moeten kunnen nemen om criminaliteit te bestrijden, waarin dataretentie een belangrijke rol kan spelen.²³⁷ Dit vloeit voort uit het feit dat in het EU-Handvest verschillende positieve verplichtingen bestaan voor overheden om

²³⁰ Bijlage 2.

²³¹ Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *pb.L.* 13 april 2006.

²³² HvJ 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, 'Digital Rights Ireland', §§ 37, 56-64.

²³³ Art. 5.1 E-Privacyrichtlijn.

²³⁴ HvJ 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, 'Tele2 Sverige AB', § 112.

²³⁵ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre'.

²³⁶ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 111; HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790, 'Privacy International/Secretary of State for Foreign and Commonwealth Affairs', §§ 59 en 69.

²³⁷ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', §§ 122-123.

maatregelen te nemen ter bescherming van het privé-, gezins- en familieleven, van iemands woning en communicatie, van iemands lichamelijke en geestelijke integriteit en om het verbod op foltering en onmenselijke en vernederende behandeling te waarborgen.²³⁸ Niettemin moet wetgeving die conflicterende grondrechten tracht te verzoenen proportioneel zijn.²³⁹ In dit verband heeft het HvJ belangrijke nieuwe inzichten verschaft.

103. Om aan het evenredigheidsbeginsel te voldoen dient het nationaal recht duidelijk aan te geven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van metagegevens kan worden genomen.²⁴⁰ Een regeling die voorziet in de bewaring van persoonsgegevens, moet derhalve steeds beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel.²⁴¹ Grosso modo maakt het HvJ aldus een tweevoudig onderscheid op basis van de te bewaren gegevens en het nagestreefde doel. Enerzijds stelt het dat de waarborging van nationale veiligheid een ingrijpendere inbreuk op de privacy kan rechtvaardigen dan de bestrijding van zware criminaliteit en de handhaving van de openbare veiligheid.²⁴² Anderzijds oordeelde het HvJ dat de bewaring van identificatiegegevens en IP-adressen van de oorsprong van de communicatie minder ingrijpend is voor de privacy dan de bewaring van verkeers- en locatiegegevens. Op basis van dit tweevoudige onderscheid kan een algemene dan wel gerichte bewaring als gerechtvaardigd worden beschouwd.

104. Het HvJ stelt dat een algemene bewaring van metadata mogelijk is voor identificatiegegevens.²⁴³ Identificatiegegevens verschaffen namelijk geen informatie over de datum, het tijdstip, de duur en de ontvangers van de communicatie, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd, en levert dus geen informatie op over het privéleven.²⁴⁴ Het HvJ oordeelt dan ook dat het Unierecht zich niet verzet tegen een wettelijke maatregel op grond waarvan aanbieders van elektronische communicatiediensten verplicht zijn om de gegevens inzake de burgerlijke identiteit van alle gebruikers gedurende een niet nader bepaalde periode te bewaren ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid, zonder dat het daarbij hoeft te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid.²⁴⁵

105. Een algemene bewaring van verkeers- en locatiegegevens is daarentegen slechts toegestaan in het kader van de waarborging van de nationale veiligheid, mits er voldoende concrete aanwijzingen bestaan voor een reële, actuele of voorzienbare ernstige bedreiging van de nationale veiligheid.²⁴⁶ De nationale veiligheid betreft *“de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de*

²³⁸ *Ibid*, §§ 124-128.

²³⁹ *Ibid*, § 130.

²⁴⁰ *Ibid*, § 132.

²⁴¹ *Ibid*, § 133.

²⁴² *Ibid*, § 136.

²⁴³ *Ibid*, § 157; HvJ 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788, ‘Ministerio Fiscal’, §§ 59-62.

²⁴⁴ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, ‘La Quadrature du Net/Premier ministre’, § 157.

²⁴⁵ *Ibid*, § 159.

²⁴⁶ *Ibid*, § 137.

fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig".²⁴⁷ Ook moeten er bijkomende waarborgen geboden worden in dit kader. Zo kan het bevel om preventief gegevens te bewaren van alle gebruikers slechts worden opgelegd voor een periode die niet langer nodig is dan strikt noodzakelijk, en aldus zolang de bedreiging blijft voortduren.²⁴⁸ Daarnaast hecht het HvJ ook belang aan de toetsing door een rechterlijke of onafhankelijke bestuurlijke autoriteit van het bevel. Het doel van die toetsing is om na te gaan of er zich effectief een bedreiging voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.²⁴⁹

106. Het HvJ maakt echter een uitzondering voor IP-adressen die aan de bron van de communicatie zijn gekoppeld. Hoewel deze gegevens eveneens als verkeersgegevens worden beschouwd, acht het HvJ deze categorie gegevens van minder gevoelige aard dan de andere verkeersgegevens, aangezien ze los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat.²⁵⁰ Het HvJ bevestigt in dit verband dat het algemeen bewaren van IP-adressen niet in strijd is met het Unierecht.²⁵¹ Het HvJ koppelt hieraan wel de voorwaarden dat het gebruik van dergelijke gegevens gepaard moet gaan met stringente waarborgen, de bewaartermijn beperkt dient te zijn tot het strikt noodzakelijke en dat dit uitsluitend mogelijk is met het oog op de bestrijding van ernstige criminaliteit of het voorkomen van ernstige bedreigingen voor de openbare of nationale veiligheid.²⁵²

107. Het HvJ herhaalde daarna dat in het kader van verkeers- en locatiegegevens ter bestrijding van zware criminaliteit en ter preventie van ernstige bedreigingen van de openbare veiligheid, enkel een gerichte bewaring mogelijk is.²⁵³ In dit licht is het belangrijk dat de categorieën te bewaren gegevens, de geviseerde communicatiemiddelen, de betrokken personen en de duur van de bewaring steeds beperkt zijn tot wat strikt noodzakelijk is.²⁵⁴ Daarnaast mag de maatregel niet langer gelden dan noodzakelijk is in het licht van het ermee beoogde doel.²⁵⁵ In het kader van de afbakening van de betrokken personen dienen objectieve factoren gehanteerd te worden waarmee kan worden gemikt op de personen van wie de verkeers- en locatiegegevens, althans indirect, een verband tonen met ernstige strafbare feiten en waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare of nationale veiligheid kan worden voorkomen.²⁵⁶ De personele beperking kan echter ook vervangen worden voor een geografische afbakening.²⁵⁷ Dat kan bijvoorbeeld wanneer de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in één of meer geografische gebieden sprake

²⁴⁷ *Ibid*, § 135.

²⁴⁸ *Ibid*, § 138.

²⁴⁹ *Ibid*, § 139.

²⁵⁰ *Ibid*, § 152.

²⁵¹ *Ibid*, § 155.

²⁵² *Ibid*, §§ 155-156.

²⁵³ *Ibid*, §§ 141-147.

²⁵⁴ *Ibid*, §§ 147-148.

²⁵⁵ *Ibid*, § 151.

²⁵⁶ *Ibid*, §§ 148-149.

²⁵⁷ *Ibid*, § 150.

is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd. Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.²⁵⁸

108. Ter bepaling van de draagwijdte van de gegevensbewaring is de concrete invulling van het begrip 'ernstige of zware criminaliteit' van cruciaal belang. Het HvJ heeft tot op heden geen uniforme, algemene definitie gehanteerd met betrekking tot welke misdrijven precies onder dit begrip vallen.²⁵⁹ Hierdoor beschikken de lidstaten over een zekere beoordelingsmarge. Aangenomen kan worden dat misdrijven die een schending inhouden van het verbod op foltering, onmenselijke of vernederende behandeling, het recht op eerbiediging van het privéleven, alsook misdrijven tegen de lichamelijke en geestelijke integriteit van de persoon, in het bijzonder wanneer zij op basis van criminologische modellen significant leed bij slachtoffers veroorzaken, als 'ernstig' kunnen worden gekwalificeerd.²⁶⁰

109. Tot slot oordeelde het HvJ in het arrest QDN ook over opvragingen in real time van verkeers- en locatiegegevens. Een dergelijke maatregel stelt de bevoegde autoriteiten in staat om voor de duur van de machtiging continu en in real-time in de gaten te houden met wie, met welke middelen en hoelang de betrokken personen communiceren, alsook waar zij verblijven en waarheen zij zich verplaatsen.²⁶¹ Het HvJ oordeelde dat de toepassing van zo'n indringende maatregel beperkt moet worden tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op een of andere manier betrokken zijn bij terroristische misdrijven.²⁶² Een loutere beperking tot terroristische misdrijven lijkt echter een te enge interpretatie van het arrest.²⁶³ Rekening houdend met de ingrijpende aard van de maatregel, kunnen de formuleringen van het HvJ erop wijzen dat het gebruik van realtime-retentie enkel als een uitzonderlijke maatregel toelaatbaar is. Dit impliceert dat dergelijke inzet slechts gerechtvaardigd is wanneer dit strikt noodzakelijk is voor het voorkomen of opsporen van ernstige strafbare feiten.²⁶⁴ Bovendien dient de machtiging ook steeds verleend te worden door een rechterlijke instantie of een onafhankelijke autoriteit waarvan de beslissing bindend is, en gebaseerd is op objectieve, in de nationale wetgeving vastgestelde criteria.²⁶⁵

²⁵⁸ *Ibid*, § 150.

²⁵⁹ Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001, 57-58; ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 8-11; ROYER S. en VERBRUGGEN F., 'Tussen helder en donker: mooie zebra of grijze ezel? Veiligheid en privacy via transparantie en opaciteit 20 jaar later' in DE HERT P. en GUTWIRTH S. (eds.), *Strafrecht in dialoog*, Intersentia, 2023, (133) 141; verzoek de Hoge Raad der Nederlanden van 6 april 2022 in de zaak C-241/22.

²⁶⁰ ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 8-11.

²⁶¹ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 184.

²⁶² *Ibid*, § 188.

²⁶³ DE KEERSMAECKER R. en VAN DE HEYNING C. 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *T.Strafr.* 2021/4, (171) 179-181.

²⁶⁴ *Ibid*, 181-182.

²⁶⁵ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 189.

110. Uit het arrest QDN kan worden geconcludeerd dat de bewaarplicht in de meeste gevallen gericht moet zijn en slechts bij uitzondering algemeen van aard kan zijn. Dit vormt een uitdaging voor opsporingsinstanties, aangezien een potentiële bron van cruciale informatie met betrekking tot mogelijke daders daardoor grotendeels verloren gaat. Politieën diensten beschikken immers niet vooraf over kennis omtrent de plaats, het tijdstip en de dader van een misdrijf. Pas nadat een misdrijf heeft plaatsgevonden, kan in het kader van een strafrechtelijk onderzoek worden vastgesteld welke metadata relevant zijn.²⁶⁶ Met name in onderzoeken naar onbekende daders leidt dit tot het verlies van een aanzienlijke hoeveelheid potentieel waardevolle informatie.

Afdeling 2: Dataretentiewet

111. De eerste Belgische dataretentiewet werd ingevoerd naar aanleiding van de omzetting van de toenmalige Dataretentierichtlijn.²⁶⁷ Deze wet werd echter volledig vernietigd, gelet op de rechtspraak van het HvJ over de onverenigbaarheid van een algemene bewaarplicht met de fundamentele rechten inzake privacy en gegevensbescherming.²⁶⁸ Ook de daaropvolgende wetgeving, die wederom voorzag in een algemene en ongedifferentieerde bewaring van gegevens, werd door het Grondwettelijk Hof vernietigd, ditmaal naar aanleiding van het arrest QDN.²⁶⁹ De wettelijke grondslag voor de bewaarplicht voor operatoren viel aldus opnieuw volledig weg. Ongeveer anderhalf jaar later ondernam de wetgever een nieuwe poging met de invoering van aangepaste regelgeving inzake dataretentie, die geacht wordt in overeenstemming te zijn met de rechtspraak van het HvJ.²⁷⁰ Deze nieuwe wet is *ratione personae* van toepassing op aanbieders van elektronische communicatiediensten en -netwerken, en *ratione materiae* op identificatie-, verkeers- en locatiegegevens die voortvloeien uit elektronische communicatie.²⁷¹

112. Zoals gedacht, werd tegen deze wet opnieuw weerstand geboden. Enkele mensenrechtenorganisaties en andere professionele organisaties diende namelijk vernietigingsberoepen in tegen de nieuwe dataretentiewet. Dit is echter weinig verrassend, gezien

²⁶⁶ ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 7.

²⁶⁷ Wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van Strafvordering, *BS* 23 augustus 2013; Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *pb.L.* 13 april 2006.

²⁶⁸ GwH 11 juni 2015, 84/2015, overw. B.11-B.12; VERSTRAELEN S., 'De vernietiging van de Belgische Dataretentiewet met terugwerkende kracht: de bescherming van het privéleven primeert (noot onder GwH 11 juni 2015)', *NC* 2015, (492) 492-496; CONINGS C., 'Dataretentie en privacy (noot onder GwH 15 juni 2015)', *NJW* 2015, (911) 911-913; CARTON A., 'De Belgische dataretentiewetgeving na het vernietigingsarrest van 11 juni 2015: another one bites the dust? (noot onder GwH 15 juni 2015)', *Computerrecht* 2015/5, (251) 251-256; CONINGS C. en VERBRUGGEN F., 'Grondwettelijk Hof plaatst reperateurs dataretentiewet voor moeilijke opdracht', *Juristenkrant* 2015/312, (1) 1-3.

²⁶⁹ GwH 19 juli 2018, 96/2018; GwH 22 april 2021, 57/2021; VAN DE HEYNING C., 'Overzicht van rechtspraak – Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog (noot onder GwH 19 juli 2018)', *T.Strafr.* 2019/1, (38) 40.

²⁷⁰ Wet 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, *BS* 8 augustus 2022; Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001, 3.

²⁷¹ Art. 126/1, §1, lid 1 WEC; art. 126/2, §2 WEC.

de kritiek die vanuit de rechtsleer en de Raad van State reeds werd geuit.²⁷² Desondanks blijkt de nieuwe dataretentiewet in overeenstemming te zijn met de rechtspraak van het HvJ, zoals bevestigd door het Grondwettelijk Hof.²⁷³ Voorlopig, in afwachting van enkele prejudiciële vragen aan het HvJ, is de nieuwe dataretentiewet aldus een feit.

113. De wetgever opteerde opnieuw voor een algemene en ongedifferentieerde bewaarplicht in een aantal specifieke gevallen. Het gaat hierbij om de identificatiegegevens of metagegevens in het licht van een ernstige bedreiging voor de nationale veiligheid.²⁷⁴ Daarnaast opteert de wetgever ook voor een gerichte bewaring van verkeers- en locatiegegevens, gebaseerd op geografische criteria.²⁷⁵ Ook wordt de mogelijkheid voorzien voor de PdK en de onderzoeksrechter om een gerichte bewaring te bevelen in het kader van een concreet dossier.²⁷⁶ Tot slot voorziet de wetgever ook in waarborgen betreffende de toegang tot de bewaarde gegevens (Cf. *infra*, nrs. 142-145).²⁷⁷

114. Artikel 126, §1 Wetboek elektronische communicatie (hierna: WEC)²⁷⁸ somt primair de gegevens op die door de operatoren te allen tijde bewaard moeten worden. Dit betreft onder meer de contactgegevens van een abonnee, het IP-adres aan de bron van de verbinding en de internationale identificatie van mobiele apparatuur, zoals het IMEI-nummer.²⁷⁹ Het HvJ acht de algemene bewaring van deze gegevens toelaatbaar, aangezien zij geen directe inzichten verschaffen in de inhoud of specifieke details van communicatie (Cf. *supra*, nr. 104). De bewaartermijn voor de meeste identificatiegegevens wordt in de regel vastgesteld op een periode van twaalf maanden, en gaat voor het overgrote deel van de identificatiegegevens in na het beëindigen van het gebruik van de elektronische communicatiedienst, waardoor deze gegevens bewaard kunnen blijven tot twaalf maanden na het laatste gebruik.²⁸⁰

115. In het kader van verkeers- en locatiegegevens is een algemene bewaring slechts mogelijk is in het licht van nationale veiligheid (Cf. *supra*, nr. 105). Artikel 126/2 WEC somt de gegevens op die operatoren in beginsel enkel in geval van gerichte bewaring dienen bij te houden. Echter, wanneer het Coördinatieorgaan voor de dreigingsanalyse (OCAD) een dreiging van niveau 3 of hoger voor het gehele grondgebied vaststelt, is er voor die gegevens automatisch een algemene en ongedifferentieerde bewaarplicht voorzien.²⁸¹ Dat niveau stemt overeen met een mogelijke en

²⁷² Advies RvS 28 juni 2021, nr. 69.381/4, 141; ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 1-22; FLUMIAN B. en FRANSSEN V., 'Le nouveau cadre légal belge en matière de conservation de données de communications électroniques' in MASSET A. en FRANSSEN V. (eds.), *Le droit pénal et la procédure pénale en constante évolution*, Anthemis, 2022, (315) 351; ROYER S. en CAREEL S., 'Voorontwerp dataretentiewet: derde keer, goede keer?', *Juristenkrant* 2021/432, (10) 10-11; VAN MUYLDER C., 'La conservation des données de télécommunication à des fins de poursuites pénales – Influence de la jurisprudence européenne sur le droit belge', *Dr.pén.entr.* 2022, (343) 365.

²⁷³ GwH 26 september 2024, 97/2024, ECLI:BE:GHCC:2024:ARR.097.

²⁷⁴ Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001, 6.

²⁷⁵ *Ibid.*, 9-13.

²⁷⁶ *Ibid.*, 6-9.

²⁷⁷ *Ibid.*, 13-15.

²⁷⁸ Dit wetboek werd geïmplementeerd door middel van de wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, *BS* 31 december 2021.

²⁷⁹ Art. 126, §1, 3°, 15° en 16° WEC.

²⁸⁰ Art. 126, §2, lid 1 WEC.

²⁸¹ Art.126/3, §2, lid 2 WEC.

waarschijnlijke dreiging, waarbij veronderstelt kan worden dat het gebaseerd is op voldoende concrete aanwijzingen voor een ernstige bedreiging.²⁸²

Aanvullende waarborgen zijn vereist in dit kader (Cf. *supra*, nr. 105). De bewaringsmaatregel moet in de tijd worden beperkt tot wat strikt noodzakelijk is en mag slechts worden opgelegd voor een voorzienbare periode. Artikel 126/3, §2, derde lid WEC lijkt het aantal verlengingen echter niet te begrenzen. Bovendien wordt de periode waarvoor de maatregel van kracht is steeds bepaald bij koninklijk besluit (hier: KB), waarbij de termijn steeds gemotiveerd dient te worden, maar waardoor de wet zelf zwijgt over een specifieke termijn.²⁸³ Naast de temporele begrenzing is het vereist dat er toezicht wordt uitgeoefend door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit. De wetgever acht daarentegen een bevestiging van de maatregel bij KB voldoende. Dit voldoet echter niet volledig aan de door het HvJ gestelde vereisten, aangezien hierdoor geen daadwerkelijke en grondige toetsing van de maatregel plaatsvindt.²⁸⁴

116. Artikel 126/1, §1 WEC bevat een wettelijke basis voor gerichte dataretentie op basis van geografische criteria, dewelke worden gedefinieerd in artikel 126/3 WEC. Deze geografische criteria dienen verder uitgewerkt te worden bij KB. De gerichte bewaring heeft betrekking op de verkeers- en locatiegegevens, alsook bepaalde identificatiegegevens. Het HvJ heeft echter duidelijk bepaald dat met betrekking tot de verkeers- en locatiegegevens enkele waarborgen voor ogen dienen te worden gehouden (Cf. *supra*, nr. 107). Zo is het bewaren van deze metagegegevens slechts mogelijk voor het bestrijden van ernstige criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid. Daarnaast dienen de categorieën van de te bewaren gegevens, betrokken communicatiemiddelen, betrokken personen en duur beperkt te worden tot wat strikt noodzakelijk is.

117. Artikel 126/1, §1, lid 3 WEC vermeldt duidelijk dat de gegevens enkel bewaard kunnen worden in het licht van ernstige criminaliteit, de vrijwaring van nationale veiligheid, de preventie van ernstige dreigingen van de openbare orde en voor de bescherming van de vitale belangen van de persoon. De wetgever geeft evenwel geen verdere toelichting bij de concrete inhoud of afbakening van deze begrippen.

118. In het kader van de gerichte bewaring wordt geopteerd voor een afbakening op basis van geografische criteria.²⁸⁵ De geografische koppeling gebeurt op basis van de netwerkinfrastructuur van de operatoren, zoals de locatie van gebruikte zendmasten bij mobiele communicatie, of gelogde IP-adressen en, in sommige gevallen, de locatie van het gebruikte wifi-punt of modem bij internetverkeer.

²⁸² Art. 11, §6, lid 2, 3^o Koninklijk besluit tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, BS 1 december 2012.

²⁸³ Art. 126/3, §2, lid 3 WEC.

²⁸⁴ ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', NC 2023/1, (1) 12-13.

²⁸⁵ Art. 126/3 WEC.

119. Op basis hiervan opteert de wetgever voor drie categorieën 'vaste' geografische zones. In eerste instantie bepaald artikel 126/3, §3 WEC een lijst van twaalf geografische zones voor bewaring in het kader van bedreigingen tegen de nationale veiligheid of voor het plegen van zware criminaliteit. Het gaat hier onder meer over luchthavens, gevangenissen, havens, ... Deze lijst kan echter wel worden uitgebreid bij KB.²⁸⁶ Ten tweede bepaalt artikel 126/3, §4 WEC de zones in het licht van ernstige bedreigingen voor de vitale belangen van het land of de essentiële behoeften van de bevolking. Te denken valt aan gemeentehuizen en stadshuizen, grensgemeenten en ziekenhuizen. Opnieuw kan deze lijst uitgebreid worden bij KB.²⁸⁷ De derde categorie van zones betreft de supra- en internationale instellingen.²⁸⁸ Voor elk van de drie bovenstaande categorieën dient de perimeter bepaald te worden bij KB, waarbij aandacht besteed moet worden dat de perimeter niet te breed mag worden ingesteld om een disproportionele bewaring te vermijden.²⁸⁹

120. Naast de vaste geografische zones worden er ook zones gecreëerd die afhangen van de hoeveelheid en soort strafbare feiten die er gepleegd worden.²⁹⁰ In eerste instantie kunnen er gegevens bewaard worden in geografische zones waarvoor minstens dreigingsniveau 3 geldt.²⁹¹ Daarnaast laat de wetgever de bewaring afhangen van het aantal misdrijven opgesomd in artikel 90ter, §§2-4 Sv.²⁹² Zo wordt gesteld dat er minstens drie misdrijven per 1.000 inwoners per jaar vastgesteld dienen te worden over een gemiddelde van de drie voorbije kalenderjaren. Is dat het geval, dan kunnen de gegevens worden bijgehouden op het niveau van het arrondissement of de politiezone.²⁹³ De reden waarom beroep gedaan wordt op vastgestelde feiten bedoeld in artikel 90ter, §§ 2-4 Sv. wordt volgens de wetgever verklaard door het feit dat hierin de vormen van criminaliteit worden opgesomd die over het algemeen als ernstig worden beschouwd.²⁹⁴ Toch rijst de vraag of alle misdrijven opgesomd in deze bepalingen daadwerkelijk binnen de draagwijdte van het begrip 'zware criminaliteit' vallen (Cf. *supra*, nr. 108).²⁹⁵ De opsomming in de betrokken bepaling is immers dermate uitgebreid dat het twijfelachtig is of elk misdrijf op deze lijst als ernstig kan worden gekwalificeerd. Zo wordt onder meer het misdrijf diefstal vermeld, wat zowel eenvoudige winkeldiefstal als de diefstal van een kostbare juwelencollectie kan omvatten. Deze ruime interpretatie bemoeilijkt een coherente en werkbare afbakening van het begrip 'ernstige criminaliteit'.²⁹⁶

²⁸⁶ Art. 126/3, §3, m) WEC.

²⁸⁷ Art. 126/3, §4, g) WEC.

²⁸⁸ Art. 126/3, §6, lid 1 WEC.

²⁸⁹ Art. 126/3, §6, lid 1 WEC.

²⁹⁰ Art. 126/3, § 1 WEC.

²⁹¹ Art. 126/3, §2 WEC.

²⁹² Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001, 56.

²⁹³ Art. 126/3, §1, lid 1 WEC.

²⁹⁴ Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001, 55-56.

²⁹⁵ ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 14; ROYER S. en VERBRUGGEN F., 'Tussen helder en donker: mooie zebra of grijze ezel? Veiligheid en privacy via transparantie en opaciteit 20 jaar later' in DE HERT P. en GUTWIRTH S. (eds.), *Strafrecht in dialoog*, Intersentia, 2023, (133) 141.

²⁹⁶ ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 11; ROYER S. en VERBRUGGEN F., 'Tussen helder en donker: mooie zebra of grijze ezel? Veiligheid en privacy via transparantie en opaciteit 20 jaar later' in DE HERT P. en GUTWIRTH S. (eds.), *Strafrecht in dialoog*, Intersentia, 2023, (133) 141.

121. Binnen het kader van gerichte dataretentie werd geen temporele beperking voorzien. Dit vloeit voort uit het feit dat wijzigingen in de geografische zones steeds bij wet moeten worden doorgevoerd. Volgens de wetgever zou het herhaaldelijk opstarten van het wetgevend proces bij het wegvallen van de noodzaak tot bewaring leiden tot rechtsonzekerheid. Wel is een jaarlijkse evaluatie met de mogelijkheid tot wetsherziening voorzien.²⁹⁷ Het criterium van strikte noodzakelijkheid wordt echter overschreden wanneer geografische zones slechts éénmaal per jaar kunnen worden aangepast. Dit wijst op een lacune in de wetgeving.²⁹⁸

122. Ondanks het ontbreken van een expliciete temporele beperking, wordt wel een wettelijk kader geboden met betrekking tot de bewaartermijnen. De gegevens die op grond van artikel 126/2 WEC gericht worden bewaard, kennen in principe een bewaartermijn van twaalf maanden.²⁹⁹ Voor de gegevens die worden bewaard in de geografische zones, zoals bepaald in artikel 126/3, §1 WEC, geldt echter een afwijkende regeling. De bewaartermijn van deze gegevens is afhankelijk van de mate van criminaliteit binnen specifieke gerechtelijke arrondissementen of politiezones. Hoe meer strafbare feiten per 1.000 inwoners zijn gepleegd over de afgelopen drie kalenderjaren, des te langer de gegevens mogen worden bewaard. De termijn bedraagt zes maanden bij drie of vier strafbare feiten, negen maanden bij vijf of zes strafbare feiten, en twaalf maanden bij zeven of meer strafbare feiten.³⁰⁰

123. De wetgever heeft ook geopteerd voor een bijkomende aanvulling op de algemene en gerichte bewaring in de nieuwe dataretentiewet, namelijk de mogelijkheid voor een bevel tot gerichte bewaring (realtime-bewaring). Dat bevel kan door de PdK worden opgelegd in het kader van een opsporingsonderzoek naar misdaden en wanbedrijven die bestraft worden met een correctionele gevangenisstraf van ten minste één jaar, en kan worden gericht aan operatoren en dienstverleners van een elektronisch communicatienetwerk.³⁰¹ Het bevel maakt het mogelijk om aan de operator of dienstverstrekker de verplichting op te leggen identificatie-, locatie- en verkeersgegevens te bewaren. In een schriftelijke beslissing moet de PdK echter wel steeds aanduiden op welke personen, communicatiemiddelen of plaatsen de bewaring betrekking heeft, aangezien het nog steeds om een gerichte bewaring gaat.³⁰² Zo kan een gerichte bewaring opgelegd worden voor alle verkeersgegevens in een perimeter rond het huis waar een misdrijf is gepleegd en van alle personen die het slachtoffer hebben gekend.³⁰³

²⁹⁷ Art. 126/1, §5 WEC.

²⁹⁸ ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 16.

²⁹⁹ Art. 126/1, §1, lid 1 WEC.

³⁰⁰ Art. 126/3, §§ 1-2 WEC.

³⁰¹ Art. 39quinquies, §1 Sv.

