



UHASSELT

KU LEUVEN



Maastricht University

KNOWLEDGE IN ACTION

Faculteit Rechten

master in de rechten

Masterthesis

Data zijn goud waard: is in het kader van een strafonderzoek de aankoop door de Belgische overheid van persoonsgegevens bij gespecialiseerde commerciële dataverzamelingsbedrijven mogelijk?

Selina Panis

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.



UHASSELT

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

Data zijn goud waard: is in het kader van een strafonderzoek de aankoop door de Belgische overheid van persoonsgegevens bij gespecialiseerde commerciële dataverzamelingsbedrijven mogelijk?

Selina Panis

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

PROMOTOR :

Prof. dr. Frank VERBRUGGEN



Maastricht University

Faculteit Rechten

Master in de rechten 2024-2025

Methodologie voor masterproef: Masterscriptie

Data zijn goud waard: is in het kader van een strafonderzoek de aankoop door de Belgische overheid van persoonsgegevens bij gespecialiseerde commerciële dataverzamelingsbedrijven mogelijk?

Panis Selina (2157687)

Promotor:

Verbruggen Frank

Samenvatting

In deze gedigitaliseerde maatschappij worden steeds meer gegevens bewaard. Personen maken veelvuldig gebruik van het internet en apps. Zo communiceren personen online, delen informatie over zichzelf op sociale media, posten foto's en video's, shoppen online, gebruiken fitness- en gezondheidsapps, gebruiken bepaalde apps als GPS... Door dit gebruik laten personen bepaalde gegevens achter. Deze enorme hoeveelheid persoonsgegevens wordt bewaard door bedrijven. Vervolgens kunnen bedrijven deze persoonsgegevens verkopen aan dataverzamelingsbedrijven.

Het zou eventueel interessant kunnen zijn voor de Belgische overheid om deze persoonsgegevens aan te kopen bij gespecialiseerde commerciële dataverzamelingsbedrijven in het kader van het strafonderzoek. Hierdoor wordt er een grote hoeveelheid gegevens verkregen, in een korte tijd. Bijgevolg zou de overheid deze informatie niet zelf moeten zoeken, door gebruik te maken van andere middelen die de overheid ter beschikking heeft.

In het kader van deze masterproef, zal onderzocht worden op welke manier de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek kan worden toegepast. Daarom zal worden geanalyseerd of deze handeling kan worden beschouwd als een onderzoekshandeling. Daarnaast zal worden onderzocht of de procureur des Konings of de onderzoeksrechter bevoegd is om deze handeling te bevelen. Naar gelang de aard van de informatie, zou deze onderzoekshandeling immers een dwangmaatregel kunnen zijn. Hierbij zal het onderscheid geduid worden tussen 'gewone' gegevens en gevoelige gegevens. Voorts zal worden onderzocht wie deze aankoop betaalt, hoe het betalingsproces verloopt en op welke manier het budget bepaald wordt.

Naargelang de gevoeligheid van de informatie, kunnen eventueel fundamentele rechten en privacyregels worden geschonden. Hiervoor zullen bepaalde fundamentele rechten besproken worden. Bovendien zal er onderzocht worden of deze rechten, al dan niet kunnen worden geschonden door de onderzochte handeling. Hierbij zullen de voorwaarden waaraan de overheid moet voldoen, bij de aankoop van persoonsgegevens, om de grondrechtsbescherming te waarborgen worden besproken. Daarbij wordt het bestaan van een wettelijke basis, het nastreven van een legitiem doel, de vereiste van noodzakelijkheid van de inbreuk, de proportionaliteit en de subsidiariteit geanalyseerd. Hierbij zullen er parameters worden voorgesteld, om de noodzakelijkheid en proportionaliteit af te wegen.

Eén van deze fundamentele rechten is het recht op privacy, dat zowel het recht op eerbiediging van het privéleven, als het recht op bescherming van gegevens waarborgt. Om deze reden zal worden onderzocht welke instrumenten het gegevensbeschermingsrecht waarborgen. Hierbij zal duidelijk worden dat de Algemene Verordening Gegevensbescherming niet van toepassing is, op de verwerking van persoonsgegevens in het kader van de opsporing en het onderzoek naar strafbare feiten. Daarentegen is de privacyrichtlijn politie-justitie wel van toepassing. Om deze reden zal de privacyrichtlijn politie-justitie en Titel II van de Wet Verwerking Persoonsgegevens, waarin de richtlijn werd omgezet in België, worden geanalyseerd.

Daarnaast zal er een rechtsvergelijkend onderzoek worden gevoerd met de Verenigde Staten. Hierbij zal de relevante regelgeving, op federaal niveau en op het niveau van de deelstaten worden besproken. Daarnaast zal worden geanalyseerd, op welke manier de Amerikaanse overheid gegevens kan opvragen bij Google.

Om de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht te waarborgen, kunnen er procedurele waarborgen worden ingevoerd. Daarom zal worden onderzocht in hoeverre procedurele waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht nog kunnen waarborgen. Hierbij zal duidelijk worden vanaf welke grenzen, de grondrechtsbescherming niet langer kan worden gewaarborgd. Dit kan tot gevolg hebben dat de aankoop van persoonsgegevens en het gebruik van deze persoonsgegevens, een inbreuk vormt op een fundamenteel recht.

DANKWOORD

Deze thesis is het eindwerk van mijn tweejarige masteropleiding aan de UHasselt. Deze masteropleiding, werd voorafgegaan door een schakelprogramma van twee jaar, dat ook werd afgelegd aan de UHasselt. Ik kijk met veel dankbaarheid en voldoening terug op mijn opleiding.

Rechten studeren was al sinds lange tijd een droom voor mij. Om deze reden ben ik trots, dat ik dit traject heb mogen afleggen.

Het schrijven van deze masterproef kostte veel tijd, onderzoekswerk en doorzettingsvermogen, maar het was een zeer leerrijke ervaring. Daarom wil ik alle personen bedanken, die mij hebben geholpen tijdens het schrijven van deze masterproef. Daarnaast wil ik iedereen bedanken die mij heeft bijgestaan gedurende mijn rechtenstudie.

Hierbij wil ik mijn promotor, Frank Verbruggen, bedanken voor de kans om mijn thesis te schrijven in het domein van het strafprocesrecht. Hierdoor heb ik veel kunnen bijleren. Daarboven wil ik mijn promotor bedanken voor zijn feedback, waardoor ik mijn thesis heb kunnen verbeteren.

Daarnaast wil ik mijn dagelijkse begeleider, Pascal Beyer, bedanken voor de goede begeleiding. Hij zorgde er met de nodige feedback voor dat ik mijn masterproef steeds kon verbeteren. Ik wil hem bedanken voor de tijd die hij genomen heeft, om mij verder te helpen.

Daarboven wil ik mijn vrienden en familieleden bedanken voor de nodige steun tijdens de opleiding. Zij stonden op ieder moment voor mij klaar.

Inhoudsopgave

Deel I: Inleiding.....	1
Hoofdstuk I. Situering	1
Hoofdstuk II. Probleemstelling	4
Hoofdstuk III. Doelstelling en relevantie	6
Hoofdstuk IV. Onderzoeksvragen.....	7
Afdeling I. Centrale onderzoeksvraag	7
Afdeling II: Subonderzoeksvragen	7
Hoofdstuk V. Onderzoeksmethodologie	8
Hoofdstuk VI. Afbakening onderzoek.....	12
Deel II: Het strafrechtelijk onderzoek	17
Hoofdstuk I. Het opsporings- en gerechtelijk onderzoek	17
Hoofdstuk II. Vergelijkbare opsporingshandelingen	20
Afdeling I. Opvragen van gegevens op basis van wettelijke regels.....	21
Onderafdeling I. Opvragen van gegevens bij telecomoperatoren.....	22
Onderafdeling. II. Opvragen van gegevens bij bankinstellingen	23
Afdeling II. Beslag	25
Onderafdeling I. Klassiek beslag	25
Onderafdeling II. Databeslag.....	27
Afdeling III. DNA-onderzoek.....	29
Onderafdeling I. In het kader van het opsporingsonderzoek.....	29
Onderafdeling II. In het kader van het gerechtelijk onderzoek	30
Afdeling IV. Huiszoeking	32
Onderafdeling I. In het kader van het opsporingsonderzoek.....	32
Onderafdeling II. In het kader van het gerechtelijk onderzoek	33
Afdeling V. Doorzoeking communicatie en informaticasystemen	34
Afdeling VI Opsporen van elektronische communicatie	37
Hoofdstuk III. Dataretentie	39
Deel III: Fundamentele rechten.....	42
Hoofdstuk I. Recht op een eerlijk proces	44
Hoofdstuk II. Recht op privacy.....	47
Afdeling I: Recht op eerbiediging van het privéleven.....	48
Afdeling II. Recht op bescherming van persoonsgegevens	49

Hoofdstuk III. Recht op gelijkheid en non-discriminatie	52
Hoofdstuk IV. Recht op vrije meningsuiting	53
Deel IV. Gegevensbeschermingsrecht	54
Hoofdstuk I. Categorieën persoonsgegevens.....	54
Hoofdstuk II. Instrumenten gegevensbeschermingsrecht	58
Afdeling I. GDPR	60
Afdeling II. Privacyrichtlijn politie-justitie en Titel II Wet Verwerking Persoonsgegevens.....	62
Deel V: Vergelijking met de Verenigde Staten	69
Deel VI. De aankoop van persoonsgegevens bij dataverzamelingsbedrijven in de praktijk.....	74
Hoofdstuk I. Ethische gevaren en belangenconflict.....	74
Afdeling I. Vergoeding getuigen en informanten	74
Afdeling II. Ethische gevaren	75
Afdeling III. Belangenconflict overheid	77
Hoofdstuk II. Voordeel handeling ten opzichte van andere middelen	78
Afdeling I. Dataverzamelingsbedrijven	78
Afdeling II. Verschil met opvragen gegevens op basis van wettelijke regels, zoeking in het informatica- en communicatiesysteem en beslag.....	80
Afdeling III. Nut aankoop persoonsgegevens bij dataverzamelingsbedrijven	82
Hoofdstuk III. Bevelen handeling	85
Hoofdstuk IV. Procedurele waarborgen	88
Afdeling I. Inmenging fundamentele rechten	89
Afdeling II. Onderzoekshandeling in overeenstemming met het gegevensbeschermingsrecht	95
Onderafdeling I. Gemeenschappelijke waarborgen niet-gevoelige en gevoelige gegevens..	95
Onderafdeling II. Bijkomende waarborgen gevoelige gegevens.....	97
Afdeling. III. Controle	99
Hoofdstuk V. Betaling met betrekking tot aankoop gegevens	102
Afdeling I. Betalingsprocedure	102
Afdeling II. Vaststelling bedrag	106
Afdeling III. Budget FOD Justitie	109
Deel VII. Conclusie.....	110
Deel VIII. Bibliografie	119
Wetgeving	119
Wetgeving Amerika	122

Rechtsleer	123
Boeken	123
Tijdschriften	127
Rechtspraak.....	132
Andere bronnen.....	134

Lijst met afkortingen

AVG	Algemene Verordening Gegevensbescherming
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FOD Justitie	Federale Overheidsdienst Justitie
GBA	Gegevensbeschermingsautoriteit
GDPR	General Data Protection Regulation
GW	Grondwet
HvC	Hof van Cassatie
HvJ	Europees Hof van Justitie
K.I.	Kamer van inbeschuldigingstelling
OM	Openbaar Ministerie

Data zijn goud waard: is in het kader van een strafonderzoek de aankoop door de Belgische overheid van persoonsgegevens bij gespecialiseerde commerciële dataverzamelingsbedrijven mogelijk?

Deel I: Inleiding

Hoofdstuk I. Situering

1. **Digitalisatie** – In deze gedigitaliseerde maatschappij worden steeds meer gegevens opgeslagen. Personen maken veelvuldig gebruik van het internet en apps. Zo communiceren personen online, delen informatie over zichzelf op sociale media, posten foto's en video's, shoppen online, gebruiken fitness- en gezondheidsapps, gebruiken bepaald apps als GPS... Door dit gebruik laten personen bepaalde gegevens achter.¹ Deze enorme hoeveelheid persoonsgegevens wordt bewaard door bedrijven. Vervolgens kunnen bedrijven deze persoonsgegevens verkopen aan gespecialiseerde commerciële dataverzamelingsbedrijven.² Op basis van deze informatie kan er een beeld over een persoon worden gevormd.³
2. **Dataverzamelingsbedrijven** – Dataverzamelingsbedrijven zijn bedrijven die gegevens van personen verzamelen en opslaan.⁴ Nadien kunnen deze gegevens worden verkocht aan andere bedrijven of instanties.⁵ Meestal verkopen dataverzamelingsbedrijven deze gegevens, zonder het medeweten of toestemming van de betrokkenen.⁶ Dataverzamelingsbedrijven verzamelen identificatiegegevens, contactgegevens, gegevens met betrekking tot het online gedrag van personen, locatiegegevens, gegevens omtrent koopgedrag, financiële gegevens, gegevens met betrekking tot sociale en professionele connecties...⁷ Deze gegevens worden verzameld door middel van publieke gegevens. Daarnaast kunnen zij verzameld worden door middel van commerciële data, die verkregen wordt door middel van de aankoopgeschiedenis, loyaliteitsprogramma's, garantiebewijzen... Voorts kunnen deze gegevens worden verzameld door middel van online tracking, dit gebeurt dan door middel van cookies en trackers. Bovendien kunnen gegevens met betrekking tot sociale media verzameld worden, zoals openbare berichten, likes, volgers, check-ins... Evenzo kunnen gegevens verzameld worden, wanneer bedrijven gebruikersgegevens doorverkopen, vaak wordt de verkoop van persoonsgegevens opgenomen in de servicevoorwaarden. Bijgevolg aanvaarden personen deze servicevoorwaarden vaak, zonder deze te lezen. Ook kunnen gegevens verzameld worden door het invullen van enquêtes of winacties, waarbij gebruikers vrijwillig hun gegevens

¹ PANZAVOLTA, M., ROYER, S. en SEVERIJNS, H., 'Algemene dataretentie: ten minste houdbaar tot...?', *T. Strafr.* 2018/1, (3) 3-18.

² *Ibid.*

³ DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482.

⁴ Beslissing Gegevensbeschermingsautoriteit 16 november 2022, 163/2022., ECLI:BE:GBAPD:2022:DEC.20221116.6.

⁵ STEVENS, D., 'Privacybescherming', *Computerr.* 2023/1, (72) 72-82.; DELFORGE, A., *La jurisprudence de l'APD en matière de marketing direct*, Intersentia, 2024, 119-138, nr. 36-39.

⁶ Beslissing Gegevensbeschermingsautoriteit 16 januari 2024, 07/2024.

⁷ RUSHMEIER, H. 'Data Brokers and European Digital Legislation', *EDPL* 2023/1, (37) 37.

meedelen. Daarnaast kunnen locatiegegevens verzameld worden, doorat personen, om gebruik te maken van bepaalde apps, hun toestemming voor GPS-toegang geven. Dit is bijvoorbeeld het geval bij weerapps of fitnessapps. Bovendien kunnen gegevens met betrekking tot de gezondheid van een persoon, worden verzameld op basis van gezondheidsapps, die bijvoorbeeld het hartritme meten of het slaapritme controleren.⁸

3. **Aankoop gegevens** - Het zou eventueel interessant kunnen zijn voor de Belgische overheid om deze persoonsgegevens aan te kopen bij gespecialiseerde commerciële dataverzamelingsbedrijven en deze te gebruiken in het kader van het strafonderzoek. Hierdoor wordt er een grote hoeveelheid gegevens verkregen, in een korte tijd. Bijgevolg zou de overheid deze informatie niet zelf moeten zoeken, door gebruik te maken van andere middelen die de overheid ter beschikking heeft.⁹
4. **Proactief vs. reactief onderzoek** – De aankoop van persoonsgegevens bij dataverzamelingsbedrijven in het kader van het strafonderzoek, kan naar mijns inziens zowel worden toegepast in het kader van proactieve recherche, als in het kader van reactieve recherche.¹⁰
5. **Proactief** – Deze handeling zou in het kader van proactieve recherche kunnen worden toegepast.¹¹ In dat geval wordt de handeling toegepast, voordat er een persoon in verdenking wordt gesteld. Op deze manier kan er onderzoek worden gevoerd naar te plegen of gepleegde feiten die nog niet aan het licht werden gebracht.¹² Hiervoor moet er een redelijk vermoeden bestaan.¹³ Het doel van proactieve recherche is de ontmanteling van een crimineel netwerk of een criminele organisatie, op een later moment.¹⁴ Bovendien is proactief onderzoek uitsluitend mogelijk bij ernstige criminaliteit.¹⁵
6. **Reactief** – In tegenstelling tot bij proactieve recherche, zou de aankoop van persoonsgegevens bij dataverzamelingsbedrijven en het gebruik van deze gegevens in het

⁸ CONSTANTINESCU, E., 'What are data brokers, and how do they work?', *Proton* 20 juni 2025, [https://proton.me/blog/databrokers#:~:text=Data%20brokers%20are%20companies%20or,campaigns%20\(for%20voter%20targeting\)](https://proton.me/blog/databrokers#:~:text=Data%20brokers%20are%20companies%20or,campaigns%20(for%20voter%20targeting)) (geraadpleegd op 25 juli 2025).

⁹ VAN DE HEYNING, C., 'Not all that glitters is gold: een effectief recht op tegenspraak in tijden van bulkdata', *T.Strafr.* 2021/4, (195) 195-201.; Verordening (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 betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, *Pb. L.* 4 mei 2016, overweging (3). (Hierna: Privacyrichtlijn politie-justitie); VANSWEEVELT, T. en BROECKX, N., *Handboek gezondheidsrecht: Privacy, persoonsgegevens en beroepsgeheim*, Intersentia, 2022, 641-826.

¹⁰ VAN DEN HENDE, T., 'Het onderscheid tussen proactief en reactief onderzoek in strafzaken', *Vigiles* 2002/4, (140) 140-142.

¹¹ Art. 28bis, §2 Sv.

¹² LEESTMANS, D., 'Men moet maar eens stoppen met in vakjes te denken', *Juristenkrant* 2019/391, (10) 10-11.

¹³ Wetsontwerp tot verbetering van de strafrechtspleging in het stadium van het opsporingsonderzoek en het gerechtelijk onderzoek, KAMER, 1996-1997, 19 december 1996, nr. 857/1-96/97, 45.; Cass. 2 juni 2015, AR P.15.0263.N.

¹⁴ VAN DEN BERGE, Y., 'De kamer van inbeschuldigingstelling waakt ook over de toepassing van de bijzondere opsporingsmethoden in het proactief onderzoek', *RABG* 2012/2, (121) 121-123.; Gent 30 januari 2002, *Vigiles* 2002/4, 138, noot VAN DEN HENDE, T.

¹⁵ ROYER, S., '[Datagedreven onderzoeken] Cassatie verwerpt procedurele bezwaren tegen Sky ECC-onderzoek', *T.Strafr.* 2024/2, (99) 103.

kader van het strafonderzoek, in het kader van reactieve recherche slechts worden toegepast nadat er een persoon in verdenking wordt gesteld.¹⁶ In dat geval wordt het strafbare feit, waarvoor de persoon in verdenking werd gesteld onderzocht. Bovendien is reactieve recherche mogelijk na een klacht, vaststelling, aangifte of wanneer er ernstige aanwijzingen bestaan, met betrekking tot gepleegde of nog te plegen misdrijven.¹⁷ Zo kunnen bijvoorbeeld de huiszoeking en het afluisteren enkel gebeuren in het kader van reactieve recherche.¹⁸

7. **Individu vs. meerdere personen** – De onderzoekshandeling zou zowel betrekking kunnen hebben op het aankopen van persoonsgegevens van een individueel persoon, als op het aankopen van persoonsgegevens van meerdere personen of een bepaalde groep personen.
8. **Toestemming** - Naar mijns inziens is de aankoop van persoonsgegevens mogelijk indien de betrokkene op een geldige manier toestemming geeft. Indien er geen geldige toestemming wordt verleend door de betrokkene, is de aankoop slechts in bepaalde gevallen mogelijk, wanneer de procureur des Konings, respectievelijk de onderzoeksrechter de aankoop beveelt.

¹⁶ CONINGS, C., *Infiltratie op het internet*, Wolters Kluwer, 2022, 205-228, nr. 212.

¹⁷ CONINGS, C. en DE KEERSMAECKER, R., 'To save but not too safe: hoogste Belgische rechters zien geen graten in het decryptiebevel voor de verdachte', *T.Strafr.* 2020/3, (163) 163-175.

¹⁸ BERKMOES, H., *Inkijkoperatie ('klassiek' en in 'IT-systemen')*, Wolters Kluwer, 2023, 1-17.

Hoofdstuk II. Probleemstelling

9. **Aankoop persoonsgegevens** – In dit tijdperk van ‘big data’, wordt er een grote hoeveelheid informatie over personen bewaard. Bedrijven kunnen de informatie die zij verzamelen, verkopen aan gespecialiseerde commerciële dataverzamelingsbedrijven. Deze dataverzamelingsbedrijven kunnen deze gegevens bijgevolg doorverkopen aan andere bedrijven of instanties. Op basis van deze persoonsgegevens zou er een gedetailleerd beeld over een persoon kunnen worden gevormd.¹⁹ Het zou eventueel nuttig kunnen zijn voor de Belgische overheid om deze gegevens aan te kopen bij gespecialiseerde dataverzamelingsbedrijven in het kader van het strafonderzoek. Hierdoor wordt er immers een grote hoeveelheid gegevens verkregen, in een korte tijd. Bijgevolg zou de overheid deze informatie niet zelf moeten zoeken, door gebruik te maken van andere middelen die de overheid ter beschikking heeft.²⁰
10. **Ontbreken specifiek regelgevend kader** – Op dit moment bestaat er geen specifiek regelgevend kader dat de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid regelt. Echter is dit naar mijns inziens geen probleem, aangezien het niet noodzakelijk is dat er een specifieke wet bestaat. Bovendien impliceert het bestaan van een wet niet automatisch dat iets goed geregeld is.
11. **Fundamentele rechten** – Naargelang de aard van de informatie, ‘gewone’ of gevoelige gegevens, zou het mogelijk zijn dat deze handeling de fundamentele rechten van een persoon kan schenden.
12. **Gegevensbescherming** – Eén van deze fundamentele rechten is het recht op privacy. Het recht op privacy waarborgt zowel het recht op eerbiediging van het privéleven, als de bescherming van persoonsgegevens. Er bestaan instrumenten die regels bepalen, die verwerkers van persoonsgegevens moeten naleven, om de bescherming van persoonsgegevens te waarborgen. Bijgevolg zouden deze regels kunnen worden geschonden door de aankoop van persoonsgegevens in het kader van het strafonderzoek
13. **Ethische gevaren** – Bovendien zou de handeling enkele ethische gevaren met zich mee kunnen meebrengen. Naar mijns inziens is bijvoorbeeld één van deze gevaren, dat dataverzamelingsbedrijven de privacyregels eventueel minder zullen naleven, indien de overheid deze bedrijven betaalt voor informatie. Aangezien de verkoop van deze persoonsgegevens, voor deze bedrijven, een bepaalde winstmarge zou kunnen opleveren. Een ander ethisch gevaar, zou mijns inziens kunnen zijn, dat de enorme hoeveelheid aan bewaarde gegevens, gefilterd kan worden op basis van algoritmes. Het zou bijgevolg

¹⁹ VIANGALLI, F., *Transferts internationaux de données : entre libre circulation et impératifs sécuritaires*, Larcier, 2019, 210-211.; RUSHMEIER, H. ‘Data Brokers and European Digital Legislation’, *EDPL* 2023/1, (37) 37.

²⁰ VAN DE HEYNING, C., ‘Not all that glitters is gold: een effectief recht op tegenspraak in tijden van bulkdata’, *T.Strafr.* 2021/4, (195) 195-201.; Privacyrichtlijn politie-justitie, overweging (3).; VANSWEEVELT, T. en BROECKX, N., *Handboek gezondheidsrecht: Privacy, persoonsgegevens en beroepsgeheim*, Intersentia, 2022, 641-826.

mogelijk zijn, dat deze algoritmes gegevens selecteren op basis van criteria die discriminerend kunnen zijn.

14. **Belangenconflict overheid** – Voorts zou er een belangenconflict kunnen bestaan, indien de overheid persoonsgegevens aankoopt bij dataverzamelingsbedrijven. Aangezien de overheid er dan een voordeel bij zou kunnen hebben dat dataverzamelingsbedrijven de privacyregels niet strikt naleven.
15. **Nut** – Daarnaast is het niet zeker of deze handeling effectief een voordeel zal opleveren in het kader van het strafonderzoek. Ook is het niet zeker welk nut deze handeling heeft, ten opzichte van andere middelen.

Hoofdstuk III. Doelstelling en relevantie

16. **Doel onderzoek** – Deze masterproef heeft tot doel te onderzoeken hoe de aankoop van persoonsgegevens bij gespecialiseerde commerciële dataverzamelingsbedrijven in het kader van het strafonderzoek, in de praktijk zou kunnen worden toegepast. Daarboven wordt onderzocht in hoeverre procedurele waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht kunnen waarborgen.
17. **Te onderzoeken aspecten** – In deze masterproef wordt onderzocht hoe de aankoop van persoonsgegevens door de Belgische overheid bij dataverzamelingsbedrijven in het kader van het strafonderzoek kan worden toegepast. Hierbij zal onder andere worden onderzocht of de procureur des Konings of de onderzoeksrechter bevoegd is, om deze handeling te bevelen. Naar gelang de aard van de persoonsgegevens, zouden bovendien de fundamentele rechten van de betrokkene kunnen worden geschonden, waaronder het recht op een eerlijk proces, het recht op privacy, met inbegrip van het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens, het recht op gelijkheid en non-discriminatie en het recht op vrije meningsuiting. De GDPR-wetgeving en de privacyrichtlijn politie-justitie waarborgen het recht op bescherming van persoonsgegevens en daarmee het recht op privacy. Deze instrumenten bevatten specifieke voorwaarden die in acht moeten worden genomen, om gegevens op een rechtmatige manier te verwerken. Indien de regels die werden opgenomen in deze richtlijn, niet worden nageleefd, kan bijgevolg het recht op privacy worden geschonden.
18. **Procedurele waarborgen** – Om deze redenen kunnen er procedurele waarborgen worden ingevoerd om de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht te waarborgen. Daarom zal er worden onderzocht welke procedurele waarborgen kunnen worden ingevoerd. Bovendien zal worden geanalyseerd in hoeverre deze procedure waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht kunnen waarborgen.
19. **Relevantie** – Op dit moment wordt de onderzochte handeling in de Belgische strafrechtspraktijk, naar mijn weten, nog niet toegepast. Daarom kan dit onderzoek relevant zijn om een juridisch kader aan te reiken, dat weergeeft hoe de aankoop van persoonsgegevens bij dataverzamelingsbedrijven kan worden toegepast in het kader van het strafonderzoek. Daarbij zullen de fundamentele rechten en de privacyrechten in acht worden genomen. Hiervoor zal geduid worden in hoeverre procedurele waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht nog kunnen waarborgen.

Hoofdstuk IV. Onderzoeksvragen

Afdeling I. Centrale onderzoeksvraag

20. **Centrale onderzoeksvraag** - Om de probleemstelling en de doelstelling te beantwoorden, richt dit onderzoek zich op het beantwoorden van de centrale onderzoeksvraag: 'Op welke manier kan de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek worden toegepast en in hoeverre kunnen procedurele waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht waarborgen?'

Afdeling II: Subonderzoeksvragen

21. **Subonderzoeksvragen** - De volgende subonderzoeksvragen zullen worden geanalyseerd, om de centrale onderzoeksvraag te kunnen beantwoorden:

Subvraag 1 – 'Hoe verhoudt de aankoop van persoonsgegevens door de overheid bij dataverzamelingsbedrijven zich tot andere onderzoekshandelingen?'

Subvraag 2 – 'In welke categorieën kunnen persoonsgegevens worden ingedeeld, naargelang de aard van de informatie?'

Subvraag 3 – 'Welke privacy en fundamentele rechten kunnen eventueel worden geschonden door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek?'

Subvraag 4 - 'Op welke manier wordt de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Amerikaanse overheid in het kader van het strafonderzoek in de Verenigde Staten geregeld?'

Subvraag 5 – 'Welke ethische gevaren kunnen er bestaan bij een overheid die betaalt voor informatie in het kader van het strafrechtelijk onderzoek?'

Subvraag 6 - 'Welke procedurele waarborgen kunnen worden ingevoerd om de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht te waarborgen?'

Hoofdstuk V. Onderzoeksmethodologie

22. **Methode** - Het onderzoek richt zich op een juridisch en praktijkgericht kader, waarbij zowel rechtsdogmatische als casuïstische methoden centraal staan.
23. **Centrale onderzoeksvraag** - De centrale onderzoeksvraag in dit onderzoek is: 'Op welke manier kan de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek worden toegepast en in hoeverre kunnen procedurele waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht waarborgen?'.
24. **Evaluatieve en aanbevelende vraag** - Deze centrale onderzoeksvraag is een evaluatieve en aanbevelende onderzoeksvraag. Deze onderzoeksvraag is een evaluatieve vraag, aangezien de vraag tot doel heeft een rechtsfiguur te beoordelen of te waarderen in het licht van een vooropgestelde norm. Zo kan worden nagegaan wanneer de handeling in overeenstemming is met de fundamentele rechten, met inbegrip van het gegevensbeschermingsrecht.²¹ Deze onderzoeksvraag is ook aanbevelend, aangezien de vraag tracht te bepalen hoe het recht of een rechtsfiguur zou kunnen zijn. Deze vraag zal resulteren in een voorstel, dat aangeeft op welke manier de aankoop van persoonsgegevens bij dataverzamelingsbedrijven in het kader van het strafonderzoek, zou kunnen worden toegepast.²² Er zal dus getracht worden een aanbeveling te geven over de manier waarop de onderzochte handeling in de praktijk kan worden toegepast. Daarbij zal worden besproken wat de ethische gevaren kunnen zijn van een overheid die ervoor kiest om informatie te kopen, in de plaats van deze zelf te zoeken. Daarboven zal het belangenconflict van de overheid worden besproken. Bovendien zal het nut van deze onderzoekshandeling, ten opzichte van de bestaande middelen worden onderzocht. Er zal voorts worden onderzocht wie deze handeling kan bevelen. Daarnaast zal er worden geanalyseerd welke procedurele waarborgen kunnen worden ingevoerd. Bovendien zal worden geëvalueerd in hoeverre procedure waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht kunnen waarborgen. Daarboven zullen criteria worden aangereikt om te controleren of de handeling al dan niet noodzakelijk, proportioneel en subsidiair is. Voorts zal er ook nog worden geanalyseerd wie de aankoop betaalt, welke bedrag er wordt betaald en hoe het budget bepaald wordt.
25. **Subvragen** - Naast deze centrale onderzoeksvraag zullen er ook een aantal specifieke subonderzoeksvragen behandeld worden:
26. **Subvraag 1** - De eerste subvraag is: 'Hoe verhoudt de aankoop van persoonsgegevens door de overheid bij dataverzamelingsbedrijven zich tot andere onderzoekshandelingen?'. Deze vraag is een vergelijkende onderzoeksvraag. Aangezien de vraag meerdere

²¹ KESTEMONT, L. en SCHOUKENS, P., *Rechtswetenschappelijk schrijven*, Acco, 2020, 32.; MEULEMAN, B. en ROOSE, H., *Kennis maken - methodologie voor sociale wetenschappers*, Gent, 2021, 316-327.

²² KESTEMONT, L. en SCHOUKENS, P., *Rechtswetenschappelijk schrijven*, Acco, 2020, 32.

rechtsfiguren met elkaar vergelijkt, om de gelijkenissen of verschillen weer te geven. Dit is een interne vergelijking. Doordat er een vergelijking wordt gemaakt, binnen hetzelfde rechtstelsel.²³ In het beschrijvend gedeelte zullen een aantal onderzoekshandelingen, die vergelijkbaar zijn met de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de overheid in het kader van het strafonderzoek geanalyseerd worden. Er wordt specifiek gekozen om te vergelijken met deze onderzoekshandelingen, omdat deze onderzoekshandelingen ook betrekking hebben op het verkrijgen van persoonsgegevens of eventueel even ingrijpend kunnen zijn. Om deze redenen wordt het opvragen van gegevens bij telecomoperatoren en bankinstellingen en de medewerkingsplicht die op deze actoren rust besproken en het beslag. Daarnaast zal er vergeleken worden met het DNA-onderzoek, de huiszoeking, het opsporen van de communicatie en doorzoeking van het informaticasysteem en het opsporen van de elektronische communicatie. Op basis van deze analyse, zal in het evaluerend deel worden onderzocht of de handeling kan worden beschouwd als onderzoekshandeling. Bovendien zal worden onderzocht wat het nut kan zijn van de aankoop van persoonsgegevens bij dataverzamelingsbedrijven voor het strafonderzoek, ten opzichte van bestaande middelen. Daarnaast zal er bij het onderzoek naar hoe de praktijk er zou kunnen uitzien, worden verwezen naar deze onderzoekshandelingen. Hiervoor zal wetgeving en rechtsleer geraadpleegd worden.

27. **Subvraag 2** – De tweede subvraag is ‘In welke categorieën kunnen persoonsgegevens worden ingedeeld, naargelang de aard van de informatie?’. Dit is een beschrijvende onderzoeksvraag. Aangezien de vraag tot doel heeft het recht op een systematische wijze uiteen te zetten en bevattelijk weer te geven.²⁴ Hierbij zal worden onderzocht in welke categorieën persoonsgegevens kunnen worden ingedeeld, naargelang de aard van de informatie. Hierbij zal het onderscheid tussen niet-gevoelige en gevoelige gegevens beschreven worden. Bovendien zal worden geanalyseerd welke persoonsgegevens beschouwd worden als gevoelige gegevens. Bijgevolg zal dit onderscheid het mogelijk maken, om in het evaluatief deel te onderzoeken of er al dan niet sprake is van een dwangmaatregel. Hiervoor zal wetgeving, voorbereidende werken, rechtsleer en rechtspraak worden geanalyseerd.
28. **Subvraag 3** - De derde subvraag is: ‘Welke privacy en fundamentele rechten kunnen eventueel worden geschonden door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek?’. Dit is een beschrijvende en evaluerende onderzoeksvraag. Deze vraag is beschrijvend, aangezien de vraag tot doel heeft het recht op een systematische wijze uiteen te zetten en systematisch weer te geven.²⁵ Daarnaast is de vraag ook evaluerend, aangezien de vraag het recht of een rechtsfiguur beoordeelt in het licht van een vooropgestelde norm. Zo kan worden nagaan of de aankoop van persoonsgegevens, al dan

²³ *Ibid.*, 31.

²⁴ *Ibid.*, 30.

²⁵ *Ibid.*

niet de fundamentele rechten kan schenden.²⁶ In het beschrijvend deel zullen een aantal fundamentele rechten geanalyseerd worden, die eventueel geschonden kunnen worden, door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de overheid in het kader van het strafonderzoek. Hierbij zal het recht op een eerlijk proces, het recht op privacy, met inbegrip van het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens, het recht op gelijkheid en non-discriminatie en het recht op vrije meningsuiting worden besproken. Bovendien zullen de belangrijkste instrumenten van het gegevensbeschermingsrecht, de GDPR-wet en de privacyrichtlijn politie-justitie, worden besproken. Hierbij zullen de voorwaarden besproken worden waar de verwerking aan moet voldoen om rechtmatig te zijn, waardoor een grotere grondrechtsbescherming kan worden gewaarborgd. Daarnaast zal in het evaluatief deel worden beschreven, welke procedurele waarborgen kunnen worden ingevoerd met betrekking tot de bescherming van persoonsgegevens.