³⁰² Art. 39quinquies, §1, lid 3, gedachtestreepje 4 Sv.

³⁰³ Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001, 140.

Wat de temporele afbakening betreft, bedraagt de tijdspanne waarin de operatoren verplicht zijn gegevens te bewaren, maximum twee maanden. De gegevens kunnen daarnaast slechts bewaard blijven gedurende zes maanden. Beide termijnen kunnen echter wel worden verlengd.³⁰⁴

124. De vraag kan echter gesteld worden of deze bepaling wel in overeenstemming is met de rechtspraak van het HvJ (Cf. *supra*, nr. 109). De drempel van één jaar correctionele hoofdgevangenisstraf ligt namelijk wel heel laag. In het kader van de hervorming van het Strafwetboek³⁰⁵, waarbij de toepasselijke straffen worden onderverdeeld in verschillende niveaus, is het van belang dat de gekozen drempel voldoende hoog wordt gelegd. Daarbij rijst de vraag of de wetgever zal opteren voor niveau 2, dat een minimumgevangenisstraf van zes maanden omvat, dan wel een hoger strafniveau als uitgangspunt zal hanteren.³⁰⁶ Daarnaast lijken de aangewezen autoriteit, zijnde de PdK, en de soepele voorwaarden niet helemaal te stroken met de rechtspraak.³⁰⁷

Afdeling 3: Een bewaarplicht voor zoekmachinebedrijven?

125. De reeds bestaande dataretentiewet is van toepassing op aanbieders van elektronische communicatiediensten en -netwerken. Zoekmachine-exploitanten vallen niet onder dit toepassingsgebied, aangezien ze geen elektronische communicatiediensten aanbieden. Voor zoekmachinebedrijven geldt derhalve geen wettelijke verplichting in België om zoekgeschiedenissen en daaraan gekoppelde gegevens, zoals identificatiegegevens, IP-adressen, gegevens betreffende het tijdstip en de duur van de activiteit, de ingevoerde zoektermen, de gebruikte browser, het apparaattype en de locatie (hierna: daaraan gekoppelde gegevens), voor politionele doeleinden te bewaren. De vraag kan echter worden gesteld of eveneens de mogelijkheid bestaat om aan deze bedrijven een bewaarplicht op te leggen met betrekking tot zoekgeschiedenissen en daaraan gekoppelde gegevens.

126. Hoewel het HvJ zich niet expliciet heeft uitgesproken over een bewaarplicht met betrekking tot de zoekgeschiedenis en daaraan gekoppelde gegevens van individuen, kan op basis van de bestaande rechtspraak worden beargumenteerd dat zoekgeschiedenissen gevoeliger zijn dan louter identificatiegegevens en een IP-adres. In QDN heeft het HvJ namelijk geoordeeld dat de zoekgeschiedenis van personen, net zoals metadata, zeer gevoelige gegevens bevatten aangezien de zoekgeschiedenis informatie kan prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid. Uit deze gegevens kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, aangezien ze gebruikt kunnen worden

³⁰⁴ Art. 39*quinquies*, §1, lid 3 Sv; Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001, 141.

³⁰⁵ Wet van 29 februari 2024 tot invoering van boek I van het Strafwetboek, *BS* 8 april 2024.

³⁰⁶ Art. 36 wet van 29 februari 2024 tot invoering van boek I van het Strafwetboek, *BS* 8 april 2024.

³⁰⁷ ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 17.

om een volledig profiel van een persoon op te stellen.³⁰⁸ De zoekgeschiedenis van personen kan hierdoor worden vergeleken met verkeers- en locatiegegevens, aangezien deze eveneens een gedetailleerd en indringend profiel van een individu kunnen schetsen.³⁰⁹ In het kader van een bewaarplicht van zoekgeschiedenissen zou het HvJ o.i. waarschijnlijk oordelen dat een dergelijke maatregel een bijzonder ernstige inbreuk vormt op het recht op privacy en gegevensbescherming. Derhalve zouden de principes die gelden voor de bewaring van verkeers- en locatiegegevens eveneens van toepassing zijn op een eventuele bewaarplicht van zoekgeschiedenissen, inclusief gegevens betreffende het tijdstip en de duur van de activiteit, de ingevoerde zoektermen, de gebruikte browser, het apparaattype en de locatie (hierna: metagegevens gekoppeld aan zoekgeschiedenissen).

127. Dit impliceert dat een algemene en ongedifferentieerde bewaring van zoekgeschiedenissen, en daaraan gekoppelde metagegevens, niet toegestaan zou zijn, tenzij in het kader van de nationale veiligheid. In navolging van de reeds bestaande Belgische dataretentiewet kan als aanbeveling worden overwogen om een dergelijk regime te koppelen aan een verhoogd dreigingsniveau, bijvoorbeeld niveau drie of hoger op het gehele grondgebied, waarbij een tijdelijke algemene bewaarplicht in werking kan treden (Cf. *supra*, nrs. 105 en 115).³¹⁰ Het is aanbevolen om identificatiegegevens die gekoppeld zijn aan bijvoorbeeld een account waarmee zoekopdrachten zijn uitgevoerd, systematisch te bewaren voor alle gebruikers in het kader van de bestrijding van strafbare feiten (Cf. *supra*, nrs. 104 en 114). Daarentegen wordt aangeraden om IP-adressen die verbonden zijn aan het apparaat waarmee zoekopdrachten zijn uitgevoerd, enkel algemeen te bewaren voor zover dit noodzakelijk is voor het bestrijden van ernstige misdrijven of het voorkomen van ernstige bedreigingen voor de openbare of nationale veiligheid (Cf. *supra*, nrs. 106 en 114).³¹¹

128. Een mogelijke alternatieve benadering betreffende een bewaarplicht met betrekking tot de zoekgeschiedenis van gebruikers en daaraan gekoppelde metagegevens, zou het invoeren van een gerichte bewaarplicht zijn in het kader van ernstige criminaliteit en openbare veiligheid. Een dergelijke maatregel moet echter steeds worden beperkt tot wat strikt noodzakelijk is. In dat licht is het van essentieel belang dat de categorieën van te bewaren gegevens, de geïdentificeerde applicaties, de betrokken personen en de duur van de bewaring op duidelijke wijze worden omschreven.³¹² Wat betreft de te bewaren gegevens gaat het in dit verband onder meer om de zoekgeschiedenis, de ingevoerde zoektermen, het tijdstip en de duur van de activiteit, de gebruikte browser, het apparaattype en de locatie. De geïdentificeerde applicaties hebben betrekking op de belangrijkste zoekmachineplatformen, zoals Google Search, Bing en Yahoo Search. Met betrekking tot de aanduiding van de betrokken personen kan worden geopteerd voor zowel een personele als een geografische afbakening (Cf. *supra*, nr. 107).

³⁰⁸ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', §§ 117 en 153.

³⁰⁹ *Ibid*, § 153.

³¹⁰ Art. 126/3, §2, lid 2 WEC.

³¹¹ Art. 126, §1, 1^o-17^o WEC.

³¹² HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', §§ 147-148.

129. Aangezien zoektermbevelen voornamelijk van nut zijn in onderzoeken naar onbekende daders, lijkt een personele afbakening niet passend. Een dergelijke afbakening vereist immers dat op basis van objectieve criteria wordt bepaald wiens zoekgeschiedenis wordt bewaard, waarbij moet worden aangetoond dat de betreffende gegevens een verband vertonen met ernstige strafbare feiten en dat het verzamelen ervan bijdraagt aan de bestrijding van zware criminaliteit of het voorkomen van een ernstige bedreiging voor de openbare of nationale veiligheid. Dit impliceert dat er reeds specifieke verdachten geïdentificeerd moeten zijn, wat juist niet het geval is bij zoektermbevelen.

130. Er kan echter wel worden gekozen voor een geografische afbakening waarbij de zoekgeschiedenis en daaraan gekoppelde metagegevens, van alle gebruikers die zich fysiek binnen die afgebakende zones bevinden, wordt bewaard. De geografische herkomst van een zoekopdracht kan in dat geval worden afgeleid uit verschillende brongegevens die samen met de zoekterm worden gelogd, zoals het IP-adres van de gebruiker, de locatie van het verbonden wifi-punt of modem, of, in geval van een ingelogd account, bijkomende locatie-informatie afkomstig van apparaat- of sessiegegevens. Daarnaast zou overwogen kunnen worden om zoekopdrachten te bewaren die inhoudelijk betrekking hebben op een vooraf geografisch afgebakende locatie, ongeacht waar de gebruiker zich op dat moment bevindt.³¹³ In dat geval dient de bewaring strikt beperkt te blijven tot die ene specifieke opzoeking, waarbij enkel de zoekterm met betrekking tot de betrokken locatie wordt opgeslagen, en niet de volledige zoekgeschiedenis van de gebruiker.

131. Deze geografische afbakening zou met name kunnen gelden voor specifieke risicogebieden, die op basis van objectieve criteria als kwetsbaarder worden beschouwd vanwege een verhoogde frequentie van zware criminaliteit. Net zoals in de huidige Belgische dataretentiewet zou geopteerd kunnen worden voor vaste geografische zones of zones waarvan de afbakening afhankelijk is van een dreigingsniveau of criminaliteitscijfers (Cf. *supra*, nrs. 116-122). In het geval van dergelijke criminaliteitscijfers verdient het aanbeveling een vaste lijst van ernstige misdrijven te hanteren, zoals vervat in artikel 90ter, §§ 2–4 Sv. Deze benadering versterkt de rechtszekerheid en objectiviteit, maar vergt tevens de nodige nuance. Hoewel het hanteren van een vaste lijst op het eerste gezicht efficiënt lijkt, blijkt de ruime reikwijdte ervan problematisch. Niet alle daarin opgenomen misdrijven voldoen aan de vereiste ernst, en binnen bepaalde categorieën misdrijven doen zich aanzienlijke gradaties voor (Cf. *supra*, nr. 120). Een kritische herziening dringt zich dan ook op, waarbij misdrijven zoals informaticabedrog, private omkoping en heling bij voorkeur worden uitgesloten teneinde de proportionaliteit van de maatregel te waarborgen.³¹⁴

132. Hoewel een dergelijke geografische afbakening in bepaalde delen van België neerkomt op een de facto algemene bewaarplicht,³¹⁵ rijst de vraag of dit in de praktijk daadwerkelijk effectief zal zijn. Politiediensten zouden immers moeten hopen dat een dader precies de zoekterm invoert die zij

³¹³ O.i. vormt dit geen probleem, aangezien ook bij het verkrijgen van verkeersgegevens informatie wordt vrijgegeven over apparaten en personen waarmee is gecommuniceerd, waarbij deze zich eveneens buiten de oorspronkelijk beoogde geografische zones kunnen bevinden, zolang er een voldoende verband bestaat met de vooraf afgebakende geografische zone.

³¹⁴ ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 8-11, 14.

³¹⁵ *Ibid*, 15.

voor ogen hebben binnen de afgebakende gebieden, of dat een zoekopdracht wordt uitgevoerd met betrekking tot zo'n afgebakende locatie. Dit brengt een bijzonder geringe kans op succes met zich mee.

133. Zowel in het kader van een algemene bewaarplicht met betrekking tot de nationale veiligheid als bij een gerichte bewaarplicht van zoekgeschiedenissen en daaraan gekoppelde metagegevens, dient de maatregel strikt tijdgebonden te zijn. Hierbij is het aangeraden duidelijk te stellen dat de zoekgeschiedenissen en de daaraan gekoppelde metagegevens slechts mogen worden bewaard zolang de dreiging voor de nationale veiligheid aanhoudt. Wat betreft de gerichte bewaarplicht moet expliciet worden aangegeven dat de maatregel niet langer mag worden toegepast zodra de geografische afbakening, gebaseerd op criminaliteitscijfers of dreigingsniveau, niet meer voldoet aan de vereiste drempel van misdrijven of het dreigingsniveau niet langer van kracht is.

134. Zowel vanuit het perspectief van de AVG als in het kader van de beoordeling van de proportionaliteit van een eventuele bewaarplicht geldt dat gegevens slechts mogen worden bewaard voor zover dit noodzakelijk is voor het nagestreefde doeleinde. Dit impliceert dat steeds een concreet en duidelijk afgebakende bewaartermijn moet worden vastgelegd. In aansluiting bij de daataretentiewet kan een gedifferentieerde regeling worden aanbevolen, afhankelijk van het type gegevens dat wordt opgeslagen. In het kader van identificatiegegevens en IP-adressen kan worden geopteerd voor een bewaartermijn van twaalf maanden, te rekenen vanaf het moment van de zoekopdracht (Cf. *supra*, nr. 114). Het is aan te bevelen dat, in het kader van een algemene bewaarplicht ter bescherming van de nationale veiligheid, de zoekgeschiedenis en de daarmee samenhangende metagegevens worden bewaard gedurende de periode waarin een verhoogd dreigingsniveau van kracht is, alsook gedurende een aanvullende termijn van zes maanden na de beëindiging van dat dreigingsniveau (Cf. *supra*, nrs. 105 en 114). Voor de zoekgeschiedenis en de daaraan gekoppelde metagegevens, die bewaard worden in het licht van een gerichte bewaring, kan een termijn van twaalf maanden worden voorzien, doch beperkt tot gegevens verzameld binnen de vaste geografische zones.³¹⁶ Daarnaast kan, conform de dataretentiewet, een afwijkende regeling worden gehanteerd voor geografische zones die op basis van criminaliteitscijfers worden afgebakend. In dergelijke gevallen kan een variabele bewaartermijn worden toegepast in functie van de ernst en frequentie van strafbare feiten in de betrokken zones over de afgelopen kalenderjaren. Zo kan een termijn van zes maanden worden gehanteerd bij drie of vier geregistreerde strafbare feiten, een termijn van negen maanden bij vijf of zes feiten, en een termijn van twaalf maanden bij zeven of meer strafbare feiten (Cf. *supra*, nr. 122).³¹⁷

135. Naast preventieve gegevensbewaring kan ook realtime-bewaring van zoekgeschiedenissen en aanverwante gegevens overwogen worden, vergelijkbaar met artikel 39quinqües Sv. In een lopend strafonderzoek kunnen zoekmachinebedrijven dan verplicht worden dergelijke gegevens tijdelijk en gericht te bewaren, met betrekking tot specifieke personen, apparaten of locaties. Dit botst echter met het concept van zoektermbevelen, die juist worden ingezet wanneer de dader nog

³¹⁶ Art. 126/1, §1, lid 1 WEC.

³¹⁷ Art. 126/3, §§ 1-2 WEC.

onbekend is. In dergelijke gevallen kunnen immers geen specifieke personen of apparaten worden geïdentificeerd. Bij een bekende verdachte biedt artikel 39bis Sv. voldoende juridische basis om diens toestel, inclusief zoekgeschiedenis, uit te lezen. Bij een link met een specifiek apparaat, zijn bovendien andere onderzoeksmethoden, zoals het opvragen van verkeers- en locatiegegevens of een IT-inkijkoperatie, doorgaans meer geschikt. Ook indien er een concrete locatie is die in verband kan worden gebracht met het gepleegde misdrijf lijkt de toepassing van de zendmastbepaling meer aangewezen dan het hanteren van zoektermbevelen. Bovendien worden zoekopdrachten vaak in de voorbereidende fase van een misdrijf uitgevoerd, en is het weinig waarschijnlijk dat daders na het plegen van de feiten nog relevante zoektermen zullen invoeren. Naar onze mening lijkt, vanuit juridisch en praktisch oogpunt, een bevel tot gerichte bewaring in dit verband dan ook weinig meerwaarde te bieden.

136. Het is evident dat de bewaring van zoekgeschiedenissen en aanverwante gegevens van gebruikers aan strikte beperkingen onderhevig is, in het bijzonder wanneer dergelijke gegevens worden ingezet in het kader van zoektermbevelen die gericht zijn op de opsporing van onbekende daders. In dergelijke gevallen zijn de identiteit, de locatie en het gebruikte apparaat van de betrokkene op voorhand onbekend. Politiediensten zijn daarbij afhankelijk van de toevalligheid dat een dader precies de zoekterm gebruikt die zij hebben vastgesteld, binnen een vooraf geografisch afgebakend gebied, of inhoudelijk gelinkt aan een dergelijke locatie. Niettemin dient te worden benadrukt dat een beroep op deze bewaarplicht slechts aan de orde is wanneer geen andere rechtmatige verwerkingsgrond onder de AVG beschikbaar is. Indien een gebruiker daarentegen expliciet toestemming heeft verleend voor het bijhouden van zijn volledige zoekgeschiedenis, en eventueel ook voor het delen daarvan met opsporingsautoriteiten, kan deze toestemming dienen als zelfstandige rechtsgrond voor een ruimere bewaring van de gegevens. In een dergelijk geval is de verwerking niet langer beperkt tot een specifieke, vooraf bepaalde doelstellingen of geografische afbakening en vervallen deze bijkomende beperkingen aldus.

§ 3: Toegang tot bewaarde gegevens

137. Het is van belang voor ogen te houden dat er een onderscheid gemaakt moet worden tussen de mogelijkheid om gegevens te bewaren en de toegang tot de bewaarde gegevens door opsporingsautoriteiten. Zowel de bewaring van metadata als de toegang ertoe vormen afzonderlijke inmengingen in het recht op privacy en gegevensbescherming.³¹⁸ Het feit dat een bewaring mogelijk is, betekent niet automatisch dat opsporingsinstanties ook steeds toegang zullen hebben tot deze gegevens. In dit kader heeft het HvJ strikte criteria vastgesteld en bijzondere nadruk gelegd op de waarborging van deze fundamentele rechten.³¹⁹

138. Het is nog niet definitief uitgemaakt of de voorwaarden die het HvJ stelt aan toegang tot gegevens op basis van een wettelijke bewaarplicht, ook gelden wanneer gegevens op een andere

³¹⁸ HvJ 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, 'Digital Rights Ireland', §§ 34-35, HvJ 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788, 'Ministerio Fiscal', § 51; HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/premier ministre', § 116.

³¹⁹ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/premier ministre', §§ 166-167; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', §§ 27-59.

verwerkingsgrond worden bewaard.³²⁰ Naar onze mening is dat wel het geval. Zowel de bewaring als de toegang vormen verwerkingen in de zin van de AVG, en de vereisten die daaruit voortvloeien stemmen grotendeels overeen met de toetsingscriteria van het HvJ. Dit is logisch, aangezien zowel de AVG als de rechtspraak vertrekken vanuit dezelfde fundamentele beginselen inzake gegevensbescherming. Voor toegang tot bewaarde gegevens gelden dan ook steeds drie voorwaarden: (i) een wettelijke grondslag, wat binnen de AVG neerkomt op een geldige verwerkingsgrond, (ii) een legitiem doel, en (iii) naleving van de beginselen van noodzakelijkheid en proportionaliteit.³²¹

Afdeling 1: Voorwaarden³²²

139. Het HvJ heeft in het kader van de toegang tot de bewaarde gegevens aangenomen dat er een verband moet bestaan tussen de doelstelling van de bewaring en de doelstelling van de toegang, maar dat de toegang voor verregaandere doeleinden ook mogelijk is.³²³ Toegang tot identificatiegegevens is mogelijk voor de bestrijding van gewone misdrijven en de verstoring van de openbare orde en nationale veiligheid. De toegang tot IP-adressen en locatie- en verkeersgegevens is daarnaast slechts mogelijk voor de bescherming van de nationale veiligheid, bestrijding van ernstige misdrijven en een ernstige verstoring van de openbare orde.³²⁴ Toegang tot locatie- en verkeersgegevens is aldus steeds uitgesloten in het licht van de vervolging en bestraffing van een gewoon strafbaar feit.³²⁵ Op die manier wordt steeds een evenwicht nagestreefd tussen de ernst van de inmenging en het belang van de nagestreefde doelstelling.³²⁶

140. Het HvJ oordeelde daarnaast dat een algemene toegang tot alle bewaarde gegevens, zelfs voor redenen van nationale veiligheid, niet kan worden geacht tot het strikt noodzakelijke te zijn beperkt.³²⁷ Een nationale regeling voor toegang tot bewaarde gegevens dient derhalve duidelijke en nauwkeurige regels te bevatten die de reikwijdte en de toepassing van de betrokken maatregel

³²⁰ Verzoek de Hoge Raad der Nederlanden van 6 april 2022 in de zaak C-241/22.

³²¹ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/premier ministre', § 110; HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790, 'Privacy International/Secretary of State for Foreign and Commonwealth Affairs'; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', § 32; HvJ 21 juni 2022, C-817/19, ECLI:EU:C:2022:491, 'Ligue des droits humains', § 113.

³²² Bijlage 3.

³²³ HvJ 5 april 2022, C-140/20, ECLI:EU:C:2022:258, 'Commissioner of An Garda Síochána' § 98; HvJ 20 september 2022, C-793/19 en C-197/19, ECLI:EU:C:2022:702, 'SpaceNet en Telekom Deutschland', § 128; DE KEERSMAECKER R. en VAN DE HEYNING C. 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *T.Strafr.* 2021/4, (171) 185 -186.

³²⁴ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 166; HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790, 'Privacy International/Secretary of State for Foreign and Commonwealth Affairs', § 78; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', §§ 34-35; ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 19; DE KEERSMAECKER R. en VAN DE HEYNING C. 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *T.Strafr.* 2021/4, (171) 185.

³²⁵ JANSSEN J., 'Bewaren of beware: dataretentie en grondrecht, een moeilijk evenwicht (noot onder GwH 22 april 2021)', *R.A.B.G.* 2021/8, (673) 673-681.

³²⁶ HvJ 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788, 'Ministerio Fiscal', § 55; HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 131; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', § 32.

³²⁷ HvJ 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, 'Tele2 Sverige AB', § 119; HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790, 'Privacy International/Secretary of State for Foreign and Commonwealth Affairs', § 79-81; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', § 50.

vastleggen en minimumvereiste opleggen, zodat voldoende waarborgen geboden worden tegen misbruik.³²⁸ Die bepaling dient op basis van objectieve criteria, waaronder materiële en procedurele voorwaarden, vast te stellen in welke omstandigheden en onder welke voorwaarden toegang aan de bevoegde autoriteiten kan worden verleend, teneinde te waarborgen dat deze toegang niet verder reikt dan strikt noodzakelijk.³²⁹ In dit licht bepaalde het HvJ dat in beginsel voor het doel van bestrijding van criminaliteit de toegang slechts kan worden verleend tot de gegevens van personen die ervan worden verdacht een ernstig misdrijf te plannen, te plegen of te hebben gepleegd of op de een of andere wijze betrokken te zijn bij een dergelijk misdrijf. In bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd, zou echter ook toegang tot de gegevens van andere personen kunnen worden verleend, wanneer op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren.³³⁰

141. Tot slot bepaalt het HvJ dat voorafgaand aan de toegang tot de bewaarde gegevens er een controle door een rechter of een administratieve autoriteit uitgeoefend dient te worden, die objectief, onpartijdig en een derde dient te zijn.³³¹ Dit betekent dat de instantie zelf niet betrokken mag zijn in het onderzoek en een neutrale positie dient in te nemen ten aanzien van de betrokkenen in de zaak.³³²

Afdeling 2: Dataretentiewet

142. De wetgever heeft een aparte wettelijke bepaling gecreëerd binnen de dataretentiewet die bepaalt wie toegang heeft tot de bewaarde gegevens.³³³ Het artikel start met een opsomming wat onder 'ernstige criminaliteit' valt. De invulling van wat onder dat begrip wordt verstaan heeft namelijk een impact op de actoren die toegang hebben tot de bewaarde gegevens. In de eerste plaatst heeft het begrip betrekking op misdrijven waarvan ernstige aanwijzingen bestaan dat het strafbaar is met een minimale correctionele hoofdgevangenisstraf van één jaar.³³⁴ Ook feiten die kunnen leiden tot

³²⁸ HvJ 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, 'Digital Rights Ireland', § 54-55; HvJ 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, 'Tele2 Sverige AB', § 117; HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 132; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', § 48.

³²⁹ HvJ 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, 'Digital Rights Ireland', § 61; HvJ 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, 'Tele2 Sverige AB', § 118; HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790, 'Privacy International/Secretary of State for Foreign and Commonwealth Affairs', § 77; HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 166-167, 176 en 155-156; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', § 49; JANSSEN J., 'Bewaren of beware: dataretentie en grondrecht, een moeilijk evenwicht (noot onder GwH 22 april 2021)', *R.A.B.G.* 2021/8, (673) 673-681.

³³⁰ HvJ 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, 'Tele2 Sverige AB', § 119; HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790, 'Privacy International/Secretary of State for Foreign and Commonwealth Affairs', § 78-80; HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 188; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', §§ 41, 50; JANSSEN J., 'Bewaren of beware: dataretentie en grondrecht, een moeilijk evenwicht (noot onder GwH 22 april 2021)', *R.A.B.G.* 2021/8, (673) 673-681.

³³¹ HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', §§ 51-53; DE KEERSMAECKER R. en VAN DE HEYNING C. 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *T.Strafr.* 2021/4, (171) 187.

³³² HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', § 54.

³³³ Art. 127/1 WEC.

³³⁴ Art. 127/1, §1, 1° WEC.

een sanctie van niveau 5 of 6 zoals bedoeld in artikel XV.70 WER en feiten die een inbreuk vormen op artikel 14 en 15 Verordening Marktmisbruik vallen onder het begrip.³³⁵ Echter wordt de deur opengelaten om het begrip in de toekomst verder aan te vullen.³³⁶ In tegenstelling tot de regeling inzake de bewaarplicht, wordt het begrip 'ernstige criminaliteit' door de wetgever hier expliciet omschreven. Wat betreft de eerste categorie van misdrijven, feiten waarvoor ernstige aanwijzingen bestaan dat zij strafbaar zijn met minstens één jaar correctionele hoofdgevangenisstraf, kan worden opgemerkt dat deze drempel relatief laag ligt. Daardoor vallen ook minder ernstige feiten onder het begrip 'ernstige criminaliteit', wat niet in overeenstemming is met de rechtspraak van het HvJ (Cf. *supra*, nr. 139). Dit wordt des te problematischer in het licht van de hervorming van het Strafwetboek, waarin strafmaten worden herzien en ondergebracht in strafniveaus.

143. De toegang is niet enkel afhankelijk van het begrip 'ernstige criminaliteit', maar wordt ook gekoppeld aan de aard van de bewaarde gegevens. Zo is toegang tot de identificatiegegevens mogelijk voor de meeste actoren, zoals de autoriteiten die wettelijk gemachtigd zijn om data te hergebruiken voor doeleinden van wetenschappelijk of historisch onderzoek of voor statistische doeleinden of gerechtelijke autoriteiten die criminaliteit in het algemeen bestrijden.³³⁷ Voor de andere communicatiegegevens, zoals de verkeers- en locatiegegevens en de IP-adressen is de toegang beperkter. Met betrekking tot die gegevens kunnen enkel inlichtingen- en veiligheidsdiensten, bevoegde autoriteiten die optreden ter waarborging van de openbare veiligheid, de autoriteiten die de vitale belangen van natuurlijke personen vrijwaren, de administratieve of gerechtelijke autoriteiten die zware criminaliteit bestrijden en de autoriteiten die controle uitoefenen op de gegevensbescherming, toegang krijgen.³³⁸

144. Aan de procedurele en materiële voorwaarden die opgelegd dienen te worden, besteedt de Belgische wetgever minder aandacht. Zo werkte de wetgever de beperking van de toegang tot de strikt noodzakelijke gegevens niet uit in de dataretentiewet. Een loutere verwijzing wordt gemaakt naar een 'formele wettelijke norm'.³³⁹ Deze dient de categorie of categorieën van operatoren waaraan de autoriteit gegevens kan vragen, de categorieën van gegevens die mogen gevraagd worden, de beoogde doeleinden en de mechanismen ter controle van het verzoek door een rechterlijke instantie of door een onafhankelijke administratieve autoriteit, te preciseren.³⁴⁰

145. Deze 'formele wettelijke norm' heeft betrekking op de artikelen 46bis en 88bis Sv.³⁴¹ Op basis van artikel 46bis Sv. kan namelijk de PdK de toegang tot identificatiegegevens machtigen in het kader van wanbedrijven en misdaden (Cf. *supra*, nrs. 40-44). Artikel 88bis Sv. verleent de bevoegdheid aan de onderzoeksrechter om toegang te verschaffen tot verkeers- en locatiegegevens

³³⁵ Art. 127/1, §1, 2° en 3° WEC.

³³⁶ Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001, 100.

³³⁷ Art. 127/1, §2, 8° en 10°, en §3 WEC.

³³⁸ Art. 127/1, §2, 1°-3°, 6° en 9°, §3, lid 4, §4, lid 2 WEC.

³³⁹ Art. 127/1, §§ 2-5 WEC.

³⁴⁰ Art. 127/1, § 5, lid 1 WEC.

³⁴¹ DE KEERSMAECKER R. en VAN DE HEYNING C. 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *T.Strafr.* 2021/4, (171) 187-188.

indien er ernstige aanwijzingen zijn dat de strafbare feiten een correctionele hoofdgevangenisstraf van één jaar of zwaarder tot gevolg kunnen hebben (Cf. *supra*, nrs. 45-51).

Artikel 88bis Sv. is o.i. echter niet volledig in overeenstemming met de rechtspraak van het HvJ. Voor de toegang tot deze gegevens is expliciet bepaald dat toegang slechts is toegestaan voor de bestrijding van ernstige criminaliteit en het waarborgen van de openbare en nationale veiligheid. De rechtsleer³⁴² bekritiseert terecht of de in artikel 88bis Sv. opgesomde misdrijven daadwerkelijk als 'ernstig' kunnen worden gekwalificeerd, maar gaat volgens ons voorbij aan een ander cruciaal punt: het HvJ stelt duidelijk dat er steeds een concrete verdenking moet zijn tegen een specifieke persoon die het misdrijf heeft gepleegd. Bij een letterlijke lezing van artikel 88bis Sv. kan echter toegang worden verkregen tot gegevens van alle personen, zodra er een aanwijzing is van een concreet misdrijf. De Belgische wet lijkt genoeg te nemen met ernstige aanwijzingen over een 'ernstig misdrijf', terwijl het HvJ vereist dat er een ernstige aanwijzing is tegen een specifieke persoon. Het enkele feit dat een bepaald misdrijf is gepleegd, biedt op zichzelf onvoldoende grondslag voor de verkrijging van gegevens van alle personen. Bij afwezigheid van een duidelijk gedefinieerde reikwijdte zou dit wetshandhavers in staat stellen een aanzienlijke en ongecontroleerde beoordelingsvrijheid uit te oefenen, hetgeen hen de mogelijkheid zou bieden persoonlijke gegevens van burgers te doorzoeken in een onbeperkte zoektocht naar belastende informatie.³⁴³

Afdeling 3: Toegang door opsporingsautoriteiten bij zoektermbevelen

146. Zoektermbevelen zullen slechts effectief zijn indien opsporingsautoriteiten toegang kunnen verkrijgen tot de zoekopdracht van de gebruiker, de datum en tijd waarop de zoekopdracht werd uitgevoerd, het apparaattype, ... Zoals reeds uiteengezet heeft het HvJ zich niet expliciet uitgesproken over een bewaarplicht en toegang tot de zoekgeschiedenissen en daaraan gekoppelde gegevens van individuen (Cf. *supra*, nr. 126). Gelet op de gelijkaardige aard van de inmenging kan echter worden verdedigd dat de voorwaarden en beperkingen die het HvJ stelt aan de toegang tot metadata, mutatis mutandis ook van toepassing zijn op de toegang tot zoekgeschiedenis en de daaraan gekoppelde gegevens.

147. Zoektermbevelen verlopen in de VSA in drie fasen (Cf. *supra*, nr. 23). De tweede fase betreft het opvragen van identificatiegegevens van personen die naar een bepaalde zoekterm hebben gezocht. Voor deze stap bestaat reeds een gedetailleerd wettelijk kader, met name artikel 46bis Sv. (Cf. *supra*, nrs. 40-44). Om die reden wordt in het kader van deze analyse het aspect van de toegang tot identificatiegegevens verder buiten beschouwing gelaten.

³⁴² ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 8-11 en 14; ROYER S. en VERBRUGGEN F., 'Tussen helder en donker: mooie zebra of grijze ezel? Veiligheid en privacy via transparantie en opaciteit 20 jaar later' in DE HERT P. en GUTWIRTH S. (eds.), *Strafrecht in dialoog*, Intersentia, 2023, (133) 141; DE KEERSMAECKER R. en VAN DE HEYNING C. 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *T.Strafr.* 2021/4, (171) 186.

³⁴³ STENDER S., 'Circumventing the fourth amendment: the unconstitutional nature of geofence warrants', *U. L. Rev.* 2024/3, (733) 751.

148. Naar analogie met de rechtspraak van het HvJ zou een algemene toegang tot alle bewaarde gegevens met betrekking tot zoekgeschiedenissen, evenals de daarmee samenhangende gegevens niet toelaatbaar zijn (Cf. *supra*, nr. 140). Het is van essentieel belang dat de nationale regelgeving objectieve criteria vastlegt die bepalen in welke omstandigheden en onder welke voorwaarden toegang tot deze gegevens aan de bevoegde autoriteiten kan worden verleend.

149. Aansluiting kan worden gezocht bij de reeds uitgewerkte dataretentiewet. Het is aanbevolen dat toegang tot IP-adressen, zoekgeschiedenissen en daaraan gekoppelde metadata, slechts mogelijk is in het kader van de bestrijding van ernstige criminaliteit en het waarborgen van de openbare en nationale veiligheid (Cf. *supra*, nr. 142). Met betrekking tot de toegang door bevoegde instanties wordt aanbevolen de toegangsgraad af te stemmen op de gevoeligheid van de gegevens: naarmate de gegevens indringender zijn, dient de toegang restrictiever te worden geregeld. Voor gevoelige gegevens, zoals volledige zoekgeschiedenissen en IP-adressen, verdient het aanbeveling de toegang te beperken tot een selecte groep bevoegde instanties, waaronder inlichtingen- en veiligheidsdiensten, autoriteiten belast met openbare veiligheid, instellingen die vitale belangen beschermen, gerechtelijke autoriteiten belast met de bestrijding van zware criminaliteit, en toezichthoudende gegevensbeschermingsautoriteiten (Cf. *supra*, nr. 143).³⁴⁴

150. Teneinde de toegang tot de bewaarde gegevens daadwerkelijk te beperken tot hetgeen strikt noodzakelijk is, dienen bijkomende materiële en procedurele waarborgen te worden voorzien. Het is aangewezen om dergelijke waarborgen op te nemen in een afzonderlijke formele wettelijke bepaling in het Wetboek van Strafvordering. Deze moet duidelijke voorwaarden vastleggen voor de toegang door opsporingsautoriteiten in het kader van zoektermbevelen, evenals voor de reikwijdte en toepassing van de maatregel. Zo wordt ondubbelzinnig bepaald onder welke omstandigheden en voorwaarden toegang tot zoekgeschiedenissen en bijhorende metadata is toegelaten.

151. De bepaling moet in eerste instantie duidelijk aangeven op welke gronden een zoektermbevel kan worden gebaseerd. Toegang tot zoekgeschiedenissen en bijhorende metadata is enkel toelaatbaar ter bescherming van de nationale veiligheid, de bestrijding van ernstige misdrijven en bij ernstige verstoring van de openbare orde. Voor de afbakening van misdrijven die onder 'ernstige criminaliteit' vallen, verdient het aanbeveling aan te sluiten bij een lijst vergelijkbaar met de taplijst van artikel 90ter, §§ 2-4 Sv., die een objectieve en wettelijk verankerde basis biedt. Een vaste lijst biedt meer rechtszekerheid dan open normen of een strafdrempel, gezien haar voorafgaande beoordeling van de ernst van de misdrijven. Hierbij moet wel opnieuw de nodige nuance in acht worden genomen, en dienen bepaalde feiten, zoals informaticabedrog, private omkoping en heling, uitgesloten te worden om de proportionaliteit te waarborgen (Cf. *supra*, nrs. 108 en 120).

152. Een algemene toegang tot alle zoekgeschiedenissen is niet toegestaan, aangezien autoriteiten niet willekeurig alle zoekopdrachten kunnen doorzoeken in de hoop een verdachte te identificeren. Een dergelijke brede toegang zou immers neerkomen op een vorm van massasurveillance, wat als disproportioneel moet worden beschouwd. In het licht van de rechtspraak

³⁴⁴ Art. 127/1, §2, 1^o-3^o, 6^o en 9^o, §3, lid 4, §4, lid 2 WEC.

van het HvJ verdient aanbeveling dat de toegang tot zoekgeschiedenissen en daaraan gekoppelde gegevens beperkt blijft tot personen ten aanzien van wie concrete aanwijzingen bestaan dat zij betrokken zijn bij een misdrijf. Uitzonderlijk kan toegang tot gegevens van andere personen worden overwogen, mits objectief wordt gemotiveerd waarom die gegevens essentieel zijn voor het onderzoek (Cf. *supra*, nr. 140).³⁴⁵ In de wettelijke bepaling aangaande zoektermbevelen dient daarom expliciet bepaald te worden dat toegang enkel mogelijk is ten aanzien van personen, of informaticasystemen die geregeld worden gebruikt door personen, die op grond van precieze aanwijzingen ervan verdacht worden een strafbaar feit te hebben gepleegd of voorbereidt.³⁴⁶ Ingeval van bijzondere situaties, zoals die waarin de vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid worden bedreigd, kan de maatregel betrekking hebben op andere personen of informaticasystemen, mits op grond van objectieve elementen kan worden aangetoond dat de hieruit voortvloeiende gegevens een daadwerkelijke bijdrage kunnen leveren tot de bestrijding van dergelijke activiteiten.³⁴⁷

153. Dit roept fundamentele vragen op over de verenigbaarheid van zoektermbevelen met het vereiste van een concrete individuele verdenking. Hoewel dergelijke bevelen net gericht zijn op het identificeren van een onbekende dader, vereist het HvJ dat toegang tot communicatiegegevens in beginsel beperkt blijft tot personen tegen wie reeds concrete aanwijzingen bestaan. Het HvJ maakt daarbij duidelijk dat algemene toegang, los van individuele verdenking, onverenigbaar is met het evenredigheidsbeginsel en het recht op gegevensbescherming. Hierdoor lijkt het zoektermbevel, in zijn klassieke vorm, moeilijk verzoenbaar met het Europese toetsingskader.

154. Een alternatieve benadering die deze voorwaarde tracht te nuanceren, stelt dat bij het gebruik van scherp afgebakende zoektermen een redelijke waarschijnlijkheid kan ontstaan dat de dader van een bekend, maar onopgelost misdrijf identificeerbaar is via de gezochte digitale gegevens. Die waarschijnlijkheid hangt af van de specificiteit van de gebruikte zoekparameters en de aannemelijkheid dat deze hoofdzakelijk of uitsluitend door de dader zijn gebruikt. Naarmate het aantal potentiële gebruikers of apparaten waarop de zoekopdracht slaat toeneemt, vermindert die waarschijnlijkheid en groeit het risico op het verzamelen van een massa irrelevante gegevens.³⁴⁸ Met andere woorden: doordat in het zoektermbevel gebruik wordt gemaakt van voldoende specifiek afgebakende zoektermen, ontstaat er een redelijke waarschijnlijkheid dat de dader geïdentificeerd kan worden, precies omdat verwacht mag worden dat enkel de dader, en niet het brede publiek, deze zoekopdracht zal hebben ingevoerd. De gedachte is dat voldoende afgebakende termen impliciet tot een gerichte maatregel leiden, ook al is de verdachte formeel niet gekend. Hoewel deze interpretatie het bevel een schijn van gerichtheid geeft, ondermijnt zij de logica van het HvJ en is het weinig waarschijnlijk dat deze redenering standhoudt.

³⁴⁵ Zie redenering bij verkeers- en locatiegegevens: HvJ 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, 'Tele2 Sverige AB', § 119; HvJ 6 oktober 2020, C-623/17, ECLI:EU:C:2020:790, 'Privacy International/Secretary of State for Foreign and Commonwealth Affairs', §§ 78-80; HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/Premier ministre', § 188; HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', § 50; JANSSEN J., 'Bewaren of beware: dataretentie en grondrecht, een moeilijk evenwicht (noot onder GwH 22 april 2021)', *R.A.B.G.* 2021/8, (673) 673-681.

³⁴⁶ Naar analogie met art. 90ter, §1, lid 4 en art. 46quinquies, §3 Sv.

³⁴⁷ Naar analogie met art. 90ter, §1, lid 4 Sv.

³⁴⁸ Zie inspiratie Amerika inzake probable cause: FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Tex. L. Rev.* 2024/5, (877) 922, 929-931, 933.

155. Het verdient aanbeveling dat de wettelijke regeling inzake zoektermbevelen expliciet voorziet in duidelijke waarborgen met betrekking tot de omstandigheden waaronder een dergelijk bevel kan worden uitgevaardigd, teneinde te verzekeren dat de toegang tot gegevens niet verder reikt dan strikt noodzakelijk. Zo dient te worden bepaald dat een zoektermbevel uitsluitend kan worden ingezet indien er ernstige aanwijzingen bestaan dat het een strafbaar feit betreft dat verband houdt met de nationale of openbare veiligheid, dan wel met ernstige criminaliteit.³⁴⁹ Voorts verdient het aanbeveling te voorzien in de vereiste dat verifieerbare aanwijzingen bestaan waaruit blijkt dat de gebruikte zoekterm een rechtstreeks verband houdt met de voorbereiding of uitvoering van dat misdrijf. Een bevel mag in geen geval gebaseerd zijn op louter hypothetische risico's, noch resulteren in een algemene of ongerichte monitoring van zoekgedrag. Daarnaast wordt aanbevolen te bepalen dat een zoektermbevel slechts kan worden uitgevaardigd indien het onderzoek zulks vereist.³⁵⁰ Verder wordt aanbevolen dat enkel gebruik wordt gemaakt van een zoektermbevel wanneer andere opsporingsmethoden tekortschieten om de waarheid aan de dag te brengen.³⁵¹ Tot slot verdient het aanbeveling het proportionaliteitsvereiste expliciet te verankeren, onder meer door te bepalen dat de gebruikte zoektermen voldoende specifiek moeten zijn om willekeurige of buitensporige gegevensverzameling te vermijden, om zo een evenwicht te waarborgen tussen de belangen van de opsporing en de bescherming van de persoonlijke levenssfeer van de betrokkenen. Op deze manier worden de noodzakelijkheids-, proportionaliteits- en subsidiariteitsvereisten nageleefd.

156. De bepaling dient daarnaast de categorieën van operatoren en gegevens aan te duiden waarop een zoektermbevel betrekking kan hebben. Daarbij dient expliciet te worden voorzien dat medewerking kan worden gevorderd van zoekmachinebedrijven en van elke entiteit die op Belgisch grondgebied, op welke wijze ook, een dienst aanbiedt waarmee gebruikers zoekopdrachten kunnen uitvoeren.³⁵² Door naast de klassieke term ook een algemene functionele omschrijving op te nemen, worden toekomstige technologieën of atypische diensten met gelijkaardige functionaliteiten mee gedekt, zelfs indien zij zich niet formeel als 'zoekmachinebedrijf' profileren. Voorts moet worden gespecificeerd dat het bevel betrekking kan hebben op de ingevoerde zoektermen, alsook op metadata zoals datum, tijdstip, locatie, gebruikte browser, apparaattype en IP-adres van het gebruikte informatiesysteem.³⁵³

157. Voorts verdient het aanbeveling om in de wettelijke bepaling duidelijke grenzen te stellen aan de duur van een zoektermbevel. Zoektermbevelen zijn in de eerste plaats gericht op het retrospectief analyseren van zoekopdrachten die tijdens de voorbereidingsfase van een misdrijf werden ingevoerd (Cf. *supra*, nr. 21). Aangezien daders zelden na het plegen van het misdrijf nog gelijkaardige zoektermen gebruiken, verdient het aanbeveling om de toegangsperiode in principe te beperken tot een concreet afgebakende termijn voor het misdrijf. Alleen wanneer er gegronde redenen bestaan om aan te nemen dat de dader ook nadien nog relevante zoekopdrachten uitvoert,

³⁴⁹ Naar analogie met art. 88bis, §1, lid 1, art. 46quinquies, §1, lid 1 en art. 90ter, §1, lid 2 Sv.

³⁵⁰ Naar analogie met art. 90ter, §1, lid 2 Sv.

³⁵¹ Naar analogie met art. 88bis, §1, lid 1, art. 46quinquies, §1, lid 1 en art. 90ter, §1, lid 2 Sv.

³⁵² Naar analogie met art. 88bis, §1, lid 2, gedachtestreepje 1 en 2 en art. 90quater, §2, gedachtestreepje 1 en 2 Sv.

³⁵³ Naar analogie met art. 88bis, §1, lid 1, 1° en 2°, art. 46quinquies, §1, lid 2 en art. 90ter, §1, lid 1 Sv.

kan overwogen worden om toegang toe te staan tot gegevens van na het misdrijf. Hoe ver men terug in de tijd mag gaan, hangt af van de onderliggende juridische grondslag. In het kader van nationale veiligheid of openbare orde kan een periode van twaalf maanden gerechtvaardigd zijn. Bij ernstige criminaliteit lijkt een kortere termijn, zoals negen maanden, meer aangewezen.³⁵⁴

158. Tot slot dient de bepaling duidelijk de instantie te vermelden die voorafgaand de toegang tot de bewaarde gegevens kan machtigen. In het Belgisch strafprocesrecht verdient het aanbeveling dat de onderzoeksrechter bij uitstek bevoegd is om zoektermbevelen te machtigen, aangezien hij als onafhankelijke en onpartijdige instantie toezicht houdt op de rechtmatigheid, noodzakelijkheid en proportionaliteit van onderzoeksmethoden binnen het gerechtelijk onderzoek en de mini-instructie.³⁵⁵ Daarbij wordt aanbevolen dat de onderzoeksrechter, middels een met redenen omklede schriftelijke beslissing, expliciet motiveert op welke wijze de maatregel voldoet aan deze vereisten. In die beslissing zouden minstens de volgende elementen moeten worden opgenomen: de juridische grondslag en feitelijke omstandigheden die het bevel rechtvaardigen, de reikwijdte ervan - waaronder een voldoende afgebakende en gedetailleerde omschrijving van de betrokken zoektermen en een aanduiding van de zoekmachinebedrijven waarop het bevel betrekking heeft -, de proportionaliteit met inachtneming van de persoonlijke levenssfeer, evenals een verantwoording waarom minder ingrijpende alternatieven niet volstaan.³⁵⁶ Voorts verdient het aanbeveling dat steeds een inschatting wordt gemaakt van de operationele haalbaarheid van de maatregel, bijvoorbeeld door aan te geven dat het waarschijnlijk is dat de verdachte de betrokken zoektermen heeft ingevoerd. Tot slot dient ook de periode in het verleden waarover de vordering zich uitstrekt te worden vermeld.³⁵⁷

Het HvJ verduidelijkte in het arrest Prokuratuur dat het Openbaar Ministerie deze waarborg niet biedt, aangezien deze optreedt als openbaar aanklager en immers niet tot taak heeft om een geschil in volledige onafhankelijkheid te beslechten.³⁵⁸ Enkel in strikt afgebakende uitzonderingsgevallen, zoals bij heterdaad of in het kader van een mini-instructie, zou overwogen kunnen worden om deze bevoegdheid bij wijze van uitzondering toe te kennen aan de Pdk.³⁵⁹

§ 4: Tussenconclusie

159. De voorwaarden die het HvJ stelt aan de bewaring van online gegevens en de toegang daartoe door opsporingsautoriteiten, voortvloeiend uit het recht op privacy en gegevensbescherming zoals versterkt door de AVG, dreigen de effectiviteit van zoektermbevelen aanzienlijk te ondergraven. Voor een effectieve toepassing is het immers vereist dat relevante gegevens bewaard blijven en toegankelijk zijn, wat onder het huidige juridisch kader slechts onder strikte grenzen mogelijk is.

³⁵⁴ Naar analogie met art. 88bis, §2, gedachtestreepje 1 en 2 Sv.

³⁵⁵ VERSTRAETEN R. en VERBRUGGEN F., *Strafrecht en strafprocesrecht voor bachelors*, Intersentia, 2020, 154.

³⁵⁶ Naar analogie met art. 88bis, §1, lid 4 Sv. en art. 90quater, §1, lid 1 en 2, 1°-3° Sv.

³⁵⁷ Naar analogie met art. 88bis, §1, lid 5 Sv. en art. 90quater, §1, lid 1 en 2, 4° Sv.

³⁵⁸ HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur', §§ 55-57.

³⁵⁹ Naar analogie met art. 88bis, §1, lid 6-8 en art. 90ter, §5 Sv.

160. Een algemene bewaarplicht voor zoekmachinebedrijven, noodzakelijk om te verzekeren dat zoekgeschiedenissen en gerelateerde metadata beschikbaar blijven, stuit op aanzienlijke beperkingen in de rechtspraak van het HvJ. Dergelijke gegevens kunnen slechts algemeen worden bewaard in het licht van de nationale veiligheid. Voor doeleinden zoals de bestrijding van ernstige criminaliteit en openbare orde is enkel een gerichte bewaarplicht toelaatbaar, mits afgebakend aan de hand van objectieve criteria, zoals geografische of personele afbakening. Omdat zoektermbevelen voornamelijk worden ingezet bij onderzoeken naar onbekende daders, is een personele afbakening niet werkbaar. Een geografische afbakening lijkt dan meer aangewezen, maar beperkt de bewaring tot zoekopdrachten die binnen die zones worden uitgevoerd of betrekking hebben op locaties binnen die zones. Daardoor vallen zoekopdrachten buiten het geselecteerde geografische kader uit de bewaring, wat ertoe leidt dat potentieel cruciale informatie verloren gaat.

161. Ook de toegang tot bewaarde gegevens is strikt begrensd. Ze moet doelgebonden zijn, met dezelfde of een zwaardere doelstelling als de bewaring, en gericht, op basis van objectieve criteria. In het kader van ernstige criminaliteit vereist het HvJ bovendien dat toegang slechts wordt verleend bij concrete aanwijzingen jegens specifieke personen. Omdat zoektermbevelen net gericht zijn op de identificatie van onbekende daders, laten zij geen toegang toe op basis van vooraf geïdentificeerde personen. In de praktijk blijven ze daardoor beperkt tot uitzonderlijke situaties waarin vitale belangen, zoals nationale of openbare veiligheid, in het geding zijn. Hun operationele waarde voor de reguliere strafrechtspleging wordt zo nagenoeg uitgehold.

162. Naar onze mening wordt in de huidige rechtspraak geen adequaat evenwicht gevonden tussen enerzijds het recht op privacy en anderzijds de noodzaak tot misdaadbestrijding. De belangenafweging slaat onevenredig door in het voordeel van de bescherming van de persoonlijke levenssfeer. Gezien het toenemend gebruik van digitale middelen voor criminele doeleinden, is het noodzakelijk dat ook digitale opsporingsinstrumenten proportioneel kunnen worden ingezet. De huidige strenge toetsingsmaatstaf ondermijnt die mogelijkheid en roept vragen op over haar houdbaarheid binnen een rechtssysteem dat onder toenemende maatschappelijke druk staat.³⁶⁰

163. Hoe het HvJ zich uiteindelijk over zoektermbevelen zal uitspreken, blijft onzeker. Daarbij rijst de vraag of de bestaande strikte voorwaarden onverkort van toepassing moeten zijn, aangezien zoektermbevelen zich kenmerken door een beperkte inbreuk op de levenssfeer: ze betreffen specifiek afgebakende zoektermen en geven geen toegang tot volledige zoekgeschiedenissen. Hoewel zij potentieel een grote groep gebruikers raken, blijft hun impact beperkt.

³⁶⁰ LEFEVRE L., 'Golf van verontwaardiging na verkrachtingszaak Leuven: "Onevenwicht tussen leed van slachtoffer en gevolgen voor dader"', *VRT nws* 2 april 2025, <https://www.vrt.be/vrtnws/nl/2025/04/02/verontwaardiging-rond-verkrachtingszaak-leuven-is-groot/> (geraadpleegd op 15 mei 2025); MARTIN M., "We willen de Reuzegommers niet alleen juridisch, maar ook moreel veroordeeld zien": waarom de woede over het proces-Sanda Dia blijft', *DeMorgen* 30 mei 2023, <https://www.demorgen.be/nieuws/we-willen-de-reuzegommers-niet-alleen-juridisch-maar-ook-moreel-veroordeeld-zien-waarom-de-woede-over-het-proces-sanda-dia-blijft~b348d84f/> (geraadpleegd op 15 mei 2025); GJS, 'Minister Geens reageert op kritiek na moord op Julie Van Espen: "Ik blijf ijveren voor een betere justitie"', *Nieuwsblad* 11 februari 2020, https://www.nieuwsblad.be/cnt/dmf20200211_04843606 (geraadpleegd op 15 mei 2025).

Hoofdstuk IV. Van zoekbalk naar bewijsstuk: artikel 8 EVRM en de grenzen van privacy en gegevensbescherming in strafonderzoek

165. Zoals eerder uiteengezet, bestaan op supranationaal niveau diverse rechtsinstrumenten ter bescherming van het recht op privacy en gegevensbescherming. Deze zijn bijzonder relevant in het kader van online opsporingsmethoden, die potentieel ingrijpen in deze fundamentele rechten. Het vorige hoofdstuk behandelde de benadering binnen de Europese Unie. Dit hoofdstuk richt zich op het normatief kader van het Europees Verdrag voor de Rechten van de Mens, dat dezelfde rechten beschermt, maar met eigen accenten en toetsingscriteria.

166. In het kader van het Europees Verdrag voor de Rechten van de Mens vormt artikel 8 het centrale referentiepunt voor de beoordeling van inmengingen in het recht op privacy en gegevensbescherming. Het Europees Hof voor de Rechten van de Mens aanvaardt dat online onderzoeksmaatregelen, gelet op digitalisering en technologische ontwikkelingen, noodzakelijk kunnen zijn voor de bestrijding van criminaliteit en identificatie van daders. Dergelijke inmengingen zijn echter slechts toelaatbaar indien zij voldoen aan strikte voorwaarden ter voorkoming van willekeur en misbruik. Hoewel het Hof zich (nog) niet expliciet heeft uitgesproken over de juridische toelaatbaarheid van zoektermbevelen, is het essentieel om de bestaande rechtspraak inzake het recht op privacy en gegevensbescherming grondig te analyseren. De daarin ontwikkelde criteria zijn bepalend voor de invulling van de grenzen en voorwaarden waaraan zoektermbevelen in de toekomst zullen moeten beantwoorden.

§ 1: Reikwijdte artikel 8 EVRM

167. Het recht op privacy en gegevensbescherming wordt beschermd aan de hand van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM).³⁶¹ Op basis van die bepaling heeft eenieder recht op eerbiediging van zijn privéleven, gezinsleven, woning en briefwisseling.³⁶² Geen van deze vier belangen worden gedefinieerd in het Verdrag. Echter wordt er voor deze verdragsuitdrukkingen steeds een autonoom concept gehanteerd. Steunend op de doctrine van het “levend instrument” definieert het Hof voor de Rechten van de mens (hierna: EHRM) de reikwijdte van het artikel ruim, in lijn met sociale en technologische ontwikkelingen die zich voortdoen in onze samenleving.³⁶³ Uit de rechtspraak blijkt dat een brede waaier aan kwesties onder de bescherming van artikel 8 valt, zoals geslachtsidentiteit, huiszoeking en inbeslagname, gegevensbescherming en milieuproblematiek.³⁶⁴

³⁶¹ VANDE LANOTTE J., GOEDERTIER G., HAECK Y., GOOSSENS J. en DE PELSMAEKER T., *Belgisch publiekrecht (Boekdelen 1 en 2)*, die Keure, 2015, 450; 452; HARRIS D. J., O’BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 511.