29. **Subvraag 4** - De vierde subvraag is: 'Op welke manier wordt de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Amerikaanse overheid in het kader van het strafonderzoek in de Verenigde Staten geregeld?'. Deze vraag is vergelijkend, aangezien deze vraag twee rechtsfiguren met elkaar vergelijkt om de gelijkenissen en verschillen bloot te leggen. Dit is een externe vergelijking, omdat het een vergelijking is tussen twee verschillende rechtsstelsels, dat van België en dat van de Verenigde Staten.²⁷ In het beschrijvend gedeelte zal worden onderzocht of er in de Verenigde Staten regelgeving bestaat, die de aankoop van persoonsgegevens door de overheid bij dataverzamelingsbedrijven in het kader van het strafonderzoek regelt. Hierbij zullen de federale wetten, waaronder de privacy act en de Cloud-act, worden besproken. Daarnaast zullen de deelstaatwetten van Vermont en Californië besproken worden, die regels bevatten omtrent de aankoop van persoonsgegevens door de overheid, dit zijn de Vermont Consumer Protection Act en de California Consumer Privacy Act. Daarnaast zullen de federale wetten, waaronder de privacy act en de Cloud-act, worden besproken. Bovendien zal de mogelijkheid die de Amerikaanse overheid heeft om gegevens op te vragen bij Google kort worden besproken. Hiervoor zal voornamelijk Amerikaanse wetgeving en rechtsleer bestudeerd worden.
30. **Subvraag 5** – De vijfde onderzoeksvraag is: 'Welke ethische gevaren kunnen er bestaan bij een overheid die betaalt voor informatie in het kader van het strafrechtelijk onderzoek?'. Dit is een evaluerende onderzoeksvraag, aangezien de vraag een rechtsfiguur beoordeelt in het licht van een vooropgestelde norm. Hierbij kan worden nagegaan of de rechtsfiguur eventueel nadelig is of al dan niet in overeenstemming is met bepaalde regelgeving.²⁸ Er wordt onderzocht welke ethische gevaren er kunnen bestaan, indien de overheid de

²⁶ KESTEMONT, L. en SCHOUKENS, P., *Rechtswetenschappelijk schrijven*, Acco, 2020, 32.; MEULEMAN, B. en ROOSE, H., *Kennis maken - methodologie voor sociale wetenschappers*, Gent, 2021, 316-327.

²⁷ KESTEMONT, L. en SCHOUKENS, P., *Rechtswetenschappelijk schrijven*, Acco, 2020, 31.

²⁸ KESTEMONT, L. en SCHOUKENS, P., *Rechtswetenschappelijk schrijven*, Acco, 2020, 32.; MEULEMAN, B. en ROOSE, H., *Kennis maken - methodologie voor sociale wetenschappers*, Gent, 2021, 316-327.

beleidsmatige keuze maakt om te betalen voor informatie, in de plaats van deze zelf te zoeken. Hiervoor zal een vergelijking worden gemaakt met de informatie die de overheid verkrijgt door informaten en getuigen. Hierbij zal ook het belangenconflict van de overheid besproken worden, aangezien de overheid er belang bij kan hebben, dat bedrijven de privacyregels niet strikt naleven, zodat de overheid meer informatie kan verzamelen. Hiervoor zal rechtsleer en rechtspraak worden geanalyseerd.

31. **Subvraag 6** - De zesde subvraag is: 'Welke procedurele waarborgen kunnen worden ingevoerd om de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht te waarborgen?'. Dit is een aanbevelende onderzoeksvraag, aangezien deze vraag tracht te bepalen wat het gewenste recht is of hoe het recht zou moeten zijn. Deze vraag zal resulteren in een voorstel om bepaalde procedure waarborgen in te voeren om de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht te waarborgen.²⁹ In het evaluerend gedeelte zal worden onderzocht welke procedurele waarborgen kunnen worden ingevoerd. Bijgevolg zal het antwoord op deze subvraag, ertoe bijdragen om de centrale onderzoeksvraag te beantwoorden. Op basis van deze subvraag, kan worden geanalyseerd in hoeverre procedurele waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht kunnen waarborgen.

²⁹ KESTEMONT, L. en SCHOUKENS, P., *Rechtswetenschappelijk schrijven*, Acco, 2020, 32.

Hoofdstuk VI. Afbakening onderzoek

32. **Keuze begrenzing** – Op dit moment wordt de aankoop van persoonsgegevens bij dataverzamelingsbedrijven in België, naar mijn weten, nog niet toegepast. Daarom is het interessant om te analyseren hoe deze handeling er in de praktijk zou kunnen uitzien. Hierbij zullen verschillende aspecten besproken worden, bijvoorbeeld wie bevoegd is om de aankoop te bevelen of wat het nut van de handeling kan zijn. In een digitaal tijdsperk, waar enorme hoeveelheden informatie wordt opgeslagen, is het mijns inziens zeer belangrijk dat de rechten van de betrokkene beschermd worden. Daarom heb ik mij in het kader van dit onderzoek, naast het onderzoeken van een mogelijke praktische toepassing van de handeling, voornamelijk gefocust op de privacy en fundamentele rechten en de manier waarop deze kunnen worden gewaarborgd. Daarom zal onderzocht worden welke procedurele waarborgen kunnen worden ingevoerd en in hoeverre deze de grondrechtsbescherming kunnen waarborgen.
33. **Begrenzing** - Vanwege de complexiteit van het onderwerp en het tijdsbestek, is het onderzoek begrensd op grootte en afbakening. De territoriale focus is beperkt tot België en de Verenigde Staten. Hierbij werd specifiek geopteerd om in het kader van het tijdsbestek, enkel een vergelijk met de Verenigde Staten te maken. Er werd specifiek gekozen voor de Verenigde Staten, omdat de industrie van de dataverzamelingsbedrijven in de Verenigde Staten succesvol en actief is. Bovendien zijn de grootste dataverzamelingsbedrijven gelegen in de Verenigde Staten. Daardoor zal er geen onderzoek worden gevoerd naar het rechtstelsel van andere landen.³⁰
34. **Europese regelgeving** - Dit betekent dat er in het kader van dit onderzoek enkel Europese, Belgische of Amerikaanse wetgeving, rechtsleer en rechtspraak zal worden geanalyseerd. Aangezien de onderzoeksvraag zich richt op de Belgische overheid die gegevens aankoopt bij dataverzamelingsbedrijven, zal uitsluitend Europese wetgeving die werd omgezet in België worden besproken. Bovendien zal uitsluitend de huidige relevante wetgeving worden besproken. Bijgevolg zal er niet worden onderzocht, welke regels er in het verleden van toepassing waren.
35. **Aankoop gegevens** - Het onderzoek zal afgebakend zijn tot de aankoop van persoonsgegevens door de overheid in het kader van het strafonderzoek en de rechtmatigheid van deze handeling. Daarom zal er niet worden onderzocht op welke manier dataverzamelingsbedrijven deze gegevens op een geldige manier kunnen verkrijgen. Daarnaast zal de verwerking van persoonsgegevens door dataverzamelingsbedrijven niet worden geanalyseerd.
36. **Verwerking gegevens** - Hierbij zal er slechts zeer beperkt worden onderzocht op welke manier de overheid, de aangekochte persoonsgegevens moet verwerken. Bijgevolg zal uitsluitend de bewaringstermijn, de beperkte toegang van personen tot de gegevens en

³⁰ *Supra* nr. 187.

beveiliging van de gegevens kort worden aangehaald met betrekking tot de procedurele waarborgen. Om deze reden zullen de specifieke regels omtrent de verwerking van deze gegevens door de overheid, zoals wie de verwerker en verwerkingsverantwoordelijke is, niet worden besproken. Bovendien zullen de specifieke rechten die de betrokkene heeft bij de verwerking, waaronder het recht op inzage en het recht rectificatie, niet worden onderzocht. Enkel de beginselen van de verwerking zullen geduid worden.

37. **Spanningsveld strafrecht vs. gegevensbeschermingsrecht** – Voorts zal het spanningsveld tussen het gegevensbeschermingsrecht en het straf- en strafprocesrecht niet geanalyseerd worden. Er zal slechts worden benadrukt dat de regels van het strafprocesrecht voorrang hebben op deze van het gegevensbeschermingsrecht. De precieze tegenstrijdigheden tussen beide rechtstakken zullen bijgevolg niet nader geanalyseerd worden.
38. **Geen interviews of enquêtes** - Bovendien zullen er geen diepte-interviews of enquêtes worden afgenomen. Hierdoor beperkt het onderzoek zich tot een monodisciplinair onderzoek. Bijgevolg zal er geen interdisciplinair onderzoek gevoerd worden.
39. **Gericht onderzoek** - Door deze focus blijft het onderzoek gericht en zorgt het voor het bieden van concrete inzichten, evaluaties en aanbevelingen.

Hoofdstuk VII. Onderzoeksplan

40. **Inleiding** - Het onderzoek start met een inleiding, die aangeeft dat er in deze digitaliserende maatschappij steeds meer data wordt bewaard en dat deze data door bedrijven kan worden verkocht aan dataverzamelingsbedrijven. Hierbij wordt kort geduid wat dataverzamelingsbedrijven zijn, welke gegevens deze bedrijven verzamelen en op welke manier deze gegevens worden verzameld. Daarna wordt het precieze probleem gekaderd en wordt het onderzoek afgebakend.
41. **Beschrijvend gedeelte** - Nadien komt het theoretische en juridische kader aanbod. Dit vormt de basis voor het onderzoek en bestaat uit verschillende hoofdstukken. Eerst zal er een beschrijvend gedeelte volgen en nadien een aanbevelend en evaluerend gedeelte. In het eerste deel van het beschrijvend gedeelte, zal het opsporingsonderzoek, het gerechtelijk onderzoek en de mini-instructie worden geanalyseerd. Daarna zullen een aantal onderzoekshandelingen geanalyseerd worden, die vergelijkbaar zijn met de onderzochte handeling, aangezien deze handelingen ook betrekking hebben op het verzamelen van persoonsgegevens en in bepaalde gevallen de fundamentele rechten en vrijheden kunnen schenden. De onderzoekshandelingen die besproken worden zijn het opvragen van gegevens op basis van wettelijke regels, het klassiek beslag en het databeslag, de zoeking in het informatica- en communicatiesysteem, het opsporen van elektronische communicatie, het DNA-onderzoek en de huiszoeking. Daarnaast zal de evolutie van de dataretentiewet kort worden besproken. Hierbij is vooral het standpunt van het Grondwettelijk Hof relevant. Hiervoor zal de relevante wetgeving uit het Belgische strafwetboek, de voorafgaande titel van het wetboek van strafvordering, het wetboek van strafvordering en de verschillende dataretentiewetten worden geanalyseerd. Ook zal de rechtsleer en rechtspraak van het Grondwettelijk Hof met betrekking tot de dataretentiewetten worden geanalyseerd.
42. **Grond- en mensenrechten** - In het tweede deel zullen enkele fundamentele rechten nader geanalyseerd worden. Hierbij zal het recht op een eerlijk proces, het recht op privacy, met inbegrip van het recht op eerbiediging van persoonsgegevens en het recht op bescherming van persoonsgegevens, het recht op gelijkheid en non-discriminatie en het recht op vrije meningsuiting bestudeerd worden. Daarnaast zullen de voorwaarden waaraan voldaan moet zijn, om de grondrechtsbescherming te waarborgen, worden besproken. Hierbij wordt het bestaan van een wettelijke basis, het nastreven van een legitiem doel in een democratische samenleving en de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit besproken. Hiervoor zal het Europees Verdrag voor de Rechten van de Mens, het Handvest van de Europese Unie en de Belgische Grondwet geanalyseerd worden. Bovendien zal ook rechtsleer en rechtspraak bestudeerd worden.
43. **Gegevensbeschermingsrecht** - In het derde deel wordt het gegevensbeschermingsrecht onderzocht. Vooreerst zullen de persoonsgegevens, naargelang de aard van de informatie, ingedeeld worden. Hierbij zal het verschil tussen 'gewone' en gevoelige gegevens

besproken worden. Nadien zullen de belangrijkste richtlijnen met betrekking tot het gegevensbeschermingsrecht besproken worden. Bijgevolg zal eerst de AVG besproken worden, hieruit zal blijken dat deze verordening niet van toepassing is, met betrekking tot de verwerking van persoonsgegevens in het kader van de opsporing en het onderzoek naar strafbare feiten. Desalniettemin is de privacyrichtlijn politie-justitie wel van toepassing op deze verwerking. Bijgevolg zal deze richtlijn diepgaander worden geanalyseerd. Bovendien werd de AVG, in België omgezet in Titel I Wet Verwerking Persoonsgegevens. Daarnaast werd de privacyrichtlijn politie-justitie omgezet in Titel II van dezelfde wet. Hiervoor zal wetgeving, voorbereidende werken, rechtsleer en rechtspraak worden geanalyseerd.

44. **Rechtsvergelijkend onderzoek** – Daarnaast zal er een rechtsvergelijkend onderzoek gevoerd worden met de Verenigde Staten. Hierbij zal worden onderzocht hoe de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de overheid in het kader van het strafonderzoek in de Verenigde Staten geregeld wordt en welke regelgeving daarbij relevant is. Daarbij zal op federaal niveau, de privacy act en de Cloud-act worden besproken. Ook de deelstaatwetten in California en Vermont die relevant zijn, zullen worden besproken, dit zijn de California Consumer Privacy Act en de Vermont Consumer Protection Act. Bovendien zal geanalyseerd worden op welke manier de Amerikaanse overheid gegevens kan opvragen bij Google. Hierbij zal Amerikaanse regelgeving, rechtsleer en internetbronnen worden geraadpleegd.
45. **Aanbevelend/evaluerend deel** – Na het beschrijvend deel, volgt het evaluerend/aanbevelend deel. In dit deel, zullen op basis van de informatie die onderzocht werd in het beschrijvend deel, verschillende aspecten worden geanalyseerd en getracht worden een aanbeveling te geven. Eerst zullen de ethische gevaren van een overheid die betaalt voor informatie en het belangenconflict van de overheid bij het aankopen van persoonsgegevens bij dataverzamelingsbedrijven worden besproken. Daarnaast zal geanalyseerd worden hoe de onderzoekshandeling er zou kunnen uitzien. Nadien zal het nut van deze onderzoekshandeling in vergelijking met andere middelen worden besproken. Vervolgens zal worden onderzocht om welke redenen de fundamentele rechten kunnen worden geschonden door de handeling. Hierbij zal worden aangegeven welke procedurele waarborgen kunnen worden ingevoerd, om de grondrechtsbescherming te waarborgen en in hoeverre deze procedurele waarborgen de grondrechtsbescherming kunnen waarborgen. Nadien zal worden besproken hoe ervoor kan worden gezorgd, dat de regels van de privacyrichtlijn politie-justitie kunnen worden gerespecteerd. Daarnaast zal worden onderzocht welke procedurele waarborgen het gegevensbeschermingsrecht kunnen waarborgen en in hoeverre deze procedurele waarborgen de bescherming van het gegevensbeschermingsrecht, en bijgevolg de grondrechtsbescherming, kunnen waarborgen. Nadien zullen de regels met betrekking tot de betaling van prestatieverleners op basis van het Koninklijk Besluit en de Wet Gerechtskosten worden besproken. Bovendien zal de bijzondere regeling met betrekking tot de betaling van prestaties, verleend door telecomoperatoren worden besproken. Op basis daarvan zal worden onderzocht op welke manier het betalingsproces met betrekking tot de aankoop van

gegevens bij dataverzamelingsbedrijven, zou kunnen verlopen. Daarnaast zal er worden geanalyseerd of er een bedrag per geleverde dienst of een forfaitair bedrag moet worden bepaald. Daarboven zal worden onderzocht hoe dit bedrag wordt vastgesteld. Bovendien zal worden onderzocht hoe het budget wordt bepaald. Hiervoor zal wetgeving, rechtsleer en rechtspraak geraadpleegd worden.

46. **Conclusie** - Op het einde van het onderzoek wordt getracht een concreet antwoord op de centrale onderzoeksvraag te formuleren. Hierbij zal worden omschreven hoe de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek kan worden toegepast. Daarnaast zal omschreven worden in hoeverre procedurele waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht kunnen waarborgen. Hierbij zal ook aangegeven worden vanaf welke grenzen de grondrechtsbescherming niet langer gewaarborgd zal zijn. Indien de grondrechtsbescherming niet langer gewaarborgd is, kan het zijn dat de handeling de fundamentele rechten, waaronder het recht op privacy schendt.

Deel II: Het strafrechtelijk onderzoek

Hoofdstuk I. Het opsporings- en gerechtelijk onderzoek

47. **Inleiding** – In dit hoofdstuk zal het onderscheid tussen het opsporingsonderzoek en het gerechtelijk onderzoek geanalyseerd worden. Bovendien zal de mini-instructie omschreven worden. Dit hoofdstuk heeft tot doel te analyseren of het mogelijk is om tijdens het opsporingsonderzoek, respectievelijk het gerechtelijk onderzoek, dwangmaatregelen te bevelen.
48. **Opsporingsonderzoek** – In België wordt een onderscheid gemaakt tussen het opsporingsonderzoek en het gerechtelijk onderzoek. Het opsporingsonderzoek staat onder leiding van de procureur des Konings, terwijl het gerechtelijk onderzoek wordt gevoerd door de onderzoeksrechter.³¹ Het doel van het opsporingsonderzoek is het opsporen van misdrijven en de daders hiervan. Daarnaast behoort ook het verzamelen van bewijs tot de het doel van het opsporingsonderzoek.³² Hierbij zullen er geen significante inbreuken worden gemaakt op de individuele rechten en vrijheden van de in verdenking gestelde.³³ Dit aangezien de opsporingshandelingen, die geleid worden door de procureur des Konings in principe geen dwangmaatregelen mogen uitmaken.³⁴ Daarentegen kan de onderzoeksrechter in het kader van het gerechtelijk onderzoek wel opsporingshandelingen uitvoeren, die een dwangmaatregel uitmaken.³⁵
49. **Heterdaad** – Niettegenstaande het verbod dat van toepassing is op de procureur des Konings om dwangmaatregelen te nemen, is het de procureur des Konings toegestaan om dwang te gebruiken, in het kader van het opsporingsonderzoek, bij een situatie op heterdaad. In dit geval beschikt de procureur des Konings over een bijzondere onderzoeksbevoegdheid. Deze bijzondere onderzoeksbevoegdheid blijft bestaan, zolang de heterdaadsituatie voortduurt of tot het moment waarop de onderzoeksrechter wordt gevorderd.³⁶
50. **Gerechtelijk onderzoek** – Het doel van het gerechtelijk onderzoek is het opsporen van misdrijven en de daders hiervan en het verzamelen van bewijs.³⁷ In tegenstelling tot de procureur des Konings, beschikt de onderzoeksrechter over de bevoegdheid om meer ingrijpende maatregelen te nemen. Dit heeft tot gevolg dat de onderzoeksrechter onderzoekshandelingen kan stellen die dwangmaatregelen impliceren. Deze

³¹ DERUYCK, F., *Overzicht van het Belgisch Strafprocesrecht: Het opsporingsonderzoek*, die Keure, 2024, 78-123, nr. 196.

³² Art. 28bis, §1, eerste lid Sv.

³³ BAILLIEUX, A., *Afstand van recht in de strafprocedure: Zelfbeschikking bij een traditionele afhandeling van een strafprocedure*, Intersentia, 2019, 143-364, nr. 200.

³⁴ Art. 28bis, §3 Sv.

³⁵ EVERS, F. en VAN CAUWENBERGE, K., *Op-recht-uit. Een hulde aan Alain Bloch: De onderzoeksrechter*, die Keure, 2022, 150-151.

³⁶ DERUYCK, F., *Overzicht van het Belgisch Strafprocesrecht: Het opsporingsonderzoek*, die Keure, 2024, 78-123, nr. 201.

³⁷ Art. 55 Sv.

dwangmaatregelen kunnen leiden tot inbreuken op de individuele rechten en vrijheden.³⁸ Zo dient de onderzoeksrechter zelf te beoordelen of het al dan niet noodzakelijk is om dwangmaatregelen te nemen, die een inbreuk kunnen maken op de individuele rechten en vrijheden van de betrokkene.³⁹

51. **Mini-instructie** – Voorts bestaat er de mogelijkheid tot het uitvoeren van een mini-instructie.⁴⁰ In dit geval kan de procureur des Konings tijdens het opsporingsonderzoek, de onderzoeksrechter vorderen om een bepaalde onderzoekshandeling te verrichten, waarvoor de procureur des Konings zelf niet bevoegd is. Hierbij wordt geen gerechtelijk onderzoek ingesteld.⁴¹ Na het uitvoeren van deze onderzoekshandeling kan de onderzoeksrechter beslissen om het onderzoek verder te laten uitvoeren door de procureur des Konings of om het onderzoek naar zich toe te trekken en bijgevolg zelf het onderzoek voort te zetten.⁴²
52. **Uitsluitingen mini-instructie** – Echter zijn een aantal onderzoekshandelingen van het toepassingsgebied van de mini-instructie uitgesloten. De uitsluitingen betreffen ingrijpende onderzoekshandelingen, zoals het bevel tot aanhouding, de zoeking in het communicatie- en informaticasysteem, de huiszoeking, de observatie met technische hulpmiddelen om zich te verwerven in een woning en de inkijkoperatie in de woning.⁴³ Aangezien deze onderzoekshandelingen ingrijpende gevolgen kunnen hebben, mogen deze handelingen uitsluitend uitgevoerd worden in het kader van het gerechtelijk onderzoek, onder leiding van de onderzoeksrechter.⁴⁴
53. **Machtiging** – Eveneens heeft de onderzoeksrechter de bevoegdheid om de procureur des Konings te machtigen om een bepaalde opsporingshandeling uit te voeren.⁴⁵ Zo kan de onderzoeksrechter de procureur des Konings ook machtigen om een bijzondere opsporingsmethode uit te voeren.⁴⁶
54. **Onderzoekshandelingen binnen het gerechtelijk onderzoek** – In het kader van het gerechtelijk onderzoek is de onderzoeksrechter bevoegd om de volgende onderzoekshandelingen te stellen; huiszoeking en inbeslagname; aanhouding en in verdenkingstelling van een verdachte; ondervraging van de in verdenkinggestelde,

³⁸ DERUYCK, F., *Overzicht van het Belgisch Strafrechtsprocesrecht: Het gerechtelijk onderzoek*, die Keure, 2024, 124-170, nr. 310.

³⁹ Art. 56, §1 Sv.

⁴⁰ EVERS, F. en VAN CAUWENBERGE, K., *Op-recht-uit. Een hulde aan Alain Bloch: De onderzoeksrechter*, die Keure, 2022, 150-151.

⁴¹ BAILLIEUX, A., *Afstand van recht in de strafprocedure: Zelfbeschikking bij een traditionele afhandeling van een strafprocedure*, Intersentia, 2019, 143-364, nr. 200.

⁴² Art. 28septies Sv.

⁴³ BRULOOT, D., DE GROOTE, B. en DE CORTE, R., *Privaatrecht in hoofdlijnen: Strafrecht en strafrechtspleging*, LeA Uitgevers, 2022, 346, nr. 523.

⁴⁴ *Ibid.*

⁴⁵ *Ibid.*, 345-521.

⁴⁶ Art. 46septies Sv.; Art. 47sexies, §7 Sv.; EVERS, F. en VAN CAUWENBERGE, K., *Op-recht-uit. Een hulde aan Alain Bloch: De onderzoeksrechter*, die Keure, 2022, 150.; Art. 56bis Wet 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden, BS 12 mei 2003.

opsporing van telecommunicatie; onderzoek aan het lichaam; telefoontap en DNA-onderzoek.⁴⁷

55. **Aankoop persoonsgegevens** – Op dit moment bestaat er nog geen specifiek regelgevend kader met betrekking tot de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de overheid, dit hoeft echter geen probleem te vormen. Aangezien er wel andere regelgeving bestaat, waaronder het wetboek van strafvordering.

⁴⁷ Wetboek van Strafvordering

Hoofdstuk II. Vergelijkbare opsporingshandelingen

56. **Onderzoekshandelingen** - In dit hoofdstuk zal de volgende subvraag worden onderzocht: 'Hoe verhoudt de aankoop van persoonsgegevens door de overheid bij dataverzamelingsbedrijven zich tot andere onderzoekshandelingen?'. Bijgevolg zullen er in dit hoofdstuk een aantal onderzoekshandelingen geanalyseerd worden, die worden toegepast in het kader van het strafonderzoek. Er werd specifiek geopteerd om deze onderzoekshandelingen te bespreken, aangezien deze handelingen vergelijkbaar zijn met de aankoop van persoonsgegevens in het kader van het strafonderzoek. De handeling die besproken wordt in het kader van deze masterproef, zou naar gelang de aard van de aangekochte gegevens, eventueel de individuele rechten en vrijheden kunnen schenden.⁴⁸ Waardoor dit in bepaalde gevallen een ingrijpende maatregel kan zijn. De onderzoekshandelingen die besproken worden zijn vergelijkbaar, aangezien deze ook betrekking hebben op het verzamelen van persoonsgegevens en omdat deze in bepaalde gevallen even ingrijpend en verregaand kunnen zijn als de onderzochte handelingen, waardoor eventueel het recht op privacy zou kunnen worden geschonden. Op basis van de informatie in dit hoofdstuk, zal in het evaluatief deel worden onderzocht wat het nut is van de onderzochte handeling, in vergelijking met de bestaande middelen.⁴⁹
57. **Vergelijkbare onderzoekshandelingen** - De onderzoekshandelingen die nader worden onderzocht in dit hoofdstuk zijn; het opvragen van gegevens op basis van wettelijke regels; het klassiek beslag en het databeslag; het DNA-onderzoek; de huiszoeking; het opsporen van communicatie en doorzoeking van het informaticasysteem en het opsporen van de elektronische communicatie.

⁴⁸ *Supra* nr. 236.

⁴⁹ *Infra* nr. 227-233.

Afdeling I. Opvragen van gegevens op basis van wettelijke regels

58. **Medewerkingsplicht** - De gerechtelijke overheden, waaronder de procureur des Konings en de onderzoeksrechter, kunnen bepaalde gegevens opvragen bij verschillende actoren op basis van wettelijke regels. Bovendien rust op deze actoren, waaronder telecomoperatoren of dienstenverstrekkers van communicatie en bankinstellingen, een medewerkingsplicht.⁵⁰ Dit heeft tot gevolg dat deze actoren verplicht zijn om de opgevraagde gegevens mee te delen aan de procureur des Konings of de onderzoeksrechter.⁵¹
59. **Geen informatie creëren** - Bovendien heeft de medewerkingsplicht van de actoren uitsluitend betrekking op het verstrekken van informatie die de actor onder zich heeft. Bijgevolg impliceert de medewerkingsplicht niet dat bepaalde gegevens door de actor moeten worden gecreëerd.⁵² De dataretentiewet bepaalt met betrekking tot de telecomoperatoren, welke gegevens bewaard moeten blijven, zodat gerechtelijke overheden deze kunnen opvragen in het kader van het strafonderzoek.⁵³

⁵⁰ KB van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 8 oktober 2013.; KB 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten met betrekking tot elektronische communicatie, *BS* 8 november 2010.; KB 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 109ter, E, § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *BS* 10 februari 2003.

⁵¹ BERKMOES, H., *Identificatie van (gebruikers van) elektronische communicatie*, Wolters Kluwer, 2023, 1-55.

⁵² CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Intersentia, 2017, 189-287, nr. 300 en 459.

⁵³ 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.

Onderafdeling I. Opvragen van gegevens bij telecomoperatoren

60. **Telecomoperator** - Vooreerst kan de procureur des Konings rechtstreeks gegevens opvragen bij telecomoperatoren of dienstenverstrekkers van communicatie omtrent de identificatie van gebruikers of de identificatie van diensten.⁵⁴ Daarnaast kan de onderzoeksrechter of in bepaalde gevallen de procureur des Konings, gegevens zoals verkeers- en locatiegegevens opvragen. Zo kunnen er historische gegevens en gegevens in reële tijd worden opgevraagd.⁵⁵ Voorts kan de onderzoeksrechter, en in bepaalde gevallen de procureur des Konings, de communicatie van personen onderscheppen.⁵⁶ Daarnaast kan de onderzoeksrechter of in bepaalde gevallen de procureur des Konings, de telecomoperator verplichten inlichtingen te verstrekken of zijn medewerking te verlenen, om toegang te krijgen tot het communicatie- en informaticasystemen.⁵⁷ Het opsporen van communicatie en het doorzoeken van communicatie- en informaticasystemen zal later in deze masterproef diepgaander geanalyseerd worden.⁵⁸
61. **Coördinatiecel** - Daarnaast heeft de wetgever ervoor geopteerd om binnen elke operator en dienstenverstrekker, de groep van personen die deze opdrachten uitvoeren zo beperkt mogelijk te houden. Dit heeft tot doel de geheimhouding van de onderzoeken van de bevoegde overheden en de privacy van de geïdentificeerde personen maximaal te beschermen. Bijgevolg vormen deze personen de 'Coördinatiecel Justitie'. Bovendien moet deze coördinatiecel verplicht worden opgericht.⁵⁹ Daarnaast moet het personeel, dat werkzaam is in deze cel worden gescreend.⁶⁰

⁵⁴ Art. 46bis Sv.

⁵⁵ Art. 88bis Sv.

⁵⁶ Art. 90ter Sv.; Art. 90quater, §2 Sv.

⁵⁷ Art. 90ter Sv., Art. 90quater, §4 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. 55-2572/001, 142.

⁵⁸ *Infra* nr. 93-101 en 102-106.

⁵⁹ BERKMOES, H., *Identificatie van (gebruikers van) elektronische communicatie*, Wolters Kluwer, 2023, 1-55.

⁶⁰ Art 126/1, §1 Wet 13 juni 2005 betreffende de elektronische communicatie, BS 20 juni 2005.; Art 2 KB 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 109ter, E, § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, BS 10 februari 2003.; Art 2 KB 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten met betrekking tot elektronische communicatie, BS 8 november 2010.

Onderafdeling. II. Opvragen van gegevens bij bankinstellingen

62. **Opsporingsonderzoek** - Naast telecomoperatoren en dienstenverstrekkers van communicatie, zijn ook bankinstellingen verplicht hun medewerking te verlenen. Het is mogelijk voor de procureur des Konings om de lijst van bepaalde bankrekeningen, bankkluizen, of financiële instrumenten te vorderen, waarvan de verdachte titularis of gevolmachtigde uiteindelijke gerechtigde is.⁶¹ Bovendien kan de procureur des Konings in voorkomend geval alle verdere gegevens met betrekking tot deze bankkluizen, of financiële instrumenten vorderen. Daarnaast kan de procureur des Konings gegevens opvragen omtrent de bankverrichtingen die in een bepaald tijdvak zijn uitgevoerd, met inbegrip van de bijzonderheden betreffende de rekening van herkomst of bestemming. Daarboven kan de procureur des Konings de gegevens vorderen van de titularissen of gevolmachtigde, die in een bepaald tijdvak toegang hebben of hadden tot deze bankkluizen.⁶² Bovendien is het opvragen van voorgaande gegevens slechts mogelijk indien er ernstige aanwijzingen bestaan dat de gepleegde misdrijven kunnen worden gestraft met een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf.⁶³
63. **Vordering** - In het geval dat de procureur des Konings deze gegevens wil opvragen, moet de procureur des Konings deze gegevens vorderen door middel van een schriftelijke en met redenen omklede beslissing.⁶⁴ Hierbij moet de procureur des Konings nauwkeurig beschrijven welke inlichtingen hij vordert en in welke vorm deze aan hem moeten worden meegedeeld.⁶⁵
64. **Gerechtelijk onderzoek** - Indien er een gerechtelijk onderzoek werd ingesteld, kan de onderzoeksrechter deze gegevens opvragen bij de bank of een kredietinstelling, onder dezelfde vormvoorden en vormvoorschriften, als deze waaraan de procureur des Konings zich dient te houden.⁶⁶
65. **Weigering medewerkingsplicht** - De bank of kredietinstelling is verplicht om deze gegevens mee te delen, indien deze worden opgevraagd door de procureur des Konings of de onderzoeksrechter. Indien een persoon weigert om deze gegevens mee te delen, de gegevens niet meedeelt in werkelijke tijd of de gegevens niet meedeelt op het tijdstip dat werd opgenomen in de vordering, kan deze persoon worden gestraft met een geldboete van honderd tot 30.000 euro.
66. **Geheimhoudingsplicht** - Daarnaast is iedere persoon, die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, verplicht om deze

⁶¹ Art. 2, 1° Wet 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, BS 4 september 2002.

⁶² Art. 46quater, §1 Sv.

⁶³ *Ibid.*

⁶⁴ *Ibid.*, §4.

⁶⁵ *Ibid.*

⁶⁶ Art. 46quater Sv.

informatie geheim te houden. Indien een persoon deze geheimhoudingsplicht schendt, kan deze persoon hiervoor worden gestraft.⁶⁷

⁶⁷ *Ibid.*, §4.

Afdeling II. Beslag

Onderafdeling I. Klassiek beslag

67. **Klassiek beslag** – In deze onderafdeling zal het klassiek beslag geanalyseerd worden. De procureur des Konings, respectievelijk de onderzoeksrechter kunnen beslag leggen op de voorwerpen die de waarheid kunnen achterhalen en de zaken die kunnen worden verbeurdverklaard, waaronder zaken die het voorwerp van het misdrijf uitmaken of er uit voort komen en op de vermogensvoordelen die rechtstreeks uit het misdrijf zijn verkregen, op de goederen en waarden die in de plaats ervan zijn gesteld en op de inkomsten uit de belegde voordelen en op vermogensvoordelen die het resultaat zijn van het bijzonder onderzoek naar vermogensvoordelen.⁶⁸ In kader van het klassiek beslag kunnen elektronische gegevens op zich staand niet in beslag worden genomen, de materiële drager van deze gegevens kan wel in beslag worden genomen.⁶⁹
68. **Opsporingsonderzoek** - Het wetboek van strafvordering bepaalt dat dwang uitzonderlijk mogelijk is in het kader van het strafonderzoek.⁷⁰ Het recht van beslag van de procureur des Konings vormt een uitzondering op het principe dat het opsporingsonderzoek geen dwangmaatregelen toelaat. Vroeger kon de procureur des Konings slechts beslag leggen bij situaties van heterdaad. Nu kan de procureur des Konings ook beslag leggen buiten situaties van heterdaad.⁷¹
69. **Gerechtelijk onderzoek** - Indien er een gerechtelijk onderzoek werd ingesteld, is de onderzoeksrechter bevoegd tot de inbeslagneming. Geen enkele wets- of verdragsbepaling verplicht de onderzoeksrechter alle stukken bij een huiszoeking in beslag te nemen. De onderzoeksrechter moet enkel die stukken in beslag nemen, waarvan de onderzoeksrechter oordeelt dat de stukken kunnen bijdragen tot de waarheidsvinding.⁷²
70. **Politiediensten** - In de praktijk gebeurt het niet vaak dat de procureur des Konings of de onderzoeksrechter persoonlijk een inbeslagneming verricht. Het materiële werk wordt doorgaans door de politiediensten uitgevoerd. In geval van heterdaad hebben officieren van gerechtelijke politie, hulpofficieren van de procureur des Konings, een eigen bevoegdheid tot inbeslagneming, die verbonden is met het huiszoekingsrecht in de woning van de verdachte. Daarnaast kan de onderzoeksrechter opdracht tot huiszoekingen en

⁶⁸ Art. 35 Sw.; Art. 42 Sw.; Art. 43quater Sw.; DESTERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017, 1-62, nr. 24-30.; ROYER, S., *Strafrechtelijk beslag: digiproof en (mult)functioneel*, die Keure, 2020, 39-140, nr. 40-56.