³⁶² Art. 8.1 EVRM.

³⁶³ HARRIS D. J., O’BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 509.

³⁶⁴ EHRM 27 juni 2017, 931/13, ECLI:CE:ECHR:2017:0627JUD000093113, ‘Satakunnan Markkinapörssi Oy en Satamedia Oy/Finland’; EHRM 24 juni 2019, 54414/13 en 54264/15, ECLI:CE:ECHR:2019:0124JUD005441413, ‘Cordella e.a./Italië’; EHRM 8 juni 2022, 53069/15, ECLI:CE:ECHR:2022:0308JUD005306915, ‘Sabani/België’; EHRM 8 september 2022, 3153/16 en 27758/18, ECLI:CE:ECHR:2022:0908JUD000315316, ‘Drelon/Frankrijk’.

168. Politionele onderzoeksdaten kunnen een inmenging vormen in het recht op eerbiediging van privé-, familie- en gezinsleven, met name wanneer persoonsgegevens worden verzameld, geraadpleegd, opgeslagen of verwerkt in het kader van een strafrechtelijk onderzoek.³⁶⁵ De bescherming van deze gegevens vormt een essentieel onderdeel van artikel 8 EVRM.³⁶⁶ Elke verwerking³⁶⁷ van informatie over een geïdentificeerde of identificeerbare persoon³⁶⁸ valt onder deze bescherming, ongeacht of het gaat om rechtstreeks verstrekte gegevens, zoals gebruikersnaam of leeftijd, of om indirect verkregen gegevens, zoals zoekgeschiedenis of locatiegegevens.³⁶⁹ Voorbeelden hiervan zijn het opvragen van abonneegegevens die gekoppeld zijn aan een IP-adres of het verzamelen en bewaren van GPS-gegevens die iemands verplaatsingen aanduiden.³⁷⁰

169. Niet elke verwerking van persoonsgegevens valt evenwel onder de reikwijdte van artikel 8 EVRM. Volgens de rechtspraak van het EHRM is dit slechts het geval wanneer sprake is van een redelijke verwachting van privacy.³⁷¹ In de meeste gevallen waarin persoonsgegevens worden verwerkt met het oog op een strafrechtelijk onderzoek of het verzamelen van bewijs voor gerechtelijke procedures, heeft het EHRM echter geoordeeld dat dergelijke verwerkingen binnen de werkingssfeer van artikel 8 vallen en een inmenging in het privéleven van de betrokkene uitmaken.³⁷²

³⁶⁵ EHRM 2 augustus 1984, 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179, 'Malone/Verenigd Koninkrijk'; EHRM 26 maart 1987, 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881, 'Leander/Zweden', § 48; EHRM 28 oktober 1994, 14310/88, ECLI:CE:ECHR:1994:1028JUD001431088, 'Murray/Verenigd Koninkrijk', §§ 84-86; EHRM 16 februari 2000, 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, 'Amann/Zwitserland', § 65; EHRM 4 mei 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, 'Rotaru/Roemenië', §§ 46; EHRM 25 september 2001, 44787/98, ECLI:CE:ECHR:2001:0925JUD004478798, 'P.G. en J.H./Verenigd Koninkrijk', § 42; EHRM 4 december 2008, 30562/04, 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, 'S. en Marper/Verenigd Koninkrijk', § 67; EHRM 10 maart 2009, 4378/02, ECLI:CE:ECHR:2009:0310JUD000437802, 'Bykov/Rusland'; EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, 'Uzun/Duitsland'; EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland'; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence, 31 augustus 2024, 34, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 511; 542; VANDE LANOTTE J., GOEDERTIER G., HAECK Y., GOOSSENS J. en DE PELSMAEKER T., *Belgisch publiekrecht* (Boekdelen 1 en 2), die Keure, 2015, 486-487.

³⁶⁶ EHRM 26 maart 1987, 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881, 'Leander/Zweden', § 48; EHRM 25 februari 1997, 22009/93, ECLI:CE:ECHR:1997:0225JUD002200993, 'Z./Finland', § 95; EHRM 27 juni 2017, 931/13, ECLI:CE:ECHR:2017:0627JUD000093113, 'Satakunnan Markkinapörssi Oy en Satamedia Oy/Finland', § 137; EHRM 9 maart 2023, 36345/16, ECLI:CE:ECHR:2023:0309JUD003634516, 'L.B./Hongarije', § 103; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence, 31 augustus 2024, 62, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

³⁶⁷ Art. 2 (c) Verdrag ter bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Hierna: Verdrag 108), BS 30 december 1993.

³⁶⁸ Artikel 2 (a) Verdrag 108; EHRM 16 februari 2000, 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, 'Amann/Zwitserland', § 65; EHRM 27 oktober 2009, 21737/03, ECLI:CE:ECHR:2009:1027JUD002173703, 'Haralambie/Roemenië', § 77.

³⁶⁹ EHRM 5 september 2017, 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608, 'Bărbulescu/Roemenië', §§ 74-81; EHRM 28 maart 2023, 34467/15, ECLI:CE:ECHR:2023:0328JUD003446715, 'Sârbu/Roemenië', §§ 39-41; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence, 31 augustus 2024, 7, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

³⁷⁰ EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, 'Uzun/Duitsland', §§ 49-53; EHRM 24 april 2018, 62357/14, ECLI:CE:ECHR:2018:0424JUD006235714, 'Benedik/Slovenië', §§ 108-109.

³⁷¹ EHRM 3 april 2007, 62617/00, ECLI:CE:ECHR:2007:0403JUD006261700, 'Copland/Verenigd Koninkrijk Kingdom', §§ 41-42; EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, 'Uzun/Duitsland', § 44; Cass. 7 juni 2016, P.16.0294.N/1, ECLI:BE:CASS:2016:ARR.20160607.7; EHRM 5 september 2017, 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608, 'Bărbulescu/Roemenië', § 73; EHRM 24 april 2018, 62357/14, ECLI:CE:ECHR:2018:0424JUD006235714, 'Benedik/Slovenië', §101; DE HERT P., 'Het Europees Hof Rechten van de Mens erkent publieke privacy', *NJW* 2002/4, (116) 120.

³⁷² EHRM 19 mei 1994, 15225/89, ECLI:CE:ECHR:1994:0519REP001522589, 'Friedl/Oostenrijk', §§ 50- 51; EHRM 17 juli 2003, 63737/00, ECLI:CE:ECHR:2003:0717JUD006373700, 'Perry/Verenigd Koninkrijk', §§ 39-43; EHRM

170. In het kader van artikel 8 EVRM kan sprake zijn van een inbreuk op het recht op respect voor privéleven en correspondentie wanneer nationale wetgeving autoriteiten toegang verleent tot opgeslagen (communicatie)gegevens.³⁷³ Dit kan zowel gegevens betreffen die door de autoriteiten zelf zijn verzameld tijdens onderzoeken³⁷⁴, als inhoud en metadata van internetcommunicatie die door exploitanten of aanbieders van elektronische communicatienetwerken worden vrijgegeven³⁷⁵. Ook wanneer dergelijke aanbieders verplicht worden persoonsgegevens, zoals naam, adres of IP-adres, op te slaan, vormt dit een inmenging in de persoonlijke levenssfeer van de betrokkenen.³⁷⁶ Het EHRM heeft geoordeeld dat zulke inmengingen slechts toelaatbaar zijn indien zij voldoen aan de vereisten van legaliteit, noodzakelijkheid en proportionaliteit in een democratische samenleving. Dit onderstreept de noodzaak van strikte waarborgen en toezicht bij het reguleren van gegevensopslag en gegevenstoegang door nationale autoriteiten.

§ 2: Grenzen van toelaatbare inmenging

171. Het recht op eerbiediging van het privé-, familie- en gezinsleven is geen absoluut recht. Artikel 8.2 EVRM bevat een zogenaamde 'escapeclause', waarin wordt bepaald: "*Geen inmenging van enig openbaar gezag is toegestaan met betrekking tot de uitoefening van dit recht, tenzij deze inmenging bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van*

2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, 'Uzun/Duitsland', §§ 51-52; EHRM 18 oktober 2016, 61838/10, ECLI:CE:ECHR:2016:1018JUD006183810, 'Vukota-Bojić/Zwitserland', §§ 57-59; EHRM 17 oktober 2019, 1874/13, 8567/13, ECLI:CE:ECHR:2019:1017JUD000187413, 'López Ribalda e.a./Sapnje', § 94; EHRM 28 maart 2023, 34467/15, ECLI:CE:ECHR:2023:0328JUD003446715, 'Sârbu/Roemenië', §§ 38 en 41; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 544.

³⁷³ EHRM 18 mei 2010, 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905, 'Kennedy/Verenigd Koninkrijk', §§ 123-124; EHRM 11 januari 2022, 70078/12, ECLI:CE:ECHR:2022:0111JUD007007812, 'Ekimdzhiev e.a./Bulgarije', §§ 262-277; 371-384; EHRM 13 februari 2024, 33696/19, ECLI:CE:ECHR:2024:0213JUD003369619, 'Podchasov/Rusland', §§ 54-55; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, *Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence*, 31 augustus 2024, 39, 48, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

³⁷⁴ EHRM 6 september 1978, 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971, 'Klass e.a./Duitsland', § 41; EHRM 16 februari 2000, 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, 'Amann/Zwitserland', § 69; EHRM 4 mei 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, 'Rotaru/Roemenië', § 46; EHRM 4 december 2008, 30562/04 en 30566/04; ECLI:CE:ECHR:2008:1204JUD003056204, 'S. en Marper/Verenigd Koninkrijk', § 67; EHRM 18 april 2013, 19522/09, ECLI:CE:ECHR:2013:0418JUD001952209, 'M.K./Frankrijk', § 29; EHRM 22 juni 2017, 8806/12, ECLI:CE:ECHR:2017:0622JUD000880612, 'Aycaguer/Frankrijk', § 33; EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden', § 167; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 516-517; DE WAEL F., 'Europese rechtspraak in kort bestek (noot onder EHRM 23 juni 2022)', *T.Strafr.* 2022/5, (309) 309.

³⁷⁵ EHRM 2 augustus 1984, 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179, 'Malone/Verenigd Koninkrijk', § 84; EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland', § 171; EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden', § 14; EHRM 11 januari 2022, 70078/12, ECLI:CE:ECHR:2022:0111JUD007007812, 'Ekimdzhiev e.a./Bulgarije', §§ 262-277; 371-384; EHRM 13 februari 2024, 33696/19, ECLI:CE:ECHR:2024:0213JUD003369619, 'Podchasov/Rusland', §§ 54-55; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, *Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence*, 31 augustus 2024, 160, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng; DE HERT P., 'Het Europees Hof Rechten van de Mens erkent publieke privacy', *NJW* 2002/4, (116) 120.

³⁷⁶ EHRM 24 april 2018, 62357/14, ECLI:CE:ECHR:2018:0424JUD006235714, 'Benedik/Slovenië', § 96; EHRM 30 januari 2020, 50001/12, ECLI:CE:ECHR:2020:0130JUD005000112, 'Breyer/Duitsland', § 81; EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden', §§ 238-245; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013, 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 324-331; VAN DE HEYNING C., 'Overzicht van rechtspraak - Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog (noot onder GwH 19 juli 2018)', *T.Strafr.* 2019/1, (38) 41.

de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of ter bescherming van de rechten en vrijheden van anderen."³⁷⁷ Hieruit volgt dat inmenging slechts gerechtvaardigd is indien aan drie cumulatieve voorwaarden is voldaan: (i) een wettelijke basis, (ii) een legitiem doel, en (iii) noodzakelijkheid in een democratische samenleving.³⁷⁸

Afdeling 1: Bij wet voorzien

172. In het licht van het rechtszekerheidsbeginsel is het in de eerste plaats vereist dat een inmenging in het recht op eerbiediging van het privéleven gebaseerd is op een specifieke wettelijke grondslag. Deze vereiste beperkt zich niet tot het louter bestaan van een nationale bepaling, maar heeft tevens betrekking op de kwaliteit van die wettelijke norm. De betrokken regelgeving moet in overeenstemming zijn met het beginsel van 'the rule of law' en dient derhalve voldoende duidelijk, toegankelijk en voorzienbaar te zijn. Dit houdt in dat de wettelijke bepaling individuen toereikende aanwijzingen moet geven over de omstandigheden en voorwaarden waaronder de bevoegde autoriteiten gerechtigd zijn maatregelen te nemen die een inmenging vormen in rechten die onder het Verdrag vallen.³⁷⁹

173. Daarnaast vereist 'the rule of law' dat het nationale recht adequate waarborgen bevat ter bescherming tegen misbruik en willekeurige inmenging door de autoriteiten.³⁸⁰ Welke waarborgen geboden dienen te worden, hangt af van de aard van de toegepaste onderzoeksmethode en de intensiteit van de daarmee gepaard gaande inmenging. Hoewel het EHRM in de regel vergelijkbare waarborgen vereist, past het bij ingrijpendere maatregelen een strengere toets toe teneinde willekeur en misbruik te voorkomen.³⁸¹

³⁷⁷ Art. 8.2 EVRM.

³⁷⁸ HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 510.

³⁷⁹ EHRM 21 juni 2011, 30194/09, ECLI:CE:ECHR:2011:0621JUD003019409, 'Shimovolos/Rusland', § 68; EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland', §§ 228-236; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 333-334; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 538; TERSAGO P., 'Europese rechtspraak in kort bestek (noot onder EHRM 26 oktober 2023)', *T.Strafr.* 2024/3, (192) 192.

³⁸⁰ EHRM 10 maart 2009, 4378/02, ECLI:CE:ECHR:2009:0310JUD000437802, 'Bykov/Rusland', § 81; EHRM 14 januari 2021, 59648/13, ECLI:CE:ECHR:2021:0114JUD005964813, 'Vig/Hongarije', § 62; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence, 31 augustus 2024, 8, 12, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

³⁸¹ EHRM 6 september 1978, 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971, 'Klass e.a./Duitsland', §§ 44, 49; EHRM 26 maart 1987, 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881, 'Leander/Zweden', §§ 51, 60; EHRM 4 mei 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, 'Rotaru/Roemenië', § 59; EHRM 31 mei 2005, 64330/01, ECLI:CE:ECHR:2005:0531JUD006433001, 'Antunes Rocha/Portugal', § 76; EHRM 29 juni 2006, 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, 'Weber en Saravia/Duitsland', § 94; EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, 'Uzun/Duitsland', § 66; EHRM 11 januari 2022, 70078/12, ECLI:CE:ECHR:2022:0111JUD007007812, 'Ekimdzhev e.a./Bulgarije', § 77; EHRM 4 juli 2023, 11519/20, ECLI:CE:ECHR:2023:0704JUD001151920, 'Glukhin/Rusland', § 82; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence, 31 augustus 2024, 8, 19, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Data protection, 31 December 2020, 28, <https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0>.

A. Gerichte geheime surveillancemethoden³⁸²

174. Zoals eerder aangegeven kan artikel 8 EVRM worden geschonden wanneer nationale wetgeving autoriteiten toegang verleent tot bewaarde (communicatie)gegevens (Cf. *supra*, nr. 170). De rechtspraak over privacy en gegevensbescherming in strafonderzoeken focust daarbij hoofdzakelijk op gerichte geheime surveillancemethoden, zoals informaticazoekingen, telefoontap en het registreren van communicatiemetadaten.³⁸³ Deze technieken zijn voornamelijk gericht op het verzamelen van communicatiegegevens, waaronder de inhoud van communicatie, tijdstip en duur van gesprekken, gecontacteerde nummers en locatiegegevens.³⁸⁴ Gelet op het ingrijpende karakter van dergelijke maatregelen is het van essentieel belang dat zij worden omkaderd door doeltreffende waarborgen tegen misbruik.³⁸⁵

175. Volgens de rechtspraak van het EHRM dient nationale wetgeving inzake gerichte surveillancemaatregelen minstens zes fundamentele waarborgen te omvatten, namelijk: (i) een nauwkeurige omschrijving van de strafbare feiten die de toepassing van de maatregel rechtvaardigen, (ii) de afbakening van de categorieën personen op wie de maatregel van toepassing kan zijn, (iii) een beperking van de duur van de maatregel, (iv) procedurevoorschriften voor het verzamelen, gebruiken en opslaan van de verkregen gegevens, (v) waarborgen die gelden bij de verstrekking van gegevens aan derden, en (vi) voorwaarden waaronder de verzamelde opnames moeten of kunnen worden gewist of vernietigd.³⁸⁶

³⁸² Bijlage 4.

³⁸³ EHRM 6 september 1978, 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971, 'Klass e.a./Duitsland', § 44; EHRM 31 juli 2012, 36662/04, ECLI:CE:ECHR:2012:0731JUD003666204, 'Drakšas/Litouwen', § 54; EHRM 24 april 2018, 62357/14, ECLI:CE:ECHR:2018:0424JUD006235714, 'Benedik/Slovenië', §§ 108-109; VANDE LANOTTE J., GOEDERTIER G., HAECK Y., GOOSSENS J. en DE PELSMAEKER T., *Belgisch publiekrecht (Boekdelen 1 en 2)*, die Keure, 2015, 469.

³⁸⁴ EHRM 2 augustus 1984, 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179, 'Malone/Verenigd Koninkrijk', §§ 63-89; EHRM 24 april 1990, 11801/85, ECLI:CE:ECHR:1990:0424JUD001180185, 'Kruslin/Frankrijk', §§ 25-36; EHRM 16 februari 2000, 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, 'Amann/Zwitserland', 20, §§ 45-62; EHRM 18 februari 2003, 58496/00, ECLI:CE:ECHR:2003:0218JUD005849600, 'Prado Bugallo/Spanje', §§ 28-33; EHRM 3 april 2007, 62617/00, ECLI:CE:ECHR:2007:0403JUD006261700, 'Copland/Verenigd Koninkrijk', §§ 41-42; EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, 'Uzun/Duitsland', § 66; EHRM 15 januari 2015, 68955/11, ECLI:CE:ECHR:2015:0115JUD006895511, 'Dragojević/Kroatië', §§ 85-102; EHRM 28 mei 2019, 173/15, ECLI:CE:ECHR:2019:0528JUD000017315, 'Liblik e.a./Estland', §§ 132-143; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, *Guide to the Case-Law of the of the European Court of Human Rights – Data protection*, 31 December 2020, 35, <https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0>.

³⁸⁵ EHRM 30 juli 1998, 58/1997/842/104e8, ECLI:CE:ECHR:1998:0730JUD002767195, 'Valenzuela Contreras/Spanje', § 46; EHRM 29 juni 2006, 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, 'Weber en Saravia/Duitsland', § 95; EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland', §§ 231; EHRM 27 juni 2017, 931/13, ECLI:CE:ECHR:2017:0627JUD000093113, 'Satakunnan Markkinapörssi Oy en Satamedia Oy/Finland', § 137; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 538; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, *Guide to the Case-Law of the of the European Court of Human Rights – Data protection*, 31 December 2020, 34, <https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0>.

³⁸⁶ EHRM 24 april 1990, 11105/84, ECLI:CE:ECHR:1990:0424JUD001110584, 'Huvig/Frankrijk', § 34; EHRM 24 april 1990, 11801/85, ECLI:CE:ECHR:1990:0424JUD001180185, 'Kruslin/Frankrijk', §§ 33-35; EHRM 30 juli 1998, 58/1997/842/1048, ECLI:CE:ECHR:1998:0730JUD002767195, 'Valenzuela Contreras/Spanje', § 46; EHRM 16 februari 2000, 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, 'Amann/Zwitserland', 20, §§ 56-58; EHRM 29 juni 2006, 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, 'Weber en Saravia/Duitsland', § 95; EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland', §§ 231; 238-301; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 539; DE Wael F., 'Europese rechtspraak in kort bestek (noot onder EHRM 23 juni 2022)', *T.Strafr.* 2022/5, (309) 311.

176. Naast de zes kernvereisten erkent het EHRM ook andere essentiële waarborgen, zoals de duidelijke afbakening van de bevoegde autoriteiten die de maatregel mogen toestaan, uitvoeren en controleren, evenals de beschikbaarheid van doeltreffende rechtsmiddelen.³⁸⁷

De controle van dergelijke maatregelen kan plaatsvinden in drie fasen: bij het bevel, tijdens de uitvoering en na afloop. Voor de eerste twee fasen is effectieve controle cruciaal, met bijzondere aandacht voor (i) de bevoegde autoriteit, (ii) de reikwijdte van de controle en (iii) de inhoud van de maatregel.³⁸⁸ Het is van fundamenteel belang dat de toestemming voor de maatregel wordt verleend door een onafhankelijke instantie, bij voorkeur aan de hand van een voorafgaande rechterlijke machtiging.³⁸⁹ Dit is echter niet steeds vereist, mits er achteraf een doeltreffende rechterlijke toetsing van de onderzoeksmaatregel plaatsvindt.³⁹⁰ Wat de reikwijdte van de controle betreft, moet de bevoegde autoriteit kunnen nagaan of er sprake is van een redelijke verdenking jegens de betrokkene, en in het bijzonder of er feitelijke aanwijzingen bestaan dat deze persoon strafbare feiten voorbereidt, pleegt of heeft gepleegd. Voorts dient te worden beoordeeld of de maatregel voldoet aan het vereiste van 'noodzakelijkheid in een democratische samenleving', en of zij evenredig is aan het nagestreefde legitieme doel.³⁹¹ Ten slotte moet de maatregel voldoende specifiek zijn en duidelijk gericht op een geïdentificeerd persoon.³⁹² Na beëindiging van het onderzoek is het bovendien van cruciaal belang dat de betrokken personen toegang hebben tot een rechtsmiddel om de rechtmatigheid van de getroffen maatregelen te betwisten.³⁹³

177. Diverse kritische kanttekeningen dienen in overweging te worden genomen met betrekking tot de zoektermbevelen. Deze onderzoeksmaatregel is tot op heden niet expliciet beoordeeld door het EHRM, waardoor er geen rechtspraak bestaat over de toepasselijke juridische waarborgen bij de inzet ervan. Zoektermbevelen kunnen niet zonder meer worden gelijkgesteld met bestaande vormen van gerichte geheime surveillance. In tegenstelling tot methoden die gericht zijn op de interceptie of verzameling van communicatie- en metagegevens, beogen zoektermbevelen de identificatie van personen aan de hand van ingevoerde zoektermen. Het voorwerp en de toepassingswijze van deze maatregel wijken daardoor wezenlijk af van bestaande opsporingsinstrumenten.

178. De lijn van de waarborgen die vereist zijn in het kader van gerichte surveillancemethoden kunnen volgens ons toch worden doorgetrokken naar zoektermbevelen. Verschillende redenen kunnen hiervoor worden aangehaald.

³⁸⁷ EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland', §§ 232; EHRM 15 juni 2021, 73357/14, ECLI:CE:ECHR:2021:0615DEC007335714, 'Falzarano/Italië', §§ 27-29; TERSAGO P., 'Europese rechtspraak in kort bestek (noot onder EHRM 26 oktober 2023)', *T.Strafr.* 2024/3, (192) 192-193.

³⁸⁸ EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland', §§ 233-234; 257.

³⁸⁹ *Ibid.*, § 258; VAN DE HEYNING C., 'Ernst van het misdrijf is een onvoldoende reden om procedurele garanties voor de zoeking in informaticasystemen te omzeilen (noot onder EHRM 30 mei 2017)', *T.Strafr.* 2017/6, (365) 366.

³⁹⁰ EHRM 30 september 2019, 8429/05, ECLI:CE:ECHR:2014:0930JUD000842905, 'Prezhdarovi/Bulgarije', §§ 46-47; Cass. 5 november 2019, P.19.0426.N, ECLI:BE:CASS:2019:ARR.20191105.2, § 12.

³⁹¹ EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland', § 260.

³⁹² *Ibid.*, § 264.

³⁹³ *Ibid.*, § 234.

179. Zoals eerder uiteengezet, vereist een ingrijpendere onderzoeksmethode een strengere toetsing.³⁹⁴ Zoektermbevelen vormen volgens ons in dit opzicht een tussencategorie, gepositioneerd tussen de verkrijging van verkeers- en locatiegegevens enerzijds en de toepassing van tapmaatregelen of inkijkoperaties anderzijds (Cf. *supra*, nrs. 62-65). Hoewel het EHRM zich niet heeft uitgesproken over zoektermbevelen, heeft het in zijn rechtspraak wel de grens verduidelijkt tussen de verkeers- en locatiegegevens en communicatie-interceptie. Zo oordeelde het in zijn rechtspraak over GPS-toezicht dat deze vorm van toezicht een inmenging in het privéleven vormt, zij het in beperktere mate dan het onderscheppen van communicatiegegevens, waarbij het EHRM het onderscheppen en opnemen van communicatie beschouwt als bijzonder ingrijpend vanwege de inzichten die het verschaft in iemands gedrag, overtuigingen en emoties.³⁹⁵ Ook het doorzoeken van zoekgeschiedenis kan gevoelige informatie onthullen over denkpatronen, voorkeuren en gedragingen. Derhalve kan worden betoogd dat het gebruik van zoektermbevelen qua impact te vergelijken is met het onderscheppen van communicatie, zij het in beperktere mate. Een zoektermbevel beoogt immers enkel de identificatie van gebruikers die een specifieke zoekterm hebben ingevoerd, en heeft niet tot doel de gehele zoekgeschiedenis van een individu bloot te leggen, wat bij een tapmaatregel wel het geval is, aangezien deze de volledige inhoud van communicatie onderschept en registreert. Bijgevolg is het aangewezen dat voor zoektermbevelen gelijkaardige juridische waarborgen worden gehanteerd als die welke gelden voor het onderscheppen van communicatie, zij het met een minder stringente toetsing dan bij de tapmaatregel, doch strenger dan de toets die wordt toegepast bij het verkrijgen van verkeers- en locatiegegevens.

180. Een bijkomende reden waarom de waarborgen die gelden voor geheime surveillancemethoden ook van toepassing zouden moeten zijn op zoektermbevelen, is gelegen in de rechtspraak van het EHRM. Het EHRM heeft immers geoordeeld dat wanneer aanbieders van communicatiediensten communicatiegegevens opslaan en mogelijk toegang moeten verlenen aan autoriteiten voor wetshandavingsdoeleinden, dezelfde waarborgen moeten worden geboden als die welke gelden voor geheime surveillancemethoden.³⁹⁶ In het kader van zoektermbevelen zijn het niet de politiediensten zelf die rechtstreeks de zoekgeschiedenis van internetgebruikers doorzoeken. Deze taak rust bij zoekmachinebedrijven, die vervolgens accountinformatie overmaken aan de bevoegde autoriteiten met betrekking tot personen die specifieke zoektermen hebben ingevoerd. Wanneer

³⁹⁴ EHRM 10 februari 2009, 3514/02, ECLI:CE:ECHR:2009:0210JUD000351402, 'Eerikäinen/Finland', § 70; EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD0003562305, 'Uzun/Duitsland', § 66; EHRM 4 juli 2023, 11519/20, ECLI:CE:ECHR:2023:0704JUD001151920, 'Glukhin/Rusland', § 82; Zo oordeelde het Hof over een afbeelding van een persoon: "A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers"; EHRM 12 december 2013, 20383/04, ECLI:CE:ECHR:2013:1212JUD00203830, 'Khmel/Rusland', § 40; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence, 31 augustus 2024, 8, 19, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights – Data protection, 31 December 2020, 28, <https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0>.

³⁹⁵ EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD0003562305, 'Uzun/Duitsland', § 52; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 539-540; VANDE LANOTTE J., GOEDERTIER G., HAECK Y., GOOSSENS J. en DE PELSMACKER T., *Belgisch publiekrecht (Boekdelen 1 en 2)*, die Keure, 2015, 472.

³⁹⁶ EHRM 11 januari 2022, 70078/12, ECLI:CE:ECHR:2022:0111JUD007007812, 'Ekimdzhev e.a./Bulgarije', § 395.

dergelijke bedrijven zoekgeschiedenis bewaren en op verzoek aan handhavingsinstanties overdragen, moet aldus eenzelfde beschermingsniveau worden gegarandeerd als bij onderzoeksmethoden waarbij communicatie- of metagegevens worden opgevraagd.