⁶⁹ INCALZA, T., 'Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming', *Jura Falc.* 2011/2, (329) 329-383, nr. 358-360.; ROYER, S., *Strafrechtelijk beslag: digiproof en (mult)functioneel*, die Keure, 2020, 39-140, nr. 40-56.

⁷⁰ Art. 28bis, §3 Sv.; ROYER, S., *Strafrechtelijk beslag: digiproof en (mult)functioneel*, die Keure, 2020, 39-140, nr. 40-56.

⁷¹ Art. 28bis, §3 Sv.; DESTERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017, 1-62, nr. 24-30.

⁷² DESTERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017, 1-62, nr. 24-30.; ROYER, S., *Strafrechtelijk beslag: digiproof en (mult)functioneel*, die Keure, 2020, 39-140, nr. 40-56.

inbeslagneming geven aan een officier van gerechtelijke politie van zijn arrondissement of van het arrondissement waar de handelingen moeten plaatsvinden.⁷³

71. **Vaststellingen andere misdrijven** - Indien speurders tijdens een regelmatig bevonden huiszoeking vaststellingen doen over andere misdrijven, dan die waarvoor het gerechtelijk onderzoek loopt en tot inbeslagname overgaan, is dit volgens het Hof van Cassatie wettig.⁷⁴

⁷³ Art. 89bis Sv.; DESTERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017, 1-62, nr. 24-30.; ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020, 39-140, nr. 40-56.

⁷⁴ ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020, 39-140, nr. 47.; Cass. 29 april 2009, AR P090578F.

Onderafdeling II. Databeslag

72. **Beslag elektronische gegevens** - In deze afdeling zal het databeslag besproken worden. In principe kan door middel van het klassiek beslag de materiële drager, waarop de data zich bevindt, in beslag worden genomen. Indien de inbeslagname van de materiële drager niet wenselijk is, kan de data worden gekopieerd op dragers.⁷⁵
73. **Drager** - De data die in beslag kan worden genomen, dit wil zeggen gekopieerd, zijn de gegevens die nuttig zijn voor dezelfde doeleinden als de inbeslagneming of de gegevens die noodzakelijk zijn om deze te kunnen verstaan, bijvoorbeeld computerprogramma's. deze gegevens worden gekopieerd op een drager die toebehoort aan de overheid. Indien er een situatie van hoogdringendheid bestaat, kan gebruik worden gemaakt van dragers die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.⁷⁶
74. **Opsporingsonderzoek** - In het kader van een strafrechtelijk onderzoek kan de politie toegang nemen tot een informaticasysteem.⁷⁷ Echter heeft de politie de toestemming nodig van de procureur des Konings voor het opheffen van het betrokken informaticasysteem of voor het inzetten van technische middelen om de daarin opgeslagen gegevens te ontcijferen.⁷⁸ In het kader van databeslag, kunnen de politie en de procureur des Konings tijdens het opsporingsonderzoek uitsluitend toegang nemen tot de gegevens die zijn opgeslagen op het toestel.⁷⁹ Aangezien de politie of de procureur des Konings enkel toegang kan nemen tot de gegevens die werden opgeslagen op het toestel, moet de netwerkverbinding worden uitgeschakeld voordat de politie of de procureur des Konings toegang neemt tot de gegevens die zich op het toestel bevinden. In de wetgeving werden geen voorwaarden naar de ernst van het misdrijf of een proportionaliteitstoetsing opgenomen.⁸⁰
75. **Gegevens ontoegankelijk maken** - Indien de gegevens het voorwerp van het misdrijf vormen of voortkomen uit het misdrijf, kan de procureurs des Konings deze ontoegankelijk laten maken, door gebruik van alle passende technische middelen.⁸¹ Indien

⁷⁵ DESTERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017, 1-62, nr. 52-54.; ROYER, S. en CONINGS, C., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken', *NC 2017/4*, (311) 311-338, nr. 74-98.; ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020, 39-140, nr. 105-122.

⁷⁶ INCALZA, T., 'Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming', *Jura Falc.* 2011/2, (329) 329-383, nr. 360-365.; ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020, 39-140, nr. 105-122.

⁷⁷ Art. 39bis, §1 Sv.; ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020, 39-140, nr. 105-122.

⁷⁸ Art. 39bis, §5 Sv.

⁷⁹ VAN DE HEYNING, C., 'Het gebruik van communicatiegegevens in strafzaken: hoe het Hof van Justitie het Belgische strafrecht hertekent', *T.Strafr.* 2025/2, (66) 66-79, nr. 38.; ROYER, S. en CONINGS, C., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken', *NC 2017/4*, (311) 311-338, nr. 74-98.; ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020, 39-140, nr. 105-122.

⁸⁰ Art. 36bis, §1 Sv.

⁸¹ DESTERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017, 1-62, nr. 52-54.; ROYER, S. en CONINGS, C., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken', *NC 2017/4*, (311) 311-338, nr. 74-98.; ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020, 39-140, nr. 105-122.

inbeslagneming van de dragers of kopieën van de data niet mogelijk is om technische redenen of wegens de omvang van de gegevens, worden de passende technische middelen aangewend om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.⁸²

76. **Vertrouwelijk** - De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen en ze ter griffie te bewaren.⁸³
77. **Gerechtelijk onderzoek** - In tegenstelling tot de procureur des Konings, kan de onderzoeksrechter zich wel de toegang verschaffen tot de gegevens die niet reeds zijn opgeslagen op het moment van het beslag. Echter kan de onderzoeksrechter enkel een dergelijke zoeking van het informatica- en communicatiesysteem bevelen, indien deze noodzakelijk is om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking, indien andere maatregelen disproportioneel zouden zijn of als er een risico bestaat dat zonder deze zoeking bewijsmateriaal verloren gaat.⁸⁴
78. **Databeslag informatie zoeking** - In het geval dat door middel van de zoeking in het informatica- en communicatiesysteem in de betrokken informaticasystemen opgeslagen gegevens aangetroffen worden die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.⁸⁵
79. **Landeck-arrest** - In het Landeck-arrest oordeelde het Hof van Justitie dat toegang tot communicatiegegevens steeds een grote impact heeft op het privéleven en de bescherming van persoonsgegevens, onafhankelijk ervan of de vervolgende autoriteiten en justitie hier zelf toegang toe kunnen nemen zoals bij een databeslag dan wel of ze hier een derde voor nodig hebben zoals bij het opvragen van metagegevens van elektronische communicatie.⁸⁶

⁸² DETERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017, 1-62, nr. 52-54.; ROYER, S. en CONINGS, C., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken', NC 2017/4, (311) 311-338, nr. 74-98

⁸³ DETERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017, 1-62, nr. 52-54.; ROYER, S. en CONINGS, C., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken', NC 2017/4, (311) 311-338, nr. 74-98.; ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020, 39-140, nr. 105-122.

⁸⁴ *Supra.* nr. 93 e.v.

⁸⁵ Art. 39bis, §4 en 6 Sv.

⁸⁶ HvJ 4 oktober 2024, C-548/21, ECLI:EU:C:2024:830.; VAN DE HEYNING, C., 'Het gebruik van communicatiegegevens in strafzaken: hoe het Hof van Justitie het Belgische strafrecht hertekent', *T.Strafr.* 2025/2, (66) 66-79, nr. 42.

Afdeling III. DNA-onderzoek

Onderafdeling I. In het kader van het opsporingsonderzoek

80. **Toestemming betrokkene** – Vooreerst zal er nader worden ingegaan op het DNA-onderzoek. Dit onderzoek kan plaatsvinden tijdens het opsporingsonderzoek, onder leiding van de procureur des Koning, mits er een geldige toestemming wordt verkregen van de betrokkene.⁸⁷ De betrokkene kan slechts toestemming verlenen, indien hij ouder is dan zestien jaar. In dit geval moet de toestemming schriftelijk en op een geïnformeerde wijze worden gegeven, voorafgaand aan de afname van het DNA-staal.⁸⁸ Daarnaast moet er sprake zijn van aanwijzingen van schuld, bij het plegen van de feiten die het voorwerp zijn van het opsporingsonderzoek of gelijkaardige feiten. Hierbij moet onder gelijkaardige feiten worden verstaan: feiten die op dezelfde manier worden gekwalificeerd als het misdrijf waarvan de betrokkene beschuldigd wordt, of een aanverwante kwalificatie.⁸⁹ Indien de toestemming op een geldige wijze werd verleend, kan de procureur des Konings de afname van een referentiestaal bevelen.⁹⁰
81. **Toestemming andere persoon** – Bovendien kan de procureur des Konings van een andere persoon, dan de verdachte een DNA-staal afnemen. Dit mag uitsluiten gebeuren met de uitdrukkelijke toestemming van deze persoon. Hierbij dient net zoals bij de toestemming van de verdachte, de toestemming schriftelijk, voorafgaand en op een geïnformeerde wijze te worden verleend.⁹¹
82. **Slachtoffer** – Tevens kan de procureur des Konings een DNA-onderzoek doen uitvoeren op het lichaam van het slachtoffer, in gevallen van aanranding van de eerbaarheid of verkrachting. Evenals in bovenvermelde situaties, is hierbij een geldige toestemming van het slachtoffer vereist.⁹²

⁸⁷ Artikel 44sexies Sv.; BAILLIEUX, A., *Afstand van recht in de strafprocedure: Zelfbeschikking bij een traditionele afhandeling van een strafprocedure*, Intersentia, 2019, 143-364, nr. 195.

⁸⁸ BAILLIEUX, A., *Afstand van recht in de strafprocedure: Zelfbeschikking bij een traditionele afhandeling van een strafprocedure*, Intersentia, 2019, 143-364, nr. 196.

⁸⁹ Wetsontwerp houdende wijziging van het Wetboek van Strafvordering en van de wet van 22 maart 1999 betreffende de identificatieprocedure via DNA-onderzoek in strafzaken, KAMER, 2010-2011, 26 mei 2011, nr. 53-1504/001, 15.

⁹⁰ HERBOTS, P. en DRIESSEN, M., 'DNA-wet aangepast aan wetenschappelijke vooruitgang', *Juristenkrant* 2024/489, (3) 3-4.; LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (De onderzoekshandelingen binnen het opsporingsonderzoek): DNA-onderzoek*, Wolters Kluwer, 2023, 133-134, nr. 213-214.

⁹¹ BAILLIEUX, A., *Afstand van recht in de strafprocedure: Zelfbeschikking bij een traditionele afhandeling van een strafprocedure*, Intersentia, 2019, 143-364, nr. 197.

⁹² *Supra*, nr. 80-81.; LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (De onderzoekshandelingen binnen het opsporingsonderzoek): DNA-onderzoek*, Wolters Kluwer, 2023, 133-134, nr. 213-214.

Onderafdeling II. In het kader van het gerechtelijk onderzoek

83. **Geen toestemming** - Wanneer een DNA-onderzoek wordt uitgevoerd, zonder de toestemming van de betrokken, zal dit plaatsvinden onder leiding van de onderzoeksrechter, in het kader van een gerechtelijk onderzoek.⁹³ Zodoende kan het DNA-onderzoek in dit geval, worden beschouwd als een dwangmaatregel, die de individuele rechten en vrijheden van de betrokkene kan schenden.⁹⁴ Aangezien deze onderzoekshandeling ingrijpend is, moeten er strikte voorwaarden in acht worden genomen, voordat het onderzoek kan worden uitgevoerd.⁹⁵
84. **Dwang** – Opdat het mogelijk is om dwang te gebruiken door middel van een DNA-onderzoek, moet er een misdrijf zijn gepleegd, dat bestraft wordt met een hogere strafmaat. Wanneer er voor het misdrijf slechts werd voorzien in een minder zware strafmaat, zal het DNA-onderzoek in principe niet kunnen worden uitgevoerd zonder toestemming van de betrokkene.⁹⁶ Ter illustratie: de onderzoeksrechter kan bevelen een referentiestaal onder dwang af te nemen, van een persoon tegen wie er aanwijzingen van schuld bestaan bij het plegen van feiten die hem aanhangig zijn, indien deze feiten strafbaar zijn met een maximumstraf van vijf jaar gevangenisstraf of met een zwaardere straf. Indien het gepleegde misdrijf bestraft wordt met een gevangenisstraf, die minder dan vijf jaar bedraagt, zal de onderzoeksrechter de niet kunnen bevelen, om een referentiestaal onder dwang af te nemen.⁹⁷ In dit geval moet de onderzoeksrechter de betrokkene persoonlijk horen, voordat het referentiestaal wordt afgenomen.⁹⁸
85. **Modaliteiten** – Indien de onderzoeksrechter beveelt om een referentiestaal onder dwang af te nemen, moet de onderzoeksrechter een met redenen omklede beslissing meedelen aan de procureur des Konings. Hierbij moet de onderzoeksrechter een aantal zaken verplicht vermelden, waaronder de noodzaak om dwang te gebruiken.⁹⁹
86. **Andere personen** – Bovendien kan een DNA-onderzoek worden uitgevoerd bij een andere persoon dan de verdachte, mits deze persoon een directe band heeft met het gerechtelijk onderzoek. Daarnaast moet het gepleegde feit strafbaar zijn met een maximumstraf van

⁹³ LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (De onderzoekshandelingen binnen het opsporingsonderzoek): DNA-onderzoek*, Wolters Kluwer, 2023, 133-134, nr. 213.

⁹⁴ MORANDINI, M., HUGUES, S. en HAUSMAN, J., 'La loi ADN en pleine mutation: entre révolution spontanée et altération des droits humains?', *AJT* 2025/5, (89) 89-99.; BAILLEUX, A., 'Grootschalig DNA-onderzoek: heiligt de efficiënte strafprocedure de opoffering van de grondrechten van het individu?', *NC* 2013/44, (269) 269-285, nr. 1.

⁹⁵ BAILLEUX, A., 'Grootschalig DNA-onderzoek: heiligt de efficiënte strafprocedure de opoffering van de grondrechten van het individu?', *NC* 2013/44, (269) 269-285, nr. 1.

⁹⁶ DELBROUCK, I., *Aanranding van de eerbaarheid en verkrachting: Enige aspecten van strafprocesrecht*, die Keure, 2015, 129-131.

⁹⁷ Art. 90undecies Sv.; LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (Het gerechtelijk onderzoek): De onderzoeksdelicten binnen het gerechtelijk onderzoek*, Wolters Kluwer, 2023, 162-174, nr. 284.

⁹⁸ BAILLEUX, A., *Afstand van recht in de strafprocedure: Zelfbeschikking bij een traditionele afhandeling van een strafprocedure*, Intersentia, 2019, 143-364, nr. 198-199.

⁹⁹ Art. 90undecies, §1, 3° Sv.; LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (Het gerechtelijk onderzoek): De onderzoeksdelicten binnen het gerechtelijk onderzoek*, Wolters Kluwer, 2023, 162-174, nr. 288.

vijf jaar gevangenisstraf of een zwaardere straf.¹⁰⁰ Verder moet er een noodzaak bestaan om de dwangmaatregel uit te voeren.¹⁰¹

87. **Slachtoffer** - Gelijkaardig met het opsporingsonderzoek, kan de onderzoeksrechter een referentiestaal afnemen bij een persoon die het slachtoffer werd van aanranding van de eerbaarheid of verkrachting.¹⁰² Het slachtoffer moet zijn toestemming uitdrukkelijk, schriftelijk, geïnformeerd en voorafgaand aan de afname van het referentiestaal verlenen.¹⁰³
88. **Minderjarige** – In tegenstelling tot de procureur des Konings, is het voor de onderzoeksrechter mogelijk om een referentiestaal te laten afnemen bij een minderjarige persoon. Wanneer er een referentiestaal wordt afgenomen in het kader van het gerechtelijk onderzoek bij een minderjarige, moet deze persoon zich laten bijstaan door zijn ouders, advocaat of een andere persoon die de meerderjarigheid bereikt heeft.¹⁰⁴

¹⁰⁰ Art. 90duodecies Sv.; Art. 90undecies Sv.; LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (Het gerechtelijk onderzoek): De onderzoeksdaden binnen het gerechtelijk onderzoek*, Wolters Kluwer, 2023, 162-174, nr. 286.; BAILLIEUX, A., *Afstand van recht in de strafprocedure: Zelfbeschikking bij een traditionele afhandeling van een strafprocedure*, Intersentia, 2019, 143-364, nr. 201.

¹⁰¹ Art. 90duodecies, §1, 3° Sv.

¹⁰² *Supra.* nr. 82.

¹⁰³ Art. 90undecies Sv.; LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (Het gerechtelijk onderzoek): De onderzoeksdaden binnen het gerechtelijk onderzoek*, Wolters Kluwer, 2023, 162-174, nr. 286.

¹⁰⁴ *Ibid.*, nr. 285.

Afdeling IV. Huiszoeking

Onderafdeling I. In het kader van het opsporingsonderzoek

89. **Huiszoeking met toestemming** – De volgende onderzoekshandeling die zal besproken worden, is de huiszoeking.¹⁰⁵ Een huiszoeking kan principieel steeds met toestemming van de betrokkene gebeuren, in welk geval er geen bevel van de onderzoeksrechter vereist is. Daarentegen mag de huiszoeking met toestemming uitsluitend worden uitgevoerd, wanneer er feiten of omstandigheden voorhanden zijn, die wijzen op het bestaan van een misdrijf.¹⁰⁶ Daarnaast moet de toestemming schriftelijk worden verleend, voorafgaand aan de start van de huiszoeking en moet deze toestemming geïnformeerd zijn. Hetgeen betekent dat de betrokkene volledig op de hoogte moet zijn van de aard en de reikwijdte van de huiszoeking.¹⁰⁷
90. **Zonder toestemming** – Desalniettemin bestaan er een aantal situaties, waarbij de procureur des Konings bevoegd is om, zonder een bevel of geldige toestemming, een huiszoeking uit te voeren. Dit is onder andere het geval bij ontdekking op heterdaad.¹⁰⁸ Daarnaast kan de procureurs des Konings een huiszoeking laten uitvoeren, zonder een bevel of toestemming, indien er om hulp wordt geroepen vanuit de woning bij terrorismemisdrijven in het kader van de drugwet.¹⁰⁹ In principe moet de procureur des Konings, in alle andere gevallen, eerst een toelating verkrijgen van de onderzoeksrechter.¹¹⁰
91. **Uitvoering** – Verder kan de huiszoeking op heterdaad slechts worden uitgevoerd, zolang de heterdaadsituatie bestaat.¹¹¹ Voorts kan de huiszoeking zowel overdag, als 's nachts worden uitgevoerd.¹¹²

¹⁰⁵ CUYKENS, S., 'Les limites de l'ingérence publique dans le domicile', *Rev.trim.D.H.* 2023/135, (803) 803-825.; GDNEDASJ, S., 'Visatie: artikel 15 Grondwet biedt meer bescherming dan EVRM', *Fisc.Act.* 2018/30, (10) 10-11.

¹⁰⁶ LINERS, A., VANDERHEYDEN, K., VAN VOLSEM, F. en DE WOLF, T. *Zakboekje strafprocesrecht: (De onderzoekshandelingen binnen het opsporingsonderzoek) De huiszoeking*, Wolters Kluwer, 2023, 101-111, nr. 167.

¹⁰⁷ *Ibid.*, nr. 168.

¹⁰⁸ *Ibid.*, nr. 158.

¹⁰⁹ YPERMAN, W., 'De bestrijding van terrorisme en strafprocesrecht: vele kleintjes maken een grote', *T.Strafr.* 2019/1, (8) 8-18.; LINERS, A., VANDERHEYDEN, K., VAN VOLSEM, F. en DE WOLF, T. *Zakboekje strafprocesrecht: (De onderzoekshandelingen binnen het opsporingsonderzoek) De huiszoeking*, Wolters Kluwer, 2023, 101-111, nr. 159.; Cass. 9 november 2021, P.21.1370.N.; ARNOU, L., 'Zoeking op grond van artikel 6bis Drugwet en huiszoeking bij heterdaad zijn twee verschillende zaken', *NC* 2021/1, (34) 34-36.; VAN VOLSEM, F., 'De huiszoeking op grond van artikel 6bis, derde lid Drugwet', *RABG* 2022/18, (1322) 1322-1327.

¹¹⁰ Art. 36, 87, 88 en 89bis Sv.

¹¹¹ DE COSTER, T., 'De huiszoeking bij heterdaad en in toepassing van artikel 6bis, lid 3 van de wet van 24 februari 1921: een bron van blijvende cassatierechtspraak', *T. Strafr.* 2022/6, (325) 325-333.

¹¹² LINERS, A., VANDERHEYDEN, K., VAN VOLSEM, F. en DE WOLF, T. *Zakboekje strafprocesrecht: (De onderzoekshandelingen binnen het opsporingsonderzoek) De huiszoeking*, Wolters Kluwer, 2023, 101-111, nr. 161.

Onderafdeling II. In het kader van het gerechtelijk onderzoek

92. **Huiszoeking onder dwang** – Voorts kan de onderzoeksrechter een huiszoeking onder dwang laten uitvoeren, wanneer de onderzoeksrechter oordeelt dat de huiszoeking noodzakelijk is.¹¹³ In dat geval is het voldoende dat er ter plaatste stukken of voorwerpen zijn, die kunnen bijdragen aan het vinden van de waarheid.¹¹⁴ Het huiszoekingsbevel moet bovendien schriftelijk worden opgesteld en voor de aanvang van de huiszoeking worden afgeleverd. Verder moet de huiszoeking een aantal verplichte vermeldingen bevatten.¹¹⁵ In principe is het niet mogelijk voor de onderzoeksrechter, om een huiszoeking te verrichten tussen eenentwintig en vijf uur, behoudens uitzonderingen.¹¹⁶

¹¹³ Art. 36, 87, 88 en 89bis Sv.; LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (Het gerechtelijk onderzoek): De onderzoeksdadens binnen het gerechtelijk onderzoek*, Wolters Kluwer, 2023, 162-174, nr. 279.

¹¹⁴ LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (Het gerechtelijk onderzoek): De onderzoeksdadens binnen het gerechtelijk onderzoek*, Wolters Kluwer, 2023, 162-174, nr. 279.

¹¹⁵ *Ibid.*, nr. 280.

¹¹⁶ *Ibid.*, nr. 281.

Afdeling V. Doorzoeking communicatie en informaticasystemen

93. **Doorzoeking communicatie en informaticasysteem** – Een andere onderzoekshandeling die zal worden besproken, is het onderscheppen, kennisnemen, doorzoeken en opnemen van niet voor publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan.¹¹⁷ Deze handeling kan enkel worden bevolen in uitzonderlijke gevallen. Dit is het geval wanneer het onderzoek deze handeling vereist. Daarnaast kan de onderzoekshandeling uitsluitend worden uitgevoerd bij bepaalde strafbare feiten die werden opgenomen in de wet.¹¹⁸
94. **Ernstige feiten** - De feiten, waarbij het mogelijk is om een zoeking te bevelen, zijn voornamelijk ernstige feiten. Bovendien bevestigt de memorie van toelichting bij dataretentiewet III dat de feiten opgenomen in artikel 90 ter, §2-4 Sv., over het algemeen als ernstig worden beschouwd.¹¹⁹ Deze feiten omvatten namelijk strafbare feiten, die verband houden met zware criminaliteit tegen personen, bijvoorbeeld aanranding van minderjarigen en volwassenen en verkrachting, ontvoering en verberging van minderjarigen, belaging via elektronische communicatie. Daarnaast zijn het feiten die verband houden met de georganiseerde criminaliteit, bijvoorbeeld criminele organisatie, mensenhandel, aanzetten tot ontucht, tewerkstelling met het oog op ontucht, pooierschap en het houden van een bordeel en de aanbidding en verkoop van kinderpornografie. Daarboven hebben de feiten betrekking op andere bijzonder ernstige inbreuken die specifieke methoden voor het vergaren van informatie in beweging zetten, bijvoorbeeld inbreuken tegen de vertrouwelijkheid, de integriteit en de beschikbaarheid van informaticasystemen en de door die systemen opgeslagen, verwerkte of doorgegeven gegevens, diefstal en afpersing van nucleair materiaal en fysieke beveiliging van nucleair materiaal.¹²⁰
95. **Drempel proportionaliteit** - De lijst van strafbare feiten bedoeld in artikel 90ter, § 2 tot 4 wordt bovendien in het wetboek van strafvordering meerdere keren gebruikt als drempel voor de proportionaliteitsvereiste, voor wat betreft de opsporingsmethoden die het meest ingrijpend zijn in de persoonlijke levenssfeer.¹²¹ Dit is het geval voor: de proactieve recherche¹²², het blokkeren van banktegoeden¹²³, de inijkoperatie¹²⁴, de infiltratie¹²⁵, de observatie met gebruik van technische middelen om zicht te krijgen in de woning van een advocaat of een arts, de volledige anonimiteit van getuigen¹²⁶, de onderschepping en kennisname van communicatie die niet toegankelijk is voor het publiek

¹¹⁷ ROYER, S, 'Inlichtingen over toegang tot informaticasysteem', *T.Strafr.* 2024/4, (277) 277-278.

¹¹⁸ Art. 90ter, §2-4 Sv.

¹¹⁹ 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. 55-2572/001. 55-56.

¹²⁰ *Ibid.*

¹²¹ *Ibid.*

¹²² Art. 28bis, §2 Sv.

¹²³ Art. 46quater, §2, tweede lid Sv.

¹²⁴ Art. 46quinquies Sv.; Art. 89ter Sv.

¹²⁵ Art. 47octies Sv.

¹²⁶ Art. 86bis Sv.

en de geheime zoeking in een informaticasysteem¹²⁷, het toekennen van bijzondere beschermingsmaatregelen aan bedreigde getuigen¹²⁸ en het toekennen van bijzondere beschermingsmaatregelen aan bedreigde personen die een openbaar ambt uitoefenen¹²⁹.

96. **Bij meest ingrijpende methoden** - Voor het toepassen van de meest ingrijpende opsporingsmethoden, wordt dus telkens teruggegrepen naar de lijst van strafbare feiten opgesomd in artikel 90ter, §2 tot 4 Sv..¹³⁰
97. **Ernstige aanwijzingen** - Bovendien moeten er ernstige aanwijzingen bestaan voor het bestaan van dit strafbare feit. In dit kader komt de subsidiariteit van de onderzoekshandeling naar voren, aangezien de maatregel enkel kan worden bevolen, wanneer de overige middelen van het onderzoek niet volstaan om de waarheid aan de dag te brengen.¹³¹ Dit betekent dat wanneer er alternatieve, minder ingrijpende onderzoekshandelingen beschikbaar zijn, deze eerst moeten worden toegepast. Enkel wanneer deze onderzoekshandelingen niet het gewenste resultaat opleveren, kan de meer ingrijpende onderzoekshandeling toegepast worden.¹³²
98. **Heimelijkheid** - Vroeger werd deze onderzoekshandeling gekwalificeerd als 'tappen' of 'telefoontap'.¹³³ In tegenstelling tot voorheen, werd de onderzoekshandeling uitgebreid, en omvat deze momenteel het af luisteren van communicatie en het heimelijk doorzoeken van een informatica- of communicatiesysteem.¹³⁴
99. **Opsporingsonderzoek** - De procureur des Konings kan deze maatregel bevelen wanneer er een geldige toestemming is van de betrokkene. Daarnaast kan de procureur des Konings de maatregel bevelen bij een ontdekking op heterdaad van een gijzeling, een wederrechtelijke vrijheidsbeneming, afpersing, bij het plegen van een terroristisch misdrijf of wanneer er gedreigd wordt met het plegen van een terroristisch misdrijf.¹³⁵ Voorts kan de maatregel uitsluitend worden opgelegd binnen een termijn van 72 uur na de ontdekking van het feit. Dit kan slechts tot 72 uur na de ontdekking van dit feit. Hieruit volgt dat de procureur des Konings in alle andere gevallen, niet over de bevoegdheid beschikt om deze maatregel te bevelen.¹³⁶

¹²⁷ Art. 90ter Sv.

¹²⁸ Art. 104, §2 Sv.

¹²⁹ Art. 111quater, §1, tweede lid Sv.

¹³⁰ 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. 55-2572/001. 55-56.

¹³¹ BERKMOES, H., *Interceptie van privécommunicatie en gegevens van een informaticasysteem*, Wolters Kluwer, 2022, 263.

¹³² Art. 90 ter Sv.

¹³³ BERKMOES, H., *Interceptie van privécommunicatie en gegevens van een informaticasysteem*, Wolters Kluwer, 2022, 229-292

¹³⁴ *Ibid.*, 259.

¹³⁵ LINERS, A., VANDERHEIDEN, K., VAN VOLSEM, F. en DE WOLF, T., *Zakboekje strafprocesrecht: (Het gerechtelijk onderzoek): De onderzoeksdaaden binnen het gerechtelijk onderzoek*, Wolters Kluwer, 2023, 162-174, nr. 297.

¹³⁶ VAN DE HEYNING, C., 'Ernst van het misdrijf is een onvoldoende reden om procedurele garanties voor de zoeking in informaticasystemen te omzeilen', *T.Strafr.* 2017/6, (365) 365-367.; BERKMOES, H., *Interceptie van privécommunicatie en gegevens van een informaticasysteem*, Wolters Kluwer, 2022, 229-292.

100. **Gerechtelijk onderzoek** – Bijgevolg is de onderzoeksrechter, buiten de voornoemde situaties¹³⁷, exclusief bevoegd om de onderzoekshandeling te bevelen.¹³⁸ Opdat de onderzoeksrechter deze onderzoekshandeling kan bevelen, moet de onderzoeksrechter zijn gevorderd voor de feiten, waarvoor hij de onderzoekshandeling beveelt.¹³⁹
101. **Uitzonderlijke gevallen** – Bovendien kan de onderzoekshandeling uitsluitend worden bevolen in uitzonderlijke gevallen. Zo moet de maatregel noodzakelijk zijn voor het onderzoek. Daarnaast moeten er ernstige aanwijzingen bestaan voor een feit waarvoor de maatregel wordt bevolen en er bestaan geen andere, minder ingrijpende maatregelen, om de waarheid te achterhalen.¹⁴⁰

¹³⁷ *Supra* nr. 99.

¹³⁸ ROYER, S., 'Iedereen wordt geacht ... de toegangscode van zijn gsm te kennen', *T.Strafr.* 2023/2, (114) 114.

¹³⁹ TERSAGO, P. 'Doorzoeken van smartphones en computers: Vrijwillige afgifte vereist geen mededeling zwijgrecht of bijstand van een advocaat', *Juristenkrant* 2023/468, (10) 10-11.

¹⁴⁰ BERKMOES, H., *Interceptie van privécommunicatie en gegevens van een informaticasysteem*, Wolters Kluwer, 2022, 266.

Afdeling VI Opsporen van elektronische communicatie

102. **Opsporen elektronische communicatie** - Een andere onderzoekshandeling is het doen opsporen van elektronische communicatie of het lokaliseren van de oorsprong of de bestemming van elektronische communicatie.¹⁴¹
103. **Opsporingsonderzoek** - Tijdens het opsporingsonderzoek, heeft de procureur des Konings de mogelijkheid om de houder van een IMEI-nummer, oproepnummer, e-mailadres of IP-adres te identificeren, evenals om te achterhalen welke oproepnummers aan een bepaalde smartphone zijn verbonden.¹⁴² In het geval dat de procureur des Konings de elektronische communicatie wil laten registreren, kan de procureur des Konings hiertoe een mini-instructie instellen of de onderzoeksrechter vorderen. Bij bepaalde misdrijven, wanneer er een heterdaadsituatie is, kan de procureur des Konings wel de elektronische communicatie doen opvragen.¹⁴³
104. **Gerechtelijk onderzoek** – Voorts is de onderzoeksrechter uitsluitend bevoegd om lijsten op te vragen van elektronische communicatie. Daarnaast kan ook uitsluitend de onderzoeksrechter een zendmastbepaling bevelen en de inhoud van de communicatie opvragen. In dat geval is de onderzoeksrechter verplicht om aan de operator, de redenen mee te delen, waardoor hij oordeelt dat de onderzoekshandeling noodzakelijk is.¹⁴⁴
105. **Bevelschrift** – Bovendien kan de onderzoeksrechter deze onderzoekshandeling slechts bevelen, wanneer er ernstige aanwijzingen bestaan dat de strafbare feiten een hoofdgevangenisstraf van één jaar of een zwaardere straf tot gevolg kunnen hebben. Daarnaast moet de onderzoekshandeling noodzakelijk zijn om de waarheid te kunnen achterhalen. In dat geval moet de onderzoeksrechter in een met redenen omkleed bevelschrift, de feitelijke omstandigheden van de zaak uiteenzetten, die deze maatregel rechtvaardigen. Tevens dient de onderzoeksrechter hierbij de proportionaliteit van de maatregel te verantwoorden, met inachtneming van de persoonlijke levenssfeer. Ook moet de onderzoeksrechter de subsidiariteit ten opzichte, van andere minder ingrijpende maatregelen aantonen.¹⁴⁵ Bovendien mag de onderzoekshandeling slechts twee maanden duren, vanaf het bevelschrift.¹⁴⁶
106. **Noodzakelijkheid** – Daarnaast kan de onderzoeksrechter de zoeking in een informaticasysteem of een deel ervan, uitbreiden naar een informaticasysteem of een deel ervan dat zich op een andere plaats bevindt, dan daar waar de zoeking plaatsvindt. Ook hiervoor moeten strikte voorwaarden nageleefd worden. Zo moet het noodzakelijk zijn om de waarheid aan het licht te brengen. Voorts moeten andere maatregelen disproportioneel

¹⁴¹ ROYER, S., 'Verbod op anonieme belkaarten blijft overeind', *Juristenkrant* 2021/438, (2) 2-3.

¹⁴² DE SMET, B., *Registratie en lokalisatie van elektronische communicatie*, Wolters Kluwer, 2019, 1-61, nr. 43.

¹⁴³ *Ibid.*, nr. 44.

¹⁴⁴ DEPAEPE, H. en SEYEN, K., 'Opsporing en vervolging van misdrijven. Technische overdracht van gegevens', *NJW* 2022/454, (2) 2-9.

¹⁴⁵ Art. 88bis Sv.

¹⁴⁶ Art. 88bis Sv.; DE SMET, B., *Registratie en lokalisatie van elektronische communicatie*, Wolters Kluwer, 2019, 1-61, nr. 45.

zijn of moet er een risico bestaan dat er bewijselementen kunnen verloren gaan, zonder deze uitbreiding.¹⁴⁷

¹⁴⁷ Art. 88ter Sv.

Hoofdstuk III. Dataretentie

107. **Inleiding** - De dataretentiewetgeving bevat bepalingen omtrent de opslag van metadata door telecomoperatoren. In deze wet werden bijgevolg geen bepalingen opgenomen, die de aankoop van persoonsgegevens bij commerciële dataverzamelingsbedrijven en het gebruik ervan in het kader van het strafonderzoek regelen. Hoewel de dataretentiewet zich beperkt tot de metadata die door telecomoperatoren wordt opgeslagen, kan deze wetgeving toch van belang zijn voor het onderzoek, in het kader van deze masterproef. De gegevens die deze telecomoperatoren bewaren, zoals verkeersgegevens, locatiegegevens en identificatiegegevens zijn vergelijkbaar met de persoonsgegevens die bij commerciële dataverzamelingsbedrijven kunnen worden aangekocht. Zo kunnen verkeersgegevens en locatiegegevens als persoonsgegevens worden beschouwd, wanneer deze gegevens aan een specifiek individu kunnen worden gekoppeld.¹⁴⁸ Echter, de persoonsgegevens die kunnen worden aangekocht bij dataverzamelingsbedrijven, kunnen doorgaans in bepaalde gevallen, afhankelijk van de aard van de gegevens, nog ingrijpender en verregaander dan de gegevens die telecomoperatoren bewaren. Aangezien er bij de aankoop van persoonsgegevens bij dataverzamelingsbedrijven ook andere informatie, dan enkel verkeersgegevens, locatiegegevens of identificatiegegevens kan worden verkregen. Hierdoor zou het eventueel mogelijk zijn dat er nog meer informatie over het privéleven van een persoon wordt doorgegeven.
108. **Evolutie dataretentiewet** - In het verleden werden er verschillende dataretentiewetten uitgevaardigd, namelijk dataretentiewet I, dataretentiewet II en dataretentiewet III.¹⁴⁹ Deze wetten zijn omzettingen van richtlijnen van de Europese Unie. Deze dataretentiewetten stelde bepalingen vast omtrent de bewaring van data door telecomoperatoren van identificatie-, verkeers- en locatiegegevens van hun klanten. Het gebruik van deze gegevens, ook wel metadata genoemd, heeft tot gevolg dat er meer informatie ter beschikking is in het kader van het strafonderzoek.¹⁵⁰ Dit heeft tot gevolg dat er kan worden onderzocht, naar welke personen een bepaalde verdachte belt of berichten verstuurt. Bovendien kan er worden onderzocht welke internetsites de verdachte bezocht heeft.¹⁵¹ Daarnaast werd het mogelijk gemaakt om te bepalen wie er zich op een bepaald moment in de buurt van een plaats bevond, waar er een misdrijf werd gepleegd, door te analyseren met welke gsm-antenne er voor de laatste keer contact werd gemaakt.¹⁵² Echter werden twee van deze dataretentiewetten verworpen door het

¹⁴⁸ PANZAVOLTA, M., ROYER, S. en SEVERIJNS, H., 'Algemene dataretentie: ten minste houdbaar tot...?', *T. Strafr.* 2018/1, (3) 4, nr. 5.

¹⁴⁹ SCHRAM, F., *Handboek Privacy en Persoonsgegevens: Internationale teksten en hun neerslag in het Europese en Belgische recht*, Politeia, 2023, 322-353.

¹⁵⁰ PANZAVOLTA, M., ROYER, S. en SEVERIJNS, H., 'Algemene dataretentie: ten minste houdbaar tot...?', *T. Strafr.* 2018/1, (3) 3, nr. 1.

¹⁵¹ TERSAGO, P., 'Hergebruik van telecommunicatiegegevens in strafzaken: horen, zien en zwijgen?', *Juristenkrant* 2023/475, (4) 4.

¹⁵² HEYMANS, P. en HIROUX, H., 'Grondwettelijk Hof vernietigt wet op bijhouden van telefoondata: wat betekent dat voor jou? En voor politie en parket?', *VRT NEWS* 22 april 2021, <https://www.vrt.be/vrtnws/nl/2021/04/07/dataretentie/> (geraadpleegd op 26 juli 2025).

Grondwettelijk Hof, aangezien het Hof oordeelde dat deze wetten in strijd waren met bepaalde fundamentele rechten.¹⁵³

109. **Dataretentiewet I** – Dataretentiewet I verplichte telecomoperatoren, zoals Proximus, Telenet, Base... om identificatie-, verkeers- en locatiegegevens van al hun klanten twaalf maanden lang te bewaren. Zodoende dat deze gegevens konden worden opgevraagd in het kader van het strafonderzoek.¹⁵⁴ Het Grondwettelijk Hof oordeelde dat deze dataretentiewet in strijd is met de mensenrechten. Volgens het Hof werd het recht op privacy geschonden, aangezien de data op een algemene en ongedifferentieerde manier werd bewaard.¹⁵⁵ Immers werd de data van alle klanten over het hele Belgische grondgebied bewaard voor een termijn, die de noodzakelijke termijn overschreed.¹⁵⁶
110. **Dataretentiewet II** – Vervolgens werd dataretentiewet II aangenomen.¹⁵⁷ In vergelijking met de vorige dataretentiewet, voorzag deze wet wel in strikte waarborgen op de algemene en ongedifferentieerde bewaring.¹⁵⁸ Zo bepaalde deze wet dat wanneer er een misdrijf wordt gepleegd, dat bestraft wordt met een hogere strafmaat, er langer mag worden teruggegaan in de tijd om bepaalde gegevens op te vragen.¹⁵⁹ Evenals bij dataretentiewet I, oordeelde het Grondwettelijk Hof dat deze wet in strijd is met het recht op privacy, aangezien ook deze wet voorzag dat gegevens stelselmatig en continu werden bewaard¹⁶⁰
111. **Dataretentiewet III** – Nadien werd dataretentiewet III in 2022 aangenomen.¹⁶¹ In tegenstelling tot dataretentiewet I en II, verplichte dataretentiewet III telecomoperatoren tot een gedifferentieerde bewaring, in plaats van een ongedifferentieerde bewaring. Deze wet bepaalt dat telecomoperatoren uitsluitend data mogen bewaren van bepaalde personen of de data van personen in bepaalde gebieden. Zoals data van verdachten van misdrijven of van personen die zich bevinden in een gebied waar veel criminele feiten worden gepleegd.¹⁶² Ondanks het feit dat er op basis van deze wet nog steeds op grote schaal gegevens kunnen worden bewaard, oordeelde het Grondwettelijk Hof dat deze wet niet in strijd is met het recht van privacy. Aangezien er voldoende waarborgen werden

¹⁵³ PANZAVOLTA, M., ROYER, S. en SEVERIJNS, H., 'Algemene dataretentie: ten minste houdbaar tot...?', *T. Strafr.* 2018/1, (3) 6-8, nr. 9-13.

¹⁵⁴ Wet 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 juni 2005.; ROYER, S. en CAREEL, S., 'Houdbaarheidsdatum voor algemene dataretentie voor criminaliteitsbestrijding is verstreken', *Juristenkrant* 2020/416, (1) 1.

¹⁵⁵ GwH 11 juni 2015, 84/2015.

¹⁵⁶ CONINGS, C., 'Dataretentieplicht en privacy', *NJW* 2015, (911) 911-913.

¹⁵⁷ Wet 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016.

¹⁵⁸ PANZAVOLTA, M., ROYER, S. en SEVERIJNS, H., 'Algemene dataretentie: ten minste houdbaar tot...?', *T. Strafr.* 2018/1, (3) 8-10, nr. 14-17.

¹⁵⁹ ROYER, S. en CAREEL, S., 'Houdbaarheidsdatum voor algemene dataretentie voor criminaliteitsbestrijding is verstreken', *Juristenkrant* 2020/416, (1) 1.

¹⁶⁰ GwH 22 april 2021, 57/2021.; TERSAGO, P., 'Hergebruik van telecommunicatiegegevens in strafzaken: horen, zien en zwijgen?', *Juristenkrant* 2023/475, (4) 4.

¹⁶¹ 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.

¹⁶² VAN ROY, L. en ROYER, S., 'De nieuwe dataretentiewetgeving: over oude ketels en nieuwe soep', *NC* 2023/1, (1) 1-22.

ingevoerd, waaronder een gedifferentieerde bewaring.¹⁶³ Bovendien bepaalt deze wet specifiek welke data bewaard mag worden en wie bevoegd is om deze gegevens op te vragen. Desondanks stelde het Grondwettelijk Hof prejudiciële vragen aan het Europees Hof van Justitie met betrekking tot bepaalde aspecten van deze wet.¹⁶⁴

112. **Geen algemene ongedifferentieerde bewaring** – Op basis van een lezing van de vernietigingsarresten met betrekking tot dataretentiewet I en II kan geconcludeerd worden dat volgens het Grondwettelijk Hof, een ongedifferentieerde bewaring van gegevens en de mogelijkheid voor de bevoegde instanties om deze gegevens op te vragen, in strijd is met het recht op privacy. Aangezien hierdoor iedere persoon zou kunnen worden beschouwd als verdachte, dit zou ingaan tegen het vermoeden van onschuld.¹⁶⁵ Het vermoeden van onschuld is een algemeen beginsel in het Belgische strafrecht, dit houdt in dat iedere persoon onschuldig is, totdat het tegendeel is bewezen.¹⁶⁶
113. **Voldoende waarborgen** - Bovendien wordt door de uitspraak van het Grondwettelijk Hof met betrekking tot dataretentiewet III het belang van voldoende waarborgen aangetoond. Door het aanwezig zijn van voldoende waarborgen en te voorzien in een gedifferentieerde bewaring, oordeelde het Hof immers dat dataretentiewet niet in strijd is met het recht op privacy. Zo werd in deze wet bepaald welke data bewaard mag worden en wie bevoegd is om deze data op te vragen bij telecomoperatoren.

¹⁶³ GwH 26 september 2024, 97/2024.

¹⁶⁴ VANDENBRUWAENE, P., 'Dataretentie: de zoektocht naar een veilige haven', *RW* 2023/9, (323) 323-333.

¹⁶⁵ DUINSLAEGER, P., 'Het vermoeden van onschuld', *RW* 2017/17, (643) 643, 1.

¹⁶⁶ GwH 11 juni 2015, 84/2015.

Deel III: Fundamentele rechten

114. **Inleiding** – In het kader van deze masterproef zal onderzocht worden in hoeverre procedurele waarborgen de schending van fundamentele rechten, waaronder het gegevensbeschermingsrecht, die voortvloeit uit de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de overheid in het kader van het strafonderzoek, nog kunnen rechtvaardigen. Deze handeling, zou naargelang de aard van de informatie, eventueel individuele rechten en vrijheden van personen kunnen schenden. In dit deel zal volgende subonderzoeksvraag onderzocht worden: *'Welke privacy en fundamentele rechten kunnen eventueel worden geschonden door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek?'*. In dit deel zullen de fundamentele rechten geanalyseerd worden, in het volgende deel zullen de regels die de bescherming van persoonsgegevens waarborgen worden besproken.¹⁶⁷ Er zullen een aantal fundamentele rechten dieper geanalyseerd worden. Hierbij zullen het recht op een eerlijk proces, het recht op privacy, met inbegrip van het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens, het recht op gelijkheid en non-discriminatie en het recht op vrije meningsuiting worden besproken. Bovendien zal onderzocht worden aan welke voorwaarden moet worden voldaan, om een inmenging in een fundamenteel recht te rechtvaardigen. Indien er voldaan is aan deze voorwaarden, zal er bijgevolg een grotere grondrechtsbescherming bestaan. Later in deze masterproef zullen de redenen besproken worden, waarom de aankoop van persoonsgegevens bij dataverzamelingsbedrijven, de fundamentele rechten al dan niet kan schenden.¹⁶⁸
115. **Noodzakelijk, proportioneel en subsidiair** – Er bestaat een grotere grondrechtsbescherming wanneer de inbreuk op het fundamentele recht bij wet is vastgelegd, er een legitiem doel wordt nagestreefd en de inbreuk noodzakelijk, proportioneel en subsidiair is.¹⁶⁹ Ten eerste moet de inbreuk bij wet zijn vastgelegd. Dit betekent dat de inbreuk moet zijn vastgesteld in algemene regels. Bovendien moeten deze regels duidelijk zijn. Daarnaast moeten deze regels voldoende toegankelijk zijn voor de burger en de rechtsgevolgen van de wet moeten voorzienbaar zijn. Ten tweede moet er een bepaald legitiem doel nagestreefd worden. In bepaalde gevallen wordt dit legitiem doel opgenomen in het wetsartikel, waarin een bepaald mensenrecht wordt gewaarborgd.¹⁷⁰ Ten derde moet de inbreuk noodzakelijk zijn in een democratische samenleving.¹⁷¹ Ten laatste moet de inbreuk proportioneel en subsidiair zijn. Om proportioneel te zijn, mag de inmenging niet verder reiken dan nodig is om het doel te

¹⁶⁷ *Infra* nr. 156 e.v.

¹⁶⁸ *Infra* nr. 245 e.v.

¹⁶⁹ SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 2.

¹⁷⁰ Art. 8-11 Europees Verdrag voor de Rechten van de Mens 4 november 1950, BS 19 augustus 1955. (Hierna: EVRM)

¹⁷¹ *Ibid.*

bereiken. Daarnaast mogen er geen minder ingrijpende maatregelen bestaan om het hetzelfde doel te bereiken, om aan de voorwaarde van de subsidiariteit te voldoen.¹⁷²

¹⁷² SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het strafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 2.

Hoofdstuk I. Recht op een eerlijk proces

116. **Recht op een eerlijk proces** – Ten eerste zal het recht op een eerlijk proces geanalyseerd worden.¹⁷³ Het recht op een eerlijk proces wordt gewaarborgd door het Europees Verdrag voor de Rechten van de Mens.¹⁷⁴ In het EVRM wordt onder andere bepaald, dat bij het vaststellen van de burgerlijke rechten en verplichtingen of bij het bepalen van de gegrondheid van een tegen een persoon ingestelde strafvervolgning, eenieder het recht heeft op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn. Bovendien heeft eenieder het recht op een behandeling van zijn zaak, door een onafhankelijke en onpartijdige rechterlijke instantie.¹⁷⁵
117. **Beginselen recht op eerlijk proces** – Bovendien waarborgt het recht op een eerlijk proces diverse beginselen. Zo omvat het recht op een eerlijk proces het decisiëbeginsel. Volgens dit beginsel heeft de betrokkene het recht op een behandeling en beslissing binnen een redelijke termijn.¹⁷⁶ Daarnaast bestaat er het verdedigingsbeginsel, dit omvat het recht om te worden gehoord. Het onpartijdigheidsbeginsel daarentegen, houdt in dat de rechter op een onafhankelijke en onpartijdige manier uitspraak moet doen.¹⁷⁷ Voorts houdt het motiveringsbeginsel in, dat de uitspraak voldoende moet worden gemotiveerd.¹⁷⁸ Voorts bestaat er het beginsel van toegang tot de rechter, dit houdt in dat de betrokkene toegang moet hebben tot een rechter en een uitspraak in tweede aanleg moet kunnen verkrijgen, indien de betrokkene dat wenst. Daarnaast hebben personen het recht op bijstand van een advocaat.¹⁷⁹ Ook het openbaarheidsbeginsel moet worden nageleefd, dit heeft tot gevolg dat een betrokkene recht heeft om inzage te krijgen in alle stukken van de rechtspleging.¹⁸⁰ Eveneens heeft deze openbaarheid tot gevolg, dat de samenleving controle kan uitoefenen over het verloop van de rechtspleging.¹⁸¹ Bovendien heeft eenieder volgens het motiveringsbeginsel, recht op een motivering van de uitspraak. Daarnaast bestaat er ook nog het recht op wapengelijkheid, dit impliceert dat er een billijk en rechtvaardig evenwicht moet bestaan tussen de procespartijen.¹⁸²

¹⁷³ VAN DE HEYNING, C., 'Het Mensenrechtenhof weigert een uitzonderingsregime voor versleuteld bewijs in strafzaken', *T.Strafr.* 2024/1, (33) 33-40.

¹⁷⁴ Art. 6 EVRM; BERBUTO, S., THEVISSSEN, P. en MONVILLE, P., *Droits de la défense – L'article 6 de la Convention Européenne des Droits de l'Homme*, Wolters Kluwer, 2025, 1-33.

¹⁷⁵ Art. 6 EVRM

¹⁷⁶ HUYBRECHTS, L. en ROZIE, M., 'De rechten van de verdediging bij de behandeling ten gronde', *NC* 2008/2, (106) 109-111, nr. 18-29.

¹⁷⁷ VERNIMMEN, K., 'Verantwoordt de coronacrisis een speciale behandeling van in verdenking gestelden in voorlopige hechtenis?', *T. Strafr.* 2022/6, (315) 317.

¹⁷⁸ KUTY, F., 'Justice pénale et procès équitable', *O.C.* 2006/1, (994) 994-1003.

¹⁷⁹ VAN MOER, E., 'De rechten van verdediging in een efficiënt procesverloop', *T.Strafr.* 2024/4, (250) 250-253.; HUYBRECHTS, L. en ROZIE, M., 'De rechten van de verdediging bij de behandeling ten gronde', *NC* 2008/2, (106) 126.; PARREIN, F., 'Kroniek Hof van Cassatie – Rechtspraak publiek- en administratief recht 2022', *TBP* 2023/6, (367) 376-395, nr. 57.

¹⁸⁰ HUYBRECHTS, L. en ROZIE, M., 'De rechten van de verdediging bij de behandeling ten gronde', *NC* 2008/2, (106) 114, nr. 46.

¹⁸¹ *Ibid.*, 108-109, nr. 10-17.

¹⁸² Art. 6 EVRM; MASSCHELEIN, M., *Arbeidsgerechten en sociaal procesrecht: Beginselen die de grenzen van de rechter bepalen*, Wolters Kluwer, 2018, 285-310, nr. 616.; TUTS, P., 'Het aanvechten van internationale wapenleveringen voor de rechter: wanneer de Luikse metallo's de bui reeds voelden hangen', *TBP* 2024/1, (5) 5-28.; HUYBRECHTS, L. en ROZIE, M., 'De rechten van de verdediging bij de behandeling ten gronde', *NC* 2008/2, (106) 111-112, nr. 30-36.

118. **Onrechtmatig verkregen bewijs** - Bewijs kan als onrechtmatig worden beschouwd, indien het werd verkregen door de regels van het strafrecht te miskennen of wanneer het verkregen werd in strijd met het recht op privacy. Bovendien kan het bewijs onrechtmatig zijn, wanneer het werd verkregen door de regels van verdediging te miskennen of wanneer het recht op menselijke waardigheid hierdoor werd geschonden.¹⁸³
119. **Antigoon-leer** – Ten gevolge van de Antigoon-leer kan onrechtmatig verkregen bewijs gebruikt worden voor het vonnisgerecht. Echter zal het onrechtmatig bewijs in bepaalde gevallen geweerd worden. Zo zal het bewijs geweerd worden, indien de naleving van bepaalde vormvoorwaarden, op straffe van nietigheid, voorgeschreven wordt. Daarnaast moet het bewijs worden geweerd, indien de begane onrechtmatigheid, de betrouwbaarheid van het bewijs heeft aangetast.¹⁸⁴ Bovendien wordt het bewijs geweerd, wanneer het gebruik van het onrechtmatig verkregen bewijs in strijd zou zijn met het recht op een eerlijk proces.¹⁸⁵
120. **Arrest Van Wesenbeeck** – In het arrest Van Wesenbeeck introduceerde het EHRM een tweestappen-test, om te beoordelen of het weigeren van toegang tot bewijsmateriaal een schending van de wapengelijkheid kan teweegbrengen. Ten eerste dient onderzocht te worden of de beperking van de toegang een legitiem belang nastreeft. Vervolgens moet worden beoordeeld of de beperking in verhouding staat tot het nagestreefde doel. Wanneer tijdens het onderzoek bulkdata wordt gebruikt, moeten de partijen de mogelijkheid hebben om de selectiecriteria te kennen, die werden gehanteerd. Daarnaast moeten de partijen over de mogelijkheid beschikken om zelf selectiecriteria aan te brengen.¹⁸⁶
121. **Arrest Einarsson** – In het arrest Einarsson benadrukt het EHRM dat het de mogelijkheid voor de verdediging, tot controle wil waarborgen, maar dat het Hof een efficiënte bewijsverzameling niet wil belemmeren. Daarnaast formuleerde het EHRM in dit arrest drie fundamentele principes met betrekking tot het gebruik van bulkdata in strafrechtelijke onderzoeken.¹⁸⁷
122. **Principes Einarsson** - Zo is er geen principieel recht van toegang tot bulkdata in zover de vervolgende partij hier geen toegang tot heeft genomen of kennis van heeft gekregen. Echter geldt het recht op toegang wel indien die vervolgende partij kennisnam van deze data. Bijgevolg is dit recht op toegang van toepassing, indien de vervolgende partij enkel kennisnam van deze data, om te beoordelen welke data al dan niet nuttig zou kunnen zijn in het kader van het onderzoek. Bovendien kan de toegang enkel geweigerd worden, indien deze toegang wordt geweigerd, om een legitiem doel na te streven. Daarnaast moet de

¹⁸³ *Ibid.*, nr. 38.

¹⁸⁴ HUYBRECHTS, L. en ROZIE, M., 'De rechten van de verdediging bij de behandeling ten gronde', *NC* 2008/2, (106) 112-114, nr. 37-45.

¹⁸⁵ Cass. 14 oktober 2003, *RW* 2003/04, 814, concl. DE SWAEF.; M., HUYBRECHTS, L. en ROZIE, M., 'De rechten van de verdediging bij de behandeling ten gronde', *NC* 2008/2, (106) 112-113, nr. 38.

¹⁸⁶ EHRM 18 september 2017, 67496/10 en 52936/12.

¹⁸⁷ EHRM 7 februari 2018, 24703/15.

weigering strikt noodzakelijk zijn en er moet worden voorzien in procedurele garanties om de wapengelijkheid niet in het gedrang te brengen. Voorts heeft de verdedigende partij het recht om de criteria te kennen, die gehanteerd werden om de bulkdata te filteren. Daarnaast kan de verdedigende partij zoekcriteria suggereren. Vervolgens zal een gebrek aan toegang tot de geselecteerde data of de zoekcriteria op zich niet resulteren in een onherstelbare schending van de rechten van de verdediging.¹⁸⁸

¹⁸⁸ EHRM 7 februari 2018, 24703/15.

Hoofdstuk II. Recht op privacy

123. **Recht op privacy** – In het kader van dit hoofdstuk zal het recht op privacy diepgaander geanalyseerd worden.¹⁸⁹ Het recht op privacy wordt in verschillende rechtsinstrumenten gewaarborgd. Zo waarborgt het Europees Verdrag voor de Rechten van de Mens het recht op privéleven voor eenieder.¹⁹⁰ Bovendien waarborgt de Grondwet dat eenieder recht heeft op de eerbiediging van zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.¹⁹¹ Daarnaast waarborgt het Handvest van de Grondrechten van de Europese Unie de eerbiediging van het privéleven van eenieder, zijn familie- en gezinsleven, zijn woning en zijn communicatie.¹⁹²
124. **Aspecten** – Het recht op privacy waarborgt zowel het recht op eerbiediging van het privéleven, als het recht op bescherming van persoonsgegevens.¹⁹³

¹⁸⁹ LANCKSWEERDT, E., 'De toekomst van de mensenrechten in turbulente tijden', *Juristenkrant* 2025/506, (12) 12-13.

¹⁹⁰ Art. 22 EVRM

¹⁹¹ Art. 22 Gecoördineerde Grondwet van 17 februari 1994, *BS* 17 februari 1994 (Hierna: GW)

¹⁹² Art. 7 Handvest van de grondrechten van de Europese Unie van 26 oktober 2012, *Pb. L.* 26 oktober 2012. (Hierna: Handvest van de grondrechten van de Europese Unie)

¹⁹³ DE BRUYNE, J., VALCKE, P., HENDRICKX, V. en GIELEN, G., *Technologie en recht, online privacy*, Owl Press Legal, 2025, 339-427, nr. 341.

Afdeling I: Recht op eerbiediging van het privéleven

125. **Recht op eerbiediging van het privéleven** – Het recht op privacy waarborgt het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens. In deze afdeling zal het recht op eerbiediging van het privéleven besproken worden. Het recht op eerbiediging van het privéleven beschermt ieder individu tegen het ongewenst binnendringen van zijn persoonlijke levenssfeer. Daarnaast beschermt het recht op eerbiediging van het privéleven de burger ook voor het openbaar maken van zijn persoonlijke levenssfeer. Bovendien waarborgt het recht op eerbiediging van het privéleven, het recht om met rust te worden gelaten. Hier wordt ook naar verwezen als 'the right to be let alone'.¹⁹⁴
126. **EVRM** – Het Europees Verdrag voor de Rechten van de Mens waarborgt het recht op privacy, met daarin begrepen het recht op eerbiediging van het privéleven. Het EVRM waarborgt dat eenieder het recht heeft op eerbiediging van zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling. Bovendien is er geen inmenging van enig openbaar gezag toegestaan met betrekking tot de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving nodig is in het belang van 's lands 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 voor de bescherming van de rechten en vrijheden van anderen.¹⁹⁵
127. **Inmenging mensenrecht** – Wanneer de overheid handelt in strijd met het recht op eerbiediging van het privéleven, zal er een grotere grondrechtsbescherming bestaan, wanneer er aan bepaalde voorwaarden is voldaan. Hiervoor moet er een wettelijke basis bestaan. Bovendien moet deze wettelijke basis voldoende duidelijk zijn, nauwkeurig en voorspelbaar zijn. Voorts moet er een legitiem doel worden nagestreefd. Daarboven moet de inmenging noodzakelijk, proportioneel en subsidiair zijn.¹⁹⁶

¹⁹⁴ DEBRUYNE, N. *Commerciële exploitatie de menselijke afbeelding, naam en stem: Deel I: Normatief kader en commercialisering*, die Keure, 2021, 27-50, nr. 85.

¹⁹⁵ Art. 8 EVRM; CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593.; SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 2.

¹⁹⁶ SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 2.

Afdeling II. Recht op bescherming van persoonsgegevens

128. **Bescherming persoonsgegevens** – In deze afdeling zal het recht op bescherming van persoonsgegevens besproken worden.¹⁹⁷ Uit de rechtspraak van het EHRM blijkt dat het recht op bescherming van persoonsgegevens behoort tot het recht op privacy.¹⁹⁸ Bovendien is het recht op bescherming van persoonsgegevens een onderdeel van het dataproctierecht.¹⁹⁹
129. **Handvest** - Het Handvest van de Grondrecht van de Europese Unie waarborgt het recht op bescherming van persoonsgegevens. Hierin wordt bepaald dat eenieder recht heeft op bescherming van zijn persoonsgegevens.²⁰⁰ Bovendien moeten deze persoonsgegevens eerlijk verwerkt worden. Voorts kan de verwerking slechts plaatsvinden om bepaalde doeleinden na te streven. Daarnaast is de verwerking van persoonsgegevens slechts mogelijk, wanneer de betrokkene toestemming geeft of op basis van een gerechtvaardigde grondslag, die in de wet wordt opgenomen.²⁰¹
130. **Rechtvaardiging inmenging** – Bovendien moeten beperkingen op erkende rechten en vrijheden, die werden opgenomen in het Handvest, bij wet worden vastgesteld. Daarnaast moeten de beperkingen de wezenlijke inhoud van de erkende rechten en vrijheden eerbiedigen.²⁰² Voorts moet bij de beperking, het evenredigheidsbeginsel in acht worden genomen. Dit heeft tot gevolg dat beperkingen slechts kunnen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.²⁰³
131. **EVRM** – Daarboven wordt het recht op bescherming van persoonsgegevens door het EVRM gewaarborgd.²⁰⁴ Zoals reeds aangehaald, beschermt het EVRM het recht op eerbiediging van het privéleven van een persoon, het gezinsleven van een persoon en het huis en de briefwisseling van een persoon.²⁰⁵

¹⁹⁷ PYPE, L., 'De verwerking van persoonsgegevens door de pers: ook de AVG vraagt om een afweging tussen de persvrijheid en het recht op de eerbiediging van het privéleven', *TPP* 2023/2, (4) 4-14.

¹⁹⁸ SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 2.; CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593, nr. 607.; EHRM 4 mei 2000, 28341/95.; EHRM 4 december 2008, 30562/04 en 30566/04.; EHRM 28 november 2011, 30194/09.

¹⁹⁹ CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593, nr. 607.

²⁰⁰ Art. 8 Handvest van de grondrechten van de Europese Unie

²⁰¹ *Ibid.*

²⁰² SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 2.

²⁰³ Art. 52, lid 1 Handvest van de grondrechten van de Europese Unie

²⁰⁴ Art. 8 EVRM

²⁰⁵ *Supra* nr. 126.; Art. 8 EVRM

132. **Definitie persoonsgegevens** – Persoonsgegevens kunnen gedefinieerd worden als gegevens die betrekking hebben op een geïdentificeerd of identificeerbaar persoon. Indien deze persoonsgegevens betrekking hebben op het privéleven van een persoon, genieten zij bescherming door middel van het recht op privacy, dat werd opgenomen in het EVRM.²⁰⁶
133. **Transparantie** - Het recht op bescherming van persoonsgegevens heeft tot gevolg, dat de persoonsgegevens die een persoon aan verschillende bedrijven toevertrouwt, niet zonder de toestemming van deze persoon mogen worden verweven. Bovendien moeten de persoonsgegevens die worden meegedeeld aan bedrijven, op een transparante manier worden verwerkt. Daardoor moet de betrokkene over voldoende informatie beschikken omtrent de verwerking van zijn persoonsgegevens.²⁰⁷
134. **Rechtvaardiging** – Wanneer de overheid persoonsgegevens wil gebruiken die beschermd worden door het recht op privacy, met inbegrip van het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens, dat gewaarborgd wordt in het EVRM, zal de overheid bijgevolg moeten voldoen aan de voorwaarden die werden opgenomen bij de bepaling die dit recht waarborgt.²⁰⁸ Zoals eerder aangehaald, moet er een wettelijke basis bestaan.²⁰⁹ Daarnaast moet de inmenging een legitiem doel nastreven. Dit legitiem doel kan bijvoorbeeld de bescherming van het land, de openbare veiligheid, de bescherming van de openbare orde, de voorkoming van strafbare feiten, de bescherming van de goede zeden of de bescherming van de rechten en vrijheden van anderen zijn.²¹⁰ Wanneer de overheid voldoet aan deze voorwaarden, zal de verwerking gerechtvaardigd zijn. Dit betekent dat de grondrechtbescherming groter zal zijn. Wanneer de overheid daarentegen deze voorwaarden niet naleeft, kan er geen legitieme verwerking plaatsvinden.²¹¹ Bovendien moet de verwerking van persoonsgegevens in verhouding zijn tot het recht op bescherming van persoonsgegevens.²¹²
135. **Rechtspraak** – Uit een lezing van de rechtspraak komt naar voren dat het Grondwettelijk Hof slechts in vijf van de drieëndertig arresten, waarbij het Hof de proportionaliteitstest toepaste, oordeelde het dat het recht op bescherming van persoonsgegevens werd geschonden.²¹³

²⁰⁶ CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593, nr. 613.; EHRM 26 maart 1987, 9248/81.

²⁰⁷ CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593, nr. 607.

²⁰⁸ Art. 8 EVRM; Art. 8.2 EVRM

²⁰⁹ *Supra* nr. 115.

²¹⁰ Art. 8.2 EVRM

²¹¹ CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593, nr. 613.

²¹² SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 2-3.

²¹³ VROONEN, B., 'De strengere evenredigheidstoets bij het recht op bescherming van persoonsgegevens: lucky shot of kentering in de rechtspraak?', *TBP* 2024/9, (580) 580-586.

136. **Schending rechtspraak** - Redenen die het Grondwettelijk Hof aanvoerde om tot een schending van het recht op bescherming van persoonsgegevens te besluiten, betroffen onder meer het ontbreken van een maximumtermijn voor het bewaren van persoonsgegevens.²¹⁴ Daarnaast waren er een aantal zaken, waarbij het Grondwettelijk Hof oordeelde dat de maatregel, die een schending van de bescherming van persoonsgegevens tot gevolg had, niet noodzakelijk was.²¹⁵
137. **Arrest omtrent vingerafdrukken in identiteitskaart** – In de strijd tegen identiteitsfraude wenste de wetgever vingerafdrukken te laten opnemen in de identiteitskaart. Hierbij moet worden benadrukt dat vingerafdrukken ook kunnen worden beschouwd als persoonsgegevens. Volgens de verzoekende partij was het opnemen van vingerafdrukken in de identiteitskaart niet noodzakelijk, aangezien er al andere maatregelen bestaan om identiteitsfraude tegen te gaan. Echter hield Het Grondwettelijk Hof in zijn uitspraak, de bestaande maatregelen buiten beschouwing. Bijgevolg oordeelde het Grondwettelijk Hof dat de opname van vingerafdrukken in de identiteitskaart het recht op bescherming van persoonsgegevens niet schendt. Daarnaast oordeelde het Hof dat het opnemen van vingerafdrukken relevant is om het vooropgestelde doel na te streven.²¹⁶

²¹⁴ GwH 9 december 2021, 177/2021.; GwH 22 september 2022, 110/2022.

²¹⁵ GwH 22 april 2021, 57/2021.; GwH 12 oktober 2023, 131/2023.

²¹⁶ GwH 14 januari 2021, 2/2021.

Hoofdstuk III. Recht op gelijkheid en non-discriminatie

138. **Inleiding** – Bij de reeds besproken fundamentele rechten, waaronder het recht op een eerlijk proces en het recht op privacy, met inbegrip van het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens²¹⁷, zal waarschijnlijk de kans groter zijn dat deze rechten kunnen worden geschonden, indien de overheid persoonsgegevens aankoopt in het kader van het strafonderzoek. Er bestaan echter ook nog andere mensenrechten die hierdoor eventueel zouden kunnen worden geschonden. Deze rechten zijn onder andere, het recht op gelijkheid en non-discriminatie en het recht op vrije meningsuiting. Bijgevolg zal in dit hoofdstuk het recht op gelijkheid en non-discriminatie kort besproken worden.
139. **EVRM** – Vooreerst wordt het recht op gelijkheid en non-discriminatie gewaarborgd door het EVRM. Dit recht impliceert dat het genot van de rechten en vrijheden is verzekerd zonder enig onderscheid op welke grond ook zoals geslacht, ras, kleur, taal, godsdienst, politieke of andere overtuiging, nationale of maatschappelijke afkomst, het behoren tot een nationale minderheid, vermogen, geboorte of andere status.²¹⁸
140. **Recht op gelijkheid en non-discriminatie** – Daarnaast wordt het recht op gelijkheid en non-discriminatie gewaarborgd door de Grondwet. Het recht op gelijkheid en non-discriminatie heeft tot gevolg dat alle Belgen gelijk voor de wet zijn.²¹⁹ Bovendien moet het genot van de rechten en vrijheden aan de Belgen toegekend, verzekerd worden zonder discriminatie.²²⁰

²¹⁷ *Supra* nr. 116-137.

²¹⁸ Art. 14 EVRM

²¹⁹ Art. 10 GW; VANDENHOLE, W., *Economische, sociale en culturele rechten: Verbod op discriminatie en recht op gelijke behandeling*, Wolters Kluwer, 2021, 203-257, nr. 415.