B. Bulkinterceptie³⁹⁷

181. Een kritische lezer zal opmerken dat zich een bijkomende problematiek voordoet. Zoektermbevelen worden immers aangewend in situaties waarin de dader onbekend is, terwijl de eerder besproken waarborgen betrekking hebben op maatregelen die zijn gericht op communicatie- en metagegevens van reeds geïdentificeerde verdachten. Bij zoektermbevelen ontbreekt deze persoonsgerichte focus. Het gaat om een techniek waarbij potentieel duizenden tot miljoenen individuen worden gescreend op hun zoekgeschiedenis, met als doel na te gaan of zij een specifieke zoekterm hebben ingevoerd.

182. Een soortgelijke problematiek kan gevonden worden bij bulkinterceptie. Bulkinterceptiemaatregelen worden doorgaans ingezet voor het verzamelen van buitenlandse inlichtingen en het identificeren van nieuwe bedreigingen, afkomstig van zowel bekende als onbekende actoren.³⁹⁸ Daarbij wordt op grote schaal (in bulk) gegevens verzameld en opgevraagd van operatoren of dienstverstrekkers, zonder dat er op dat moment specifieke verdachten of doelwitten zijn geïdentificeerd.³⁹⁹ Dit slaat op een algemene bewaarplicht, gecombineerd met de mogelijkheid voor rechtshandavingsinstanties om nadien toegang te verkrijgen tot deze gegevens.⁴⁰⁰ Gezien een beoordeling van het volledige gegevensvolume zowel praktisch onhaalbaar als disproportioneel zou zijn, wordt voorafgaand aan de analyse een selectie- en filterprocedure toegepast.⁴⁰¹ Deze selectie gebeurt aan de hand van gerichte zoekopdrachten en filters. Er wordt gebruikgemaakt van specifieke criteria, ook wel 'selectoren'⁴⁰² genoemd, om relevante informatie te identificeren. Deze selectoren variëren van 'sterke selectoren', zoals specifieke e-mailadressen, telefoonnummers of IP-adressen die direct aan een individu kunnen worden gekoppeld, tot 'zwakke selectoren', zoals algemene termen of trefwoorden die een breder scala aan resultaten opleveren en

³⁹⁷ Bijlage 4.

³⁹⁸ X, 'noot onder EHRM 19 juni 2018', *T.Strafr.* 2019/1, (47) 64; JANSEN R.H.T., 'Big Brother Watch e.a., Centrum för Rättvisa en het toezicht op de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2022/51, (97) 97, 99; COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence, 31 augustus 2024, 159, https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

³⁹⁹ EHRM (Grote Kamer) 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 240; EHRM (Grote Kamer) 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 326; ROYER S., 'Cassatie verwerpt procedurele bezwaren tegen Sky ECC-onderzoek (noot onder cass. 14 juni 2023)', *T.Strafr.* 2024/2, (99) 100; VAN DE HEYNING C., 'Overzicht van rechtspraak - Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog (noot onder GwH 19 juli 2018)', *T.Strafr.* 2019/1, (38) 41; X, 'noot onder EHRM 19 juni 2018', *T.Strafr.* 2019/1, (47) 55.

⁴⁰⁰ VAN DE HEYNING C., 'Overzicht van rechtspraak - Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog (noot onder GwH 19 juli 2018)', *T.Strafr.* 2019/1, (38) 41.

⁴⁰¹ VAN DE HEYNING C., 'Not all that glitters is gold: een effectief recht op tegenspraak in tijden van bulkdata (noot EHRM 7 november 2017)', *T.Strafr.* 2021/4, (195) 195.

⁴⁰² Selectoren betreffen specifieke parameters of zoekcriteria die worden gebruikt om bepaalde gegevens uit de grote hoeveelheid verzamelde informatie te filteren.

minder direct aan specifieke personen zijn gekoppeld.⁴⁰³ Op deze manier verschuift het proces geleidelijk naar het richten op specifieke individuen.⁴⁰⁴

183. Net als bij bulkinterceptie worden bij de zoektermbevelen op grote schaal gegevens onderzocht, waarbij slechts een klein deel - of in het slechtste geval geen - nuttig zal zijn voor het onderzoek en kan leiden tot de identificatie van een mogelijke verdachte. Ook hierbij wordt gewerkt met een selectieproces, waarbij een specifieke zoekterm fungeert als een soort selector om relevante gegevens op te sporen binnen een grotere dataset. Zoektermbevelen kunnen dan ook worden begrepen als een bijzondere vorm van bulkinterceptie, aangezien zij veronderstellen dat zoekgeschiedenissen op grote schaal moeten worden bewaard en opsporingsautoriteiten toegang kunnen verkrijgen tot deze gegevens. Dit werpt belangrijke vragen op over de rechtmatigheid van dergelijke methoden, aangezien deze de privacy van een groot aantal onschuldige individuen kunnen schenden.⁴⁰⁵

184. Ondanks het ingrijpende karakter van bulkinterceptie, waaronder een algemene en ongedifferentieerde bewaarplicht als specifieke toepassing valt, aanvaardt het EHRM dat dergelijke maatregelen in overeenstemming kunnen zijn met het EVRM, mits zij noodzakelijk zijn ter bestrijding van ernstige criminaliteit of ter bescherming van de nationale of openbare veiligheid.⁴⁰⁶ Tegelijkertijd wijst het EHRM op het aanzienlijke risico van misbruik, waardoor het recht op eerbiediging van het privéleven ernstig kan worden aangetast. In dit verband erkent het EHRM weliswaar een ruime beoordelingsmarge voor de lidstaten bij het al dan niet invoeren van een bulkinterceptieregime, maar benadrukt het dat een zwaardere toetsing vereist is dan bij gerichte interceptie.⁴⁰⁷

185. Het is evident dat de eerste twee van de zes minimumwaarborgen (Cf. *supra*, nr. 175) die gelden voor gerichte interceptie niet zonder meer toepasbaar zijn op een wettelijk kader voor bulkinterceptie. Eveneens verliest de vereiste van een redelijke verdenking aan relevantie in deze context, aangezien het doel van bulkinterceptie niet primair gericht is op het onderzoeken van een specifiek individu.⁴⁰⁸ Niettemin benadrukt het EHRM dat, wanneer een staat

⁴⁰³ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 241; 260; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 327; 346; VAN DE HEYNING C., 'Overzicht van rechtspraak - Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog (noot onder GwH 19 juli 2018)', *T.Strafr.* 2019/1, (38) 42.

⁴⁰⁴ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 267; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 353.

⁴⁰⁵ ROYER S., 'Cassatie verwerpt procedurele bezwaren tegen Sky ECC-onderzoek (noot onder cass. 14 juni 2023)', *T.Strafr.* 2024/2, (99) 103, 104; JANSEN R.H.T., 'Big Brother Watch e.a., Centrum för Rättvisa en het toezicht op de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2022/51, (97) 97.

⁴⁰⁶ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 237, 284-288; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 340, 368-371; EHRM 29 juni 2006, 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, 'Weber en Saravia/Duitsland, § 94.

⁴⁰⁷ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 261; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 347; X, 'noot onder EHRM 19 juni 2018', *T.Strafr.* 2019/1, (47) 64; JANSEN R.H.T., 'Big Brother Watch e.a., Centrum för Rättvisa en het toezicht op de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2022/51, (97) 97.

⁴⁰⁸ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 262; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big

bulkinterceptiemaatregelen inzet, de nationale wetgeving gedetailleerde regels moet bevatten met betrekking tot de omstandigheden waaronder autoriteiten tot bulkinterceptie mogen overgaan. De wetgeving dient met name op voldoende duidelijke wijze vast te leggen op welke juridische gronden toestemming kan worden verleend voor het op grote schaal verwerken van (communicatie)gegevens, en onder welke voorwaarden dit kan.⁴⁰⁹ De overige vier door het EHRM geformuleerde minimumwaarborgen blijven onverminderd van toepassing op bulkinterceptie. Deze waarborgen zijn essentieel om de proportionaliteit en rechtsstatelijke controle op grootschalige gegevensverzameling te waarborgen.⁴¹⁰

186. Net als bij gerichte interceptie vergt ook bulkinterceptie bijzondere aandacht voor toezicht en toetsing. Gezien de grootschalige aard en het inherente misbruikrisico is dergelijk toezicht zelfs des te crucialer. Het EHRM oordeelde dat bulkinterceptiemaatregelen moet worden onderworpen aan zogeheten 'end-to-end safeguards', wat betekent dat in elke fase van het proces controlemechanismen op nationaal niveau vereist zijn. Dit houdt in dat toezicht moet worden uitgeoefend vanaf het begin van de maatregel - wanneer het doel en de reikwijdte van de bulkoperatie worden vastgesteld en toestemming wordt verleend - tot aan het gebruiken, het delen en het bewaren van gegevens.⁴¹¹

Een essentiële waarborg in dit kader is dat de toestemming voor bulkinterceptie steeds moet worden verleend door een onafhankelijke instantie, bij voorkeur een rechter, die op de hoogte moet worden gesteld van zowel het doel van de maatregel als de aard van de te onderscheppen gegevens. Daarbij is het cruciaal dat elke fase van het proces, waaronder de initiële machtiging, eventuele verlengingen, het gebruik, de opslag, de verdere verstrekking en de uiteindelijke verwijdering van het onderschepte materiaal, steeds onder toezicht blijft van een onafhankelijke autoriteit. Deze autoriteit dient bij iedere stap te toetsen of de maatregel voldoet aan de vereisten van noodzakelijkheid en proportionaliteit.⁴¹² Daarnaast moet er een effectief rechtsmiddel beschikbaar zijn waarmee de rechtmatigheid van de maatregel kan worden aangevochten. De effectiviteit van een dergelijk rechtsmiddel hangt af van de bevoegdheden en procedurele garanties waarover de bevoegde instantie beschikt. Het is hierbij van belang dat de toetsende instantie onafhankelijk is, zij het niet noodzakelijkerwijze gerechtelijk van aard. De beslissingen van deze instantie dienen voldoende gemotiveerd en juridisch bindend te zijn. Bovendien moet zij de bevoegdheid hebben om

Brother Watch e.a./Verenigd Koninkrijk', § 348; JANSEN R.H.T., 'Big Brother Watch e.a., Centrum för Rättvisa en het toezicht op de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2022/51, (97) 101.

⁴⁰⁹ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 262; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 348.

⁴¹⁰ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 262; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 348.

⁴¹¹ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 264; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 349-350; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 539.

⁴¹² EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 265-270; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 351-356.

de maatregel te beëindigen en het door de maatregel verkregen materiaal te vernietigen indien blijkt dat deze onrechtmatig of disproportioneel was.⁴¹³

187. Ook in het licht van de selectoren die worden gehanteerd om specifieke personen te identificeren dienen extra waarborgen geboden te worden. Het gebruik van elk van deze selectoren moet door de rechtshandhavinginstanties worden gerechtvaardigd, met inachtneming van de beginselen van noodzakelijkheid en evenredigheid. Deze rechtvaardiging moet nauwgezet worden geregistreerd en onderworpen aan een proces van voorafgaande interne machtiging waarbij afzonderlijk en objectief wordt nagegaan of aan de vereiste van noodzakelijkheid en evenredigheid zijn voldaan.⁴¹⁴

188. De volgende acht waarborgen dienen derhalve te worden gerespecteerd in het kader van bulkinterceptie: (i) de juridische gronden waarop de maatregel kan worden toegestaan, (ii) de specifieke omstandigheden waaronder de maatregel mag worden toegepast, (iii) de procedure die gevolgd moet worden voor het verlenen van de machtiging, (iv) procedures voor de selectie, analyse en het gebruik van het onderschepte materiaal, (v) voorzorgsmaatregelen die genomen moeten worden bij de verstrekking van het materiaal aan derden, (vi) beperkingen met betrekking tot de duur van de maatregel, de opslag van het materiaal en de voorwaarden waaronder dit moet worden gewist of vernietigd, (vii) procedures en modaliteiten voor toezicht door een onafhankelijke autoriteit op de naleving van de bovengenoemde waarborgen, evenals de bevoegdheden van deze autoriteit bij vaststelling van niet-naleving, (viii) procedures voor een onafhankelijke toetsing ex post van de naleving van deze waarborgen en de bevoegdheden waarover de toezichthoudende instantie beschikt om gevallen van niet-naleving aan te pakken.⁴¹⁵

Afdeling 2: Legitieme doelstelling

189. Een inmenging in het recht op eerbiediging van het privé-, familie- en gezinsleven is toegestaan wanneer er een legitiem doel is. Artikel 8.2 EVRM somt deze doelstellingen limitatief op: nationale veiligheid, openbare veiligheid, economisch welzijn van het land, bescherming van de openbare orde, voorkoming van strafbare feiten, bescherming van gezondheid of goede zeden, en bescherming van de rechten en vrijheden van anderen.

190. In het licht van strafrechtelijke onderzoeksstrategieën die een inbreuk kunnen vormen op artikel 8 EVRM wordt voornamelijk de bescherming van de openbare orde, het voorkomen van

⁴¹³ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 271-273; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 357-359.

⁴¹⁴ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 269; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 355.

⁴¹⁵ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 275; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 361; X, 'noot onder EHRM 19 juni 2018', *T.Strafr.* 2019/1, (47) 58.

strafbare feiten, de veiligheid van het land, de openbare veiligheid en de rechten en vrijheden van anderen opgeworpen.⁴¹⁶

Afdeling 3: Noodzakelijk in democratische samenleving

191. Indien is voldaan aan de wettelijke vereisten en de legitieme doelstelling, dient de betreffende maatregel nog een laatste, stringente toets te doorstaan alvorens een inmenging als gerechtvaardigd kan worden beschouwd. Deze toets betreft de beoordeling of de maatregel 'noodzakelijk is in een democratische samenleving'. Volgens de rechtspraak van het EHRM impliceert het begrip 'noodzaak' dat elke inmenging in de bescherming van persoonsgegevens moet beantwoorden aan een dringende maatschappelijke behoefte, waarbij de bevoegde autoriteiten een zekere mate van beoordelingsvrijheid toekomt.⁴¹⁷ Om vast te stellen of de bestreden maatregel daadwerkelijk noodzakelijk is in een democratische samenleving, moet worden onderzocht of de aangevoerde rechtvaardigingsgronden zowel relevant als toereikend zijn en of de genomen maatregelen evenredig zijn in verhouding tot de nagestreefde doelstellingen.⁴¹⁸

192. Bij de beoordeling van de proportionaliteit van een maatregel in relatie tot het nagestreefde doel hanteert het EHRM doorgaans een aantal fundamentele criteria. Deze beoordeling hangt af van alle relevante omstandigheden van het specifieke geval, waaronder de aard, omvang en duur van de voorgenomen maatregelen, de juridische en feitelijke gronden die de maatregel rechtvaardigen, de bevoegdheden van de betrokken autoriteiten met betrekking tot goedkeuring, uitvoering en toezicht, evenals de rechtsmiddelen die het nationale recht biedt om de rechtmatigheid en evenredigheid van de maatregel te waarborgen.⁴¹⁹ Bij politionele bevelen wordt daarnaast ook rekening gehouden met de ernst van het strafbare feit, de wijze en omstandigheden van uitvaardiging (waaronder de beschikbaarheid van bewijsmateriaal), de inhoud en reikwijdte van het bevel, de geboden waarborgen ter beperking van de gevolgen, en de mogelijke reputatieschade.⁴²⁰ Deze toetsingscriteria vertonen een sterke samenhang met de waarborgen die noodzakelijk zijn ter voorkoming van willekeur en misbruik, teneinde de maatregel in overeenstemming te brengen met de fundamentele principes van de 'rule of law'. Het EHRM heeft dan ook herhaaldelijk geoordeeld dat de eis van 'in overeenstemming met de wet' dermate nauw verbonden is met het criterium van 'noodzakelijkheid in een democratische samenleving', dat beide voorwaarden in onderlinge samenhang dienen te worden geanalyseerd.⁴²¹ Dit geldt eveneens voor grootschalige en ongerichte

⁴¹⁶ EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, 'Uzun/Duitsland', § 77; EHRM 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, 'Ben Faiza/Frankrijk', § 77; EHRM 18 januari 2022, 14833/18, ECLI:CE:ECHR:2022:0118JUD001483318, 'Adomaitis/Litouwen', § 84.

⁴¹⁷ EHRM 17 april 2012, 20071/07, ECLI:CE:ECHR:2012:0417JUD002007107, 'Piechowicz/Polen', § 212; X., noot onder EHRM 19 juni 2018, *T.Strafr.* 2019/1, (47) 56.

⁴¹⁸ EHRM 25 februari 1997, 22009/93, ECLI:CE:ECHR:1997:0225JUD002200993, 'Z./Finland', § 94; EHRM 18 oktober 2011, 16188/07, ECLI:CE:ECHR:2011:1018JUD001618807, 'Khelili/Zwitserland', § 62; EHRM 6 november 2018, 25527/13, ECLI:CE:ECHR:2018:1106JUD002552713, 'Vicent Del Campo/Spanje', § 46.

⁴¹⁹ EHRM 6 september 1978, 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971, 'Klass e.a./Duitsland', § 50; EHRM 29 juni 2006, 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, 'Weber en Saravia/Duitsland', § 106; EHRM 9 juni 2009, 72094/01, ECLI:CE:ECHR:2009:0609JUD007209401, 'Kvasnica/Slowakije', § 80; EHRM 18 mei 2010, 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905, 'Kennedy/Verenigd Koninkrijk', § 153; EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland', § 232.

⁴²⁰ EHRM 6 oktober 2016, 33696/11, ECLI:CE:ECHR:2016:1006JUD003369611, 'K.S. and M.S./Duitsland', § 44.

⁴²¹ EHRM 4 december 2008, 30562/04, 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, 'S. en Marper/Verenigd Koninkrijk', § 99; EHRM 9 juni 2009, 72094/01, ECLI:CE:ECHR:2009:0609JUD007209401, 'Kvasnica/Slowakije', § 84; EHRM 18 mei 2010, 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905,

surveillancemaatregelen, zoals bulkinterceptie, waarbij het EHRM heeft benadrukt dat dergelijke ingrijpende inbreuken op het recht op privacy enkel gerechtvaardigd kunnen worden indien zij voldoen aan strikte waarborgen en effectieve controlemechanismen.⁴²²

193. In het algemeen hanteert het EHRM bij de toetsing van de noodzaak van een maatregel die specifiek ingrijpt in de bescherming van persoonsgegevens nog een aantal bijkomende fundamentele criteria. Zo wordt rekening gehouden met de verplichting om de verzameling van persoonsgegevens tot een minimum te beperken en te waarborgen dat deze, gelet op de doeleinden waarvoor zij worden verwerkt, accuraat, toereikend, relevant en niet excessief zijn. Daarnaast wordt belang gehecht aan de beperking van de bewaartermijn van de gegevens, het gebruik ervan in overeenstemming met het oorspronkelijke doeleinde van de verzameling, en de transparantie van de gegevensverwerking.⁴²³ Deze vereisten vertonen aanzienlijke overeenkomsten met de fundamentele principes die in acht genomen moeten worden binnen het kader van de AVG (Cf. *supra*, nrs. 68-97). Om die reden wordt hieraan geen verdere aandacht besteed.⁴²⁴

§ 3: Zoektermbevelen in het licht van artikel 8 EVRM

Afdeling 1: Reikwijdte

194. Het staat buiten kijf dat zoektermbevelen een inmenging vormen in het recht op privacy en, in samenhang daarmee, in de bescherming van persoonsgegevens, zoals gewaarborgd in artikel 8 EVRM. Deze inmenging manifesteert zich zowel op het niveau van de bewaring en verwerking van gegevens door de zoekmachinebedrijven als op het niveau van de autoriteiten die toegang verkrijgen tot deze gegevens.⁴²⁵ De autoriteiten verkrijgen hiermee toegang tot persoonlijke gegevens zonder expliciete toestemming van de betrokkenen, die zich er bovendien vaak niet van bewust zijn dat hun gegevens worden verzameld en verwerkt. Dit werpt fundamentele vragen op over de rechtmatigheid van dergelijke maatregelen en de grenzen die daaraan dienen te worden gesteld binnen het kader van het recht op privacy en gegevensbescherming.

'Kennedy/Verenigd Koninkrijk', § 155; EHRM 4 juli 2023, 11519/20, ECLI:CE:ECHR:2023:0704JUD001151920, 'Glukhin/Rusland', § 78; HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023, 538; 539.

⁴²² EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden', § 237; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 323.

⁴²³ Art. 5 Verdrag 108.

⁴²⁴ EHRM 7 september 1998, 47/1998/950/1165, ECLI:CE:ECHR:1998:0907JUD003093096, 'B.B./Frankrijk'; EHRM 19 oktober 2005, 32555/96, ECLI:CE:ECHR:2005:1019JUD003255596, 'Roche/Verenigd Koninkrijk'; EHRM 6 juni 2006, 62332/00, ECLI:CE:ECHR:2006:0606JUD006233200, 'Segerstedt-Wiberg e.a./Zweden'; EHRM 4 december 2008, 30562/04, 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, 'S. en Marper/Verenigd Koninkrijk'; EHRM 27 oktober 2009, 21737/03, ECLI:CE:ECHR:2009:1027JUD002173703, 'Haralambie/Roemenië'; EHRM 17 december 2009, 16428/05, ECLI:CE:ECHR:2009:1217JUD001642805, 'Gardel/Frankrijk'; EHRM 17 december 2009, 22115/06, ECLI:CE:ECHR:2009:1217JUD002211506, 'M.B./Frankrijk'; EHRM 18 oktober 2011, 16188/07, ECLI:CE:ECHR:2011:1018JUD001618807, 'Khelili/Zwitserland'; EHRM 13 november 2012, 43932/08, ECLI:CE:ECHR:2012:1113JUD004393208, 'Joanna Szulc/Polen'; EHRM 18 april 2013, 19522/09, ECLI:CE:ECHR:2013:0418JUD001952209, 'M.K./Frankrijk'; EHRM 4 juni 2013, 7841/08 en 57900/12; ECLI:CE:ECHR:2013:0604DEC000784108, 'Peruzzo en Martens/Duitsland'; EHRM 7 juni 2016, 30083/10, ECLI:CE:ECHR:2016:0607JUD003008310, 'Karabeyoğlu/Turkije'; EHRM 22 juni 2017, 8806/12, ECLI:CE:ECHR:2017:0622JUD000880612, 'Aycaguer/Frankrijk'; EHRM 13 juli 2017, 45245/15, ECLI:CE:ECHR:2020:0213JUD004524515, 'Gaughran/Verenigd Koninkrijk'; EHRM 8 september 2022, 3153/16 en 27758/18, ECLI:CE:ECHR:2022:0908JUD000315316, 'Drelon/Frankrijk'; EHRM 20 juni 2023, 36705/16, ECLI:CE:ECHR:2023:0620JUD003670516, 'Margari/Griekeland'.

⁴²⁵ X, 'noot onder EHRM 19 juni 2018', *T.Strafr.* 2019/1, (47) 55.

Afdeling 2: Grenzen van toelaatbare inmenging

A. Bij wet voorzien

195. Zoals eerder besproken, doet zich bij zowel bulkinterceptie als zoektermbevelen een vergelijkbare privacyproblematiek voor (Cf. *supra*, nrs. 182-183). In beide gevallen is sprake van een aanzienlijke inmenging in de persoonlijke levenssfeer van duizenden, zo niet miljoenen individuen. Hoewel het EHRM zich nog niet expliciet heeft uitgesproken over zoektermbevelen, lijkt het aangewezen dat dezelfde waarborgen gelden als bij bulkinterceptie, gelet op de gelijkenissen in aard, omvang en methode. Zowel de algemene en ongedifferentieerde bewaarplicht van zoekgeschiedenissen en gerelateerde gegevens als de toegang daartoe door opsporingsinstanties vergen toepassing van de door het EHRM geformuleerde waarborgen.

196. De vraag rijst hoe de vereiste waarborgen concreet moeten worden ingevuld in het kader van zoektermbevelen en de daarmee gepaard gaande bewaring van zoekgeschiedenissen en gerelateerde gegevens. Wat de eerste vereiste betreft, namelijk het bestaan van duidelijke en precieze juridische gronden, kan worden aanbevolen dat een dergelijke bewaring, evenals de toegang ertoe, slechts toelaatbaar is indien zij strikt noodzakelijk is in het belang van nationale veiligheid, de openbare orde of de voorkoming en opsporing van ernstige criminaliteit (Cf. *supra*, nr. 184).⁴²⁶ In dit verband is het van essentieel belang dat deze doelstellingen ondubbelzinnig worden afgebakend. Een vage of te ruime formulering verhoogt immers het risico op willekeur en misbruik. Anderzijds kunnen ruimer omschreven doelstellingen onder bepaalde voorwaarden aanvaardbaar zijn, mits zij worden gecompenseerd door robuuste aanvullende waarborgen.⁴²⁷ Wat betreft de afbakening van het begrip 'ernstige criminaliteit' verdient het aanbeveling aan te sluiten bij een lijst vergelijkbaar met de 'taplijst' zoals opgenomen in artikel 90ter, §§ 2-4 Sv. Daarbij dient evenwel nuance betracht te worden, waarbij bepaalde misdrijven, zoals informaticabedrog, private omkoping en heling, moeten worden uitgesloten om de proportionaliteit van de maatregel te waarborgen (Cf. *supra*, nr. 120). Deze benadering sluit tevens aan bij de aanbevelingen die in het kader van het Unierecht en de relevante Europese rechtspraak zijn geformuleerd met betrekking tot de voorwaarden voor een algemene bewaarplicht en toegang tot gegevens (Cf. *supra*, nr. 151).

197. De tweede vereiste betreft de omstandigheden waaronder de maatregel mag worden toegepast. In het kader van een regeling rond zoektermbevelen zullen deze omstandigheden mogelijk ruim worden geïnterpreteerd, aangezien het doelwit van de surveillance de opgezochte zoektermen in de zoekgeschiedenis is, en niet de apparaten waarmee de zoekopdracht is uitgevoerd, noch de identiteit van de persoon die een specifieke term heeft ingevoerd. In dit opzicht is het van fundamenteel belang dat voldoende voorzienbaarheid wordt gegarandeerd, zodat gebruikers in redelijke mate kunnen inschatten wanneer en onder welke voorwaarden hun zoekgeschiedenis aan toezicht kan worden onderworpen. Het EHRM heeft erkend dat staten de mogelijkheid moeten

⁴²⁶ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 284-288; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 368-371.

⁴²⁷ EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 370.

behouden om in te spelen op technologische ontwikkelingen, en dat het daarom onder omstandigheden gerechtvaardigd kan zijn om bredere segmenten van dataverkeer te monitoren.⁴²⁸ Zoals eerder uiteengezet in het kader van de aanbevelingen inzake zoektermbevelen binnen het Unierechtelijke kader, is het essentieel dat een dergelijke wettelijke regeling voldoet aan de vereisten van noodzakelijkheid, subsidiariteit en proportionaliteit (Cf. *supra*, nr. 155).⁴²⁹ Een fundamenteel verschil met de rechtspraak van het HvJ betreft het feit dat het EHRM aanvaardt dat algemene bewaring en toegang tot gegevens mogelijk is, zonder dat deze personeel of geografisch afgebakend dient te worden, of de toegang beperkt moet blijven tot personen ten aanzien van wie concrete aanwijzingen bestaan van betrokkenheid bij een strafbaar feit (Cf. *supra*, nrs. 107 en 140). Dit illustreert dat onder het toezichtskader van het EHRM ruimere toepassingsvoorwaarden mogelijk zijn voor het toestaan van zoektermbevelen en het bewaring van relevante gegevens.

198. De derde vereiste heeft betrekking op de procedurele voorwaarden die in acht moeten worden genomen bij het verlenen van een machtiging tot het uitvoeren van een zoektermbevel. Gelet op het Belgische strafprocesrecht, waarin een fundamenteel onderscheid wordt gemaakt tussen de bevoegdheden van de PdK en die van de onderzoeksrechter, verdient het aanbeveling om de bevoegdheid tot het uitvoeren van een zoektermbevel in beginsel toe te kennen aan de onderzoeksrechter. Enkel in strikt afgebakende gevallen kan overwogen worden deze bevoegdheid aan de PdK toe te kennen (Cf. *supra*, nr. 158). In alle andere gevallen dient, zoals eerder aanbevolen in het licht van de EU-regelgeving, de onderzoeksrechter via een gemotiveerde schriftelijke beslissing te toetsen of de maatregel voldoet aan de vereisten van rechtmatigheid, noodzakelijkheid, subsidiariteit en proportionaliteit (Cf. *supra*, nr. 158).⁴³⁰

199. Voorts is het noodzakelijk dat er voldoende procedurele waarborgen worden uitgewerkt met betrekking tot de selectie, analyse, het gebruik en de opslag van de verkregen gegevens. Deze procedureregels kunnen bij voorkeur nader worden gespecificeerd in een afzonderlijk KB, teneinde de praktische uitvoering op een gestandaardiseerde en controleerbare wijze te organiseren. In het kader van het selectieproces is het essentieel dat gebruik wordt gemaakt van vooraf bepaalde, duidelijk omschreven selectoren, met name specifieke zoektermen, die een aantoonbare relevante band vertonen met het onderzochte misdrijf. Indien de initiële selectie aanleiding geeft tot een te ruime of onbeheersbare hoeveelheid gegevens, dient het mogelijk te zijn om, binnen de grenzen van het oorspronkelijke bevel, bijkomende of meer verfijnde zoektermen toe te passen teneinde het relevante gegevensvolume te reduceren. Daarnaast dient ook duidelijk aangegeven te worden op welke categorieën van operatoren en gegevens een zoektermbevel betrekking kan hebben (Cf. *supra*, nr. 156). Wat de analyse betreft, verdient het aanbeveling dat deze wordt uitgevoerd door een daartoe aangestelde analist, die zich uitsluitend beperkt tot de gegevens die rechtstreeks voortvloeien uit de toepassing van de onderzochte zoektermen, zodat de analyse geen betrekking

⁴²⁸ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, § 292.

⁴²⁹ *Ibid*, §§ 289-294; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 372-376.

⁴³⁰ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 295-302; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 377-383.

kan hebben op de gehele zoekgeschiedenis van gebruikers. De analist kan daarbij tevens nagaan of de verwerking van de gegevens geen disproportionele inmenging in de persoonlijke levenssfeer tot gevolg heeft, en welke corrigerende maatregelen kunnen worden getroffen om deze inbreuk te minimaliseren. Het is daarnaast van cruciaal belang dat de gegevens uitsluitend mogen worden gebruikt voor het specifieke onderzoek waarvoor het bevel is afgegeven, dat informatie over onschuldige derden niet mag worden gebruikt en onmiddellijk dient te worden verwijderd, en dat betrokkenen na afloop van het onderzoek geïnformeerd dienen te worden, met de mogelijkheid om bezwaar of klacht in te dienen. Ten slotte dienen er passende waarborgen te worden ingebouwd met betrekking tot de opslag van de gegevens, dewelke moeten worden opgeslagen op een veilige en afgeschermd locatie, waarbij de toegang strikt beperkt is tot daartoe bevoegde personen. Daarnaast dienen er duidelijke richtlijnen te worden opgesteld met betrekking tot de mogelijkheid van het maken van kopieën en de beveiliging van de opgeslagen gegevens.⁴³¹

200. Evenals de regels met betrekking tot de selectie, analyse en opslag van gegevens, dienen er eveneens expliciete bepalingen te worden opgenomen over de duur van de maatregel, de opslagtermijn en de procedures voor het wissen en vernietigen van het verzamelde materiaal. De laatste twee aspecten kunnen opnieuw bij voorkeur worden geregeld in een KB. Wat betreft de duur van zoektermbevelen dient rekening te worden gehouden met de ernst van het misdrijf, de waarschijnlijkheid dat de zoektermen op korte termijn nog relevante resultaten opleveren, en de impact op de privacy van de betrokkenen. Voor een specifieke aanbeveling met betrekking tot de duur van het bevel wordt verwezen naar de eerder geformuleerde aanbeveling in het licht van de toepasselijke EU-regelgeving en relevante rechtspraak (Cf. *supra*, nr. 157). Met betrekking tot de maximale bewaartermijn wordt aanbevolen dat gegevens slechts worden bewaard gedurende de periode die strikt noodzakelijk is voor het strafrechtelijk onderzoek. Daarbij kan worden aangesloten bij de eerder geformuleerde aanbeveling inzake bewaarplicht in het kader van het Unierecht (Cf. *supra*, nr. 134). Daarnaast dienen er vernietigingsprocedures te worden vastgesteld die waarborgen dat gegevens worden verwijderd of gewist zodra de maximale bewaartermijn is verstreken, of wanneer blijkt dat de gegevens niet langer relevant zijn voor het onderzoek.⁴³²

201. Wat betreft de regels met betrekking tot de toegang tot het verzamelde materiaal door derden, heeft het EHRM geoordeeld dat een voldoende waarborg bestaat wanneer toegang uitsluitend wordt verleend aan personen die daadwerkelijk een noodzaak hebben om kennis te nemen van het materiaal, overeenkomstig het zogenaamde 'need-to-know'-beginsel. Dit beginsel houdt in dat toegang alleen wordt verleend wanneer dit strikt noodzakelijk is voor de uitvoering van taken die verband houden met de vastgestelde doelen van de maatregel, namelijk nationale of openbare veiligheid of de bestrijding van ernstige criminaliteit.⁴³³ In het kader van zoektermbevelen kunnen

⁴³¹ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 303-316; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 384-391.

⁴³² EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 331-344; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 400-405.

⁴³³ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden, §§ 331-344; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 317-330.

opsporingsautoriteiten dan ook toegang krijgen tot de gegevens, mits dit noodzakelijk is voor het voortzetten van het onderzoek.

202. Tot slot dient er aandacht besteed te worden aan de procedures en modaliteiten voor toezicht en onafhankelijke toetsing ex post van zoektermbevelen. Binnen het Belgische strafprocesrecht ziet de onderzoeksrechter toe op de rechtmatigheid, noodzakelijkheid en proportionaliteit van onderzoeksmethoden tijdens het gerechtelijk onderzoek en de mini-instructie.⁴³⁴ Dit toezicht dient ook van toepassing te zijn op zoektermbevelen.⁴³⁵ Daarnaast vervult de Kamer van Inbeschuldigingstelling (hierna: KI) een toezichthoudende rol binnen het gerechtelijk onderzoek. Indien de KI tijdens haar controle een onregelmatigheid, een verzuim of een nietigheid vaststelt dat de geldigheid van een onderzoekshandeling aantast, beschikt zij over de bevoegdheid om de nietigheid van die handeling uit te spreken.⁴³⁶ Wat betreft de ex post facto toetsing binnen het Belgische strafprocesrecht, bestaan er verschillende waarborgen. Zo kan de raadkamer, hetzij ambtshalve, hetzij op verzoek van een partij, de nietigheid uitspreken van onderzoekshandelingen die met onregelmatigheden, verzuim of nietigheden gepaard gaan.⁴³⁷ Tegen beslissingen van de raadkamer staat hoger beroep open bij de KI, ook wanneer deze weigert een gevraagde nietigheid uit te spreken.⁴³⁸ Indien evenwel geen beroep werd ingesteld en de KI zich niet over het middel heeft uitgesproken, blijft het mogelijk om dit alsnog aan het vonnisgerecht voor te leggen.

Wanneer een zoektermbevel wordt toegepast in het kader van een mini-instructie, en dus binnen de context van een opsporingsonderzoek, treden de raadkamer en de KI niet op als controleorganen. In dergelijke gevallen moeten partijen eventuele onregelmatigheden met betrekking tot de onderzoekshandelingen aan het vonnisgerecht voorleggen als procedurefout. Op het onderscheid waarbij in het gerechtelijk onderzoek aanzienlijk meer procedurele waarborgen gelden dan in het opsporingsonderzoek, is reeds kritiek geuit, en er wordt gewerkt aan mogelijke wetwijzigingen om deze discrepantie te remediëren.⁴³⁹

B. Legitieme doelstelling

203. De rechtvaardigingsgronden voor strafrechtelijke onderzoeksstrategieën, zoals de bescherming van de openbare orde, het voorkomen van strafbare feiten, de nationale en openbare veiligheid, en de rechten en vrijheden van anderen, zullen ook van toepassing zijn in het kader van zoektermbevelen.

⁴³⁴ VERSTRAETEN R. en VERBRUGGEN F., *Strafrecht en strafprocesrecht voor bachelors*, Intersentia, 2020, 154.

⁴³⁵ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden', §§ 345-535; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', §§ 406-412.

⁴³⁶ Art. 235bis, § 6 Sv.

⁴³⁷ Art. 131, §1 SV.

⁴³⁸ Art. 135, §§ 1-2 Sv.

⁴³⁹ VERSTRAETEN R. en BAILLEUX A., 'Het voorstel van een nieuw wetboek van straffordering: algemene beginselen en fase van het onderzoek' in BAILLEUX A., SPRIET B., VAN HERPE R., VANHEUL J., VERBRUGGEN F. en VERSTRAETEN R. (eds.), *Themis 110 – Straf- en strafprocesrecht*, die Keure, 2019, (143).

C. Noodzakelijk in democratische samenleving

204. Of een maatregel die zoekmachinebedrijven verplicht om gegevens van individuen die bepaalde zoektermen hebben ingevoerd op te slaan en door te geven aan politionele instanties, de toets van noodzakelijkheid in een democratische samenleving zal doorstaan, zal afhankelijk zijn van een beoordeling per geval, rekening houdend met de bovenvermelde criteria. Cruciaal in deze beoordeling zal de vraag zijn of de strafrechtelijke legitieme doelstelling daadwerkelijk opweegt tegen de aanzienlijke inbreuk op het recht op privacy en gegevensbescherming. Dit geldt met name gezien het grootschalige karakter van de maatregel, waarbij de zoekgeschiedenis van duizenden mensen wordt onderzocht en op basis daarvan gegevens worden verstrekt aan politiediensten.

§ 4: Tussenconclusie

205. Het is duidelijk dat het EHRM een soepelere benadering hanteert dan het HvJ ten aanzien van een algemene bewaarplicht en nationale regelgeving die de toegang tot dergelijke bewaarde gegevens regelt in het kader van strafrechtelijke onderzoeken. Volgens het EHRM is een algemene gegevensbewaring met bijhorende toegang niet per definitie ingrijpender dan een gerichte maatregel, op voorwaarde dat er voldoende doeltreffende waarborgen bestaan ter bescherming van willekeur en machtsmisbruik. Tegelijkertijd benadrukt het EHRM wel dat in gevallen van algemene dataretentie en toegang de beoordelingsmarge van de lidstaten kleiner is, en dat strengere en uitgebreidere waarborgen vereist zijn dan bij gerichte onderzoeksmethodes.⁴⁴⁰

206. De door het EHRM gestelde waarborgen in het kader van bulkinterceptiemaatregelen, waaronder een algemene bewaarplicht en algemene toegang tot gegevens, zijn dubbelzinnig geformuleerd en laten ruimte voor uiteenlopende interpretaties. Deze vaagheid weerspiegelt de ruime beoordelingsmarge die het EHRM aan de lidstaten toekent op het vlak van opsporingsmaatregelen. Hoewel het EHRM in essentie gelijkaardige vereisten oplegt als het HvJ, zoals voorafgaande rechterlijke toetsing, een beperkt toepassingsgebied, een begrensde bewaartermijn en het naleven van het noodzakelijkheidsbeginsel, formuleert het deze in minder strikte en meer open bewoordingen. In het kader van zoektermbevelen impliceert dit dat lidstaten over een zekere beleidsruimte beschikken bij de invulling van deze waarborgen. Niettemin verdient het aanbeveling terughoudendheid te betrachten en geen al te soepele benadering te hanteren, teneinde de maatregel te laten slagen voor de noodzakelijkheidstoets.

207. Samenvattend kan worden aangenomen dat, indien zoektermbevelen aan het EHRM zouden worden voorgelegd, het Hof zou verlangen dat dergelijke maatregelen worden omkaderd door duidelijke juridische gronden, nauw omschreven toepassingsvoorwaarden, een voorafgaande machtigingsprocedure, regels omtrent selectie, analyse, gebruik, doorgifte, bewaring en vernietiging van gegevens, alsook door een onafhankelijk toezichtmechanisme en een ex post toetsing door een onafhankelijke instantie.

⁴⁴⁰ EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden', § 261; EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk', § 347; X, 'noot onder EHRM 19 juni 2018', *T.Strafr.* 2019/1, (47) 64; JANSSEN R.H.T., 'Big Brother Watch e.a., Centrum för Rättvisa en het toezicht op de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2022/51, (97) 97.

208. O.i. hanteert het EHRM, in vergelijking met het HvJ, een meer evenwichtige benadering ten aanzien van de verhouding tussen het recht op privacy en de noodzaak tot misdaadbestrijding. Door lidstaten beoordelingsruimte te laten bij de concretisering van de opgelegde waarborgen, worden innovatieve en ingrijpende online onderzoeksmethoden niet op voorhand uitgesloten. Binnen dit jurisprudentieel kader lijkt de inzet van zoektermbevelen een kans op slagen te hebben, op voorwaarde dat de door het EHRM gestelde waarborgen op correcte en voldoende zorgvuldige wijze worden uitgewerkt.

209. Het is evenwel onzeker in hoeverre de door het EHRM geformuleerde waarborgen onverkort van toepassing moeten zijn op zoektermbevelen, gezien het specifieke karakter van deze maatregel. Hoewel dergelijke bevelen potentieel een brede gebruikersgroep treffen, beperken zij zich tot gerichte zoekopdrachten en impliceren zij geen volledige inzage in iemands zoekgeschiedenis. De concrete impact op de persoonlijke levenssfeer is daardoor minder uitgesproken, wat mogelijk aanleiding geeft tot een meer genuanceerde beoordeling.

Conclusie

211. Dit onderzoek tracht een antwoord te bieden op de volgende centrale onderzoeksvraag: *"In welke mate is een onderzoeksmethode waarbij onbekende daders worden opgespoord op basis van gebruikte zoektermen juridisch mogelijk binnen het Belgisch wetgevend kader, vanuit Europees (Unie)rechtelijk perspectief?"*.

212. Hoewel zoektermbevelen de opsporing van misdrijven ten goede zou komen, blijkt uit dit onderzoek dat de implementatie ervan geen vanzelfsprekendheid is in het licht van de strikte voorwaarden die voortvloeien uit het recht op privacy en gegevensbescherming, zoals neergelegd in artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, de Algemene Verordening Gegevensbescherming en artikel 8 van het Europees Verdrag voor de Rechten van de Mens. Deze normen worden versterkt door de rechtspraak van het Hof van Justitie van de Europese Unie en het Europees Hof voor de Rechten van de Mens, die het belang van privacy en gegevensbescherming consequent onderstrepen. Vanuit dit normatieve kader wordt een aanbeveling geformuleerd over de juridische toelaatbaarheid en toepassingsvoorwaarden van zoektermbevelen in België.

213. In eerste instantie verdient het aanbeveling om, ter waarborging van de effectiviteit van zoektermbevelen, een wettelijke bewaarplicht in te voeren die zoekmachinebedrijven verplicht tot het bewaren van zoekgeschiedenissen en gerelateerde gegevens. Een opsporingsmethode die afhankelijk is van gegevensinzage is immers slechts doeltreffend indien die gegevens ook effectief bewaard zijn. De invoering van een bewaarplicht is echter niet evident, aangezien het grootschalig verzamelen van persoonsgegevens een verregaande inmenging in het recht op privacy en gegevensbescherming inhoudt. Zowel het HvJ als het EHRM hebben zich uitgesproken over een dergelijke maatregel in het licht van elektronische communicatie. Het EHRM aanvaardt in principe bulkinterceptiemaatregelen, mits voorzien van waarborgen ter voorkoming van willekeur en misbruik, maar laat daarbij een ruime appreciatiemarge aan de lidstaten. Het HvJ daarentegen hanteert streng afgebakende voorwaarden en benadrukt het uitzonderlijke karakter van een algemene bewaarplicht, waarbij het overwegend opteert voor gerichte gegevensbewaring. Gelet op de vaagheid van de waarborgen vereist door het EHRM en de duidelijk omschreven, strengere voorwaarden van het HvJ, dient, overeenkomstig artikel 53 EVRM en artikel 53 van het EU-Handvest, de voorkeur te worden gegeven aan de beschermingsnormen zoals ontwikkeld in de rechtspraak van het HvJ, aangezien deze het hoogste beschermingsniveau bieden.

214. In overeenstemming met de rechtspraak van het HvJ aangaande het creëren van een bewaarplicht inzake elektronische communicatie kan een aanbeveling gedaan worden hoe regelgeving aangaande een bewaarplicht ten aanzien van zoekmachinebedrijven van zoekgeschiedenissen, en daaraan gekoppelde gegevens, zoals identificatiegegevens, IP-adressen, gegevens betreffende het tijdstip en de duur van de activiteit, de ingevoerde zoektermen, de gebruikte browser, het apparaattype en de locatie voor politionele doeleinden te bewaren, eruit zou moeten zien. Identificatiegegevens van gebruikers kunnen te allen tijde worden bewaard met het oog op bestrijding van gewone strafbare feiten en andere hogere rechtsdoeleinden. Voor IP-adressen

gekoppeld aan het apparaat waarmee zoekopdrachten zijn uitgevoerd kan eveneens een algemene bewaarplicht worden overwogen, maar dan slechts in het kader van de bestrijding van zware criminaliteit en ter bescherming van de nationale en openbare veiligheid. Aangezien zoekgeschiedenissen en de daaraan gekoppelde metadata een diepgaand inzicht verschaffen in het privéleven van de gebruiker, kan een algemene bewaarplicht met betrekking tot deze gegevens enkel worden gerechtvaardigd indien zij noodzakelijk is ter bescherming van de nationale veiligheid. Voor doeleinden in verband met zware criminaliteit en de handhaving van de openbare orde komt slechts een gerichte dataretentie in aanmerking. Een dergelijke gerichte bewaring kan bijvoorbeeld worden gerealiseerd door zoekgeschiedenissen uitsluitend op te slaan binnen afgebakende risicogebieden, bepaald op basis van objectieve criteria zoals een verhoogde frequentie van zware criminaliteit of een verhoogd dreigingsniveau. Alternatief kan worden voorzien in de bewaring van zoekopdrachten die verband houden met dergelijke risicogebieden, ongeacht de verblijfplaats van de gebruiker, op voorwaarde dat de retentie strikt beperkt blijft tot die zoekopdrachten en niet de volledige zoekgeschiedenis omvat.

215. Overeenkomstig de vereisten van de Algemene Verordening Gegevensbescherming en het proportionaliteitsbeginsel, dat vereist dat inmenging in de persoonlijke levenssfeer niet verder reikt dan strikt noodzakelijk, dient steeds een duidelijk afgebakende bewaartermijn te worden vastgelegd. In aansluiting op de dataretentiewet inzake elektronische communicatie wordt een gedifferentieerde regeling aanbevolen, afgestemd op het type gegevens. Voor identificatiegegevens en IP-adressen kan een bewaartermijn van twaalf maanden worden gehanteerd. Voor zoekgeschiedenissen en bijbehorende metadata wordt een termijn tussen zes en twaalf maanden aangewezen, afhankelijk van de ernst en frequentie van de betrokken strafbare feiten. In het kader van een algemene bewaarplicht ter bescherming van de nationale veiligheid kan bewaring gerechtvaardigd zijn zolang een concrete dreiging voor de nationale veiligheid voortduurt, aangevuld met een periode van zes maanden na het wegvallen van die dreiging.

216. Wanneer de relevante gegevens zijn opgeslagen, is een afzonderlijke wettelijke grondslag vereist die de toegang tot deze gegevens door politionele instanties regelt. Het enkele feit dat gegevens rechtmatig worden bewaard, impliceert immers niet dat bevoegde autoriteiten automatisch of onbeperkt toegang verkrijgen. De Belgische wetgever dient daarom te voorzien in een duidelijke wettelijke basis die zoektermbevelen reguleert, waarbij expliciet wordt bepaald onder welke voorwaarden autoriteiten toegang kunnen verkrijgen tot gegevens van personen die een bepaalde zoekterm hebben ingevoerd.

217. De toegang tot bewaarde gegevens vormt, net als de bewaring zelf, een ernstige inmenging in het recht op privacy en gegevensbescherming van gebruikers. Het EHRM past in dit verband dezelfde algemeen geformuleerde waarborgen toe als bij een bewaarplicht, aangezien zowel gegevensbewaring als toegang tot deze gegevens worden beschouwd als onderdelen van bulkinterceptiemaatregelen. Het HvJ daarentegen hanteert scherp afgebakende en strikt geformuleerde voorwaarden voor een legitieme toegang. Gelet op het hogere beschermingsniveau dat door het HvJ wordt gewaarborgd, dient diens benadering ook in dit verband voorrang te krijgen.

218. Een nationale regeling inzake zoektermbevelen dient, conform de rechtspraak van het HvJ, duidelijke en nauwkeurige bepalingen te bevatten over de reikwijdte en toepassing van de maatregel, evenals heldere materiële en procedurele voorwaarden vast te stellen zodat duidelijk is onder welke omstandigheden en onder welke voorwaarden toegang aan bevoegde autoriteiten kan worden verleend. Zo is het in eerste instantie aanbevolen om duidelijk aan te geven welke instanties toegang kunnen krijgen tot de bewaarde gegevens. In aansluiting op de bestaande dataretentiewetgeving kan worden aanbevolen om de toegangsgraad afhankelijk te maken van de gevoeligheid van de betrokken gegevens. Voor gevoelige gegevens, zoals zoekgeschiedenissen en IP-adressen, verdient het aanbeveling de toegang te beperken tot een beperkte groep bevoegde instanties, waaronder inlichtingen- en veiligheidsdiensten, openbare veiligheidsautoriteiten, instellingen belast met de bescherming van vitale belangen, gerechtelijke autoriteiten en toezichthoudende gegevensbeschermingsautoriteiten.

De nationale bepaling inzake zoektermbevelen dient duidelijke bepalingen te bevatten omtrent de toepasselijke juridische gronden, de omstandigheden die een bevel rechtvaardigen, de reikwijdte, de duur van de maatregel en de vereiste voorafgaande controle door een onafhankelijke instantie. De juridische grondslagen dienen beperkt te blijven tot ernstige misdrijven en bedreigingen van de nationale of openbare veiligheid, bij voorkeur vastgelegd in een geactualiseerde versie van de taplijst. De vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit moeten concreet worden ingevuld, onder meer door het bepalen dat een zoektermbevel slechts kan worden uitgevaardigd wanneer andere opsporingsmethoden tekortschieten, en de betrokken zoektermen duidelijk af te bakenen zodat het proportioneel blijft in het licht van het privéleven van betrokkene. Volgens het HvJ is bovendien slechts gerichte toegang toelaatbaar, wat betekent dat het bevel beperkt moet blijven tot personen die verdacht worden van betrokkenheid bij een ernstig misdrijf. Enkel in uitzonderlijke gevallen kan toegang worden uitgebreid tot anderen. De bepaling moet voorts preciseren dat het bevel gericht is op zoekmachinebedrijven en enkel toegang verleent tot ingevoerde zoektermen en bijhorende metadata. Wat de temporele reikwijdte betreft, wordt aanbevolen de toegang te beperken tot een vooraf bepaalde periode voor het misdrijf: maximaal twaalf maanden bij nationale veiligheid of openbare orde, en bij voorkeur korter (bijvoorbeeld negen maanden) bij ernstige criminaliteit. Tot slot dient de machtiging voor het bevel principieel bij de onderzoeksrechter te liggen, met slechts beperkte uitzonderingen voor de PdK.

219. De voorwaarden en grenzen die het HvJ stelt in het licht van een bewaarplicht en toegang daartoe, ondermijnt de effectiviteit van zoektermbevelen. Het feit dat een bewaarplicht voor zoekgeschiedenissen en daaraan gekoppelde metadata enkel in uitzonderlijke gevallen, met name bij nationale veiligheid, algemeen kan worden opgelegd, en voor ernstige criminaliteit en openbare orde slechts een gerichte bewaring toelaat, heeft tot gevolg dat veel cruciale gegevens niet kunnen worden opgeslagen. Aangezien wordt aanbevolen te werken met een geografische afbakening, vallen zoekopdrachten buiten het geselecteerde geografische kader buiten de reikwijdte van de bewaring, wat ertoe leidt dat potentieel waardevolle informatie verloren gaat. Het HvJ beperkt de toegang tot bewaarde gegevens bovendien in aanzienlijke mate, aangezien het vereist dat deze steeds gericht is. Aangezien zoektermbevelen net gericht zijn op de identificatie van onbekende daders, veronderstellen zij geen vooraf geïdentificeerde personen, waardoor zij moeilijk verzoenbaar zijn met

de vereiste van gerichte toegang. In de praktijk zouden zoektermbevelen daardoor beperkt moeten blijven tot uitzonderlijke situaties waarin vitale belangen, zoals nationale of openbare veiligheid, in het geding zijn. Hierdoor verliezen zoektermbevelen grotendeels hun nut binnen het klassieke strafrechtelijk onderzoek.

220. Naar onze mening slaagt de huidige rechtspraak van het HvJ er niet in een adequaat evenwicht te waarborgen tussen enerzijds het recht op privacy en anderzijds de noodzaak tot effectieve misdaadbestrijding. Het HvJ lijkt de bescherming van de persoonlijke levenssfeer onevenredig te laten primeren, hetgeen leidt tot een aanzienlijke beperking van de opsporingsmogelijkheden binnen het digitale domein. In een context waarin misdrijven steeds vaker digitaal worden voorbereid, is een proportionele uitbreiding van de opsporingscapaciteiten noodzakelijk. De waarborgen die het EHRM in het kader van bulkinterceptie oplegt, waarbij een zekere beoordelingsvrijheid aan de lidstaten wordt gelaten voor de invulling ervan binnen nationale wetgeving, bieden volgens ons een evenwichtigere benadering tussen het recht op privacy en de noodzaak tot misdaadbestrijding. Juist doordat zij meer ruimte laten voor afwegingen op nationaal niveau, sluiten deze waarborgen volgens ons beter aan bij de realiteit van moderne opsporingsbehoeften.

221. Hoe de Hoven zich uiteindelijk zullen uitspreken over nationale bepalingen inzake zoektermbevelen blijft vooralsnog onzeker. Centraal staat de vraag of zij dezelfde voorwaarden en grenzen zouden toepassen als die momenteel gelden voor dataretentie en de toegang tot elektronische communicatiegegevens. Aangezien zoektermbevelen doorgaans betrekking hebben op één of meerdere specifieke zoektermen, en niet op de volledige zoekgeschiedenis van gebruikers, rijst de vraag of de bestaande beperkingen zonder meer op dit type bevel van toepassing moeten zijn. Wat wel vaststaat is dat het laatste woord over online opsporingsmethoden en hun verhouding tot het recht op privacy nog niet is gezegd. Het debat staat immers nog maar aan het begin, zeker nu technologische evoluties zowel daders als opsporingsautoriteiten steeds meer digitale mogelijkheden bieden en dit in de toekomst alleen maar verder zal toenemen.

222. De centrale onderzoeksvraag kan dan ook als volgt worden beantwoord: zoektermbevelen zijn juridisch mogelijk binnen het Belgisch kader, voor zover zij verankerd worden in een wettelijk systeem dat de Europese normen inzake privacy en gegevensbescherming volledig respecteert. De in dit onderzoek geformuleerde aanbevelingen reiken een concreet model aan waarin dergelijke bevelen grondwettelijk kunnen functioneren. De werkelijke uitdaging ligt nu in de politieke en juridische vertaling ervan. In een context van snelle digitalisering en toenemende online dreigingen is het aan de wetgever en de rechtspraak om deze opsporingsmethode niet enkel mogelijk, maar ook houdbaar te maken binnen een rechtstaat die haar kernwaarden bewaakt.