²²⁰ Art. 11 GW

Hoofdstuk IV. Recht op vrije meningsuiting

141. **Recht op vrije meningsuiting** – Het volgende fundamenteel recht dat kort zal worden besproken is het recht op vrije meningsuiting. Het recht op vrije meningsuiting wordt gewaarborgd in de Grondwet. Hierin wordt bepaald dat iedereen de vrijheid heeft om op elk gebied zijn mening te uiten²²¹. Daarnaast waarborgt het EVRM het recht op vrije meningsuiting. Hierin wordt bepaald dat eenieder het recht heeft op een vrije meningsuiting. Bovendien impliceert dit recht de vrijheid om een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of door te geven zonder de inmenging van overheidswege.²²²
142. **Andere mensenrechten** – Bovendien bestaan er nog andere fundamentele rechten, die gewaarborgd worden door het EVRM, het Handvest van de Grondrechten van de Europese Unie en de Grondwet. Dit zijn bijvoorbeeld het recht op leven²²³, het recht op vrijheid en veiligheid²²⁴, de vrijheid van vergadering en vereniging²²⁵, het recht te huwen²²⁶... Naar de bescheiden mening van de auteur zal er slechts een kleinere kans bestaan dat deze rechten worden geschonden door de besproken handeling. Bijgevolg zullen deze rechten niet geanalyseerd worden in het kader van deze masterproef.

²²¹ Art. 19 GW

²²² Art. 10 EVRM

²²³ Art. 2 EVRM

²²⁴ Art. 5 EVRM

²²⁵ Art. 11 EVRM

²²⁶ Art. 12 EVRM

Deel IV. Gegevensbeschermingsrecht

Hoofdstuk I. Categorieën persoonsgegevens

143. **Inleiding** – In dit deel zal volgende subvraag worden onderzocht: 'In welke categorieën kunnen persoonsgegevens worden ingedeeld, naargelang de aard van de informatie?'. Hierbij zal worden onderzocht in welke categorieën persoonsgegevens kunnen worden ingedeeld, naargelang de aard of gevoeligheid van de persoonsgegevens. Hierbij zal het onderscheid tussen niet-gevoelige en gevoelige gegevens geduid worden. Bovendien zal worden onderzocht welke gegevens kunnen worden beschouwd als gevoelige gegevens. Daarnaast zal worden geanalyseerd of deze gevoelige gegevens, een grotere bescherming behoeven met betrekking tot de fundamentele rechten. Op basis van dit onderscheid tussen niet-gevoelige gegevens en gevoelige gegevens, zal in het evaluatief gedeelte worden onderzocht of de aankoop van persoonsgegevens in het kader van het strafonderzoek al dan niet een dwangmaatregel zou uitmaken. Bijgevolg kan op basis daarvan worden geanalyseerd of de procureur des Konings of de onderzoeksrechter bevoegd is om de onderzochte handeling te bevelen.²²⁷
144. **Verschillende categorieën** - Persoonsgegevens kunnen worden ingedeeld in verschillende categorieën. Zo kunnen persoonsgegevens worden ingedeeld in niet-gevoelige gegevens, ook wel 'gewone' gegevens genoemd en in gevoelige gegevens, ook wel bijzondere gegevens genoemd.²²⁸ Bovendien kunnen persoonsgegevens verschillende vormen van informatie omvatten. Ter illustratie: persoonsgegevens kunnen de vorm aannemen van foto's, teksten, beeldmateriaal, geluiden en andere bestaande mediavormen.²²⁹
145. **Niet-gevoelige persoonsgegevens** - Hierbij kunnen 'gewone' of niet-gevoelige persoonsgegevens worden beschouwd als gegevens die een persoon identificeren of het mogelijk maken om een persoon te identificeren, en die niet behoren tot de categorie van gevoelige gegevens. Bijgevolg kunnen bijvoorbeeld worden beschouwd als 'gewone' gegevens; een naam, geboortedatum, een adres, telefoonnummer, e-mailadres, een IP-adres aan de bron, informatie die de betrokkene reeds openbaar maakte, foto's of video's die geen betrekking hebben op één van de categorieën die beschouwd worden als bijzonder...²³⁰ Bovendien bevestigt de memorie van toelichting bij dataretentiewet III dat gegevens die identificatiegegevens betreffen, niet-gevoelige gegevens zijn.²³¹

²²⁷ *Infra* 236 e.v.

²²⁸ DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 451-492, nr. 9-26.; Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 204.

²²⁹ DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 451-492, nr. 8.

²³⁰ *Ibid.*, nr. 12-14.

²³¹ 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. 55-2572/001, 14.

146. **Gevoelige gegevens** - Daarbij zijn gevoelige gegevens, gegevens die naar hun aard gevoelig zijn en grotere risico's met zich meebrengen met betrekking tot de grondrechten en fundamentele vrijheden. Bovendien behoeven gevoelige gegevens een grotere, specifieke bescherming.²³²
147. **Etnische of medische gegevens** – Bijgevolg kunnen als gevoelige gegevens worden beschouwd, de verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken. Daarnaast wordt de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon of gegevens over gezondheid of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid beschouwd als gevoelige gegevens.²³³
148. **Genetische gegevens** - Daarbij bepaalt de memorie van toelichting bij Titel II Wet Verwerking Persoonsgegevens, dat genetische gegevens kunnen worden gedefinieerd als persoonsgegevens met betrekking tot de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon, die unieke informatie geven over de fysiologie of de gezondheid van die natuurlijke persoon, die voortkomen uit een analyse van een biologisch monster van de betrokken persoon, met name een chromosoomanalyse, een analyse van het DNA, RNA of een analyse van een ander element waarmee soortgelijke informatie kan worden verkregen. Gezien de complexe en gevoelige aard van genetische informatie, kunnen het misbruik en hergebruik voor uiteenlopende doeleinden bijzonder schadelijk zijn voor de betrokken persoon. Discriminatie op grond van genetische kenmerken moet in beginsel worden verboden.²³⁴
149. **Gezondheidsgegevens** – Daarnaast bepaalt de memorie van toelichting bij Titel II Wet Verwerking Persoonsgegevens dat gezondheidsgegevens kunnen worden beschouwd als alle gegevens die betrekking hebben op de gezondheidstoestand van een persoon en gegevens die informatie geven over de lichamelijke of geestelijke gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst. Bovendien omvatten gezondheidsgegevens informatie over de natuurlijke persoon die is verzameld in het kader van de registratie voor of de verlening van gezondheidszorgdiensten aan die natuurlijke persoon, alsmede een aan een natuurlijke persoon toegekend nummer, symbool of kenmerk dat uitsluitend als identificatie van die natuurlijke persoon geldt voor

²³² DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 451-492, nr. 16.; *Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 451-492, nr. 9-26.; Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 130 en 175.

²³³ DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 451-492, nr. 16.; Art. 9 en 34 Wet Verwerking Persoonsgegevens; 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. 55-2572/001, 226.; CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593, nr. 614.

²³⁴ Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 64.

gezondheidsdoeleinden, de informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel of lichaamseigen stof, met inbegrip van genetische gegevens en biologische monsters, en alle informatie over bijvoorbeeld ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de fysiologische of biomedische staat van de betrokkene, ongeacht de bron, bijvoorbeeld een arts of andere gezondheidswerker, een ziekenhuis, een medisch hulpmiddel of een in-vitro diagnostische test²³⁵

150. **Foto's** – Voorts bepaald de overweging bij de GDPR dat, verwerking van foto's niet systematisch mag worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens. Aangezien foto's alleen onder de definitie van biometrische gegevens vallen, wanneer de foto's worden verwerkt met behulp van bepaalde technische middelen, die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken.²³⁶
151. **Gevoelig met betrekking tot grondrechten** - Uit de overwegingen bij de GDPR-verordening blijkt bovendien dat persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, specifieke bescherming verdienen, aangezien de context van de verwerking ervan, significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden.²³⁷
152. **Verwerking gevoelige gegevens** - Uit de memorie van toelichting bij Titel I Wet Verwerking Persoonsgegevens blijkt bovendien dat de verwerking van bijzondere of gevoelige persoonsgegevens in verhouding moet staan tot het nagestreefde doel, het wezen van het recht op gegevensbescherming moet geëerbiedigd zijn en passende en specifieke maatregelen moeten worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene²³⁸
153. **Persoonsgegevens en fundamentele rechten** - De memorie van toelichting bij Titel II Wet Verwerking Persoonsgegevens stelt dat persoonsgegevens die door hun aard bijzonder gevoelig zijn, wat betreft de grondrechten en fundamentele vrijheden, specifieke bescherming verdienen. Aangezien de context van de verwerking ervan aanzienlijke risico's voor de grondrechten en fundamentele vrijheden kan meebrengen. Bovendien dient de verwerking van gevoelige gegevens bij wet toegelaten te zijn, indien de betrokkene uitdrukkelijk heeft toegestemd met de verwerking, die een ingrijpende inbreuk vormt op zijn privacy. Bijgevolg kan de toestemming van de betrokkene op zich evenwel geen rechtsgrond vormen, voor de verwerking van gevoelige persoonsgegevens door bevoegde overheden.²³⁹

²³⁵ *Ibid.*

²³⁶ Verordening (EU) 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, overweging (51).

²³⁷ *Ibid.*

²³⁸ Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 21.

²³⁹ *Ibid.*, 77-78.

154. **IP-adressen** - Voorts oordeelde het Hof van Justitie in het *La Quadrature du Net*-arrest met betrekking tot IP-adressen, dat deze zeer privacygevoelig kunnen zijn.²⁴⁰ Aangezien IP-adressen onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld. Evenwel moet eraan worden herinnerd dat de operatoren geen IP-adressen van de bestemming mogen bewaren in het kader van de internettoegangsdienst, maar enkel de IP-adressen aan de bron van de communicatie moeten bewaren.²⁴¹ IP-adressen aan de bron, kunnen in tegenstelling tot IP-adressen aan de bestemming, het niet mogelijk maken om de volledige zoekgeschiedenis van een internetgebruiker te traceren.²⁴²
155. **Zware criminaliteit** - Zowel in het vermelde arrest, als in de memorie van toelichting bij dataretentiewet III werd benadrukt dat enkel de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, een algemene en ongedifferentieerde bewaring kunnen rechtvaardigen van enkel de IP-adressen die zijn toegewezen aan de bron van een verbinding.²⁴³

²⁴⁰ HvJ 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791.

²⁴¹ *Ibid.*

²⁴² 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. 55-2572/001, 44.

²⁴³ 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. 55-2572/001, 5 en 44.; VAN DE HEYNING, C., 'Het gebruik van communicatiegegevens in strafzaken: hoe het Hof van Justitie het Belgische strafrecht hertekent', *T.Strafr.* 2025/2, (66) 66-79, nr. 10-11.

Hoofdstuk II. Instrumenten gegevensbeschermingsrecht

156. **Inleiding** – In dit deel zal volgende subonderzoeksvraag onderzocht worden: *'Welke privacy en fundamentele rechten kunnen eventueel worden geschonden door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek?'*. Het gegevensbeschermingsrecht is een onderdeel van het recht op privacy.²⁴⁴ Aangezien het recht op privacy reeds werd besproken, zal dit in dit deel niet besproken worden.²⁴⁵ Daarentegen zullen in dit deel de privacyregels besproken worden, aan de hand van een aantal belangrijke instrumenten met betrekking tot het gegevensbeschermingsrecht, waaronder de GDPR en de privacyrichtlijn politie-justitie.
157. **GDPR** – Een belangrijk instrument binnen het gegevensbeschermingsrecht is de GDPR.²⁴⁶ Deze verordening werd in België omgezet in de Wet Verwerking Persoonsgegevens.²⁴⁷ Zoals in dit deel zal blijken, bevat deze regelgeving de algemene bepalingen met betrekking tot de bescherming van persoonsgegevens.
158. **Uitzonderingen toepassing GDPR** – Er zijn een aantal situaties waarin de GDPR niet van toepassing zal zijn.²⁴⁸ Eén van deze situaties is deze waarin persoonsgegevens verwerkt worden met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.²⁴⁹ Deze uitzondering is relevant in het kader van dit onderzoek, aangezien de onderzochte handeling zich situeert binnen het onderzoek en de opsporing van strafbare feiten. Bijgevolg zal de GDPR niet van toepassing zijn bij de aankoop van persoonsgegevens bij gespecialiseerde commerciële dataverzamelingsbedrijven en het gebruik van deze gegevens in het kader van het strafonderzoek.
159. **Privacyrichtlijn politie-justitie** – Daarentegen zal de privacyrichtlijn politie-justitie van toepassing zijn, wanneer persoonsgegevens worden verwerkt met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.²⁵⁰ Bovendien werd deze richtlijn in België

²⁴⁴ *Supra* nr. 128.

²⁴⁵ *Supra* nr. 123-137.

²⁴⁶ Verordening (EU) 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)

²⁴⁷ Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018. (Hierna: Wet Verwerking Persoonsgegevens)

²⁴⁸ DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 689-758.

²⁴⁹ *Ibid.*, nr. 734.

²⁵⁰ Privacyrichtlijn politie-justitie

omgezet in Titel II Wet Verwerking Persoonsgegevens.²⁵¹ Bijgevolg zal deze wet van toepassing zijn met betrekking tot de onderzochte handeling.

²⁵¹ Art. 25-71 Wet Verwerking Persoonsgegevens; DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 704.

Afdeling I. GDPR

160. **GDPR/AVG** – De General Data Protection Regulation, afgekort als GDPR, is één van de belangrijkste instrumenten die de verwerking van persoonsgegevens regelt.²⁵² Bovendien wordt naar deze richtlijn ook verwezen als de Algemene Verordening Gegevensbescherming of AVG.²⁵³ Voorts werd deze richtlijn in België omgezet in Titel I van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.²⁵⁴
161. **Beginnelsen verwerking** – Deze wetgeving bevat diverse bepalingen met betrekking tot de verwerking van persoonsgegevens door verwerkers, evenals de rechten die toekomen aan de betrokkene.²⁵⁵ De AVG bepaalt de beginselen die moeten worden nageleefd bij de verwerking van persoonsgegevens, die onder het toepassingsgebied van de AVG behoren.²⁵⁶ Het gaat hierbij om het beginsel van rechtmatigheid, behoorlijkheid en transparantie²⁵⁷, het beginsel van doelbepaling- en binding, het beginsel van minimale gegevensverwerking, het beginsel van juistheid, het beginsel van dataretentie, het beginsel van integriteit en vertrouwelijkheid en het verantwoordingsbeginsel.²⁵⁸
162. **Rechtvaardiging** – De AVG stelt zes rechtsgronden vast, waaraan moet worden voldaan om persoonsgegevens op een rechtmatige wijze te verwerken.²⁵⁹ Vooreerst is de verwerking rechtmatig wanneer de betrokkene een geldige toestemming verleent. Ten tweede kan het bestaan van een contractuele relatie de verwerking rechtvaardigen. Ten derde kan de verwerking gerechtvaardigd zijn, wanneer er een wettelijke verplichting met betrekking tot deze verwerking bestaat. Ten vierde is de verwerking rechtmatig, wanneer deze de bescherming van de vitale belangen van de betrokkene of andere natuurlijke personen tot gevolg heeft. Ten vijfde kan de verwerking rechtmatig zijn indien de verwerking nodig is om een taak van algemeen belang te behartigen of in het kader van het openbaar gezag. Ten laatste kan de verwerking rechtmatig zijn indien de verwerking een gerechtvaardigd belang nastreeft.²⁶⁰ Bovendien werd hierbij een onderscheid gemaakt tussen gevoelige persoonsgegevens en andere gegevens. Dit heeft tot gevolg dat er

²⁵² Verordening (EU) 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.

²⁵³ *Ibid.*

²⁵⁴ Wet Verwerking Persoonsgegevens

²⁵⁵ VAN DEN BRANDE, B., 'Ook God ontsnapt niet aan de AVG', *TPP* 2018, (34) 34-36.

²⁵⁶ ROZIE, J. en TERSAGO, P., *Ondernemingsstrafrecht: Het gegevensbeschermingsrecht vanuit strafrechtelijk perspectief. Misdrijven in de AVG en de Belgische kaderwet aangestipt*, LeA Uitgevers, 2023, 27-56, nr. 5.

²⁵⁷ BENICHIU, B., KINDT, E. en BEUDELS, M., *Informatie en recht: Informatieverplichtingen in het gegevensbeschermingsrecht: much ado about nothing?*, Intersentia, 2021, 197-234.; MICHAIL, N., 'Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union', *TBH* 2019/1, (52) 52-79, nr. 52-79.

²⁵⁸ DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 449-492, nr. 46-59.

²⁵⁹ Art. 6 AVG; DEPREZ, S., FOCQUET, A. en MANNEKENS, J., *Gegevensbescherming: Bos door de bomen*, LeA, Uitgevers, 2022, 1-11, nr. 113.

²⁶⁰ ROZIE, J. en TERSAGO, P., *Ondernemingsstrafrecht: Het gegevensbeschermingsrecht vanuit strafrechtelijk perspectief. Misdrijven in de AVG en de Belgische kaderwet aangestipt*, LeA Uitgevers, 2023, 27-56, nr. 4.; DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 449-492, nr. 61-89.; SCHRAM, F., *Handboek Privacy en Persoonsgegevens: De GDPR en de federale 'omzettingswetgeving*, Politeia, 2023, 366-448.

afzonderlijke rechtsgronden bestaan voor een rechtmatige gegevensverwerking, wanneer de verwerking betrekking heeft op gevoelige gegevens.²⁶¹

163. **Rechtspraak GBA** – De Gegevensbeschermingsautoriteit heeft een boete opgelegd aan een bedrijf, wegens de verkoop van persoonsgegevens voor commerciële doeleinden. De klantengegevens werden verkocht aan aanbieders van diensten die betrekking hebben tot kinderen en aan dataverzamelingsbedrijven. Bovendien communiceerde het bedrijf niet op een duidelijke en begrijpelijke manier over de verkoop van deze gegevens. In haar uitspraak benadrukte de Gegevensbeschermingsautoriteit dat dataverzamelingsbedrijven, vanwege het invasieve karakter van hun businessmodel, volledige transparantie moeten bieden, zodat betrokkene controle kunnen behouden over hun persoonsgegevens. Doordat het businessmodel van dataverzamelingsbedrijven zo invasief is, moeten deze bedrijven volledig transparant te werk moeten gaan, zodat de betrokkenen controle kunnen houden over hun gegevens. Bijgevolg is een onvolledige of misleidende voorstelling van het gebruik van deze gegevens, in strijd met het gegevensbeschermingsrecht.²⁶²
164. **Uitsluitingen** – Er bestaan verschillende uitsluitingen op de toepassing van de AVG. Eén van deze uitsluitingen betreft de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen met inbegrip van de bescherming tegen en de voorkoming van gebaren voor de openbare veiligheid.²⁶³ Dit betekent dat de AVG niet van toepassing is op de activiteiten van de staat op strafrechtelijk gebied. Bijgevolg zal de AVG niet van toepassing zijn op de onderzochte handeling.²⁶⁴

²⁶¹ Art. 9 AVG; DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 449-492, nr. 60.

²⁶² Beslissing Geschillenkamer Gegevensbeschermingsautoriteit van 27 januari 2021, 04/2021.

²⁶³ Art. 2, lid 2, AVG; DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 734.

²⁶⁴ Art. 10 AVG; DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 449-492, nr. 608.

Afdeling II. Privacyrichtlijn politie-justitie en Titel II Wet Verwerking Persoonsgegevens

165. **Algemeen** - Zoals reeds aangehaald, is de AVG niet van toepassing op de opsporing en het onderzoek naar strafbare feiten.²⁶⁵ Daarentegen is de Verordening (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 betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, ook wel privacyrichtlijn politie-justitie genoemd wel van toepassing op het opsporing en het onderzoek naar strafbare feiten.²⁶⁶ Bijgevolg zal deze richtlijn van toepassing zijn bij toepassing van de handeling, die in het kader van deze masterproef wordt onderzocht.
166. **Omzetting** – Bovendien werd de privacyrichtlijn politie-justitie in België omgezet in Titel II: De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.²⁶⁷
167. **AVG vs. privacyrichtlijn politie-justitie** - Wanneer een verwerking behoort tot het toepassingsgebied van de privacyrichtlijn politie-justitie, zullen de regels van deze richtlijn van toepassing zijn. Bijgevolg zullen de regels, die in de AVG werden opgenomen, in dit geval niet van toepassing zijn. Daarentegen is de omgekeerde situatie ook mogelijk.²⁶⁸ Dit is het gevolg van het principe dat de AVG de *lex generalis* vormt en de privacyrichtlijn politie-justitie de *lex specialis*.²⁶⁹
168. **Verwerking voor andere doeleinden** – Bovendien zal de privacyrichtlijn politie-justitie niet van toepassing zijn, indien de verwerking van persoonsgegevens gebeurt door de overheden die hiertoe bevoegd zijn in het kader van deze richtlijn, maar de verwerking gebeurt voor een ander doel dan de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de

²⁶⁵ *Supra* nr. 164.

²⁶⁶ DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 591.; DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 734.

²⁶⁷ Art. 25 - 71 Wet Verwerking Persoonsgegevens

²⁶⁸ DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 734.

²⁶⁹ DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 689-736.; DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 608.; Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 66-67.

bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Bijgevolg zullen in dat geval de regels van de AVG van toepassing zijn.²⁷⁰

169. **Spanningsveld strafrecht vs. gegevensbeschermingsrecht** – Daarnaast hebben de regels uit het straf- en strafprocesrecht voorrang op de regels uit het gegevensbeschermingsrecht.²⁷¹ Bijgevolg hebben de regels uit het straf- en strafprocesrecht voorrang op de regels, die werden opgenomen in de Wet Verwerking Persoonsgegevens.²⁷² In bepaalde gevallen zijn de bepalingen uit het gegevensbeschermingsrecht in strijd met de regels uit het strafrecht.²⁷³ Daardoor bepaalt de Wet Verwerking Persoonsgegevens bij ieder recht dat de betrokkene heeft, dat hiervan kan worden afgeweken door een wet, decreet of ordonnantie. Bovendien is een afwijking slechts mogelijk wanneer deze noodzakelijk en evenredig is.²⁷⁴
170. **Persoonsgegevens** – De Wet Verwerking Persoonsgegevens definieert persoonsgegevens als: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatiemiddel zoals een naam, een identificatienummer, locatiegegevens, een online identificatiemiddel of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.²⁷⁵
171. **Verwerking** - De verwerking van persoonsgegevens wordt gedefinieerd als: een bewerking of een geheel van bewerkingen 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, bekendmaking door middel van doorzending,

²⁷⁰ Privacyrichtlijn politie-justitie, overweging (11).; Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 66.; DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 738.; DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 608.

²⁷¹ DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 640.

²⁷² Art. 37, §4 Wet Verwerking Persoonsgegevens

²⁷³ DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 640.

²⁷⁴ Art. 37, §2 Wet Verwerking Persoonsgegevens; Art. 38, §2 Wet Verwerking Persoonsgegevens

²⁷⁵ Art. 26, 1° Wet Verwerking Persoonsgegevens; LIEGEOIS, Y. en BLEYEN, F., 'Na een schijnhuwelijk en een schijnscheiding thans een gedwongen opname? Of de (uitoefening van de) rechten van de natuurlijke persoon bij verwerking van diens persoonsgegevens in het strafproces', NC 2020/0, (1) 6.; SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het strafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 28.

verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.²⁷⁶²⁷⁷

172. **Verwerkingsverantwoordelijke** – De verwerkingsverantwoordelijke is de bevoegde overheid die, alleen of samen met anderen, de doeleinden van en de middelen voor de verwerking van persoonsgegevens vaststelt. Indien de doeleinden van en de middelen voor die verwerking door of krachtens een wet, een decreet of een ordonnantie zijn bepaald, is de verwerkingsverantwoordelijke de entiteit die door of krachtens de wet, het decreet of de ordonnantie als de verwerkingsverantwoordelijke wordt aangewezen.²⁷⁸
173. **Materieel element** – De richtlijn is van toepassing indien het doel van de verwerking de voorkoming, het onderzoek, de opsporing van strafbare feiten of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid is.²⁷⁹
174. **Strafbare feiten** – Om te kunnen beoordelen of er sprake is van een strafbaar feit, moet worden onderzocht of de gedraging al dan niet kan worden gekwalificeerd als onwettige gedraging. Hiervoor kan er onderzocht worden of de gedraging strafbaar is gesteld in het strafwetboek, maar dat alleen volstaat niet. Er moet tevens worden voldaan aan andere aspecten, vooraleer er sprake is van een strafbare gedraging.²⁸⁰ Zo is een aspect hiervan de aard van de overtreden norm, waarbij vooral het repressieve karakter van de sanctie centraal staat. Ten laatste wordt getoetst of er al dan niet werd voorzien in een vrijheidsberoving als sanctie.²⁸¹
175. **Personeel element** – De Wet Verwerking Persoonsgegevens bepaald welke bevoegde overheid, moet instaan voor de verwerking van persoonsgegevens, opdat deze wet van toepassing is. Bijgevolg is iedere overheidsinstantie die bevoegd is voor de voorkoming, het onderzoek, de opsporing van strafbare feiten of de vervolging van strafbare feiten of

²⁷⁶ Art. 31 Wet Verwerking Persoonsgegevens; LIEGEOIS, Y. en BLEYEN, F., 'Na een schijnhuwelijk en een schijnscheiding thans een gedwongen opname? Of de (uitoefening van de) rechten van de natuurlijke persoon bij verwerking van diens persoonsgegevens in het strafproces', *NC* 2020/0, (1) 7.; SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het strafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 33.

²⁷⁷ Art. 26, 2° Wet Verwerking Persoonsgegevens

²⁷⁸ Art. 26, 8° Wet Verwerking Persoonsgegevens; LIEGEOIS, Y. en BLEYEN, F., 'Na een schijnhuwelijk en een schijnscheiding thans een gedwongen opname? Of de (uitoefening van de) rechten van de natuurlijke persoon bij verwerking van diens persoonsgegevens in het strafproces', *NC* 2020/0, (1) 7.; Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 62.

²⁷⁹ DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 735-738.

²⁸⁰ DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 609.

²⁸¹ SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het strafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 14-15.; Privacyrichtlijn politie-justitie, overweging (13).; HvJ 22 juni 2021, C-439/19, overweging (87-91).

de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid of ieder orgaan of entiteit dat krachtens het lidstatelijke recht is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de voorkoming, het onderzoek, de opsporing van strafbare feiten of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid bevoegd voor de verwerking.²⁸²

176. **Exhaustieve lijst** – De bevoegde overheden voor de verwerking, werden exhaustief opgenomen in de wet. Bijgevolg mogen de gegevens uitsluitend worden verwerkt door een bevoegde overheid, die in deze lijst werd opgenomen. Indien dit niet het geval is, zal deze wet niet van toepassing zijn. Indien er andere overheden bevoegd zijn voor de voorkoming, het onderzoek, de opsporing van strafbare feiten of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, die niet in de lijst werden opgenomen, zullen de bepalingen van Titel II Wet Verwerking Persoonsgegevens niet van toepassing zijn op deze verwerking.²⁸³
177. **Bevoegde overheden** – De bevoegde overheden die in deze exhaustieve lijst werden opgenomen zijn: de politiediensten, de Algemene inspectie federale en lokale politie, de gerechtelijke overheden, de Dienst Enquêtes P, de Dienst Enquêtes I, de Algemene Administratie Douane en Accijnzen, de Passagiersinformatie-eenheid en de Cel voor Financiële Informatieverwerking.²⁸⁴
178. **Gerechtelijke overheid** – Bijgevolg behoren de gerechtelijke overheden tot de bevoegde overheden in het kader van deze wet.²⁸⁵ Hiertoe behoren de gemeenrechtelijke hoven en rechtbanken, de onderzoeksrechter en het Openbaar Ministerie. De memorie van toelichting bij titel II Wet Verwerking Persoonsgegevens bepaalt bovendien dat met gerechtelijke overheden worden bedoeld, alle instellingen die tot taak hebben de wet te handhaven door geschillen te beslechten. Hieronder behoren de magistraten, rechtbanken en de organen die bijdragen aan het recht spreken binnen de rechterlijke macht. Dit

²⁸² Art. 2 en 3, lid 7 Privacyrichtlijn politie-justitie; DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, 735.; DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 610.; SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 21-25.

²⁸³ Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 65.

²⁸⁴ DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020, 269-304, nr. 740-748.

²⁸⁵ *Ibid.*, nr. 742.

kunnen de griffiers, de colleges van de hoven en rechtbanken en het Openbaar Ministerie zijn.²⁸⁶

179. **Betrokkene** – Bovendien wordt er een onderscheid gemaakt tussen de verschillende betrokkenen, waarvan de persoonsgegevens verwerkt worden. Bijgevolg wordt er onderscheid gemaakt tussen verdachten, veroordeelden, slachtoffers en getuigen.²⁸⁷ Daarnaast moeten persoonsgegevens die op feiten zijn gebaseerd, indien mogelijk worden onderscheiden van persoonsgegevens die op een persoonlijk oordeel zijn gebaseerd.²⁸⁸
180. **Rechtmatige verwerking** – Een verwerking van persoonsgegevens is rechtmatig, indien ze noodzakelijk is voor de uitvoering van een opdracht. Daarnaast moet er een legitiem doel worden nagestreefd, dit doel is de verwerking de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Voorts moet de verwerking gebaseerd zijn op een wettelijke of reglementaire verplichting.²⁸⁹ Deze verplichting moet ten minste de categorieën van persoonsgegevens bepalen, die verwerkt mogen worden. Daarnaast moet deze wettelijke verplichting de doeleinden van deze verwerking bepalen.²⁹⁰
181. **Rechtmatige verwerking gevoelige gegevens** – Met betrekking tot gevoelige gegevens bepaalt de Wet Verwerking Persoonsgegevens dat deze gegevens slechts verwerkt mogen worden, indien er aan één van de opgenomen voorwaarden is voldaan. Ten eerste mogen gevoelige gegevens verwerkt worden indien dit volgens de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst is toegestaan. Ten tweede mogen deze gegevens verwerkt worden, indien de verwerking noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een andere natuurlijke persoon. Ten laatste is het mogelijk om deze gegevens te verwerken indien de verwerking betrekking heeft op gegevens die kennelijk openbaar werden gemaakt door de betrokkene.
182. **Passende waarborgen gevoelige gegevens** – Bovendien bepaalt de wet dat er voor de verwerking van gevoelige gegevens, passende waarborgen moeten worden genomen. Zo moet er voor de verwerking ten minste worden voorzien, dat de bevoegde overheid of de verwerkingsverantwoordelijke een lijst van de categorieën van personen die toegang hebben tot de persoonsgegevens opstelt. Daarboven moet een beschrijving worden

²⁸⁶ Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 60.; Art. 26, 7°, b Wet Verwerking Persoonsgegevens

²⁸⁷ Art. 6 Privacyrichtlijn politie-justitie

²⁸⁸ Art. 32, §1 Wet Verwerking Persoonsgegevens; DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 611.

²⁸⁹ Art. 37, §2 Wet Verwerking Persoonsgegevens

²⁹⁰ SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 70-72.

²⁹⁰ Art. 33 Wet Verwerking Persoonsgegevens

opgesteld, van de hoedanigheid van deze personen, ten opzichte van de verwerking van de beoogde gegevens. Voorts moet deze lijst ter beschikking worden gehouden van de bevoegde toezichthoudende autoriteit. Daarboven moet de bevoegde overheid erover waken, dat de aangewezen personen door een wettelijke of statutaire verplichting of door een evenwaardige contractuele bepaling ertoe gehouden zijn, het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.²⁹¹

183. **Verwerking** – Bovendien moeten alle persoonsgegevens op een rechtmatige en eerlijke manier worden verwerkt.²⁹² Dit betekent dat ze moeten worden verwerkt voor een welbepaald, uitdrukkelijk omschreven en legitiem doel. Dit heeft tot gevolg dat de gegevens niet op een wijze mogen worden verwerkt, die onverenigbaar is met het nagestreefde doel. Daarnaast moeten de gegevens toereikend zijn en ter zake dienend. Bovendien mogen de gegevens niet bovenmatig zijn in verhouding met de doeleinden, waarvoor de gegevens worden verwerkt. Voorts moeten de gegevens correct zijn, indien nodig moeten de gegevens worden geactualiseerd. De gegevens moeten daarnaast bewaard worden in een vorm, die het mogelijk maakt om de betrokkene niet langer te laten identificeren dan noodzakelijk is voor het verwerkingsdoel. Bovendien moet er gebruik worden gemaakt van passende technische of organisatorische maatregelen, op een manier die de beveiliging waarborgt. Zo moeten de gegevens beschermd zijn tegen een ongeoorloofde of onrechtmatige verwerking, tegen opzettelijk verlies, vernietiging en beschadiging.²⁹³
184. **Beginnelsen van de verwerking** – Bovenstaande regels zijn de beginselen van de verwerking.²⁹⁴ Deze beginselen zijn het finaliteitsbeginsel, het eerlijke- en rechtmatigheidsbeginsel, het beginsel van verenigbare verdere verwerking, nauwkeurige toereikende en bijgewerkte gegevens, ter zake dienende en niet-overmatige gegevens en de bewaringstermijn. In principe zijn deze beginselen dezelfde beginselen van verwerking, als deze die door de GDPR werden gewaarborgd. In tegenstelling tot de GDPR, werd het beginsel van transparantie niet opgenomen in de privacyrichtlijn politie-justitie of de omzetting hiervan.²⁹⁵
185. **Parlementaire voorbereiding** - Uit de parlementaire stukken blijkt dat iedere verwerking van persoonsgegevens ten aanzien van een natuurlijk persoon rechtmatig, behoorlijk en transparant moet zijn.²⁹⁶ Bovendien moet de verwerking geschieden met het

²⁹¹ Art. 34 Wet Verwerking Persoonsgegevens

²⁹² Art. 28 Wet Verwerking Persoonsgegevens

²⁹³ Art. 28 Wet Verwerking Persoonsgegevens; DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 633-634.

²⁹⁴ *Supra* nr. 183.

²⁹⁵ Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 71.; DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 633.

²⁹⁶ Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 70-71.

oog op specifieke, bij wet vastgestelde doeleinden. Bovendien mogen rechtshandavingsinstanties activiteiten verrichten met het oog op voorkoming, het onderzoek, de opsporing van strafbare feiten of de vervolging van strafbare feiten, de uitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Echter moeten deze activiteiten bij wet worden vastgesteld en een noodzakelijke, evenredige maatregel vormen in een democratische samenleving, met inachtneming van de legitieme belangen van de natuurlijke persoon, wiens gegevens verwerkt worden.²⁹⁷

186. **Noodzakelijkheid en proportionaliteit** – Bovendien wordt in de parlementaire stukken benadrukt dat er niet bovenmatig veel gegevens mogen worden verzameld. Daarnaast mogen deze gegevens niet langer worden bewaard dan noodzakelijk is, in het kader van het verwerkingsdoel. Voorts mogen gegevens enkel verwerkt worden, indien het doel van de verwerking niet redelijkerwijs op een andere manier kan worden verwezenlijkt.²⁹⁸

²⁹⁷ *Ibid.*, 70.