Lijst van geraadpleegde werken

§ 1: Wetgeving

België

Wetten in materiële zin

Koninklijk besluit van 8 februari 2011 tot wijziging van het koninklijk besluit van 9 januari 2003 tot uitvoering van de artikelen 46bis, § 2, eerste lid, 88bis, § 2, eerste en derde lid en 90quater, § 2, derde lid van het Wetboek van Strafvordering en van artikel 109terE, § 2 van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *BS* 23 februari 2011.

Koninklijk besluit tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging, *BS* 1 december 2012.

Wetboek van strafvordering, *BS* 17 november 1808.

Wet van 11 februari 1991 tot invoeging van een artikel 88bis in het Wetboek van Strafvordering, *BS* 16 maart 1991.

Wet van 5 augustus 1992 op het politieambt, *BS* 22 december 1992.

Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privécommunicatie en -telecommunicatie, *BS* 24 januari 1995.

Wet tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, *BS* 22 september 1998.

Wet van 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001.

Wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, *BS* 12 mei 2003.

Wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005.

Wet van 27 december 2005 houdende diverse bepalingen, *BS* 30 december 2005.

Wet van 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90decies van het Wetboek van Strafvordering, *BS* 23 augustus 2013.

Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016.

Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, *BS* 17 januari 2017.

Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018.

Wet van 5 mei 2019 houdende diverse bepalingen in strafzaken en inzake erediensten, en tot wijziging van de wet van 28 mei 2002 betreffende de euthanasie en van het Sociaal Strafwetboek, *BS* 24 mei 2019.

Wet van 21 december 2021 houdende omzetting van het Europees Wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, *BS* 31 december 2021.

Wet 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, *BS* 8 augustus 2022.

Wet van 29 februari 2024 tot invoering van boek I van het Strafwetboek, *BS* 8 april 2024.

Parlementaire stukken en voorbereidende werken

Advies RvS 28 juni 2021, nr. 69.381/4.

Ontwerp van wet ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie, SENAAT, 1992-1993, 18 mei 1994, nr. 843/2.

Ontwerp van wet tot invoeging van een artikel 90bis in het Wetboek van Strafvordering, SENAAT, 1990-1991, 20 november 1990, nr. 1118/2.

Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecomunicaties, KAMER, 2015-2016, 8 juli 2016, nr. 54K1966/001.

Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, KAMER, 2021-2022, 17 maart 2022, nr. 55K2572/001.

Wetsontwerp inzake informaticacriminaliteit, KAMER, 1999-2000, 3 november 1999, nr. 50K0213/001.

Wetsontwerp inzake informaticacriminaliteit, KAMER, 1999-2000, 24 maart 2000, nr. 50K0213/004.

Wetsontwerp tot wijziging van artikel 46bis van het Wetboek van strafvordering, SENAAT, 2005-2006, 31 juli 2006, nr. 3-1824/1.

Wetsontwerp tot invoeging van een artikel 90bis in het Wetboek van Strafvordering, KAMER, 1984-1985, 28 juni 1985, nr. 45K1234/002.

Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, KAMER, 1996-1997, 12 november 1997, nr. 49K1075/001.

Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, KAMER, 1996-1997, 12 november 1997, nr. 49K1075/007.

Wetsontwerp tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie, SENAAT, 1997-1998, 25 maart 1998, nr. 1-828/3.

Amerika

Wetten in materiële zin

Assembly Bill A84A van State of New York van 6 januari 2021.

Electronic Keyword and Location Amendments HB0251 van State of Utah van 26 januari 2021.

Europa

Wetten in materiële zin

Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden van 4 november 1950, BS 19 augustus 1955.

Handvest van de grondrechten van de Europese Unie, Pb.C. 83, 30 maart 2010.

Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, Pb.L. 23 november 1995.

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 (richtlijn betreffende privacy en elektronische communicatie), *Pb.L.* 31 juli 2002.

Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, *pb.L.* 13 april 2006.

Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad, *Pb.L.* 4 mei 2016.

Verdrag ter bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, *BS* 30 december 1993.

Verordening 2016/679 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, *Pb.L.* 4 mei 2016.

§ 2: Rechtspraak

België

HvB Antwerpen 15 november 2017, nr. 2016/CO/1006, *Juristenkrant* 2017/359.

Cass. 23 juni 1999, P.99.0663.F, ECLI:BE:CASS:1999:ARR.19990623.13.

Cass. 28 december 2004, P.04.1647.F, ECLI:BE:CASS:2004:ARR.20041228.1.

Cass. 19 januari 2005, P.04.1383.F, ECLI:BE:CASS:2005:ARR.20050119.6.

Cass. 10 november 2009, P.09.1584.F, ECLI:BE:CASS:2009:ARR.20091110.3.

Cass. 18 januari 2011, P.10.1347.N, ECLI:BE:CASS:2011:CONC.20110118.1.

Cass. 24 mei 2011, P.11.0909.N, ECLI:BE:CASS:2011:ARR.20110524.10.

Cass. 7 juni 2016, P.16.0294.N/1, ECLI:BE:CASS:2016:ARR.20160607.7.

Cass. 5 november 2019, P.19.0426.N, ECLI:BE:CASS:2019:ARR.20191105.2.

GwH 11 juni 2015, 84/2015.

GwH 19 juli 2018, 96/2018.

GwH. 6 december 2018, 174/2018.

GwH 22 april 2021, 57/2021.

GwH 26 september 2024, 97/2024, ECLI:BE:GHCC:2024:ARR.097.

Amerika

U.S. Court of Appeal for the Fourth Circuit 9 juli 2024, nr. 22-4489, 'United States/Chatrie'.

U.S. Court of Appeal for the Ninth Circuit 9 april 2020, 956 F.3d 589, 'In re Facebook, Inc. Internet Tracking Litig.'.

U.S. Court of Appeal for the Third Circuit 11 december 2014, 806 F.3d 125, 'In re Google Inc. Cookie Placement Consumer Priv. Litig.'.

U.S. District Court for the Northern District of Illinois Eastern Division 24 augustus 2020, 481 F. Supp. 3d 730, 'In re Search of Info. Stored at Premises Controlled by Google'.

U.S. Supreme Court 18 december 1967, 389 U.S. 347, 'Katz/United States'.

U.S. Supreme Court 21 april 1976, 425 U.S. 435, 'United States/Miller'.

U.S. Supreme Court 20 juni 1979, 442 U.S. 735, 'Smith/Maryland'.

U.S. Supreme Court 28 november 1979, 444 U.S. 88, 'Ybarra/Illinois'.

U.S. Supreme Court 8 juni 1983, 462 U.S. 213, 'Illinois/Gates'.

U.S. Supreme Court 2 januari 2012, 615 F. 3d 544, 'United States/Jones'.

U.S. Supreme Court 22 juni 2018, 138 S. Ct. 2206, 'Carpenter/United States'.

U.S. Supreme Court Colorado 16 oktober 2023, nr. 23SA12, 'People/Seymour'.

Hof van Justitie

HvJ 24 november 2011, C-70/10, ECLI:EU:C:2011:771, 'Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs'.

HvJ 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238, 'Digital Rights Ireland'.

HvJ 13 mei 2014, C-131/12, ECLI:EU:C:2014:317, 'Google Spain en Google Inc./Agencia Española de Protección de Datos en Mario Costeja González'.

HvJ 1 oktober 2015, C-230/14, ECLI:EU:C:2015:639, 'Weltimmo s.r.o./Nemzeti Adatvédelmi és Információszabadság Hatóság'.

HvJ 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779, 'Patrick Breyer/Bondsrepubliek Duitsland'.

HvJ 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970, 'Tele2 Sverige AB'.

HvJ 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788, 'Ministerio Fiscal'.

HvJ 24 september 2019, C-507/19, ECLI:EU:C:2019:772, 'Google LCC/Commission nationale de l'informatique et des libertés'.

HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, 'La Quadrature du Net/premier ministre'.

HvJ 6 oktober 2020, C-623/14, ECLI:EU:C:2020:790, 'Privacy International/Secretary of State for Foreign and Commonwealth Affairs'.

HvJ 2 maart 2021, C-746/18, ECLI:EU:C:2021:152, 'Prokuratuur'.

HvJ 5 april 2022, C-140/20, ECLI:EU:C:2022:258, 'Commissioner of An Garda Síochána'.

HvJ 21 juni 2022, C-817/19, ECLI:EU:C:2022:491, 'Ligue des droits humains'.

HvJ 20 september 2022, C-793/19 en C-749/19, ECLI:EU:C:2022:702, 'SpaceNet en Telekom Deutschland'.

Verzoek de Hoge Raad der Nederlanden van 6 april 2022 in de zaak C-241/22.

Europees Hof voor de Rechten van de Mens

EHRM 6 september 1978, 5029/71, ECLI:CE:ECHR:1978:0906JUD000502971, 'Klass e.a./Duitsland'.

EHRM 2 augustus 1984, 8691/79, ECLI:CE:ECHR:1984:0802JUD000869179, 'Malone/Verenigd Koninkrijk'.

EHRM 26 maart 1987, 9248/81, ECLI:CE:ECHR:1987:0326JUD000924881, 'Leander/Zweden.
 EHRM 24 april 1990, 11105/84, ECLI:CE:ECHR:1990:0424JUD001110584, 'Huvig/Frankrijk'.
 EHRM 24 april 1990, 11801/85, ECLI:CE:ECHR:1990:0424JUD001180185, 'Kruslin/Frankrijk'.
 EHRM 19 mei 1994, 15225/89, ECLI:CE:ECHR:1994:0519REP001522589, 'Friedl/Oostenrijk'.
 EHRM 28 oktober 1994, 14310/88, ECLI:CE:ECHR:1994:1028JUD001431088, 'Murray/Verenigd Koninkrijk'.
 EHRM 25 februari 1997, 22009/93, ECLI:CE:ECHR:1997:0225JUD002200993, 'Z./Finland'.
 EHRM 30 juli 1998, 58/1997/842/1048, ECLI:CE:ECHR:1998:0730JUD002767195, 'Valenzuela Contreras/Spanje'.
 EHRM 7 september 1998, 47/1998/950/1165, ECLI:CE:ECHR:1998:0907JUD003093096, 'B.B./Frankrijk'.
 EHRM 16 februari 2000, 27798/95, ECLI:CE:ECHR:2000:0216JUD002779895, 'Amann/Zwitserland'.
 EHRM 4 mei 2000, 28341/95, ECLI:CE:ECHR:2000:0504JUD002834195, 'Rotaru/Roemenië'.
 EHRM 25 september 2001, 44787/98; ECLI:CE:ECHR:2001:0925JUD004478798, 'P.G. en J.H./Verenigd Koninkrijk'.
 EHRM 18 februari 2003, 58496/00, ECLI:CE:ECHR:2003:0218JUD005849600, 'Prado Bugallo/Spanje'.
 EHRM 17 juli 2003, 63737/00, ECLI:CE:ECHR:2003:0717JUD006373700, 'Perry/Verenigd Koninkrijk'.
 EHRM 31 mei 2005, 64330/01, ECLI:CE:ECHR:2005:0531JUD006433001, 'Antunes Rocha/Portugal'.
 EHRM 19 oktober 2005, 32555/96, ECLI:CE:ECHR:2005:1019JUD003255596, 'Roche/Verenigd Koninkrijk'.
 EHRM 6 juni 2006, 62332/00, ECLI:CE:ECHR:2006:0606JUD006233200, 'Segerstedt-Wiberg e.a./Zweden'.
 EHRM 29 juni 2006, 54934/00, ECLI:CE:ECHR:2006:0629DEC005493400, 'Weber en Saravia/Duitsland'.
 EHRM 3 april 2007, 62617/00, ECLI:CE:ECHR:2007:0403JUD006261700, 'Copland/Verenigd Koninkrijk'.
 EHRM 4 december 2008, 30562/04, 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, 'S. en Harper/Verenigd Koninkrijk'.
 EHRM 10 februari 2009, 3514/02, ECLI:CE:ECHR:2009:0210JUD000351402, 'Eerikäinen e.a./Finland'.
 EHRM 10 maart 2009, 4378/02, ECLI:CE:ECHR:2009:0310JUD000437802, 'Bykov/Rusland'.

EHRM 9 juni 2009, 72094/01, ECLI:CE:ECHR:2009:0609JUD007209401, 'Kvasnica/Slowakije'.

EHRM 27 oktober 2009, 21737/03, ECLI:CE:ECHR:2009:1027JUD002173703, 'Haralambie/Roemenië', § 77.

EHRM 17 december 2009, 16428/05, ECLI:CE:ECHR:2009:1217JUD001642805, 'Gardel/Frankrijk'.

EHRM 17 december 2009, 22115/06, ECLI:CE:ECHR:2009:1217JUD002211506, 'M.B./Frankrijk'.

EHRM 18 mei 2010, 26839/05, ECLI:CE:ECHR:2010:0518JUD002683905, 'kennedy/Verenigd Koninkrijk'.

EHRM 2 september 2010, 35623/05, ECLI:CE:ECHR:2010:0902JUD003562305, 'Uzun/Duitsland'.

EHRM 21 juni 2011, 30194/09, ECLI:CE:ECHR:2011:0621JUD003019409, 'Shimovolos/Rusland'.

EHRM 18 oktober 2011, 16188/07, ECLI:CE:ECHR:2011:1018JUD001618807, 'Khelili/Zwitserland'.

EHRM 17 april 2012, 20071/07, ECLI:CE:ECHR:2012:0417JUD002007107, 'Piechowicz/Polen'.

EHRM 31 juli 2012, 36662/04, ECLI:CE:ECHR:2012:0731JUD003666204, 'Drakšas/Litouwen'.

EHRM 13 november 2012, 43932/08, ECLI:CE:ECHR:2012:1113JUD004393208, 'Joanna Szulc/Polen'.

EHRM 18 april 2013, 19522/09, ECLI:CE:ECHR:2013:0418JUD001952209, 'M.K./Frankrijk'.

EHRM 4 juni 2013, 7841/08 en 57900/12; ECLI:CE:ECHR:2013:0604DEC000784108, 'Peruzzo en Martens/Duitsland'.

EHRM 12 december 2013, 20383/04, ECLI:CE:ECHR:2013:1212JUD00203830, 'Khmel/Rusland'.

EHRM 15 januari 2015, 68955/11, ECLI:CE:ECHR:2015:0115JUD006895511, 'Dragojević/Kroatië'.

EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, 'Roman Zakharov/Rusland'.

EHRM 7 juni 2016, 30083/10, ECLI:CE:ECHR:2016:0607JUD003008310, 'Karabeyoğlu/Turkije'.

EHRM 6 oktober 2016, 33696/11, ECLI:CE:ECHR:2016:1006JUD003369611, 'K.S. and M.S./Duitsland'.

EHRM 18 oktober 2016, 61838/10, ECLI:CE:ECHR:2016:1018JUD006183810, 'Vukota-Bojić/Zwitserland'.

EHRM 22 juni 2017, 8806/12, ECLI:CE:ECHR:2017:0622JUD000880612, 'Aycaguer/Frankrijk'.

EHRM 13 juli 2017, 45245/15, ECLI:CE:ECHR:2020:0213JUD004524515, 'Gaughran/Verenigd Koninkrijk'.

EHRM 5 september 2017, 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608, 'Bărbulescu/Roemenië'.

EHRM 27 juni 2017, 931/13, ECLI:CE:ECHR:2017:0627JUD000093113, 'Satakunnan Markkinapörssi Oy n Satamedia Oy/Finland'.

ECHR 8 februari 2018, 31446/12, ECLI:CE:ECHR:2018:0208JUD003144612, 'Ben Faiza/Frankrijk'.

EHRM 24 april 2018, 62357/14, ECLI:CE:ECHR:2018:0424JUD006235714, 'Benedik/Slovenië'.

EHRM 6 november 2018, 25527/13, ECLI:CE:ECHR:2018:1106JUD002552713, 'Vicent Del Campo/Spanje'.

EHRM 28 mei 2019, 173/15, ECLI:CE:ECHR:2019:0528JUD000017315, 'Liblik e.a./Estland'.

EHRM 24 juni 2019, 54414/13 en 54264/15; ECLI:CE:ECHR:2019:0124JUD005441413; 'Cordella e.a./Italië'.

EHRM 30 september 2019, 8429/05, ECLI:CE:ECHR:2014:0930JUD000842905, 'Prezhdarovi/Bulgarije'.

EHRM 17 oktober 2019, 1874/13, 8567/13, ECLI:CE:ECHR:2019:1017JUD000187413, 'López Ribalda e.a./Spanje'.

EHRM 30 januari 2020, 50001/12, ECLI:CE:ECHR:2020:0130JUD005000112, 'Breyer/Duitsland'.

EHRM 14 januari 2021, 59648/13, ECLI:CE:ECHR:2021:0114JUD005964813, 'Vig/Hongarije'.

EHRM 25 mei 2021, 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208, 'Centrum för Rättvisa/Zweden'.

EHRM 25 mei 2021, 58170/13, 62322/14 en 24960/15; ECLI:CE:ECHR:2021:0525JUD005817013; 'Big Brother Watch e.a./Verenigd Koninkrijk'.

EHRM 15 juni 2021, 73357/14, ECLI:CE:ECHR:2021:0615DEC007335714, 'Falzarano/Italië'.

EHRM 11 januari 2022, 70078/12, ECLI:CE:ECHR:2022:0111JUD007007812, 'Ekimdzhiev e.a./Bulgarije'.

EHRM 18 januari 2022, 14833/18, ECLI:CE:ECHR:2022:0118JUD001483318, 'Adomaitis/Litouwen'.

EHRM 8 juni 2022, 53069/15, ECLI:CE:ECHR:2022:0308JUD005306915, 'Sabani/België'.

EHRM 8 september 2022, 3153/16 en 27758/18, ECLI:CE:ECHR:2022:0908JUD000315316, 'Drelon/Frankrijk'.

EHRM 9 maart 2023, 36345/16; ECLI:CE:ECHR:2023:0309JUD003634516, 'L.B./Hongarije'.

EHRM 28 maart 2023, 34467/15, ECLI:CE:ECHR:2023:0328JUD003446715, 'Sârbu/Roemenië'.

EHRM 20 juni 2023, 36705/16, ECLI:CE:ECHR:2023:0620JUD003670516, 'Margari/Griekeland'.

EHRM 4 juli 2023, 11519/20, ECLI:CE:ECHR:2023:0704JUD001151920, 'Glukhin/Rusland'.

EHRM 13 februari 2024, 33696/19, ECLI:CE:ECHR:2024:0213JUD003369619, 'Podchasov/Rusland'.

§ 3: Rechtsleer

België

Handboeken

CONINGS C., *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017.

DAENINCK P., *Telefonieonderzoek in het strafrecht. Het triumviraat van de artikelen 46bis, 88bis en 90ter Sv*, die Keure, 2020.

DERUYCK F., BEERNAERT M-A, BERKMOES S. e.a., *Het Strafrecht bedreven. Liber Amicorum Alain De Nauw*, die Keure, 2011.

KERKHOF J. en VAN LINTHOUT P., *Cybercrime*, Politeia, 2013.

KESTEMONT L., SCHOUKENS P., HENDRICKX K. en TERRY E. (red.), *Rechtswetenschappelijk schrijven*, Acco, 2017.

VERSTRAETEN R., *Handboek Strafvordering*, Maklu 2012.

VERSTRAETEN R. en VERBRUGGEN F., *Strafrecht en strafprocesrecht voor bachelors*, Intersentia, 2020.

Bijdrage in verzamelwerken

CONINGS C. en ROYER S., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken' in Vlaamse Conferentie Balie Antwerpen (ed.), *Topic bewijs- en procesrecht*, Intersentia, 2017, 99.

DEWANDELEER D., 'Misdrijven en strafonderzoek in de IT-context' in VERSTRAETEN R. en VERBRUGGEN F. (ed.), *Straf- en strafprocesrecht*, die Keure, 2010, 125.

DE SMET B., 'Registratie en lokalisatie van telecommunicatie' in X. (ed.), *Strafrecht en strafvordering. Artikelsgewijze commentaar van rechtspraak (Comm.Straf.)*, Kluwer, 2018, 1.

VAN LINTHOUT P. en KERKHOF J., 'Actuele uitdagingen in cybercrime voor de advocatuur en de magistratuur: vervolgen en verdedigen met een bot scalpel?' in LIEVENS A., VALCKE P., DUMORTIER J., GRAUX H., KERKHOF J., LEFEVER K., SOMERS G., VAN LINTHOUT P., WAUTERS E. (eds.), *Themis 81 - ICT- en mediarecht*, die Keure, 2013, 27.

Bijdrage in wetenschappelijke tijdschriften

CONINGS C., 'Speuren op sociale media: de nieuwigheden op een rij', *P&R* 2020/1, 3.

DE SCHEPPER K. en VERBRUGGEN F., 'Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners', *T.Strafr.* 2013/3, 143.

HERBOTS P., 'Rol van onderzoeksrechter bij retroactieve lokalisatie telefoongesprekken', *Juristenkrant* 2004/89, 9.

ROYER S., 'Hof van Cassatie cryptisch over verbod op encryptie', *Juristenkrant* 2025/505, 1.

VANDROMME S., 'Ook louter lokaliseren van gsm in werking vereist bevelschrift onderzoeksrechter', *Juristenkrant* 2011/231, 3.

VERBRUGGEN F. en ROYER S., 'Veroordeling Skype niet verbroken, vele vragen blijven onbeantwoord', *RW* 2018-2019/37, 1442.

Noten en conclusies

DE SMET B., 'Opvangen van signalen van gsm-toestellen als onderzoeksdaad (noot onder Cass. 10 november 2009)', *RW* 2010-2011/31, 1302.

DE SWAEF M., 'Conclusie bij Cass. 18 januari 2011', *NC* 2011, ECLI:BE:CASS:2011:CONC.20110118.1, 84.

KENNES L., 'Le repérage téléphonique relatif à une période révolue (noot onder Cass. 16 april 2003 en Cass. 21 april 2004)', *JT* 2004/6155, 820.

KERKHOF J., 'Het onderscheppen van communicatie in de praktijk: wie, wat, waar en wanneer? (noot onder Cass. 16 december 2014)', *T.Strafr.* 2015/4-5, 235.

VANDEZANDE N., 'Yahoo! Als operator of verstrekker (noot onder cass. 18 januari 2011)', *AM* 2011/2, 220.

VAN DAALEN O., 'De verplichting die er in de praktijk op neerkomt dat encryptietechnologie wordt verzwakt, is in strijd met artikel 8 EVRM (noot onder EHRM 13 februari 2024)', *Computerrecht* 2024/98, 184.

VAN DE HEYNING C., 'Noot onder cass. 19 februari 2019', *T.Strafr.* 2019/6, 349.

Varia

GJS, 'Minister Geens reageert op kritiek na moord op Julie Van Espen: "Ik blijf ijveren voor een betere justitie"', *Nieuwsblad* 11 februari 2020, https://www.nieuwsblad.be/cnt/dmf20200211_04843606 (geraadpleegd op 15 mei 2025).

LEFEVRE L., 'Golf van verontwaardiging na verkrachtingszaak Leuven: "Onevenwicht tussen leed van slachtoffer en gevolgen voor dader"', *VRT nws* 2 april 2025, <https://www.vrt.be/vrtnws/nl/2025/04/02/verontwaardiging-rond-verkrachtingszaak-leuven-is-groot/> (geraadpleegd op 15 mei 2025).

MARTIN M., '“We willen de Reuzegommers niet alleen juridisch, maar ook moreel veroordeeld zien”: waarom de woede over het proces-Sanda Dia blijft', *DeMorgen* 30 mei 2023, <https://www.demorgen.be/nieuws/we-willen-de-reuzegommers-niet-alleen-juridisch-maar-ook-moreel-veroordeeld-zien-waarom-de-woede-over-het-proces-sanda-dia-blijft~b348d84f/> (geraadpleegd op 15 mei 2025).

Amerika

Bijdrage in wetenschappelijke tijdschriften

BAJPAI A., GUPTA A. en SHAH M.G., 'Search and seizure of electronic devices in India: time for a change?', *28 International Journal of Evidence & Proof* 2024/4, 298.

BAMBAUER J.R., 'Filtered dragnets and the anti-authoritarian Fourth Amendment', *97 Southern California Law Review* 2024/3, 571.

CHAN H., 'Wrong Search at the Wrong Time: Keyword Search Warrants and the Fourth Amendment', *45 Cardozo Law Review* 2023/1, 271.

DRANA D., 'Why it's time to ban geofence searches in light of *United States v. Chatree*', *38 Berkeley Technology Law Journal* 2023/4, 1307.

EDONA C.C., 'Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants', *97 Washington Law Review* 2022/4, 977.

FAN M.D., 'Big Data Searches and the Future of Criminal Procedure', *102 Texas Law Review* 2024/5, 877.

FAN M.D., 'Suspecting with Data', *109 Minnesota Law Review* 2024, 1.

FOLEY J., 'Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases', *22 Berkeley Technology Law Journal* 2007/1, 477.

FRANKSON, J.P., 'Reverse Search Warrants: Economically Beneficial?', *18 Journal of Law, Economics & Policy* 2023/2, 355.

LONG-KELLOUGH A., 'IF I DIE, DELETE MY BROWSER HISTORY: THE FOURTH AMENDMENT IMPLICATIONS OF REVERSE KEYWORD SEARCH WARRANTS', *52 Capital University Law Review* 2024/1, 1.

RADFORD M., 'Back to the future: revisiting state constitutions to protect against new technological intrusions', *81 Washington and Lee Law Review (Wash. & Lee L. REV.)* 2024/4, 1641.

SHAMONA J., 'The Unconstitutionality of Geofence Warrants', *6 University of Central Florida Department of Legal Studies Law Journal* 2023, 71.

SINHA M., 'The automated fourth amendment', *73 Emory Law Journal* 2024/3, 589.

STENDER S., 'Circumventing the fourth amendment: The Unconstitutional Nature of Geofence Warrants', *Utah Law Review* 2024/3, 733.

TURSI R., 'Gone Fishing: Casting a Wide Net Using Geofence Warrants', *98 Washington Law Review* 2023/1, 323.

WINTERS H., 'An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants', *107 Minnesota Law Review* 2023/3, 1369.

Dissenting opinion

MÁRQUEZ J., 'Dissenting opinion bij U.S. Supreme Court Colorado 16 oktober 2023', No. 23SA12, 'People/Seymour'.

Europa

Handboeken

HARRIS D. J., O'BOYLE M., BATES E. P. en BUCKLEY C.M., *Law of the European Convention on Human Rights*, Oxford University Press, 2023.

VANDE LANOTTE J., GOEDERTIER G., HAECK Y., GOOSSENS J. en DE PELSMAEKER T., *Belgisch publiekrecht (Boekdelen 1 en 2)*, die Keure, 2015.

Bijdrage in verzamelwerken

CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I., 'hoofdstuk 1 – Overkoepelende principes' in CONIX S., PEETERS L., VAN LOON W., PEETERS L. en VERHELST I. (eds.), *Werk & Privacy*, Intersentia, 2019, 3.

DE POORTER I., 'De GDPR of Algemene Verordening Gegevensbescherming (AVG) – Een algemene inleiding' in Instituut Financieel Recht (ed), *Financiële regulering: een dwarsdoorsnede*, Intersentia, 2019, 449.

FEYS M. en MOREL C., 'De nieuwe Verordening Gegevensbescherming: een algemeen overzicht van de (nieuwe) verplichtingen rond gegevensbescherming' in Orde van Advocaten bij de balie te Gent (ed.), *De advocaat als generalist*, Intersentia, 2018, 125.

FLUMIAN B. en FRANSSEN V., 'Le nouveau cadre légal belge en matière de conservation de données de communications électroniques' in MASSET A. en FRANSSEN V. (eds.), *Le droit pénal et la procédure pénale en constante évolution*, Anthemis, 2022, 315.

FOCQUET A. en DECLERCK E., 'Hoofdstuk 1 – Verwerking van persoonsgegevens' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, 5.