²⁹⁸ *Ibid.*

Deel V: Vergelijking met de Verenigde Staten

187. **Inleiding** - In het kader van dit onderzoek zal er een rechtsvergelijkend onderzoek gevoerd worden met de Verenigde Staten. In dit deel zal volgende subvraag onderzocht worden: *'Op welke manier wordt de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Amerikaanse overheid in het kader van het strafonderzoek in de Verenigde Staten geregeld?'*. Er wordt specifiek gekozen om een vergelijking te maken met de Verenigde Staten, aangezien daar veel data wordt opgeslagen. Voorts is de industrie van de dataverzamelingsbedrijven in de Verenigde Staten succesvol en actief. Bovendien zijn de grootste dataverzamelingsbedrijven gelegen in de Verenigde Staten.²⁹⁹ Daarnaast worden dataverzamelingsbedrijven, die data opslaan en verkopen, in de Verenigde Staten 'data brokers' genoemd.³⁰⁰ Bijgevolg zal er in dit deel voornamelijk geanalyseerd worden welke regelgeving er in de Verenigde Staten reeds bestaat met betrekking tot dit thema. Bovendien zal er kort worden ingegaan op het opvragen van persoonsgegevens door de Amerikaanse overheid bij Google. Daarnaast zullen de gelijkenissen en verschillen met België aangehaald worden.
188. **Grondwet Amerika** – Vooreerst verbiedt het vierde amendement van de Amerikaanse Grondwet huiszoekingen en inbeslagnames, indien deze onredelijk zijn. Dit amendement bepaalt: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Bijgevolg hebben Amerikaanse burgers het recht om beschermd te worden in hun huizen. Bovendien worden ook de bezittingen van burgers beschermd. Voorts moeten bevelschriften worden verleend door een rechter of magistraat. Bovendien moeten deze bevelschriften gerechtvaardigd worden door een aannemelijke oorzaak. Ook moeten de bevelschriften een eed of verklaring bevatten en een beschrijving van de te onderzoeken plaats, de in beslag te nemen goederen of de personen die moeten worden aangehouden.³⁰¹
189. **Gebrek aan wetgeving** - In de Verenigde Staten bestaan er federale wetten en deelstaatwetten. Op dit ogenblik bestaat er nog geen wet op federaal niveau die bepalingen betreft omtrent de verwerking van persoonsgegevens door dataverzamelingsbedrijven. Desalniettemin bestaan er wel deelstaatwetten, die betrekking hebben op de verwerking van persoonsgegevens door dataverzamelingsbedrijven. Deze deelstaatwetten werden uitgevaardigd door de deelstaten Vermont en Californië.³⁰²
190. **Vermont Consumer Protection Act** - De deelstaatwet die Vermont uitvaardigde, is de Vermont Consumer Protection Act. Deze wet verplicht dataverzamelingsbedrijven

²⁹⁹ RUSHMEIER, H. 'Data Brokers and European Digital Legislation: What are data brokers?' *EDPL* 2023/1, 28.

³⁰⁰ *Ibid.*

³⁰¹ U.S. Const. amend. IV. (1789).

³⁰² California State Legislature. (2018). *California Consumer Privacy Act of 2018*, Cal. Civ. Code § 1798.100 et seq. Vermont General Assembly. (n.d.). *Vermont Consumer Protection Act*, 9 V.S.A. § 2451 et seq.

transparant te zijn over de manier waarop deze bedrijven persoonsgegevens verzamelen, gebruiken en delen.³⁰³

191. **California Consumer Privacy Act** – Daarnaast regelt ook de deelstaatwet van Californië de verwerking van persoonsgegevens door dataverzamelingsbedrijven. Dit wordt geregeld door de California Consumer Privacy act of 2018.³⁰⁴ Deze wet verplicht dataverzamelingsbedrijven om hun praktijken met betrekking tot de privacy van personen openbaar te maken. Bovendien krijgen gebruikers op basis van deze deelstaatwet bepaalde rechten met betrekking tot hun persoonsgegevens.³⁰⁵ Op deze manier krijgen gebruikers meer controle over hun persoonlijke gegevens, die door dataverzamelingsbedrijven worden opgeslagen.³⁰⁶
192. **Recht op informatie** – Daarnaast hebben personen op basis van deze wet het recht om te weten welke persoonlijke informatie een bedrijf over hen verzamelt en op welke manier deze informatie wordt gebruikt en gedeeld. Bovendien hebben personen het recht om persoonlijke informatie die verzameld werd, te laten verwijderen. Voorts hebben personen het recht af te zien van de verkoop of het delen van hun persoonlijke informatie. Ook hebben ze het recht op non-discriminatie bij het uitoefenen van de rechten die ze door deze wet verkregen hebben.³⁰⁷
193. **Recht op rectificatie** – Bovendien werden er in november 2020 nog twee nieuwe rechten toegevoegd. Daardoor hebben personen het recht om onjuiste informatie die een bedrijf over deze persoon verzameld, te laten corrigeren. Bovendien hebben personen het recht om het gebruik en de openbaarmaking van gevoelige persoonlijke informatie die over hen werd verzameld te beperken.³⁰⁸
194. **Privacy Act** – Op federaal niveau bestaat er de gewone privacywet, dit is The Privacy Act of 1974. Deze privacywet bepaalt regels omtrent de verzameling, de bewaring, het gebruik en de verspreiding van persoonsgegevens over individuen door federale agentschappen. Bovendien verplicht de privacywet agentschappen om personen te informeren, omtrent het documentensysteem dat deze agentschappen gebruiken. Voorts hebben personen het recht om toegang te krijgen tot hun dossier en kunnen personen bewaarde gegevens laten corrigeren. Daarnaast worden er regels opgesteld omtrent het bijhouden van dossiers door het agentschap.³⁰⁹ Daarboven verbiedt deze wet de openbaarmaking van persoonsgegevens uit een bestandsysteem, zonder de schriftelijke toestemming van de betrokkene.

³⁰³ Vermont General Assembly. (n.d.). *Vermont Consumer Protection Act*, 9 V.S.A. § 2451 et seq.

³⁰⁴ BENSOUSSAN, A., HENROTTE, J., GALLARDO, M. en FANTI, S., [General Data Protection Regulation] Annexes,, Wolters Kluwer, 2018, 439-572.

³⁰⁵ California State Legislature. (2018). *California Consumer Privacy Act of 2018*, Cal. Civ. Code § 1798.100 et seq.

³⁰⁶ *Ibid.*

³⁰⁷ *Ibid.*

³⁰⁸ *Ibid.*

³⁰⁹ *Ibid.*

195. **Uitzonderingen** - Echter bestaan op deze schriftelijke toestemming een aantal uitzonderingen, in welk geval de toestemming van de betrokkene niet vereist is. Eén van deze uitzonderingen 'de law enforcement request': "No agency shall disclose any record which is contained in a system of records ...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure would be to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought."³¹⁰
196. **Gevolg Privacy Act** - Dit heeft tot gevolg dat, wanneer persoonsgegevens worden doorgegeven aan een andere instantie, met inbegrip van een instantie onder jurisdictie of toezicht van de Verenigde Staten, voor een civielrechtelijke of strafrechtelijke wethandhavingsactiviteit, en indien deze activiteit wettelijk is toegestaan, geen schriftelijke toestemming van de betrokkene vereist is, op voorwaarde dat het hoofd van de ontvangende instantie een schriftelijk verzoek heeft ingediend bij de instantie die de gegevens bewaard. Dit verzoek moet duidelijk het gewenste deel en de activiteit waarvoor de gegevens worden opgevraagd vermelden.³¹¹ Indien aan deze voorwaarden is voldaan, kunnen de gegevens overgemaakt worden zonder de toestemming van de betrokkene.
197. **CLOUD-act** – Voorts werd in 2018 de Cloud-act aangenomen. Deze act geeft opsporings- en veiligheidsdiensten het recht om gegevens te vorderen van Amerikaanse providers van elektronische communicatiediensten. Bovendien kunnen de opsporings- en veiligheidsdiensten deze gegevens opvragen, indien providers in andere landen gelokaliseerd zijn. Indien de diensten gegevens opvragen van providers, die in andere landen gelokaliseerd zijn, kan dit strijdig zijn met de regels met betrekking tot de GDPR. Om dit probleem te verhelpen, kunnen lidstaten bilaterale verdragen sluiten met de Verenigde Staten. Hierin kunnen er regels worden uitgewerkt, met betrekking tot de overdracht van deze gegevens.³¹²
198. **Google** – Bovendien kunnen de Verenigde Staten door zich op de Cloud-act te beroepen, gegevens opvragen bij Google. Google LLC is een Amerikaans bedrijf, waarop de Amerikaanse wetgeving bijgevolg van toepassing zal zijn. Indien de Amerikaanse overheid in het kader van een strafonderzoek persoonsgegevens wil verkrijgen van Google, zal de overheid een gerechtelijk bevel moeten verkrijgen voor de verstrekking van niet-content gegevens. Bijgevolg kan enkel op die manier de overdracht van persoonsgegevens worden

³¹⁰ I.S.C. §552a (b)(7) (2018). *California Consumer Privacy Act of 2018*, Cal. Civ. Code § 1798.100 et seq.

³¹¹ *Ibid.*

³¹² U.S. Congress. (2018). *Clarifying Lawful Overseas Use of Data Act* (H.R. 4943).

afgedwongen. Bovendien moet de overheid beschikken over een huiszoekingsbevel, indien de overheid gegevens omtrent de inhoud van de communicatie wil verkrijgen.³¹³

199. **Google geolocatie-gegevens** – Om te achterhalen wie de Capitool-bestormers van 6 januari 2021 zijn, vroeg de Amerikaanse overheid persoonsgegevens op bij Google. Hierbij vroeg de overheid bij Google de geolocatie-gegevens op van personen die gebruik maken van de functie 'locatiegeschiedenis'. Deze functie registreert de locaties van personen in een tijdlijn. Bijgevolg gaf Google de gegevens door van de personen, die zich op het moment van de bestorming rondom het Capitool bevonden.³¹⁴
200. **NSL** – Daarboven kan de overheid, indien de aanvraag tot het verkrijgen van gegevens betrekking heeft tot de nationale veiligheid, een 'National Security Letter' gebruiken om de overdracht van de gegevens af te dwingen bij Google. Hiervoor is geen rechtelijke toestemming vereist. Echter zullen hierbij slechts beperkte gegevens van abonnees worden overgedragen.³¹⁵
201. **FISA** – Daarnaast kan de overheid FISA-bevelen gebruiken. FISA-bevelen zijn machtigingen die worden verleend onder de Foreign Intelligence Surveillance Act. Deze bevelen kunnen worden gebruikt voor elektronische toezicht en de verstrekking van opgeslagen gegevens af te dwingen bij GOOGLE.
202. **Informereren aan betrokkene** – Bovendien informeert Google de gebruiker van het account over het verzoek van de overheid. Daarentegen wordt de gebruiker niet geïnformeerd, indien dit wettelijk verboden is.³¹⁶
203. **Vergelijking** – Wanneer de aankoop van persoonsgegevens bij commerciële dataverzamelingsbedrijven in de Verenigde Staten wordt vergeleken met België, valt op dat er net zoals in België, in de Verenigde Staten geen specifieke regelgeving bestaat, die deze handeling regelt. In tegenstelling tot België, bestaat er in de Verenigde Staten wel wetgeving met betrekking tot het opvragen van persoonsgegevens bij dataverzamelingsbedrijven of met de betrekking tot de verwerking van persoonsgegevens door dataverzamelingsbedrijven. Deze regelgeving wordt in de Verenigde Staten opgenomen in de twee deelstaatswetten, van Vermont en Californië. Ook de Cloud-act en de Privacy Act zijn in dit kader relevant. Bovendien kan de Amerikaanse overheid op basis van deze Cloud-act persoonsgegevens opvragen bij Google. Zo werden in de Verenigde Staten zelfs persoonsgegevens opgevraagd bij Google, om te achterhalen wie de Capitool-

³¹³ U.S. Congress. (2018). *Clarifying Lawful Overseas Use of Data Act* (H.R. 4943).

³¹⁴ WEINER, R. en HARWELL, D. 'Google location data was used to find Jan. 6 rioters. It's disappearing', *The Washington Post* 8 januari 2024, <https://www.washingtonpost.com/dc-md-vi/2024/01/06/jan-6-google-location-warrants/> (geraadpleegd op 19 juli 2025).

³¹⁵ Google, 'Government requests', *Google Transparency Report* 20 januari 2025, <https://transparencyreport.google.com/governmentrequests> (geraadpleegd op 18 juli 2025)

³¹⁶ *Ibid.*

bestormers zijn. Daarnaast kan de Amerikaanse overheid ook persoonsgegevens opvragen bij Google door middel van een NSL of FISA-bevel.

Deel VI. De aankoop van persoonsgegevens bij dataverzamelingsbedrijven in de praktijk

Hoofdstuk I. Ethische gevaren en belangenconflict

204. **Inleiding** - In dit hoofdstuk zal de volgende subvraag onderzocht worden: 'Welke ethische gevaren kunnen er bestaan bij een overheid die betaalt voor informatie in het kader van het strafrechtelijk onderzoek?' In dit hoofdstuk zal worden onderzocht welke de ethische gevaren zijn van een overheid die betaalt voor informatie, in de plaats van deze informatie zelf te gaan zoeken. Hierbij zal er vergeleken worden met de ethische gevaren, die kunnen bestaan bij het betalen van getuigen en informanten, in ruil voor informatie. Daarbij zal de vergoeding van getuigen en informaten besproken worden. Daarnaast zal er onderzocht worden of er een belangenconflict kan bestaan, wanneer de overheid persoonsgegevens aankoopt bij dataverzamelingsbedrijven.

Afdeling I. Vergoeding getuigen en informaten

205. **Vergoeding getuigen** - Vooreerst worden getuigen betaald om een getuigenis af te leggen. De vergoeding waar de getuige recht op heeft, door het afleggen van een getuigenis in strafzaken, wordt gelijkgesteld met gerechtskosten.³¹⁷ Bovendien hebben getuigen recht op een vergoeding voor bepaalde verplaatsingskosten.³¹⁸ Deze verplaatsingskosten worden berekend per afgelegde kilometer. Het tarief dat een getuige ontvangt voor het afleggen van een getuigenis, bedraagt in het jaar 2025, tweeëntwintig euro en vijftien cent.³¹⁹
206. **Gunst informanten** - Bovendien hebben informanten ook recht op een vergoeding, deze vergoeding is een gunst. Deze gunsten verdient de informant in ruil voor de informatie die hij geeft en voor de veiligheidsrisico's die de informant lijdt. Vooreerst kunnen gunsten uitsluitend worden toegekend aan, in het nationaal controlesysteem geregistreerde informanten. Voorts moeten deze gunsten worden aangevraagd door de lokale informantenbeheerder. Nadien moeten de gunsten door de nationale informantenbeheerder toegekend worden. Daarboven worden de gunsten toegekend in functie van het verstrekken van correcte informatie, in het bijzonder, het verstrekken van correcte en nog niet bekende informatie die leidde tot een nieuw onderzoek, informatie die het succes van een lopend onderzoek in belangrijke mate heeft beïnvloed of die criminele processen of samenwerkingsverbanden zichtbaar maakt of een beter inzicht hierover verschaft. Daarboven wordt bij het bepalen van de gunst minstens rekening gehouden met

³¹⁷ Art. 42, 5° KB Gerechtskosten

³¹⁸ Art. 29-32 KB Gerechtskosten

³¹⁹ Omz. 131/12 over de indexering van de tarieven van de gerechtskosten in strafzaken en de gelijkgestelde kosten, BS 9 januari 2025, 1346.

het belang van de informatie voor het uiteindelijke resultaat, het gelopen risico inzake de afscherming van de informant, de prioriteit van het fenomeen of de dader of dadergroep.³²⁰

Afdeling II. Ethische gevaren

207. **Inleiding** - In deze afdeling zullen de ethische gevaren, die er volgens mijn bescheiden mening bestaan, met betrekking tot de aankoop van informatie door de overheid worden geanalyseerd. Hierbij zal een vergelijking worden gemaakt, met de ethische gevaren die kunnen bestaan met betrekking tot het betalen van getuigen en informanten.
208. **Onjuiste informatie** - Vooreerst bestaat het gevaar dat de persoonsgegevens die de overheid aankoopt bij dataverzamelingsbedrijven, niet juist zijn of niet volledig zijn. Daarnaast bestaat er het gevaar dat er een onjuist beeld van de realiteit wordt gevormd, indien verschillende gegevens met elkaar worden verweven. Wanneer de bedrijven bovendien worden betaald voor het verstrekken van deze gegevens, kan het zijn dat bedrijven vooral aan de winstmarge van hun bedrijf zullen denken, in de plaats van het vooruithelpen van het strafonderzoek. Wanneer dataverzamelingsbedrijven gegevens doorgeven, om een vergoeding van de overheid te krijgen, kan het zijn dat de bedrijven bewust gegevens doorgeven die niet volledig zijn of niet correct zijn. Daarbij kan het gevaar bestaan dat de dataverzamelingsbedrijven de privacyregels zullen schenden, zodat deze bedrijven meer informatie aan de overheid kunnen verkopen en bijgevolg meer kunnen verdienen. Bijgevolg zou dit de integriteit van het strafonderzoek in gedrang kunnen brengen
209. **Vergelijking getuigen en informanten** - In vergelijking met getuigen en informanten, kan het zijn dat de getuigen of informanten bewust of onbewust verkeerde informatie geven. Dit kan het geval zijn indien ze zichzelf willen beschermen of anderen in diskrediet willen brengen. Met betrekking tot getuigen, bestaat volgens mij niet het gevaar dat de getuigen foute informatie zullen doorgeven om geld te verdienen, aangezien de vergoeding die getuigen ontvangen slechts gering is. Bij informanten daarentegen, zou het wel kunnen dat de informanten bewust verkeerde informatie doorgeven of extra informatie verzinnen, om aanspraak te kunnen maken op een vergoeding of om een hogere vergoeding te krijgen. De geldelijke gunst, waar informanten recht op hebben, varieert immers naargelang de informatie.
210. **Criminele feiten** - Een gevoeligheid op ethisch vlak met betrekking tot informanten is dat informanten, informatie moeten verkrijgen door zelf eventueel strafbare feiten te plegen, aangezien zij zich begeven in het crimineel milieu, om informatie te verkrijgen. Daarbij kan het in bepaalde gevallen ook voorkomen, dat informanten doen alsof ze meewerken met de overheid, maar in de realiteit nog steeds tot het crimineel milieu behoren. Naar mijns inziens is dit niet vergelijkbaar met de aankoop van persoonsgegevens bij

³²⁰ Art. 8 KB 6 januari 2011 tot bepaling van de werkingsregels van de nationale en lokale informantenbeheerders en van de contactambtenaren, BS 18 januari 2011.; BERKMOES, H., *Informatenwerking (bijzondere opsporingsmethoden)*, Wolters Kluwer, 2022, 187-188.

dataverzamelingsbedrijven. Aangezien dataverzamelingsbedrijven immers geenszins strafbare feiten moeten plegen om de informatie te verzamelen. Van dataverzamelingsbedrijven wordt bovendien verwacht dat deze bedrijven de regels, waaronder de privacyregels, strikt naleven.

211. **Concurrerende bedrijven** - Voorts zou het kunnen dat dataverzamelingsbedrijven onderling zullen concurreren om diensten te mogen leveren aan de overheid, daardoor kan het ook zijn dat de bedrijven, misschien sneller privacyregels zullen kunnen schenden, om meer informatie te bekomen. Dataverzamelingsbedrijven zouden immers meer winst kunnen maken, indien hun bedrijf gegevens kan verkopen aan de overheid.
212. **Algoritmes** - Bovendien bestaat het gevaar dat de grote hoeveelheid aan gegevens door artificiële intelligentie of algoritmes gefilterd wordt. Daardoor kan het zijn dat de gegevens niet op een objectieve manier geselecteerd worden. Daarnaast kan het gevaar bestaan dat de algoritmes, informatie filteren op basis van discriminerende elementen. Hierdoor kan er bijvoorbeeld discriminatie ontstaan, met betrekking tot personen van een andere etnische afkomst of personen met een ander geloofsovertuiging. In vergelijking met getuigen en informanten, kan het zijn dat ook getuigen en informanten informatie geven, die beïnvloed is door hun eigen mening en eigen ervaringen. Bijgevolg kan het hierdoor zijn dat ook deze informatie niet volledig objectief is of een vertekende versie van de waarheid is. Daarnaast kunnen getuigen of informanten ook discrimineren. Daardoor zouden getuigen of informanten, bijvoorbeeld indien ze racistisch zouden zijn, informatie kunnen doorgeven die vertekend is, door een bepaald beeld dat deze getuigen of informanten hebben.
213. **Vertrouwen burger** – Daarnaast bestaat het gevaar dat de burger de overheid minder vertrouwt, indien de overheid persoonsgegevens van deze burgers aankoopt en op deze manier zeer veel informatie over het privéleven van een persoon kan verkrijgen.
214. **Overmatige gegevens** – Indien de overheid onbeperkt toegang heeft tot persoonsgegevens via dataverzamelingsbedrijven, kan dit bovendien leiden tot ongepaste of buitensporige overheidscontrole. Hierbij bestaat het gevaar dat de overheid de aangekochte gegevens niet louter in het kader van het strafonderzoek zou gebruiken, maar ook voor controle over de burgers of om bepaalde gedragingen van burgers te achterhalen.

Afdeling III. Belangenconflict overheid

215. **Belangenconflict** – Het zou eventueel mogelijk zijn dat er een belangenconflict bestaat in hoofde van de overheid, indien de overheid persoonsgegevens aankoopt bij dataverzamelingsbedrijven. Aangezien de overheid er immers belang bij zou kunnen hebben, dat dataverzamelingsbedrijven de privacyregels niet correct naleven. Een schending van deze regels, zou er dan bijgevolg toe leiden dat de overheid meer informatie kan verkrijgen.
216. **Gedrag** - Om dit te verhelpen kan de overheid specifieke regels of een soort van gedragscode opstellen, die bepaalt welke gegevens de overheid kan aankopen. De overheid kan dan beslissen om uitsluitend informatie aan te kopen, indien de gegevens verkregen zijn, zonder een inbreuk te maken op de regels van het gegevensbeschermingsrecht.
217. **Gegevensbeschermingsautoriteit** - Bovendien houdt de Gegevensbeschermingsautoriteit toezicht op de verwerking van persoonsgegevens door bedrijven. Bijgevolg oefent de Gegevensbeschermingsautoriteit toezicht uit op de verwerking van persoonsgegevens door dataverzamelingsbedrijven.³²¹ Dus zelfs indien het de overheid ten goede zou kunnen komen, als dataverzamelingsbedrijven de regels niet correct naleven, de gegevensbeschermingsautoriteit controleert de verwerking van persoonsgegevens door deze bedrijven en kan deze bestraffen indien nodig.
218. **Uitbesteding aan buitenlandse bedrijven** – Daarnaast zou de overheid eventueel aan buitenlandse, private bedrijven, kunnen uitbesteden, wat de overheid zelf niet mag doen. Bijgevolg zou de overheid dan in het buitenland persoonsgegevens kunnen laten bewaren en aankopen. Dit zou ethisch niet correct zijn, aangezien daardoor de persoonsgegevens van Belgische rijkswoners, in het buitenland zouden terechtkomen. Voorts zou het kunnen dat het bedrijf waar de overheid dan mee samenwerkt gelegen is, in een land dat minder strikte gegevensbeschermingsrechten heeft als België, waardoor de gegevens niet voldoende beschermd zijn.

³²¹ *Infra.* nr. 274.

Hoofdstuk II. Voordeel handeling ten opzichte van andere middelen

219. **Inleiding** - In dit hoofdstuk zal besproken worden wat dataverzamelingsbedrijven zijn, welke gegevens deze bedrijven bewaren en op welke manier deze bedrijven persoonsgegevens kunnen verzamelen. Bovendien zal volgende onderzoeksvraag verder onderzocht worden, op basis van de informatie, die onderzocht werd in het beschrijvend gedeelte: 'Hoe verhoudt de aankoop van persoonsgegevens door de overheid bij dataverzamelingsbedrijven zich tot andere onderzoekshandelingen?'. Hierbij zal worden nagegaan of de aankoop van persoonsgegevens bij dataverzamelingsbedrijven in het kader van het strafonderzoek al dan niet zou kunnen worden beschouwd als een onderzoekshandeling. Daarnaast wordt geanalyseerd, op welke aspecten de onderzochte handeling verschilt met de opvraging van gegevens op wettelijke basis, zoeking in een informatica- en communicatiesysteem en beslag. Hierbij wordt specifiek vergeleken met deze handelingen, aangezien deze handelingen ook betrekking hebben op het verkrijgen van persoonsgegevens in het kader van het strafonderzoek. Er zal worden bekeken waarom de aankoop van persoonsgegevens bij dataverzamelingsbedrijven, een voordeel zou kunnen opleveren in het kader van het strafonderzoek. Daarbij zal onderzocht worden, waarom deze handeling nuttig kan zijn in vergelijking met andere middelen.

Afdeling I. Dataverzamelingsbedrijven

220. **Dataverzamelingsbedrijven** – Dataverzamelingsbedrijven zijn bedrijven die gegevens van burgers verzamelen, bewaren en verkopen. Wanneer deze gegevens worden verzameld, kunnen deze gegevens eventueel worden samengevoegd tot gedetailleerde profielen. Meestal worden de persoonsgegevens verkocht zonder medeweten of toestemming van de betrokkene.³²²
221. **Gegevens** - Er bestaat geen exhaustieve lijst van de gegevens die dataverzamelingsbedrijven verzamelen. Enkele voorbeelden van de gegevens die dataverzamelingsbedrijven verzamelen zijn, onder andere identiteits- en contactgegevens, zoals een naam, geboortedatum, telefoonnummers, e-mailadressen, adressen... Bovendien kunnen deze bedrijven demografische gegevens verzamelen, zoals geslacht, leeftijd, etniciteit, burgerlijke staat, opleiding, of het beroep. Daarnaast kunnen dataverzamelingsbedrijven gegevens met betrekking tot het onlinegedrag van personen verzamelen, zoals bezochte websites, zoekgeschiedenis, aangeklikte advertenties, activiteiten op sociale media, online aankopen en inschrijvingen voor nieuwsbrieven. Daarboven kunnen locatiegegevens worden verzameld en koopgewoonten, zoals het winkelgedrag van personen, merkvoorkeuren, klantenkaarten, abonnementen en geanonimiseerd creditcardgebruik. Bovendien kunnen deze bedrijven financiële gegevens verzamelen of gezondheidsgegevens verzamelen. Evenzo kunnen gegevens met betrekking tot een persoon zijn levensstijl en overtuigingen worden verzameld, zoals

³²²Beslissing Gegevensbeschermingsautoriteit
ECLI:BE:GBAPD:2022:DEC.20221116.6.

hobby's, politieke voorkeur, religieuze voorkeur, persoonlijkheidskenmerken en mediagewoonten. Daarboven kunnen gegevens met betrekking tot sociale en professionele connecties bewaard worden, zoals informatie over de gezinsleden van een persoon, over familieleden, vrienden, collega's... en nog vele andere informatie.³²³

222. **Verzamelmethode** - Deze gegevens worden verzameld door middel van publieke gegevens. Daarnaast kunnen deze gegevens worden verzameld door middel van commerciële data, die verkregen wordt door middel van de aankoopgeschiedenis, loyaliteitsprogramma's, garantiebewijzen... Voorts kunnen deze gegevens worden verzameld door middel van online tracking, dit gebeurt dan door middel van cookies en trackers. Bovendien kunnen gegevens met betrekking tot sociale media verzameld worden, zoals openbare berichten, likes, volgers, check-ins... Evenzo kunnen gegevens verzameld worden, wanneer bedrijven gebruikersgegevens doorverkopen. Vaak wordt de verkoop van persoonsgegevens opgenomen in de servicevoorwaarden. Bijgevolg aanvaarden personen deze servicevoorwaarden vaak, zonder deze te lezen. Ook kunnen gegevens verzameld worden door het invullen van enquêtes of winacties, waarbij gebruikers vrijwillig hun gegevens meedelen. Daarnaast kunnen locatiegegevens verzameld worden, doorat personen om gebruik te maken van bepaalde apps, hun toestemming voor GPS-toegang geven, door foto's met geolocatie, door WIFI-connecties. Dit is bijvoorbeeld het geval bij weerapps of fitnessapps. Ook gegevens met betrekking tot de gezondheid van een persoon, kunnen worden verzameld op basis van gezondheidsapps, die bijvoorbeeld het hartritme meten of het slaapritme controleren.³²⁴ Naar mijns inziens zouden deze gegevens zowel kunnen worden aangekocht in het kader van proactieve recherche als reactieve recherche. De onderzoekshandeling zou bovendien zowel betrekking kunnen hebben op het aankopen van persoonsgegevens van een individueel persoon, als op het aankopen van persoonsgegevens van meerdere personen of een bepaalde groep personen.³²⁵

³²³ CONSTANTINESCU, E., 'What are data brokers, and how do they work?', *Proton* 20 juni 2025, [https://proton.me/blog/databrokers#:~:text=Data%20brokers%20are%20companies%20or,campaigns%20\(for%20voter%20targeting\)](https://proton.me/blog/databrokers#:~:text=Data%20brokers%20are%20companies%20or,campaigns%20(for%20voter%20targeting)) (geraadpleegd op 25 juli 2025).

³²⁴ STEVENS, D., 'Privacybescherming', *Computerr*. 2023/1, (72) 72-82.; DELFORGE, A., *La jurisprudence de l'APD en matière de marketing direct*, Intersentia, 2024, 119-138, nr. 36-39.; DE BOIS, A., *Commercieel gebruik van persoonsgegevens*, Intersentia, 2017, 1-62, nr. 42-43.; CONSTANTINESCU, E., 'What are data brokers, and how do they work?', *Proton* 20 juni 2025, [https://proton.me/blog/databrokers#:~:text=Data%20brokers%20are%20companies%20or,campaigns%20\(for%20voter%20targeting\)](https://proton.me/blog/databrokers#:~:text=Data%20brokers%20are%20companies%20or,campaigns%20(for%20voter%20targeting)) (geraadpleegd op 25 juli 2025).

³²⁵ *Supra* nr. 4-8.

Afdeling II. Verschil met opvragen gegevens op basis van wettelijke regels, zoeking in het informatica- en communicatiesysteem en beslag

223. **Onderzoekshandeling** - Naar mijn mening, zou de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de overheid in het kader van het strafonderzoek, kunnen worden beschouwd als een onderzoekshandeling. Aangezien deze handeling, zoals hierboven reeds uiteengezet werd, vergelijkbaar is met andere onderzoekshandelingen.³²⁶ Bovendien bestaan er ook andere onderzoekshandelingen die betrekking hebben op het verkrijgen van persoonsgegevens. Deze persoonsgegevens kunnen dan worden opgevraagd bij telecomoperatoren, dienstenverstrekkers van communicatie of bankinstellingen of deze gegevens kunnen verkregen worden door de zoeking in het informatica- en communicatiesysteem en deze data kan in beslag genomen worden. Als deze handelingen worden beschouwd als onderzoekshandelingen, dan kan de onderzochte handeling mijns inziens ook worden beschouwd als onderzoekshandeling. Daarboven worden bij de aankoop van persoonsgegevens bij dataverzamelingsbedrijven, nog andere gegevens en meer gegevens verkregen dan bij de andere onderzoekshandelingen. Waarbij het in bepaalde gevallen, mijns inziens nog ingrijpender zou kunnen zijn, wanneer de aankoop betrekking heeft op gevoelige gegevens. Daarom zie ik bijgevolg geen redenen waarom deze handeling niet als onderzoekshandeling zou kunnen worden beschouwd.
224. **Verschil met gegevens opvragen** - Naar mijn mening verschilt de aankoop van persoonsgegevens bij dataverzamelingsbedrijven van de opvraging van gegevens op wettelijke basis, aangezien deze opvraging van gegevens betrekking heeft op gegevens waarover telecomoperatoren, dienstenverstrekkers van communicatie en bankinstellingen over beschikken.³²⁷ Hierbij werd het opvragen van gegevens bij dataverzamelingsbedrijven niet opgenomen. Daarboven is er naar mijns inziens een verschil met betrekking tot de gegevens die kunnen worden verkregen. In het kader van het opvragen van gegevens, hebben de gegevens betrekking op de informatie waarover telecomoperatoren of bankinstelling beschikken. De gegevens die kunnen worden aangekocht bij dataverzamelingsbedrijven zijn mijns inziens ruimer, aangezien deze gegevens ook betrekking hebben op andere soorten informatie.
225. **Databeslag opsporingsonderzoek** - Naar mijn mening verschilt deze handeling ook van het beslag, waaronder het databeslag dat door de procureur des Konings kan worden gelegd.³²⁸ Aangezien de procureur des Konings uitsluitend beslag kan leggen op de gegevens die zich reeds op de materiële drager bevinden, hierbij moet de internetconnectie uitgezet worden. Mij lijkt hierbij dat de gegevens waarover dataverzamelingsbedrijven beschikken, ruimer kunnen zijn dan deze die een persoon reeds heeft opgeslagen op een materiële gegevensdrager. Enkele gegevens zouden waarschijnlijk overeenstemmen, maar mijns inziens zullen de gegevens waarover databedrijven beschikken niet standaard op een laptop of smartphone of dergelijke, aanwezig zijn. Denk maar aan gegevens die

³²⁶ *Supra* nr. 56 e.v.

³²⁷ *Supra* nr. 58-66.

³²⁸ *Supra* nr. 67-79.

dataverzamelingsbedrijven verkrijgen op basis van cookies, enquêtes of gegevens die deze bedrijven verkregen door apps, niet al deze gegevens staan ook opgeslagen op de computer van een persoon. Bovendien kan het zijn dat bepaalde informatie niet langer terug te vinden is op een materiële gegevensdrager, terwijl dataverzamelingsbedrijven deze informatie eventueel wel hebben opgeslagen.

226. **Zoeking** – Mijns inziens is de onderzochte handeling meer vergelijkbaar met de zoeking in het informatica- en communicatiesysteem door de onderzoeksrechter en klassiek of databaseslag, op de informatie die verkregen werd door middel van deze zoeking, door de onderzoeksrechter.³²⁹ Volgens mij kunnen er door de zoeking in het communicatie- en informaticasysteem, gelijkaardige gegevens gevonden worden als bij de onderzochte handeling. Mijns inziens zullen de aangekochte gegevens bij dataverzamelingsbedrijven ook betrekking hebben op informatie die niet met de zoeking kan worden verkregen. Bovendien zal er door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven een grotere hoeveelheid gegevens worden verkregen. Daarboven zal de aankoop waarschijnlijk in een kortere tijdspanne, gegevens opleveren dan een zoeking.

³²⁹ Art. 39bis, §4-6 Sv.

Afdeling III. Nut aankoop persoonsgegevens bij dataverzamelingsbedrijven

227. **Nut handeling** – Mijns inziens kan de aankoop van persoonsgegevens bij dataverzamelingsbedrijven nuttig zijn in het kader van het strafonderzoek, aangezien er informatie kan verzameld worden, die misschien niet door middel van andere middelen kan worden achterhaald. Het grootse verschil met betrekking tot andere middelen is, mijns inziens, de hoeveelheid van informatie die kan worden verkregen, in tegenstelling tot de andere middelen en de snelheid van het verkrijgen van deze gegevens. Een ander voordeel is daarboven, dat de overheid de informatie niet zelf moet zoeken. Volgens mij kan er met geen van de andere middelen, op zich staand, dezelfde informatie en dezelfde hoeveelheid aan informatie worden verkregen. Eventueel zou het mogelijk zijn om gelijkaardige gegevens en dezelfde hoeveelheid gegevens te verkrijgen door verschillende onderzoekshandelingen te combineren, maar dan nog lijkt het mij sterk dat er dan evenveel gegevens zouden worden verzameld.
228. **Verschillen** – Het aankopen van persoonsgegevens bij dataverzamelingsbedrijven, in de plaats van deze zelf te zoeken, zou tijd kunnen besparen. Zo zou de procureur des Konings of de onderzoeksrechter en politiediensten niet meer ter plaatste moet gaan voor bijvoorbeeld een huiszoeking of beslag. Door de tijd die deze actoren besparen, kunnen zij meer werk steken in andere taken. Daardoor kunnen deze actoren efficiënter werken. Bovendien is er minder medewerking nodig van andere actoren, zoals telecomoperatoren, bankinstellingen of IT'ers, die bijvoorbeeld de beveiliging van een informaticasysteem moeten opheffen.
229. **Voorbeeld 1** - Hierbij zal ik enkele voorbeelden toelichten, die het nut van de handeling, ten opzichte van andere middelen duiden. Bijvoorbeeld, dataverzamelingsbedrijven kunnen informatie met betrekking tot gezondheidsapps verkopen, bepaalde van deze apps slaan gegevens op over de hartslag van een persoon. In het kader van het strafonderzoek, zou op basis van deze gegevens onderzocht kunnen worden, hoe hoog de hartslag van een verdachte of in verdenking gestelde was op het moment van de criminele feiten. Bijgevolg zou het bijvoorbeeld kunnen, hierbij wens ik te benadrukken dat dit natuurlijk niet altijd zo is, dat de hartslag van een persoon hoger is, wanneer iemand een moord pleegt. Deze gegevens kunnen mijns inziens niet door middel van andere middelen verkregen worden, tenzij deze gegevens kunnen worden teruggevonden in het kader van de zoeking in het informatica- en communicatiesysteem.
230. **Voorbeeld 2** - Door middel van locatiegegevens uit apps of foto's met geolocatie, kan gesitueerd worden waar een persoon zich op een bepaald moment bevond, er zijn zelfs apps die de volledige route die een persoon aflegt precies opslaan. Deze gegevens kunnen aangekocht worden bij dataverzamelingsbedrijven. Daarnaast kunnen deze gegevens eventueel ook verkregen worden door het onderzoek bij telecomoperatoren, door zendmastbepalingen, door ANPR-gegevens of camera's. Wanneer deze gegevens op die manier worden verkregen, zal de route waarschijnlijk nog moeten worden geconstrueerd.

Terwijl bij de aankoop van gegevens, deze gegevens meteen ter beschikking staan. Dit kan bijgevolg tijd besparen en eventueel kan de route die kan worden aangekocht, zelf nog preciezer zijn.

231. **Voorbeelden** - Door middel van de gegevens die worden aangekocht, kan onderzocht worden met welke personen iemand contact heeft. Dit kan ook opgespoord worden door andere technieken, zoals het opsporen van elektronische communicatie of een zoeking in het informatica- en communicatiesysteem, maar waarschijnlijk beschikken de dataverzamelingsbedrijven over nog ruimere informatie en er moet niet worden samengewerkt met de telecomoperatoren of er moet niet in een systeem naar informatie worden gezocht. Daarnaast kunnen er gegevens worden aangekocht, die betrekking hebben op het koopgedrag van een persoon. Op basis van deze gegevens zou kunnen worden onderzocht of er in het kader van een overval bijvoorbeeld verdachte voorwerpen werden gekocht. Hiervoor kan dan de koopgeschiedenis van de verdachte onderzocht worden. Deze gegevens zouden waarschijnlijk ook door andere middelen worden gezocht, maar als de koopgeschiedenis kan worden aangekocht bespaart het tijd en eventueel kan de koopgeschiedenis duidelijker en preciezer zijn.
232. **Historische gegevens** - Een groot verschil is volgens mij ook, dat bijvoorbeeld met betrekking tot telecomoperatoren, de gegevens slechts een beperkte tijd mogen worden bewaard, op basis van de dataretentiewetten. Dataverzamelingsbedrijven zullen de gegevens waarschijnlijk voor een langere termijn bijhouden, aangezien er voor dataverzamelingsbedrijven geen verplichting bestaat om bepaalde gegevens bij te houden. Wel moeten dataverzamelingsbedrijven de regels, die werden opgenomen in de AVG naleven. Daarboven zou het ook kunnen dat bepaalde informatie, ook door middel van een zoeking in het communicatie- en informaticasysteem kan worden verkregen. Echter zou het kunnen dat een persoon bijvoorbeeld vaak van laptop of smartphone wisselt of bepaalde informatie niet meer terug te vinden is in het systeem. Terwijl die informatie wel werd opgeslagen door dataverzamelingsbedrijven. Bovendien zitten gegevens bij dataverzamelingsbedrijven verspreidt over verschillende dataverzamelingsbedrijven, in de plaats dat alle gegevens bij één bedrijf werden opgeslagen.
233. **Onderzoek** - Hierbij moet wel worden benadrukt dat de grote hoeveelheid informatie niet automatisch een voordeel is. Zo werd er reeds onderzoek gedaan, waaruit bleek dat meer informatie niet noodzakelijk een groter voordeel oplevert. Uit dit onderzoek van het Controleorgaan op de politionele organisatie, bleek dat de grote hoeveelheid aan data niet altijd betere resultaten oplevert, aangezien gegevens in bepaalde gevallen onbruikbaar

kunnen zijn.³³⁰ In dit onderzoek was de databank gericht op terrorisme, er waren veel hits maar er waren ook veel valse matches.³³¹

³³⁰ COC, 'Bijzonder toezicht op de passagiersinformatie-eenheid door het Controleorgaan op de politionele informatie in het kader van zijn controle en toezichtbevoegdheden als bevoegde Toeziendhoudende autoriteit', *Controleorgaan op de politionele informatie 11 oktober 2022*, www.controleorgaan.be/files/DAB21001-Rapport-BELPIE_Publieke-versie_nl_00069899.pdf (geraadpleegd op 27 juli 2025).

³³¹ *Ibid.*

Hoofdstuk III. Bevelen handeling

234. **Inleiding** - In deze afdeling zal worden geanalyseerd waar de handeling zich situeert in het strafonderzoek en wie bevoegd is om de handeling te bevelen. Hierbij zal op basis van de indeling van persoonsgegevens nagegaan worden, of deze handeling al dan niet een dwangmaatregel uitmaakt. Op basis daarvan zal worden bepaald of de onderzoeksrechter of de procureurs des Konings bevoegd is. Daarboven zal er worden onderzocht bij welke misdrijven, of met welke minimumstraf misdrijven moeten worden bestraft, om deze handeling te kunnen bevelen.
235. **Gevoeligheid gegevens** - Zoals reeds besproken kunnen persoonsgegevens ingedeeld worden in 'gewone', dit wil zeggen niet-gevoelige gegevens, en gevoelige gegevens. Gevoelige gegevens zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon of gegevens over gezondheid of gegevens met betrekking tot iemand seksueel gedrag of seksuele gerichtheid.³³²
236. **Dwangmaatregel** - Een dwangmaatregel is een maatregel, die de inbreuk van de fundamentele rechten van een persoon tot gevolg kan hebben. Mijns inziens zullen 'gewone' gegevens niet direct de fundamentele rechten schenden. Daarom zou de aankoop en het gebruik in het strafonderzoek van 'gewone' gegevens, volgens mij geen dwangmaatregel uitmaken. Gevoelige gegevens daarentegen zouden mijns inziens, wel een schending van de fundamentele rechten tot gevolg kunnen hebben. Bijgevolg kan de aankoop en het gebruik van gevoelige gegevens, naar mijns inziens wel beschouwd worden als een dwangmaatregel. Zoals reeds besproken, kan de procureur des Konings geen onderzoekshandelingen uitvoeren die een dwangmaatregel uitmaken, behoudens uitzonderingen, bijvoorbeeld in het kader van een situatie op heterdaad.³³³ De onderzoeksrechter kan wel onderzoekshandelingen uitvoeren die een dwangmaatregel uitmaken.³³⁴
237. **Bevoegd voor aankoop** - Mijns inziens is de procureur des Konings bevoegd voor de aankoop van persoonsgegevens, indien deze aankoop betrekking heeft op niet-gevoelige gegevens. Aangezien er dan geen sprake is van een dwangmaatregel. De onderzoeksrechter kan niet-gevoelige aankopen, indien er een gerechtelijk onderzoek werd ingesteld.

³³² DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019, 451-492, nr. 16.; Art. 9 en 34 Wet Verwerking Persoonsgegevens; 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. 55-2572/001, 226.; CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593, nr. 614.

³³³ *Supra* nr. 48-49.

³³⁴ *Supra* nr. 50.

238. **Onderzoeksrechter** - Wanneer de aankoop betrekking heeft op gevoelige gegevens, zouden deze naar mijn mening, aangezien de aankoop van gevoelige gegevens een dwangmaatregel zou uitmaken, in principe uitsluitend kunnen worden bevolen door de onderzoeksrechter.
239. **Uitzonderingen** - Eventueel zou er kunnen worden voorzien dat de procureur des Konings gevoelige gegevens kan aankopen, indien er een heterdaadsituatie bestaat, vergelijkbaar met andere onderzoekshandelingen.³³⁵ Zo kan bijvoorbeeld de procureur des Konings een huiszoeking bevelen wanneer er sprake is van een heterdaadssituatie. Bijgevolg zou er bijvoorbeeld kunnen worden beslist, dat de aankoop van gevoelige gegevens door de procureur des Konings, mogelijk is bij een ontdekking op heterdaad van een gijzeling, een wederrechtelijke vrijheidsbeneming, afpersing, bij het plegen van een terroristisch misdrijf of wanneer er gedreigd wordt met het plegen van een terroristisch misdrijf. Dit zou vergelijkbaar zijn met de situaties van heterdaad, waarbij de procureur des Konings een zoeking in het informatica- en communicatiesysteem kan bevelen.³³⁶ De procureur des Konings zou bovendien de handeling kunnen bevelen, indien er een geldige toestemming werd verkregen van de betrokkene.³³⁷ Hierbij moet er op worden gewezen dat met betrekking tot de zoeking in een informatica- en communicatiesysteem, het EHRM reeds oordeelde dat een toestemming met de zoeking, onder dreiging van de uitvoering van de zoeking, deze toestemming de inmenging in het recht op privacy niet uitsluit.³³⁸
240. **Mini-instructie** – Daarboven zou deze handeling mijns inziens kunnen worden uitgevoerd door middel van een mini-instructie. De handeling is immers niet opgenomen in de lijst van onderzoekshandelingen, waarbij een mini-instructie is uitgesloten.³³⁹ Echter zou de handeling ook kunnen worden uitgesloten van de mini-instructie, aangezien de handeling zo ingrijpend is. De gegevens die verkregen worden door de zoeking in een informatica- en communicatiesysteem zijn vergelijkbaar, met de gegevens die verkregen worden door middel van de aankoop van gegevens bij dataverzamelingsbedrijven. Aangezien deze onderzoekshandeling werd uitgesloten van de mini-instructie, zou het naar mijn inziens een logisch gevolg zijn dat de aankoop van persoonsgegevens bij dataverzamelingsbedrijven ook wordt uitgesloten van de mini-instructie. Aangezien er bij de aankoop van persoonsgegevens, waarschijnlijk nog een grotere hoeveelheid gegevens verkregen wordt.³⁴⁰
241. **Minimumstraf of ernstige criminele feiten** - Bij de aankoop van gevoelige gegevens moet de grondrechtsbescherming gewaarborgd worden. Daarom moet de inmenging onder meer noodzakelijk, proportioneel en subsidiair zijn. Bovendien moet zowel bij gevoelige,

³³⁵ *Supra* nr. 56 e.v.

³³⁶ *Supra* nr. 99.

³³⁷ *Supra* nr. 56 e.v. en nr. 153.

³³⁸ CONINGS, C. *Klassiek en digitaal speuren naar strafrechtelijk bewijs: Normatief kader*, Intersentia, 2017, 379-593, nr. 630.; EHRM 18 april 2013, 26419/10.

³³⁹ BRULOOT, D., DE GROOTE, B. en DE CORTE, R., *Privaatrecht in hoofdlijnen: Strafrecht en strafrechtspleging*, LeA Uitgevers, 2022, 346, nr. 523.

³⁴⁰ Art. 28septies Sv.

als niet-gevoelige gegevens de privacyrichtlijn politie-justitie worden nageleefd. Zo bepaalt ook deze richtlijn, dat de verwerking van persoonsgegevens noodzakelijk, proportioneel en subsidiair moet zijn, om rechtmatig te zijn. Met betrekking tot de vereisten van noodzakelijkheid en proportionaliteit, zou ervoor kunnen worden geopteerd om te bepalen dat de onderzoekshandeling, bijvoorbeeld pas kan worden bevolen, indien er ernstige aanwijzingen bestaan, dat de gepleegde misdrijven kunnen worden gestraft met een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf. Het bepalen van een minimumstraf, zou vergelijkbaar zijn met het opvragen van bankgegevens.³⁴¹ Eventueel zou er met betrekking tot de aankoop van gevoelige gegevens, aangezien deze handeling ingrijpend zou zijn, eventueel kunnen worden geopteerd voor een hogere minimumstraf, van bijvoorbeeld twee jaar. Naar mijns inziens, zou de grondrechtsbescherming echter nog meer gewaarborgd zijn, indien de handeling uitsluitend kan worden bevolen, bij onderzoek naar ernstige criminele feiten. Om te bepalen welke criminele feiten, kan de lijst met strafbare feiten, opgenomen in artikel 90ter, §2-4 Sv. worden gebruikt. Aangezien de lijst van strafbare feiten, die werden opgenomen in dit artikel, in het wetboek van strafvordering meerdere malen wordt gehanteerd als drempel voor de proportionaliteitsvereiste, voor wat betreft de opsporingsmethoden die het meest ingrijpend zijn in de persoonlijke levenssfeer.³⁴²

242. **Niet-gevoelige gegevens** – Met betrekking tot de aankoop van niet-gevoelige gegevens, kan dan bepaald worden dat de handeling bij alle misdrijven mogelijk is. Om te voldoen aan de proportionaliteitsvereiste, kan er mijns inziens voor worden geopteerd, om te bepalen dat de handeling slechts mogelijk is, indien er ernstige aanwijzingen bestaan, dat de gepleegde misdrijven kunnen worden gestraft met een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf.
243. **Bevelschrift** - De procureur des Konings of de onderzoeksrechter kunnen, naargelang de aard van de informatie beslissen om de aankoop te bevelen. Mijns inziens kan de aankoop worden bevolen, door middel van een bevelschrift. Hierin kan meegedeeld worden op welke gegevens de aankoop precies betrekking heeft en kunnen de feitelijke omstandigheden van de zaak worden uiteengezet, die deze maatregel rechtvaardigen. Tevens dient de procureur des Konings of de onderzoeksrechter, die de handeling beveelt, de noodzakelijkheid, proportionaliteit en subsidiariteit van de maatregel te verantwoorden, met inachtneming van de persoonlijke levenssfeer van de betrokkene. Zo moet onder andere, bij de huiszoeking en het opvragen van elektronische communicatie ook een bevelschrift worden opgesteld.³⁴³

³⁴¹ *Supra* nr. 62.

³⁴² *Supra* nr. 94-96.

³⁴³ *Supra* nr. 92 en 105.

Hoofdstuk IV. Procedurele waarborgen

244. **Inleiding** – In deze afdeling zal de volgende onderzoeksvraag geanalyseerd worden: 'Welke procedurele waarborgen kunnen worden ingevoerd om de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht te waarborgen?' Bovendien zal op basis van de gegevens die werden onderzocht in het beschrijvend gedeelte, de volgende onderzoeksvraag verder geanalyseerd worden: 'Welke privacy en fundamentele rechten kunnen eventueel worden geschonden door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek?'. Naargelang de aard van de persoonsgegevens, niet-gevoelige of gevoelige gegevens, zouden er eventueel fundamentele rechten kunnen geschonden worden. In dit hoofdstuk zal worden nagegaan, waarom bepaalde fundamentele rechten al dan niet kunnen worden geschonden, door de aankoop van persoonsgegevens. Om de fundamentele rechten, met inbegrip van het gegevensbeschermingsrecht van de betrokkene zoveel mogelijk te waarborgen, kunnen er bovendien procedurele waarborgen worden ingevoerd. Om het gegevensbeschermingsrecht te waarborgen, moeten de regels van de privacyrichtlijn politie-justitie worden nageleefd. Doorheen deze afdeling zullen de procedurele waarborgen worden besproken.

Afdeling I. Inmenging fundamentele rechten

245. **Inleiding** – In het beschrijvend gedeelte van deze masterproef werden een aantal fundamentele rechten besproken.³⁴⁴ Deze fundamentele rechten zouden eventueel geschonden kunnen worden, door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven. Zo zou eventueel het recht op een eerlijk proces, het recht op privacy, met inbegrip van het recht op eerbiediging van het privéleven en het recht op bescherming van persoonsgegevens³⁴⁵, het recht op gelijkheid en non-discriminatie³⁴⁶ en het recht op vrije meningsuiting³⁴⁷ kunnen worden geschonden.
246. **Aard informatie** – Hierbij moet worden herhaald, dat de aankoop van persoonsgegevens bij dataverzamelingsbedrijven met betrekking tot niet-gevoelige gegevens, mijns inziens waarschijnlijk geen inbreuk van de fundamentele rechten tot gevolg zal hebben.³⁴⁸ Daarentegen zal de aankoop van gevoelige gegevens eventueel wel kunnen leiden tot een schending van de fundamentele rechten.³⁴⁹ Om deze redenen zal in dit kader alleen de eventuele schending van fundamentele rechten met betrekking tot de aankoop van gevoelige persoonsgegevens worden besproken
247. **Schending recht op eerlijk proces** – Naar mijn bescheiden mening zou het recht op een eerlijk proces in strafzaken, door de handeling, kunnen worden geschonden.³⁵⁰ Aangezien het gevolg van de aankoop van persoonsgegevens, zou kunnen zijn dat bewijs op een onrechtmatige wijze wordt verkregen.³⁵¹ Daarnaast zou de vereiste transparantie, om een eerlijk proces te voeren, kunnen verdwijnen. Bovendien kan de hoeveelheid aan informatie worden beschouwd als bulkdata. Hierdoor zou het moeilijker kunnen zijn voor de verwerende partij, om te weten welke data werd gebruikt om de strafbare feiten te onderzoeken. Daarnaast kan de wapengelijkheid in het gedrang komen. Aangezien het Openbaar Ministerie, als vervolgende partij, dan over meer mogelijkheden beschikt dan de verwerende partij. Daarboven is het niet zeker of de gegevens die worden aangekocht effectief betrouwbaar zijn, waardoor ook het recht op een eerlijk proces kan worden geschonden.
248. **Schending recht op privacy** – Daarnaast zou mijns inziens het recht op privacy kunnen worden geschonden, aangezien de overheid ongewenst zou binnendringen in het privéleven van de betrokkene.³⁵² Aangezien er door de aangekochte gegevens veel informatie over het privéleven van de betrokkene kan worden blootgelegd. Echter bepaalt de privacyrichtlijn politie-justitie dat de gegevens kunnen worden verwerkt, in het kader

³⁴⁴ *Supra* nr. 114 e.v.

³⁴⁵ Art. 8 EVRM

³⁴⁶ Art. 10-11 GW

³⁴⁷ Art. 10 EVRM

³⁴⁸ *Supra* nr. 236.

³⁴⁹ *Ibid.*

³⁵⁰ *Supra* nr. 116-122.

³⁵¹ HUYBRECHTS, L. en ROZIE, M., 'De rechten van de verdediging bij de behandeling ten gronde', NC 2008/2, (106) 109-111, nr. 18-29.

³⁵² *Supra* nr. 123-137.

van de opsporing en het onderzoek naar strafbare feiten, indien er aan bepaalde voorwaarden werd voldaan.³⁵³ Wanneer niet aan deze voorwaarden werd voldaan, kan het recht op privacy worden geschonden. Bovendien kan het recht op privacy worden geschonden, indien de procureur des Konings de aankoop van gevoelige gegevens zou bevelen, zonder dat er een geldige toestemming van de betrokkene werd verkregen en zonder dat er een heterdaadsituatie bestaat. Aangezien de procureur des Konings niet bevoegd is om dwangmaatregelen uit te oefenen, behoudens in uitzonderlijke omstandigheden. Daarboven zou het recht op privacy kunnen worden geschonden, indien de onderzoeksrechter de aankoop van gevoelige gegevens beveelt, terwijl er niet voldaan is aan de vereisten van het bestaan van een wettelijke basis, een legitiem doel na te streven, noodzakelijkheid, proportionaliteit en subsidiariteit. Daarnaast kan het recht op privacy worden geschonden, indien de verwerking niet geschiedt volgens de regels opgenomen in Titel II Wet Verwerking Persoonsgegevens, bijvoorbeeld de regels met betrekking tot de beveiliging van gegevens, regels omtrent gebruik voor andere doeleinden, regels omtrent doorgifte...³⁵⁴

249. **Schending recht op gelijkheid en non-discriminatie** – Naar mijns inziens kan bovendien het recht op gelijkheid en non-discriminatie worden geschonden door de onderzochte handeling.³⁵⁵ Aangezien dataverzamelingsbedrijven, naar mijn mening immers van bepaalde personen zeer veel informatie kunnen verzamelen en van anderen slechts weinig. Doordat sommige personen zeer veel gebruik maken van internet of apps en daardoor informatie delen en andere personen slechts weinig. Daarboven zouden dataverzamelingsbedrijven, bijvoorbeeld minder gegevens kunnen verzamelen van personen die hun gegevens beter weten te beveiligen of dergelijke. Echter is naar mijns inziens de voornaamste reden dat het recht op gelijkheid en non-discriminatie zou kunnen worden geschonden, de filtering van de grote hoeveelheid data op basis van algoritmes, die misschien data selecteren op basis van criteria, die discriminerend kunnen zijn.
250. **Schending recht op vrije meningsuiting** - Het recht op vrije meningsuiting zou naar mijns inziens, eventueel kunnen worden geschonden.³⁵⁶ Aangezien het gebruik van aangekochte gegevens kan leiden tot een afschrikkend effect op personen die bepaalde standpunten willen uiten, hun mening willen uitspreken of bepaalde activiteiten willen ondernemen. Bijgevolg zou dit kunnen leiden tot zelfcensuur, aangezien personen zich zorgen kunnen maken over de gevolgen van het uiten van hun mening. Hierdoor durven personen bijvoorbeeld misschien minder te delen of minder hun mening te uiten op het internet.

³⁵³ *Supra* nr. 180.

³⁵⁴ Art. 25-71 Wet Verwerking Persoonsgegevens

³⁵⁵ *Supra* nr. 138-140

³⁵⁶ *Supra* nr. 141-142.

251. **Rechtvaardiging inmenging** – Zoals bleek uit het onderzoek, kan de overheid een inmenging in de fundamentele rechten rechtvaardigen.³⁵⁷ Hiervoor moet er voldaan zijn aan bepaalde voorwaarden. Deze voorwaarden zijn het bestaan van een wettelijke basis, het nastreven van een legitiem doel en de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit van de inmenging.³⁵⁸ Bijgevolg zal de grondrechtsbescherming gewaarborgd zijn, indien aan deze voorwaarden is voldaan. Mijns inziens moet de procureur des Konings, respectievelijk de onderzoeksrechter, wanneer hij de aankoop beveelt nagaan of de inbreuk noodzakelijk, proportioneel en subsidiair is.
252. **Wettelijke basis** – Op dit moment bestaat er geen specifiek, duidelijk regelgevend kader over de aankoop van persoonsgegevens. Echter vormt dit geen probleem, aangezien andere bestaande regelgeving, zoals het wetboek van strafvordering of andere regels, naar mijn mening een voldoende wettelijke basis zijn. Wel zou mijns inziens een grotere grondrechtsbescherming bestaan, indien er een duidelijk wetgevend kader bestaat, dan wanneer er geen duidelijk wetgevend kader bestaat. In deze regelgeving zouden passende waarborgen kunnen worden opgenomen, bijvoorbeeld welke persoonsgegevens kunnen worden aangekocht, voor welke doeleinden worden deze gegevens kunnen worden verwerkt, wie deze persoonsgegevens kan opvragen... Het is belangrijk dat de wet, bijvoorbeeld het wetboek van strafvordering toegankelijk wordt gemaakt voor de burgers. Daarnaast moet de wet duidelijk opgesteld zijn, zodat burgers de rechtsgevolgen van hun handelen kunnen inschatten. Met betrekking tot de transparantie, kan de overheid meedelen aan de burger dat de overheid persoonsgegevens kan aankopen bij dataverzamelingsbedrijven in het kader van het strafonderzoek en welke gegevens er kunnen worden aangekocht.
253. **Legitiem doel** – Daarnaast moet er een legitiem doel worden nagestreefd. Dit doel zou mijns inziens in het kader van het strafonderzoek, bijvoorbeeld de veiligheid van het land, de openbare veiligheid en de bescherming van de openbare orde of de verwerking, de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid kunnen zijn.³⁵⁹ Ook andere legitieme doelen zijn mogelijk. Bijgevolg is mijns inziens voldaan aan deze voorwaarde.
254. **Noodzakelijkheid** – Opdat de handeling noodzakelijk moet zijn, moet de handeling voldoen aan de vereisten van subsidiariteit en proportionaliteit. De handeling is noodzakelijk, indien deze handeling nodig is om onderzoek te voeren naar strafbare feiten. Met betrekking tot de noodzakelijkheid, mogen er niet meer gegevens bewaard worden dan nodig.

³⁵⁷ *Supra* nr. 115.

³⁵⁸ SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het stafprocesrecht en politierecht: De wet op het politieambt na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie*, die Keure, 2023, 295-381, nr. 2.

³⁵⁹ Art. 27 Wet Verwerking Persoonsgegevens

255. **Subsidiariteit** – Om te voldoen aan de vereiste van de subsidiariteit, mogen er geen minder ingrijpende maatregelen voorhanden zijn, dan de aankoop van persoonsgegevens bij dataverzamelingsbedrijven. Bijgevolg moet indien er een minder ingrijpende maatregel bestaat, geopteerd worden voor de minst ingrijpende maatregel. Bijgevolg zal de vereiste van subsidiariteit niet voldaan zijn, indien er gekozen werd voor de aankoop van gegevens, terwijl er andere minder ingrijpende maatregelen voorhanden waren. Indien bijvoorbeeld de gegevens kunnen verkregen worden door de geldige toestemming van een betrokkene of door een gewone opzoeking, moet voor deze minder ingrijpende maatregelen worden gekozen.
256. **Proportionaliteit** – Daarnaast mag de onderzoekshandeling niet verder reiken dan nodig is om een bepaald doel te bereiken, om aan de vereiste van proportionaliteit te voldoen. Bijgevolg moet de handeling in verhouding zijn tot het nagestreefde doel. Het doel dat nagestreefd wordt in het kader van het strafonderzoek, is het achterhalen van de waarheid. Mijns inziens zal de onderzoekshandeling bijvoorbeeld niet proportioneel zijn indien de handeling wordt toegepast, bij het onderzoeken van minder ernstige misdrijven, bijvoorbeeld een diefstal zonder braak. Daarentegen zal de handeling wel proportioneel zijn indien er onderzoek wordt gevoerd naar ernstige criminele feiten. Om deze proportionaliteit te beoordelen kan er verwezen worden naar de misdrijven opgenomen in artikel 90ter, §2-4 Sv., aangezien deze misdrijven meerdere keren worden gebruikt als drempel voor de proportionaliteitsvereiste voor wat betreft de opsporingsmethoden die het meest ingrijpend zijn in de persoonlijke levenssfeer.³⁶⁰ Bijgevolg zou er om de proportionaliteit te waarborgen, kunnen worden beslist om gegevens uitsluitend op te vragen, indien er onderzoek wordt gedaan naar misdrijven, die worden beschouwd als ernstige misdrijven.³⁶¹
257. **Parameters** – Hierbij zullen er enkele parameters aangereikt worden die naar mijn bescheiden mening, kunnen gebruikt om de proportionaliteit te beoordelen. Vooreerst kan de doelmatigheid van de handeling worden gebruikt als criterium. Hierbij verwijst doelmatigheid naar de vraag of de handeling of inbreuk op het fundamentele recht daadwerkelijk bijdraagt aan het beoogde doel. Bijvoorbeeld, wanneer verzamelde gegevens niet bruikbaar zijn of niet kunnen bijdragen aan het gestelde doel, kan de handeling als disproportioneel worden beschouwd. Bijgevolg moeten gegevens effectief kunnen bijdragen aan het strafonderzoek. Ook wanneer er gegevens worden verzameld die niet relevant zijn voor het onderzoek of overmatig veel gegevens worden verzameld, kan de handeling als disproportioneel worden beschouwd. Stel bijvoorbeeld dat er in de loop der tijd meer onderzoek wordt gevoerd naar de effectiviteit van het gebruik van gegevens, verkregen uit informatie die dataverzamelingsbedrijven opslaan en hieruit blijkt dat de informatie niet of slechts in beperkte mate kan bijdragen aan het doel van het

³⁶⁰ *Supra* nr. 94-96.

³⁶¹ *Supra* nr. 94.; Art. 90ter, §1-4 Sv.

strafonderzoek, dan zou de handeling, mijns inziens niet langer proportioneel kunnen zijn. Tenzij de effectiviteit kan worden verbeterd.

258. **Belangenafweging** - Daarnaast kan er een belangenafweging worden gemaakt, om de proportionaliteit te beoordelen. Hierbij wordt de mate van schade voor de betrokkene afgewogen tegen het beoogde doel. Zo kan het bijvoorbeeld gerechtvaardigd zijn om meer ingrijpende maatregelen te nemen in onderzoeken naar zwaardere criminaliteit, terwijl dit minder proportioneel zou zijn bij lichtere misdrijven. Het nadeel voor de betrokkene moet dus in verhouding staan tot het beoogde doel, waarbij moet worden nagegaan of het nadeel groot of gering is.
259. **Aard gegevens en hoeveelheid** – Bovendien spelen de aard van de gegevens en de hoeveelheid van de verzamelde gegevens een rol, bij de beoordeling van de proportionaliteit. Hoe gevoeliger de informatie is of hoe groter de hoeveelheid gegevens, des te sterker moet de rechtvaardiging voor het ingrijpen zijn. Aangezien de proportionaliteitsvereiste misschien minder snel voldaan is, indien er zeer veel gegevens of bijzonder gevoelige gegevens worden verzameld. De proportionaliteit moet dus altijd zorgvuldig worden beoordeeld, door de mate van inbreuk op de rechten van de betrokkene, de verwachte effectiviteit en noodzakelijkheid van de handeling.
260. **Gegevens van andere personen** - Wanneer er bijvoorbeeld in het kader van reactieve recherche persoonsgegevens aangekocht worden van de verdachte of in verdenking gestelde, dan kunnen de persoonsgegevens gebruikt worden in het strafonderzoek dat tegen deze verdachte of in verdenking gestelde gericht is. In dat geval zou er mijns inziens binnen het vooropgestelde doel gehandeld worden. Echter kan het zijn dat wanneer persoonsgegevens verwerkt worden, er ook informatie verkregen wordt over andere personen. Stel dat hierdoor andere strafbare feiten aan het licht zouden komen, die een andere persoon dan de in verdenking gestelde heeft gepleegd, zou het vooropgestelde doel, mijns inziens voorbij worden gegaan, indien er op basis van deze gegevens een strafonderzoek wordt ingesteld, tegen andere personen.
261. **Gedifferentieerd** – In het beschrijvend deel werden de arresten van het Grondwettelijk Hof geanalyseerd met betrekking tot de dataretentiewetten.³⁶² Hieruit bleek dat het Grondwettelijk Hof oordeelde dat het recht van privacy werd geschonden, indien de gegevens op een ongedifferentieerde manier werden bewaard. Daarom kunnen, mijns inziens, slechts de persoonsgegevens van één of meerdere personen worden opgevraagd en niet alle gegevens, van alle personen waarover het dataverzamelingsbedrijf beschikt.³⁶³ Zo zouden in het kader van proactieve recherche naar mijns inziens enkel gegevens kunnen opgevraagd worden van bepaalde personen waarvan een vermoeden bestaat dat deze personen strafbare feiten hebben gepleegd of zullen plegen. Daarnaast zouden

³⁶² *Supra* nr. 107-113.

³⁶³ CONINGS, C., 'Dataretentieplicht en privacy', *NJW* 2015, (911) 911-913.

bijvoorbeeld de gegevens kunnen worden aangekocht van personen in een bepaald gebied, waar er bijvoorbeeld veel criminele feiten worden gepleegd. Daarnaast zouden in het kader van reactief onderzoek slechts de gegevens van een verdachte of in verdenking gestelde kunnen worden aangekocht.

262. **Voldoende waarborgen** – Bovendien werd in deze rechtspraak het belang van voldoende waarborgen aangetoond, deze kunnen er immers voor zorgen dat het recht op privacy niet geschonden wordt. Zo oordeelde het Grondwettelijk Hof met betrekking tot dataretentiewet III, dat het recht op privacy niet werd geschonden, aangezien de wet bepaald welke data mag worden bewaard en wie bevoegd is om deze op te vragen.³⁶⁴ Wanneer de aankoop van persoonsgegevens zou worden toegepast, zou naar mijn mening in gelijkaardige waarborgen kunnen worden voorzien. Zo kan worden bepaald dat de procureur des Konings, respectievelijk de onderzoeksrechter bevoegd is om de gegevens aan te kopen en andere personen niet. Daarnaast kan er gespecificeerd worden welke persoonsgegevens mogen worden opgevraagd, bijvoorbeeld identificatiegegevens, gezondheidsgegevens, financiële gegevens, gegevens met betrekking tot sociale contacten... Daarnaast mogen er bijvoorbeeld niet bovenmatig veel gegevens worden verwerkt, enkel deze die noodzakelijk zijn in het kader van het strafonderzoek. Eventueel kan er bepaald worden tot welke tijdsperiode historische gegevens mogen worden aangekocht. Bovendien kan er bepaald worden voor welke termijnen persoonsgegevens mogen worden bewaard. Bijvoorbeeld voor ernstige feiten kan er dan bijvoorbeeld langer terug in de tijd worden gegaan of kunnen de gegevens langer bewaard worden.³⁶⁵

³⁶⁴ 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.; CAREEL, S. en ROYER, S., 'Voorontwerp dataretentiewet: derde keer, goede keer?', *Juristenkrant* 2021/432, (10) 10-11.

³⁶⁵ *Supra* nr. 94-96.

Afdeling II. Onderzoekshandeling in overeenstemming met het gegevensbeschermingsrecht

263. **Rechtmatige verwerking** - Wanneer persoonsgegevens verwerkt worden in het kader van het strafonderzoek, moet bij de verwerking van niet-gevoelige en gevoelige gegevens, de regels van de privacyrichtlijn politie-justitie en Titel II van de Wet Verwerking Persoonsgegevens nageleefd worden.³⁶⁶ Er moet een wettelijke basis bestaan, een bepaald legitiem doel worden nagestreefd, de verwerking moet noodzakelijk, proportioneel en subsidiair zijn, zodat de verwerking van persoonsgegevens rechtmatig is.³⁶⁷

Onderafdeling I. Gemeenschappelijke waarborgen niet-gevoelige en gevoelige gegevens

264. **Wettelijke basis** – Met betrekking tot de wettelijke basis, verwijs ik naar hetgeen daarover uiteengezet werd bij de bespreking van de fundamentele rechten.³⁶⁸ In het kader van een rechtmatige verwerking van persoonsgegevens, moet deze verplichting ten minste de categorieën van persoonsgegevens bepalen, die verwerkt mogen worden. Daarnaast moet deze wettelijke verplichting de doeleinden van deze verwerking bepalen.³⁶⁹
265. **Legitiem doel** – Daarboven moeten de gegevens verwerkt worden om een bepaald doel na te streven. Dit doel wordt opgenomen in Titel II van de Wet Verwerking Persoonsgegevens. Deze wet bepaalt dat het doel van de verwerking, de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid moet zijn.³⁷⁰ In het kader van het strafonderzoek wordt dit doel naar mijns inziens nagestreefd, aangezien het strafonderzoek tot doel heeft strafbare feiten op te sporen of te onderzoeken.
266. **Noodzakelijkheid** – Daarnaast moet de verwerking van persoonsgegevens noodzakelijk, proportioneel en subsidiair zijn, om rechtmatig te zijn. Met betrekking tot deze vereisten, verwijs ik naar hetgeen hierover reeds werd uiteengezet bij de bespreking van de fundamentele rechten.³⁷¹ Bovendien moet de verwerking noodzakelijk zijn voor de uitvoering van een opdracht.³⁷²
267. **Waarborgen privacyrichtlijn** - Daarnaast moeten de gegevens volgens de privacyrichtlijn politie-justitie toereikend zijn en ter zake dienend. Bovendien mogen de gegevens niet bovenmatig zijn in verhouding met de doeleinden, waarvoor de gegevens worden verwerkt. Voorts moeten de gegevens correct zijn en indien nodig moeten de gegevens worden geactualiseerd. Daarboven moeten de gegevens bewaard worden in een

³⁶⁶ *Supra* nr. 165 e.v.