FOCQUET A. en DECLERCK E., 'Hoofdstuk 3 – Verwerkingsgronden' in FOCQUET A. en DECLERCK E. (eds.), *Gegevensbescherming in de praktijk*, Intersentia, 2019, 47.

ROYER S. en VERBRUGGEN F., 'Tussen helder en donker: mooie zebra of grijze ezel? Veiligheid en privacy via transparantie en opaciteit 20 jaar later' in DE HERT P. en GUTWIRTH S. (eds.), *Strafrecht in dialoog*, Intersentia, 2023, 133.

STEPPE R., 'Prijsdiscriminatie in het digitale tijdperk: beschouwingen over de nieuwe Algemene Verordening Gegevensbescherming' in STORME M. en HELSEN F. (eds.), *Innovatie en disruptie in het economisch recht*, Intersentia, 2017, 105.

VERSTRAETEN R. en BAILLEUX A., 'Het voorstel van een nieuw wetboek van strafvordering: algemene beginselen en fase van het onderzoek' in BAILLEUX A., SPRIET B., VAN HERPE R., VANHEUL J., VERBRUGGEN F. en VERSTRAETEN R. (eds.), *Themis 110 – Straf- en strafprocesrecht*, die Keure, 2019, 143.

WAEM H. en VAN EECKE P., '3 - Verwerking van persoonsgegevens' in VAN EECKE P. (ed), *Recht en elektronische handel*, Intersentia, 2021, 259.

Bijdrage in wetenschappelijke tijdschriften

CONINGS C. en VERBRUGGEN F., 'Grondwettelijk Hof plaatst reperateurs dataretentiewet voor moeilijke opdracht', *Juristenkrant* 2015/312, 1.

DE HERT P., 'Het Europees Hof Rechten van de Mens erkent publieke privacy', *NJW* 2002/4, 116.

DE KEERSMAECKER R. en VAN DE HEYNING C. 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *T.Strafr.* 2021/4, 171.

JANSEN R.H.T., 'Big Brother Watch e.a., Centrum för Rättvisa en het toezicht op de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2022/51, 97.

ROYER S en CAREEL S., 'Voorontwerp dataretentiewet: derde keer, goede keer?', *Juristenkrant* 2021/432, 10.

ROYER S. en VAN ROY L., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, 1.

VANDE VORST C., 'Algemene verordening gegevensbescherming: vijf nieuwigheden van dichterbij bekeken', *CJ* 2016/4, 75.

VAN MUYLDER C., 'La conservation des données de télécommunication à des fins de poursuites pénales – Influence de la jurisprudence européenne sur le droit belge', *Dr.pén.ent.* 2022, 343.

Noten en conclusies

CAMPOS SÁNCHEZ-BORDONA M., 'conclusie 12 mei 2016 bij HvJ, C-582/14, 'Patrick Breyer/Bondsrepubliek Duitsland', *ECLI:EU:C:2016:339*'.

CARTON A., 'De Belgische dataretentiewetgeving na het vernietigingsarrest van 11 juni 2015: another one bites the dust? (noot onder GwH 15 juni 2015)', *Computerrecht* 2015/5, 251.

CONINGS C., 'Dataretentie en privacy (noot onder GwH 15 juni 2015)', *NJW* 2015, 911.

DE WAEL F., 'Europese rechtspraak in kort bestek (noot onder EHRM 23 juni 2022)', *T.Strafr.* 2022/5, 309.

JANSSEN J., 'Bewaren of beware: dataretentie en grondrecht, een moeilijk evenwicht (noot onder GwH 22 april 2021)', *RABG* 2021/8, 673.

ROYER S., 'Cassatie verworpt procedurele bezwaren tegen Sky ECC-onderzoek (noot onder cass. 14 juni 2023)', *T.Strafr.* 2024/2, 99.

TERSAGO P., 'Europese rechtspraak in kort bestek (noot onder EHRM 26 oktober 2023)', *T.Strafr.* 2024/3, 192.

VAN DE HEYNING C., 'Ernst van het misdrijf is een onvoldoende reden om procedurele garanties voor de zoeking in informaticasystemen te omzeilen (noot onder EHRM 30 mei 2017)' *T.Strafr.* 2017/6, 365.

VAN DE HEYNING C., 'Not all that glitters is gold: een effectief recht op tegenspraak in tijden van bulkdata (noot EHRM 7 november 2017)', *T.Strafr.* 2021/4, 195.

VAN DE HEYNING C., 'Overzicht van rechtspraak - Het bewaren en gebruik van telecommunicatiegegevens in het strafrechtelijk onderzoek: de hoogste hoven in dialoog (noot onder GwH 19 juli 2018)', *T.Strafr.* 2019/1, 38.

VERSTRAELEN S., 'De vernietiging van de Belgische Dataretentiewet met terugwerkende kracht: de bescherming van het privéleven primeert (noot onder GwH 11 juni 2015)', *NC* 2015, 492.

X, 'noot onder EHRM 19 juni 2018', *T.Strafr.* 2019/1, 47.

Adviezen en richtsnoeren

COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights – Data protection, 31 December 2020, <https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0>.

COUNCIL OF EUROPE/EUROPEAN COURT OF HUMAN RIGHTS, Guide to the Case-Law of the of the European Court of Human Rights - Right to respect for private and family life, home and correspondence, 31 augustus 2024, [https://ks.echr.coe.int/documents/d/echr-ks/guide art 8 eng](https://ks.echr.coe.int/documents/d/echr-ks/guide%20art%208%20eng).

EUROPEAN DATA PROTECTION BOARD, Aanbevelingen 01/2020 inzake maatregelen ter aanvulling op doorgifte-instrumenten teneinde naleving van het beschermingsniveau van persoonsgegevens in de Unie te waarborgen, 18 juni 2020.

GROEP GEGEVENSBESCHERMING VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSgegevens, Advies 4/2007 over het begrip persoonsgegeven, 20 juni 2007, nr. 01248/07/NL, WP 136.

GROEP GEGEVENSBESCHERMING VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSgegevens, Opinion 1/2008 on data protection issues related to search engines, 4 april 2008, nr. 00737/EN, WP 148.

GROEP GEGEVENSBESCHERMING VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSgegevens, Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, 30 mei 2002, nr. 10750/02/EN/Final, WP 58.

EUROPEAN DATA PROTECTION BOARD, Richtsnoeren 3/2018 over het territoriale toepassingsgebied van de AVG (art. 3), 12 november 2019.

EUROPEAN DATA PROTECTION BOARD, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, 4 mei 2020.

GROEP GEGEVENSBESCHERMING VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSgegevens, Working Document Privacy on the Internet - An integrated EU Approach to Online Data Protection, 21 november 2000, nr. 5063/00/EN/FINAL, WP 37.

Bijlagen

Bijlage 1

Schematisch overzicht van de huidige wetsbepalingen en voorwaarden inzake online onderzoeksmethoden

ZOEKING IN INFORMATICASYSTEMEN OF DELEN ERVAN

CATEGORIE	Informaticazoeking	Netwerkwzoeking	Restcategorie
WETSBEPALING VOORWERP	Art. 39bis, §1 en §2 Sv. = het doorzoeken van informaticasysteem of delen ervan die worden aangetroffen tijdens een zoeking	Art. 88ter Sv. = het doorzoeken van informaticasystemen of delen ervan die zich op een andere plaats bevinden dan daar waar de zoeking plaatsvindt	Art. 39bis, §4 Sv. = alle andere zoekingen van informaticasystemen of delen ervan
BEVOEGDHEID	Getrapte bevoegdheid: - Beslag → officier van de gerechtelijke politie - Geen beslag → procureur des Konings	Onderzoeksrechter	Onderzoeksrechter
TOEPASSINGS- VOORWAARDEN	Geen specifieke voorwaarden MAAR artikel 8 EVRM → noodzakelijkheid in democratische samenleving: - Proportionaliteit - Subsidiariteit	Twee voorwaarden: - Noodzakelijk voor waarheidsvinding - Disproportionaliteit maatregelen OF risico op het verloren gaan van bewijsselementen	Twee voorwaarden: - Noodzakelijk voor waarheidsvinding - Disproportionaliteit andere maatregelen OF risico op het verloren gaan van bewijsselementen
VORM	Wet schrijft geen specifieke vorm voor	Principeel schriftelijk Uitz. Mondeling ingeval van uiterst dringende noodzakelijkheid	Principeel schriftelijk Uitz. Mondeling ingeval van uiterst dringende noodzakelijkheid
VOORBEELD	Tijdens een huiszoeking worden verschillende computers gevonden en in beslag genomen. Deze informaticasystemen kunnen worden doorzocht.	Tijdens een huiszoeking wordt een computer gevonden, die verbonden is met een telefoontoestel. Dit telefoontoestel, dat zich op afstand bevindt, kan worden doorzocht.	Het rechtstreeks uitvoeren van een zoeking in een systeem op afstand vanaf de computers van de overheid, indien het informaticasysteem niet werd aangetroffen tijdens de zoeking en niet uitgebreid kan worden.

WETSBEPALING	IDENTIFICATIE	REGISTRATIE/ LOKALISATIE	TAPMAATREGEL	IT-INKIJKOPERATIE
VOORWERP	Art. 46bis Sv. = identificatie van abonnee of gewoontelijke gebruiker van een dienst of de identificatie van diensten waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk wordt gebruikt	Art. 88bis Sv. = het opsporen van verkeersgegevens van elektronische communicatie van waaruit of waarnaar elektronische communicaties worden gedaan of het lokaliseren van de oorsprong of bestemming van elektronische communicatie	Art. 90ter Sv. = het, met heimelijk oogmerk, niet voor publiek toegankelijke communicatie of gegevens van een informatiesysteem of een deel ervan met technische hulpmiddelen onderscheppen, er kennis van nemen, doorzoeken en opnemen	Art. 46quinquies juncto art. 89ter Sv. = buiten medeweten van de eigenaar, bezitter of de gebruiker en zonder hun toestemming, toegang verschaffen tot een het informatiesysteem en het doorzoeken
BEVOEGDHEID	Procureur des Konings	Onderzoeksrechter	Onderzoeksrechter	Onderzoeksrechter
TOEPASSINGS- VOORWAARDEN	Twee voorwaarden: - Proportionaliteit - Subsidiariteit Misdrijven die geen correctionele hoofdgevangenisstraf van een jaar of zwaarder → gegevens van max 6 maanden voor beslissing Een met rede omklede en schriftelijke beslissing	Vier voorwaarden: - Strafdrempel - correctionele hoofdgevangenisstraf van één jaar of zwaarder - Proportionaliteit - Subsidiariteit - Noodzakelijkheid Een met rede omklede bevelschrift	Vier voorwaarden: - ernstige misdrijf uit art. 90ter, §2-4 Sv - Proportionaliteit - Subsidiariteit - Uitzonderlijk karakter → onderzoek maatregel vereist Een met rede omklede en schriftelijke machtiging	Vier voorwaarden: - ernstige misdrijf uit art. 90ter, §2-4 Sv. - Finaliteit - Proportionaliteit - Subsidiariteit Een met rede omklede en schriftelijke beslissing
VORM	Uitz. Mondeling ingeval van uiterst dringende noodzakelijkheid Er kan worden overgegaan worden tot identificatie van een gebruiker aan de hand van een EMEI-nummer van een gsm-toestel. Andersom kan nagegaan worden over welke telefoonnummers een welbepaalde persoon beschikt.	Uitz. Mondeling in spoedeisende gevallen	Uitz. Mondeling in spoedeisende gevallen	Uitz. Mondeling in spoedeisende gevallen
VOORBEELD		Onderzoeken naar welke nummers werden gebeld vanaf een welbepaald toestel of traceren waar iemand zich bevond toen hij op een bepaald moment belde of werd gebeld.	Het afluisteren van een telefoongesprek aan de hand van een verborgen microfoon.	Bij een onderzoek naar kinderpornografie kan het nuttig zijn dat in de computer gekeken wordt om zich ervan te vergewissen of er wel degelijk kinderpornografisch materiaal is aan te treffen.

Bijlage 2

Schematisch overzicht inzake bewaarplicht volgens het Hof van Justitie

BEWAARPLICHT	DOELEINDEN	VOORWAARDEN
ALGEMENE BEWARING VAN BURGERLIJKE IDENTIFICATIEGEGEVENS	Nationale veiligheid, openbare veiligheid en bestrijding criminaliteit	
ALGEMENE BEWARING VAN IP-ADRESSEN	Nationale veiligheid, openbare veiligheid en bestrijding zware criminaliteit	- Bewaartermijn niet langer dan strikt noodzakelijk - Strikte materiële en procedurele voorwaarden met betrekking tot het gebruik van de gegevens
ALGEMENE BEWARING VAN VERKEERS- EN LOCATIEGEGEVENS	Nationale veiligheid	- Concrete aanwijzingen voor een reële, actuele en voorzienbare ernstige dreiging nationale veiligheid - Maatregel niet langer dan strikt noodzakelijk - Toetsing rechterlijke of onafhankelijke bestuurlijke autoriteit
GERICHTE BEWARING VAN VERKEERS- EN LOCATIEGEGEVENS	Nationale veiligheid, openbare veiligheid en bestrijding zware criminaliteit	- Noodzakelijke afbakening ten aanzien van de categorieën te bewaren gegevens, geïsoleerde communicatiemiddelen, de duur van de bewaartermijn en een personele OF geografische afbakening - Maatregel niet langer dan strikt noodzakelijk

Bijlage 3

Schematisch overzicht inzake toegang tot bewaarde gegevens volgens het Hof van Justitie

TOEGANG	DOELEINDEN	VOORWAARDEN
BURGERLIJKE IDENTIFICATIEGEGEVENS	Doelstelling met het oog waarop de verplichting tot bewaring is opgelegd zijnde: Nationale veiligheid, openbare veiligheid en bestrijding criminaliteit	- Objectieve criteria in welke omstandigheden en onder welke voorwaarden toegang mogelijk is - Voorafgaande toetsing door rechterlijke instantie of onafhankelijke bestuurlijke entiteit
IP-ADRESSEN	Doelstelling met het oog waarop de verplichting tot bewaring is opgelegd zijnde: Nationale veiligheid, openbare veiligheid en bestrijding zware criminaliteit	- Objectieve criteria in welke omstandigheden en onder welke voorwaarden toegang mogelijk is - Voorafgaande toetsing door rechterlijke instantie of onafhankelijke bestuurlijke entiteit
VERKEERS- EN LOCATIEGEGEVENS	Doelstelling met het oog waarop de verplichting tot bewaring is opgelegd zijnde: - Algemene bewaring: nationale veiligheid - Gerichte bewaring: nationale veiligheid, openbare orde en bestrijding zware criminaliteit	- Objectieve criteria in welke omstandigheden en onder welke voorwaarden toegang mogelijk is - Voorafgaande toetsing door rechterlijke instantie of onafhankelijke bestuurlijke entiteit

Bijlage 4

Schematisch overzicht inzake surveillancemethoden in het licht van artikel 8 Europees Verdrag voor de Rechten van de Mens

SURVEILLANCEMETHODEN	GERICHTE SURVEILLANCE	BULKINTERCEPTIE
BIJ WET VOORZIEN	Wettelijke nationale basis Rule of law: - Nauwkeurige omschrijving van de strafbare feiten - Categorieën personen - Beperking duur van de maatregel - Procedure voor het verzamelen, gebruiken en opslaan van gegevens - Waarborgen inzake verstrekking gegevens aan derden - Voorwaarden betreffende vernietiging en wissing van gegevens - Procedure tot verlenen van machtiging - Ex post toetsing door onafhankelijke instantie	Wettelijke nationale basis Rule of law: - Juridische gronden - Omstandigheden die maatregel rechtvaardigen - Procedure tot verlenen van machtiging - Procedures betreffende selectie, analyse en het gebruik van gegevens - Waarborgen inzake verstrekking gegevens aan derden - Procedures betreffende de duur van de maatregel, de opslag en voorwaarden tot vernietiging en wissing van gegevens - Procedures en modaliteiten voor toezicht door onafhankelijke autoriteit - Ex post toetsing door onafhankelijke instantie
LEGITIEME DOELSTELLING	<i>"in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de</i>	IDEM

*gezondheid of de goede
zeden of **voor de
bescherming van de
rechten en vrijheden van
anderen***

**NOODZAKELIJK IN
DEMOCRATISCHE
SAMENLEVING**

- Subsidiariteitsbeginsel
- Proportionaliteitsbegin
sel

IDEM

Bijlage 5

Voorstel inzake de wettelijke regeling van zoektermbevelen in het Belgisch strafrecht

“ § 5. Opsporing via zoekgedrag

Art. 89 Sv. § 1. *De onderzoeksrechter kan de gegevens, zijnde een geanonimiseerd lijst betreffende de zoekopdracht van de gebruiker, de datum, tijd en locatie van de zoekopdracht, de gebruikte browser, het apparaattype en het IP-adres gekoppeld aan het informatiesysteem waarmee de opzoeking werd uitgevoerd, doen opsporen van personen die gezocht hebben naar zoektermen die in verband gebracht kunnen worden met een gepleegd of voorbereid misdrijf zoals bedoeld in paragraaf 2.*

Hiertoe kan hij, rechtstreeks of via de door de Koning aangewezen politiedienst, de medewerking vorderen van:

- zoekmachinebedrijven; en
- iedereen die binnen het Belgisch grondgebied, op welke wijze ook, een dienst aanbiedt of beschikbaar stelt waarbij gebruikers zoektermen kunnen invoeren met het oog op het verkrijgen van resultaten die beantwoorden aan een bepaalde zoekopdracht.

De maatregel bedoeld in deze paragraaf kan alleen worden bevolen ten aanzien van personen die op grond van precieze aanwijzingen ervan verdacht worden een strafbaar feit zoals bedoeld in paragraaf 2 te hebben gepleegd of voorbereidt, ten aanzien van de informaticasystemen die geregeld worden gebruikt door de persoon op wie een verdenking rust of ten aanzien van informaticasystemen op plaatsen waar de verdachte vermoed wordt te vertoeven. Ingeval van bijzondere situaties, zoals die waarin de vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid worden bedreigd, kan de maatregel betrekking hebben op andere personen of informaticasystemen, mits op grond van objectieve elementen kan worden aangetoond dat de hieruit voortvloeiende gegevens een daadwerkelijke bijdrage kunnen leveren tot de bestrijding van dergelijke activiteiten.

Deze maatregel kan enkel worden bevolen indien er ernstige aanwijzingen bestaan dat het een strafbaar feit betreft bedoeld in paragraaf 2, dat er concrete en verifieerbare aanwijzingen bestaan dat het gebruik van de betreffende zoekterm in verband staat met de voorbereiding of het plegen van het strafbaar feit en het bevel een redelijke kans biedt om het voorkomen van een misdrijf te bevorderen of om verdachten te identificeren. De maatregel kan slechts ingezet worden wanneer het onderzoek zulks vereist en indien de overige middelen van het onderzoek niet volstaan om de waarheid aan de dag te brengen.

De onderzoeksrechter doet in een met rede omkleed bevelschrift opgave van de feitelijke omstandigheden van de zaak die de maatregel rechtvaardigen, van de proportionaliteit met inachtneming van de persoonlijke levenssfeer, de noodzakelijkheid en de subsidiariteit ten opzichte van elke andere onderzoeksdaad. Ook vermeldt hij de reikwijdte van het bevel, inclusief een voldoende afgebakende en gedetailleerde omschrijving van de onderzochte zoektermen, de zoekmachinebedrijven of dienstverstrekkers waarop het bevel betrekking heeft en een evaluatie van de operationele haalbaarheid van de maatregel. Hij vermeldt ook de periode in het verleden waarover de vordering zich uitstrekt overeenkomstig paragraaf 5.

§ 2. De strafbare feiten die de maatregel bedoeld in paragraaf 1 kunnen wettigen zijn degene die bedoeld worden in:

- 1° de artikelen 101 tot en met 110 van het Strafwetboek;
- 1°/1 de hoofdstukken II en III van titel I, boek II van het Strafwetboek;
- 2° De artikelen 136bis, 136ter, 136quater, 136sexies en 136septies van hetzelfde Wetboek en artikel 41 van de wet van 29 maart 2004 betreffende de samenwerking met het Internationaal Strafgerechtshof en de internationale straftribunalen;
- 3° boek II, titel I ter, van hetzelfde Wetboek;
- 4° artikel 147 van hetzelfde Wetboek;
- 5° de artikelen 160, 161, 162, 163, 168, 171, 173 en 176 van hetzelfde Wetboek;
- 6° de artikelen 180 en 186 van hetzelfde Wetboek;
- 7° artikel 210bis van hetzelfde Wetboek;
- 8° de artikelen 246, 247, 248, 249, en 250 van hetzelfde Wetboek;
- 9° artikel 259bis van hetzelfde Wetboek;
- 10° artikel 314bis van hetzelfde Wetboek;

11° de artikelen 324bis en 324ter van hetzelfde Wetboek;

12° de artikelen 327, 328, 329 en 330 van hetzelfde Wetboek, voor zover een klacht is ingediend;

13° artikel 331bis van hetzelfde Wetboek;

14° artikel 347bis van hetzelfde Wetboek;

15° de artikelen 417/7 tot 417/22 van hetzelfde Wetboek;

16° artikel 417/24 van hetzelfde Wetboek;

17° de artikelen 417/25 tot 417/38, 417/44 tot 417/45, 433quater/1, 433quater/4 van hetzelfde Wetboek;

18° artikel 393 van hetzelfde Wetboek;

19° de artikelen 394 en 397 van hetzelfde Wetboek;

20° de artikelen 428 en 429 van hetzelfde Wetboek;

21° artikel 433bis/1 van hetzelfde Wetboek;

22° de artikelen 433quinquies tot 433octies van hetzelfde Wetboek;

22/1° . de artikelen 433novies/2 tot 433novies/10 van hetzelfde Wetboek;

23° artikel 434 van hetzelfde Wetboek;

24° de artikelen 468, 470, 471 en 472 van hetzelfde Wetboek;

25° artikel 475 van hetzelfde Wetboek;

26° boek II, titel IX, hoofdstuk I, sectie 2bis, en hoofdstuk Ibis van hetzelfde Wetboek;

27° artikel 505, eerste lid, 2°, 3° en 4° van hetzelfde Wetboek;

28° de artikelen 510, 511, eerste lid en 516 van hetzelfde Wetboek;

29° artikel 520 van hetzelfde Wetboek, indien de omstandigheden bedoeld in de artikelen 510 of 511, eerste lid, van hetzelfde Wetboek verenigd zijn;

30° de artikelen 550bis en 550ter van hetzelfde Wetboek;

31° artikel 2bis van de wet van 24 februari 1921 betreffende het verhandelen van giftstoffen, slaapmiddelen en verdovende middelen, psychotrope stoffen, ontsmettingsstoffen en antiseptica en van de stoffen die kunnen gebruikt worden voor de illegale vervaardiging van verdovende middelen en psychotrope stoffen;

32° de wet van 28 mei 1956 betreffende ontplofbare en voor de deflagratie vatbare stoffen en mengsels en de daarmee geladen tuigen;

33° artikel 1 van het koninklijk besluit van 12 april 1974 betreffende sommige verrichtingen in verband met stoffen met hormonale, anti-hormonale, anabole, anti-infectieuze, anti-parasitaire, en anti-inflammatoire werking, welk artikel betrekking heeft op strafbare feiten waarop overeenkomstig de wet van 24 februari 1921 betreffende het verhandelen van de giftstoffen, slaapmiddelen en verdovende middelen, ontsmettingsstoffen en antiseptica straffen worden gesteld.";

34° de artikelen 77bis tot 77quinquies van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen;

35° artikel 10, § 1, 2°, van de wet van 15 juli 1985 betreffende het gebruik bij dieren van stoffen met hormonale, anti-hormonale, beta-adrenergische of productie-stimulerende werking;

36° artikel 10 van de wet van 5 augustus 1991 betreffende de in-, uit- en doorvoer van wapens, munitie en speciaal voor militair gebruik dienstig materieel en daaraan verbonden technologie;

37° artikel 145, § 3 en § 3bis, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

38° de artikelen 8 tot 11, 14, 16, 19, 1°, 2°, 3°, 5° en 6°, 20, 22, 27 en 33 van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens, ook "wapenwet" genoemd;

39° de artikelen 21 tot 26 van het Samenwerkingsakkoord van 2 maart 2007 tussen de Federale Staat, het Vlaams Gewest, het Waals Gewest en het Brussels Hoofdstedelijk Gewest betreffende de uitvoering van de overeenkomst tot verbod van de ontwikkeling, de productie, de aanleg van voorraden en het gebruik van chemische wapens en inzake de vernietiging van deze wapens, gedaan te Parijs op 13 januari 1993;

40° artikel 47 van het decreet van het Vlaams Parlement van 15 juni 2012 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen en munitie;

41° artikel 20 van het decreet van het Waals Gewest van 21 juni 2012 betreffende de invoer, uitvoer, doorvoer en overdracht van civiele wapens en van defensiegerelateerde producten;

42° artikel 42 van de ordonnantie van het Brussels Hoofdstedelijk gewest van 20 juni 2013 betreffende de in-, uit-, doorvoer en overbrenging van defensiegerelateerde producten, ander voor militair gebruik dienstig materiaal, ordehandhavingsmateriaal, civiele vuurwapens, onderdelen, toebehoren en munitie ervan.

§ 3. Poging tot het plegen van een misdaad bedoeld in de voorgaande paragraaf kan eveneens de maatregel bedoeld in paragraaf 1 wettigen.

§ 4. Een strafbaar feit, bedoeld in de artikelen 322 of 323 van het Strafwetboek, kan eveneens een maatregel wettigen, voor zover de vereniging gevormd is met het doel een aanslag te plegen tegen de personen of eigendommen bedoeld in § 2, of om het in artikel 467, eerste lid, van het Strafwetboek bedoelde strafbare feit te begaan.

§ 5. Wat betreft de toepassing van de maatregel bedoeld in paragraaf 1 op de gegevens die worden bewaard krachtens de artikelen [dataretentiewet van toepassing op zoekmachinebedrijven], zijn de volgende bepalingen van toepassing:

- *voor een strafbaar feit die een bedreiging vormt voor de vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid mag de onderzoeksrechter in zijn bevelschrift de gegevens opvragen voor een periode van twaalf maanden voorafgaand aan het bevelschrift;*
- *voor een ander strafbaar feit bedoeld in § 2, dat niet bedoeld is in het eerste gedachtestreepje, of een strafbaar feit dat gepleegd is in het kader van een criminele organisatie als bedoeld in artikel 324bis van het Strafwetboek, kan de onderzoeksrechter de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan het bevelschrift.*

§ 6. In geval van ontdekking op heterdaad kan de procureur des Konings de maatregel bevelen voor de in §§ 2-4 bedoelde strafbare feiten. In dat geval moet de maatregel binnen de vierentwintig uur worden bevestigd door de onderzoeksrechter.

In geval van ontdekking op heterdaad en zolang de heterdaad-situatie duurt, kan de procureur des Konings de maatregel bedoeld in paragraaf 1 bevelen voor de strafbare feiten bedoeld in de artikelen 137, 347bis, 434 of 470 van het Strafwetboek. In geval van ontdekking op heterdaad kan de procureur des Konings bovendien de maatregel bedoeld in paragraaf 1 bevelen voor het in artikel 137 van het Strafwetboek bedoelde strafbare feit, met uitzondering van het in artikel 137, § 3, 6°, van hetzelfde Wetboek bedoelde strafbare feit, binnen de tweeënzeventig uur na de ontdekking van dit strafbaar feit.

In spoedeisende gevallen kan de maatregel mondeling worden bevolen. Het bevel moet zo spoedig mogelijk worden bevestigd in de vorm bepaald in het vijfde lid.

§ 7. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en op voorstel van de Minister van Justitie, de procedureregels omtrent de selectie, analyse, het gebruik, de opslag, de opslagtermijn en het wissen en vernietigen van het verkregen materiaal.

§ 8. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel en daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

Iedere persoon die de gegevens weigert mee te delen of niet meedeelt wordt gestraft met geldboete van honderd euro tot dertigduizend euro.”