³⁶⁷ *Supra* nr. 180-181.

³⁶⁸ *Supra* nr. 252.

³⁶⁹ *Supra* nr. 180.

³⁷⁰ Art. 27 Wet Verwerking Persoonsgegevens

³⁷¹ *Supra* nr. 259-261.

³⁷² *Supra* nr. 180.

vorm, die het mogelijk maakt om de betrokkene niet langer te laten identificeren dan noodzakelijk is voor het verwerkingsdoel. Bovendien moet er gebruik worden gemaakt van passende technische of organisatorische maatregelen, op een manier die de beveiliging waarborgt.³⁷³ Zo moeten de gegevens beschermd zijn tegen een ongeoorloofde of onrechtmatige verwerking, tegen opzettelijk verlies, vernietiging en beschadiging.³⁷⁴

268. **Bewaartermijn** - De memorie van toelichting bij Titel II Wet Verwerking Persoonsgegevens bepaalt daarboven dat er passende termijnen moeten worden vastgelegd voor het wissen van persoonsgegevens, bij het verstrijken van de vastgelegde termijn of voor een periodieke evaluatie van de noodzaak van de opslag of het wissen van persoonsgegevens. De maximale duur kan een aantal jaren zijn, maar ook het optreden van een factor, zoals het overlijden van de betrokkene. Er wordt eveneens voorzien dat er bij het verlopen van de termijn een analyse uitgevoerd wordt, op basis van de proportionaliteits- en noodzakelijkheidscriteria om te bepalen of de bewaring nog nodig is. Indien blijkt dat de bewaring nog nodig en proportioneel is, dan worden de gegevens bewaard gedurende een nieuwe termijn.³⁷⁵ Mijns inziens kan de overheid maximumtermijnen bepalen met betrekking tot de bewaring van persoonsgegevens. Ter vergelijking, in dataretentiewet III, werd bepaald dat gegevens langer kunnen worden bewaard naar gelang er een zwaarder misdrijf of een groter aantal misdrijven werd gepleegd.³⁷⁶ Met betrekking hierbij bepaalt het wetsontwerp bij datarichtlijn III dat hoe meer zware criminaliteit voorkomt,³⁷⁷ hoe dieper de georganiseerde of criminele activiteiten in het arrondissement geworteld zijn, en dus hoe noodzakelijker het is om in de tijd terug te gaan.³⁷⁸ Mijns inziens zouden de gegevens die werden aangekocht om ernstige criminaliteit te onderzoeken³⁷⁹, langer mogen worden bewaard dan bij andere feiten.

³⁷³ *Supra* nr. 183-184.

³⁷⁴ Art. 28 Wet Verwerking Persoonsgegevens; DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024, 385-482, nr. 633-634.

³⁷⁵ Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 73.

³⁷⁶ 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.

³⁷⁷ Art. 90ter, §2-4 Sv.

³⁷⁸ 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. 55-2572/001, 62.

³⁷⁹ *Supra* nr. 94-96.

Onderafdeling II. Bijkomende waarborgen gevoelige gegevens

269. **Verwerking gevoelige gegevens** – Met betrekking tot gevoelige gegevens bepaalt de Wet Verwerking Persoonsgegevens dat deze gegevens slechts verwerkt mogen worden, indien er aan één van de opgenomen voorwaarden is voldaan.³⁸⁰ Ten eerste mogen gevoelige gegevens verwerkt worden, indien dit volgens de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst is toegestaan. Ten tweede mogen deze gegevens verwerkt worden, indien de verwerking noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een andere natuurlijke persoon. Ten laatste is het mogelijk om deze gegevens te verwerken, indien de verwerking betrekking heeft op gegevens die kennelijk openbaar werden gemaakt door de betrokkene.³⁸¹ Mijns inziens is er voldaan aan de vereiste van een wettelijke basis.³⁸² Bijgevolg mogen de gevoelige gegevens naar mijn mening verwerkt worden.
270. **Passende waarborgen** – Bovendien bepaalt de wet dat er voor de verwerking van gevoelige gegevens, passende waarborgen moeten worden genomen. Zo moet er voor de verwerking ten minste worden voorzien, dat de bevoegde overheid of de verwerkingsverantwoordelijke een lijst van de categorieën van personen die toegang hebben tot de persoonsgegevens opstelt.³⁸³ Daarboven moet een beschrijving worden opgesteld, van de hoedanigheid van deze personen, ten opzichte van de verwerking van de beoogde gegevens. Voorts moet deze lijst ter beschikking worden gehouden van de bevoegde toezichthoudende autoriteit. Daarboven moet de bevoegde overheid erover waken, dat de aangewezen personen door een wettelijke of statutaire verplichting of door een evenwaardige contractuele bepaling ertoe gehouden zijn het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.³⁸⁴
271. **Memorie van toelichting** – Daarnaast kunnen er nog andere passende waarborgen worden genomen, om de bescherming van deze gevoelige gegevens te waarborgen. De memorie van toelichting bij Titel II Wet Verwerking Persoonsgegevens bepaalt daaromtrent dat passende waarborgen voor de rechten en vrijheden van de betrokkene, bijvoorbeeld kunnen inhouden dat de gevoelige gegevens enkel mogen worden verzameld in samenhang met andere gegevens over de natuurlijke persoon in kwestie. Bovendien moeten de verzamelde gegevens afdoende kunnen worden beveiligd. Bijgevolg kunnen er strengere regels gelden voor de toegang van het personeel van de bevoegde overheid tot de gegevens. Voorts moet de doorzending van die gegevens worden verboden. De verwerking van die gegevens dient daarbij ook bij wet toegelaten te zijn, wanneer de betrokkene uitdrukkelijk heeft toegestemd met de verwerking die een ingrijpende inbreuk vormt op zijn privacy.³⁸⁵

³⁸⁰ *Supra* nr. 181.

³⁸¹ Art. 34, §1 Wet Verwerking Persoonsgegevens

³⁸² *Supra* nr. 252-264.

³⁸³ *Supra* nr. 182.

³⁸⁴ Art. 34 Wet Verwerking Persoonsgegevens

³⁸⁵ Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001, 78.

272. **Aankoop persoonsgegevens** – Mijns inziens moet de overheid bij de verwerking van gevoelige persoonsgegevens, die werden aangekocht bij dataverzamelingsbedrijven, bovenstaande passende waarborgen effectief invoeren. Op die manier is er een grotere bescherming van het gegevensbeschermingsrecht. Zo kan de overheid naar mijn mening slechts gevoelige gegevens verzamelen, indien deze gegevens samenhangen met niet-gevoelige gegevens. Bijgevolg kunnen louter gevoelige gegevens, op zich staand niet worden aangekocht. Daarbij moet de overheid beveiligde apparaten of netwerken ter beschikking hebben, om de gegevens die werden aangekocht veilig te bewaren. Naar mijn bescheiden mening zullen slechts bepaalde personen, waaronder de procureur des Konings, respectievelijk de onderzoeksrechter toegang mogen hebben tot deze gegevens. Andere personen zouden dan in principe geen toegang mogen hebben tot deze gegevens, tenzij de toegang noodzakelijk is, in het kader van het strafonderzoek.

Afdeling. III. Controle

273. **Inleiding** – Met betrekking tot de procedurele waarborgen, zou er controle kunnen worden uitgevoerd op de bevoegde diensten, zodat deze de aangekochte gegevens niet op een onrechtmatige manier verwerken. Voorts moet er kunnen worden ingegrepen, indien de fundamentele rechten worden geschonden. In deze afdeling zal onderzocht worden of deze controle kan worden uitgeoefend door een specifiek toezichtsorgaan of dat er rechtsmiddelen openstaan voor de betrokkene, wanneer deze meent dat zijn rechten werden geschonden, door de aankoop van persoonsgegevens bij dataverzamelingsbedrijven in het kader van het strafrechtelijk onderzoek.
274. **Toezicht** – Vooreerst is met betrekking tot de verwerking van persoonsgegevens, die niet onder het toepassingsgebied van de privacyrichtlijn politie-justitie behoren, de Gegevensbeschermingsautoriteit bevoegd om toezicht op de verwerking van persoonsgegevens uit te oefenen. De Gegevensbeschermingsautoriteit is een onafhankelijk orgaan en controleert of de regels met betrekking tot de verwerking van persoonsgegevens, correct worden nageleefd.³⁸⁶ Desalniettemin zal de Gegevensbeschermingsautoriteit niet bevoegd zijn, om toezicht uit te oefenen, indien de persoonsgegevens worden verwerkt in het kader van de Wet Verwerking Persoonsgegevens. De Gegevensbeschermingsautoriteit zal wel bevoegd zijn om toezicht uit te oefenen, op de verwerking van persoonsgegevens door de dataverzamelingsbedrijven.
275. **Controleorgaan politionele informatie** – Desalniettemin zal de Gegevensbeschermingsautoriteit niet bevoegd zijn, om toezicht uit te oefenen, indien de persoonsgegevens worden verwerkt in het kader van de Wet Verwerking Persoonsgegevens. In dit geval zal immers het Controleorgaan op de politionele informatie bevoegd zijn om toezicht uit te oefenen op de verwerking van persoonsgegevens, door de bevoegde overheden. Dit controleorgaan is een onafhankelijke toezichthoudende autoriteit.³⁸⁷ Deze onafhankelijke toezichthoudende wordt opgericht door de Kamer van volksvertegenwoordigers.³⁸⁸ Bovendien voert het Controleorgaan naast het uitoefenen van toezicht, andere opdrachten uit die haar door of krachtens bepaalde wetten werden verleend.³⁸⁹
276. **Geen toezicht op onderzoeksrechter** - Echter is het Controleorgaan op de politionele informatie, niet bevoegd om toezicht uit te oefenen, indien persoonsgegevens op basis van Titel II Wet Verwerking Persoonsgegevens, verwerkt worden door de onderzoeksrechter of het Openbaar Ministerie. Dit is het gevolg van de onafhankelijkheid van de onderzoeksrechter. Het Controleorgaan op de politionele informatie zal enkel toezicht

³⁸⁶ Wet 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, BS 10 januari 2018.

³⁸⁷ Art. 71, §1 Wet Verwerking Persoonsgegevens; DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit: Toezicht op de gegevensverwerking*, Wolters Kluwer, 2020, 973-985.

³⁸⁸ Art. 71 Wet Verwerking Persoonsgegevens

³⁸⁹ *Ibid.*

houden, ten aanzien van de geïntegreerde politie, de algemene inspectie van de federale en de lokale politie en de passagiersinformatie-eenheid. Bijgevolg zou het controleorgaan, uitsluitend bevoegd zijn om toezicht uit te oefenen indien, de politiediensten aangekochte persoonsgegevens zouden verwerken.

277. **Geen toezichthoudende overheid** – Kortom, de Gegevensbeschermingsautoriteit en het Controleorgaan op de politionele diensten kunnen geen toezicht houden, indien persoonsgegevens worden verwerkt door de onderzoeksrechter of het Openbaar Ministerie. Bovendien bestaat er in België geen specifiek toezichthoudend orgaan, dat de verwerking van persoonsgegevens in het kader van het strafonderzoek door de procureur des Konings of de onderzoeksrechter controleert.
278. **K.I.** - Tijdens de loop van het strafonderzoek houdt de kamer van inbeschuldigingstelling ambtshalve toezicht op het verloop van het onderzoek. De kamer van inbeschuldigingstelling kan het strafdossier zuiveren van elke onrechtmatigheid. Er kan bij de kamer van inbeschuldigingstelling beroep worden ingesteld tegen een onderzoeksrechter die weigert om een gevraagde onderzoeksdaad uit te voeren of die weigert inzage te geven in het strafdossier. Bovendien is de kamer van inbeschuldigingstelling bevoegd om toezicht te houden op het opsporingsonderzoek en op het gerechtelijk onderzoek.³⁹⁰
279. **Hof van Cassatie** – Bovendien zullen er wel rechtsmiddelen ter beschikking staan, indien een persoon van mening is dat er een inbreuk werd gemaakt op zijn individuele rechten en vrijheden. Zo kan er reeds in eerste aanleg, voor de rechtbank die de zaak behandelt, worden aangevoerd, dat de fundamentele rechten geschonden werden. Daarnaast kan er in het kader van het hoger beroep, een schending van de fundamentele rechten worden opgeworpen. Wanneer er een vonnis is uitgesproken en de betrokkene denkt dat er procedurefouten gemaakt zijn, bijvoorbeeld doordat vormvereisten die werden voorgeschreven op straffe van nietigheid niet werden nageleefd of wanneer er rechtsregels niet correct werden nageleefd, kan de betrokkene een zaak aanhangig maken bij het Hof van Cassatie. Echter zal het Hof van Cassatie geen uitspraak doen over een bepaalde zaak, het Hof van Cassatie zal uitsluitend onderzoeken of er al dan niet procedurefouten werden gemaakt.³⁹¹
280. **EHRM** - Wanneer de betrokkene, in België, alle mogelijke rechtsmiddelen zonder succes heeft doorlopen en de betrokkene alsnog van oordeel is dat zijn individuele rechten en vrijheden werden geschonden, kan hij een zaak aanhangig maken bij het Hof voor de Rechten van de Mens gaan.³⁹² In dat geval moeten de belangen van de betrokkene,

³⁹⁰ Art. 28decies en 29 Sv.; Art. 136-136quater Sv.

³⁹¹ Art. 1110 Ger. W.

³⁹² Art. 19 e.v. EVRM

rechtsreeks en persoonlijk geschonden zijn. Het Hof zal uitsluitend onderzoeken of er al dan niet een inbreuk werd begaan met betrekking tot de fundamentele rechten.

Hoofdstuk V. Betaling met betrekking tot aankoop gegevens

Afdeling I. Betalingsprocedure

281. **Kostenstaat** - De opdrachtgever die een beroep wil doen op een prestatieverlener, moet een vordering opstellen. Hierbij wordt met opdrachtgever bedoelt, een met het onderzoek van een strafdossier belaste magistraat of een bevoegd lid van een politie- of inspectiedienst, belast met het onderzoek van een strafdossier, dat naderhand wordt overgenomen door een magistraat.³⁹³ Daarboven moet de opdrachtgever de vordering, indien mogelijk, digitaal overmaken aan de prestatieverlener. Bovendien moet de opdracht, op een nauwkeurige wijze worden omschreven in de vordering. Daarnaast moet in de vordering de draagwijdte worden vastgelegd en de termijn waarbinnen de opdracht moet worden voltooid.³⁹⁴ Bovendien stelt de prestatieverlener voor elke gevorderde prestatie een kostenstaat op. Deze kostenstaat vermeldt, voor ieder van de gedane verrichtingen, de data, het tijdstip en de duur van de prestaties.³⁹⁵ Bovendien bestaan er meerdere doelen, waarvoor een prestatieverlener kan worden aangesteld, één van deze doelen, is het zoeken naar de waarheid.³⁹⁶
282. **Centraal bureau gerechtskosten** - Met betrekking tot de betaling van gerechtskosten wordt, binnen de FOD Justitie een centraal bureau gerechtskosten opgericht. De opdracht van dit centraal bureau gerechtskosten bestaat onder meer uit de uitwerking en regelgeving inzake gerechtskosten. Daarnaast is het centraal bureau bevoegd om toezicht uit te oefenen op de arrondissementele bureaus gerechtskosten.³⁹⁷ Daarbij worden als gerechtskosten in strafzaken bedoelt, de kosten die door de FOD Justitie worden betaald of worden voorgesloten, met het oog op de terugvordering van deze kosten bij één of meer veroordeelden, schuldig verklaarde of burgerrechtelijk aansprakelijke partijen of in het ongelijk gestelde burgerlijke partijen.³⁹⁸
283. **Arrondissementeel bureau gerechtskosten** - Bovendien wordt op iedere hoofdzetel van de rechtbank van eerste aanleg, een arrondissementeel bureau gerechtskosten opgericht. Dit bureau bestaat uit een taxatiebureau en een vereffeningsbureau.³⁹⁹ Tot de taken van het taxatiebureau behoren de ontvangst, de registratie en de verificatie van de kostenstaten. Daarnaast behoren de kennisgeving van de kostenstaten aan de

³⁹³ Art. 2, §1 Wet 23 maart 2019 betreffende de gerechtskosten in strafzaken en gelijkgestelde kosten en tot invoeging van een artikel 648 in het Wetboek van strafvorderingen, *BS* 19 april 2019. (Hierna: Wet Gerechtskosten); Art. 3, §1, tweede lid Wet Gerechtskosten

³⁹⁴ Art. 5 Wet Gerechtskosten

³⁹⁵ Art. 6, §1 Wet Gerechtskosten; Art. 32 KB Gerechtskosten

³⁹⁶ Art. 3, §1, lid 3, §1 Wet Gerechtskosten

³⁹⁷ Art. 4, §1 Wet Gerechtskosten; Art. 6-8 KB 15 december 2019 tot vaststelling van de organisatie van de arrondissementele bureaus gerechtskosten en de procedure volgens dewelke gerechtskosten in strafzaken en gelijkgestelde kosten worden toegekend, geïnfotografiseerd, betaald en teruggevorderd, *BS* 27 december 2019. (Hierna: KB Gerechtskosten); DE SMEDT, B., *Handboek deskundigenonderzoek*, Wolters Kluwer, 2024, 907-916, nr. 1602-1609.

³⁹⁸ Art. 3, §1, lid 2 Wet Gerechtskosten

³⁹⁹ Art. 4, §2 Wet Gerechtskosten

opdrachtgevende magistraten en de doorzending van de kostenstaten, tot de taken van het vereffeningsbureau⁴⁰⁰

284. **Weigering kostenstaat** – Bovendien kan het taxatiebureau de kostenstaat weigeren of verminderen. Hiertoe kan het taxatiebureau overgaan, indien er vertraging was in de uitvoering van de prestatie, bij slechte uitvoering of bij facturering van de prestatie boven het vastgestelde tarief.⁴⁰¹
285. **Opdracht vereffeningsbureau** - Daarentegen bestaat de opdracht van de vereffeningsbureaus uit de controle van de kostenstaten. Hierbij wordt gecontroleerd welke opdracht er werd gegeven aan de prestatieverlener en wat op de kostenstaat werd vermeld. Daarnaast behoort de betaling van de kostenstaat tot de opdracht van de vereffeningsbureaus.⁴⁰²
286. **Uitbetaling gerechtskosten** - De uitbetaling van de kostenstaat wordt uitgevoerd door het vereffeningsbureau. Het vereffeningsbureau zet de goedgekeurde kostenstaat in betaling, indien er aan een aantal voorwaarden werd voldaan. Ten eerste moet er overeenstemming zijn tussen de vordering van de opdrachtgever, de geleverde prestatie of het resultaat ervan en hetgeen is opgenomen in de kostenstaat. Ten tweede moeten de gegevens die geleverd werden door de prestatieverlener, op de kostenstaat overeenstemmen met de gegevens in de boekhoudapplicatie. Ten derde moet het risico op dubbele betaling reeds zijn nagegaan. Ten laatste wordt er rekening gehouden met de eventueel toepasselijke bijzondere modaliteiten bij de betaling.⁴⁰³
287. **Afkeuring kostenstaat** - In het geval de kostenstaat wordt afgekeurd door het vereffeningsbureau, wordt de kostenstaat teruggestuurd naar het taxatiebureau voor correctie. Indien de voorgestelde correcties niet worden aanvaard door de prestatieverlener, kan de prestatieverlener in beroep gaan bij de directeur-generaal van de FOD Justitie.⁴⁰⁴
288. **Terugvordering gerechtskosten** - De bevoegde diensten van de FOD Justitie vorderen de gemaakte gerechtskosten terug van de in de strafzaak veroordeelde, van de schuldig verklaarde of van de burgerrechtelijk aansprakelijke betrokken partij of van de in het ongelijk gestelde burgerlijke partij.⁴⁰⁵

⁴⁰⁰ Art. 4, §3 Wet Gerechtskosten; Art. 15 KB Gerechtskosten; DE SMEDT, B., *Handboek deskundigenonderzoek*, Wolters Kluwer, 2024, 907-916, nr. 1602-1609.

⁴⁰¹ Art. 6, §1 Wet Gerechtskosten; Art. 15 en 33 KB Gerechtskosten; DE SMEDT, B., *Handboek deskundigenonderzoek*, Wolters Kluwer, 2024, 907-916, nr. 1602-1609.

⁴⁰² Art. 4, §4 Wet Gerechtskosten; Art. 16 KB Gerechtskosten; DE SMEDT, B., *Handboek deskundigenonderzoek*, Wolters Kluwer, 2024, 907-916, nr. 1602-1609.

⁴⁰³ Art. 12 KB Gerechtskosten

⁴⁰⁴ Art. 12 en 25-27 KB Gerechtskosten; DE SMEDT, B., *Handboek deskundigenonderzoek*, Wolters Kluwer, 2024, 907-916, nr. 1602-1609.

⁴⁰⁵ Art. 7 Wet Gerechtskosten

289. **Bijzondere procedure telecomoperatoren** - Bovendien bestaat er voor de uitbetaling voor diensten verleend, door telecomoperatoren een bijzondere procedure.⁴⁰⁶ Er bestaat een uitwisselingsplatform voor de vragen en antwoorden van opdrachtgevers en telecomoperatoren, NTSU/CTIF genoemd.⁴⁰⁷ De door de opdrachtgever aangeduide uitvoerende politiedienst voert de vragen die voortvloeien uit de vordering in op het daartoe bestemde uitwisselingsplatform.⁴⁰⁸ Nadien beantwoordt de Coördinatiecel Justitie van de betrokken telecomoperator de vraag, door ofwel het resultaat op te laden op het uitwisselingsplatform of door de gevraagde onderschepping van communicatie door te zenden naar het uitwisselingsplatform. Daarbij wordt de uitvoering van de maatregel geregistreerd op het uitwisselingsplatform. Vervolgens worden de resultaten aan de uitvoerende politiediensten ter beschikking gesteld, via het uitwisselingsplatform of via het telecommunicatie interceptieplatform. Nadien bezorgen de uitvoerende politiediensten de resultaten aan de opdrachtgever.⁴⁰⁹
290. **Maandelijks kostenstaat** - De telecomoperator stelt maandelijks een kostenstaat op, gebaseerd op het overzicht van de in de loop van de afgelopen maand uitgevoerde vragen, die hem door het platform werden geleverd. Vervolgens bezorgt de telecomoperator de kostenstaat aan het NTSU/CTIF. Daarbij moeten bovendien een aantal verplichte inlichtingen worden opgenomen.⁴¹⁰ De kostenstaten hieromtrent worden geverifieerd door het NTSU/CTIF. Vervolgens bezorgt het NTSU/CTIF maandelijks een lijst van de tijdens de afgelopen maand, op het uitwisselingsplatform uitgevoerde vragen, aan de Federale Overheidsdienst. Vervolgens deelt de FOD Justitie aan de griffies en de parketten, een overzicht mee van de in elk dossier terug te vorderen gerechtskosten.⁴¹¹
291. **Aankoop persoonsgegevens** - Mijns inziens zou met betrekking tot de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de overheid, de betaling kunnen verlopen conform dezelfde regels, als de regels die van toepassing zijn op alle prestatieverleners. Dit betekent dat dataverzamelingsbedrijven een kostenstaat opmaken van hun geleverde diensten en deze bezorgen aan het taxatiebureau. Na registratie, verificatie en een eventuele vermindering van de kosten, bezorgt het taxatiebureau, de kostenstaat aan het vereffeningsbureau. Wanneer aan de nodige voorwaarden is voldaan, kan het vereffeningsbureau over gaan tot betaling. Indien een dataverzamelingsbedrijf meerdere diensten per maand uitvoert, zou er naar mijn bescheiden mening eventueel een maandelijks kostenstaat kunnen worden opgemaakt. Indien deze regeling echter zou

⁴⁰⁶ Art. 18-24 KB Gerechtskosten

⁴⁰⁷ Art. 18 KB Gerechtskosten

⁴⁰⁸ Art. 19 KB Gerechtskosten; KB 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, wordt voor de uitwisseling van de vragen en de antwoorden op basis van de artikelen 46bis, 88bis en 90ter 90ter tot en met 90decies, 464/13, 464/25 en 464/26 van het Wetboek van Strafvordering, BS 10 februari 2003.; KB 8 november 2016 tot wijziging van het koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, betreffende de tarieven voor de vergoeding van de medewerking, BS 22 december 2016.

⁴⁰⁹ Art. 20 KB Gerechtskosten

⁴¹⁰ Art. 21 KB Gerechtskosten

⁴¹¹ Art. 22-24 KB Gerechtskosten

worden gevolgd, waardoor dataverzamelingsbedrijven worden betaald voor de prestaties die deze bedrijven verlenen, dan zou deze handeling gelijkaardig zijn aan het opvragen van gegevens op basis van wettelijke regels, bij bijvoorbeeld telecomoperatoren.⁴¹² Telecomoperatoren verstrekken immers ook gegevens en worden betaald voor het verstrekken van deze gegevens.⁴¹³ Met het verschil dat in dat geval gegevens worden verstrekt door dataverzamelingsbedrijven, in de plaats van telecomoperatoren. Daarom zou het met betrekking tot de onderzochte handeling, mijns inziens logischer zijn, indien dataverzamelingsbedrijven niet worden vergoed voor het verlenen van een prestatie, maar dat er betaald voor de gegevens die door de overheid worden verkregen, in dat geval zou er wel sprake zijn van de aankoop van persoonsgegevens. De aankoop van persoonsgegevens zou naar mijns inziens kunnen worden beschouwd als een gerechtskost, aangezien deze de aankoop van persoonsgegevens door de FOD Justitie kan worden betaald of worden voorgesloten, met het oog op de terugvordering van deze kosten. De aankoop draagt bovendien bij aan het doel, om naar de waarheid te zoeken. In de kostenstaat zouden dan niet hun geleverde diensten moeten worden omschreven, wel welke gegevens werden doorgegeven. Bovendien kunnen deze gerechtskosten achteraf worden verhaald van de in de strafzaak veroordeelde, van de schuldig verklaarde of van de burgerrechtelijk aansprakelijke betrokken partij of van de in het ongelijk gestelde burgerlijke partij.

⁴¹² *Supra.* nr. 58 e.v.

⁴¹³ *Infra.* nr. 295-296.

Afdeling II. Vaststelling bedrag

292. **Forfaitair vs. uurtarief** - De vergoeding van prestatieverleners wordt bepaald in een tariefbesluit. Bovendien kan deze vergoeding worden vastgesteld op basis van een forfaitair tarief of op een uurtarief. Daarbij betekent een forfaitair tarief, dat er voor de aangegeven prestatie een vast tarief geldt. Bovendien heeft dat vast tarief, behalve de te motiveren uitzonderingen, betrekking op alle onderdelen die behoren tot een bepaalde prestatie. Daarentegen wordt er een tarief per uur bepaald, indien er geen forfaitair tarief werd vastgesteld voor de aangegeven dienst. Daarboven moet de prestatieverlener bij een uurtarief, het aantal uren dat hij heeft gepresteerd en de omstandigheden die hem recht geven op de daarbij horende toeslagen bewijzen.⁴¹⁴
293. **Uitzondering gerechtskosten** – Bovendien werd in het Koninklijk Besluit gerechtskosten een lijst opgenomen met diensten, die niet in aanmerking komen als gerechtskosten.⁴¹⁵ Hierbij valt op dat de kosten van een eenvoudige kennisname van informatie over de houder van een bankrekening of van financiële activa, met inbegrip van de identificatie van de houder, natuurlijke of rechtspersoon van een bankrekening en de identificatiegegevens van volmachthouders om die rekening te gebruiken niet worden beschouwd. Daarnaast wordt de kennisname van informatie omtrent het type rekening, de IBAN-code en de data van opening en sluiting van de rekening niet beschouwd als gerechtskost.⁴¹⁶ Ook uit de omzendbrief blijkt dat deze dienst gratis wordt verleend.⁴¹⁷
294. **Vaststelling tarieven en indexering** – De Koning bepaalt, bij besluit vastgesteld na overleg in de ministerraad, de lijsten van de gerechtskosten en hun tarifiering, tariefbesluiten genaamd. Bovendien moeten deze tariefbesluiten, bij wet worden bekrachtigd binnen vierentwintig maanden volgend op de datum van de bekendmaking in het Belgisch Staatsblad. Bij gebrek aan bekrachtiging binnen deze termijn, houden deze besluiten op uitwerking te hebben.⁴¹⁸ Daarboven worden de bedragen, die werden opgenomen in de tariefbesluiten, elk jaar op 1 januari aangepast aan de afgevlakte gezondheidsindex van de voorgaande maand december. De minister van Justitie maakt na elke indexatie van de tarieven overzichtslijsten daarvan, schalen genaamd, bekend in het Belgisch Staatsblad. De bedragen worden bekendgemaakt door middel van een ministeriële omzendbrief in het Belgisch Staatsblad. Bovendien moeten de geïndexeerde tarieven worden bekendgemaakt, in het Belgisch staatsblad voor 30 januari.⁴¹⁹ Voor het jaar 2025 werden tarieven gepubliceerd in omzendbrief 131/12 over de indexering van de tarieven van de gerechtskosten in strafzaken en de gelijkgestelde kosten.⁴²⁰

⁴¹⁴ Art. 32 KB Gerechtskosten

⁴¹⁵ Art. 35-36 KB Gerechtskosten

⁴¹⁶ Art. 36, 1° KB Gerechtskosten

⁴¹⁷ Omz. 131/12 over de indexering van de tarieven van de gerechtskosten in strafzaken en de gelijkgestelde kosten, BS 9 januari 2025.

⁴¹⁸ Art. 11-12 Wet Gerechtskosten

⁴¹⁹ Art. 28-30 KB Gerechtskosten; Art. 9 en 11 Wet Gerechtskosten

⁴²⁰ Omz. 131/12 over de indexering van de tarieven van de gerechtskosten in strafzaken en de gelijkgestelde kosten, BS 9 januari 2025.

295. **Betaling telecomoperatoren** – Met betrekking tot de betaling voor diensten die geleverd worden door telecomoperatoren, bestaat er een bijzondere regeling.⁴²¹ Dit heeft tot gevolg dat bepaalde prestaties die telecomoperatoren verrichten, worden betaald per dienst. De prestaties die worden bepaald per dienst zijn de opvraging van historische gegevens, opvragen van verkeers- of lokalisatiegegevens in reële tijd, bevraging van mastgegevens, vragen tot medewerking voor onderschepping van communicaties en de vraag voor uitzonderlijke verzoeken. De bijlage bij het Koninklijk Besluit, dat de medewerkingsplicht van de telecomoperatoren regelt, bepaalt deze tarieven.⁴²²
296. **Jaarlijks forfait** – In tegenstelling tot de betaling per dienst, worden de andere prestaties die geleverd worden door de telecomoperatoren, vergoed door een jaarlijks forfait. Bovendien is dit jaarlijks forfait verschillend, naargelang de prestaties worden verleend door een grote of kleine telecomoperator. Daarvoor neemt de minister van Justitie jaarlijks een besluit, na het overleg tussen FOD Justitie, NTSU en BIPT om de verdeelsleutel vast te leggen. Bovendien zal deze verdeelsleutel gebaseerd zijn op een voortschrijdend gemiddelde van vijf jaar, van de vijf grootste prestaties qua bedragen.⁴²³
297. **Aankoop persoonsgegevens** – Deze algemene betalingsregels, zouden mijns inziens ook kunnen worden toegepast op de aankoop van persoonsgegevens bij dataverzamelingsbedrijven. Volgens mij kan hiervoor beter geopteerd worden voor een forfaitair bedrag, dan voor een bedrag per uur. Aangezien een bedrag per uur de kosten waarschijnlijk zou kunnen doen stijgen. Er zou een forfaitair bedrag kunnen worden bepaald per geleverde dienst. Echter zou dit mijns inziens zeer excessief kunnen zijn, aangezien de kosten dan zeer hoog zouden kunnen oplopen. Wanneer er een kost per geleverde dienst wordt bepaald, zou dit eventueel kunnen impliceren dat de dataverzamelingsbedrijven meer persoonsgegevens willen bewaren. Eventueel zou dit tot gevolg kunnen hebben dat deze bedrijven sneller geneigd kunnen zijn om de regels met betrekking tot gegevensbescherming niet strikt na te leven. Aangezien het beschikken van meer gegevens, dan zou kunnen zorgen voor meer gevraagde diensten. Meer diensten zou dan meer betalingen opleveren.⁴²⁴ Daarom lijkt het mij verkieselijk dat, net zoals bij telecomoperatoren, een forfait per jaar wordt betaald aan de dataverzamelingsdiensten, die diensten verrichten voor de overheid. Tenzij een overheid slechts enkele malen

⁴²¹ KB 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, wordt voor de uitwisseling van de vragen en de antwoorden op basis van de artikelen 46bis, 88bis en 90ter tot en met 90decies, 464/13, 464/25 en 464/26 van het Wetboek van Strafvordering, *BS* 10 februari 2003.; KB 8 november 2016 tot wijziging van het koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, betreffende de tarieven voor de vergoeding van de medewerking, *BS* 22 december 2016.

⁴²² Art. 2 Bijlage bij het koninklijk besluit van 8 november 2016 tot wijziging van het koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, betreffende de tarieven voor de vergoeding van de medewerking, *BS* 22 december 2016.

⁴²³ Art. 3 Bijlage bij het koninklijk besluit van 8 november 2016 tot wijziging van het koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, betreffende de tarieven voor de vergoeding van de medewerking, *BS* 22 december 2016.

⁴²⁴ *Infra* nr. 204 e.v.

gebruikmaakt van de diensten van een dataverzamelingsbedrijf, in dat geval zou er eventueel wel een forfaitair bedrag per dienst kunnen worden betaald. Bovendien kan ervoor geopteerd worden, om net zoals bij telecomoperatoren, enkele diensten te bepalen waarbij er wel een forfaitair bedrag per dienst wordt betaald. Ter illustratie: dit zou eventueel mogelijk zijn indien er zeer specifieke verzoeken gesteld worden of wanneer er een tijdslijn moet worden opgesteld, die betrekking heeft op historische en recente gegevens. Dit is volgens mij echter niet verkieselijk, aangezien dit voor de FOD Justitie meer kosten met zich zou meebrengen, dan wanneer er een jaarlijks forfait wordt betaald. Mijns inziens zou het bedrag dat aan de dataverzamelingsbedrijven wordt betaald, echter niet het bedrag voor een geleverde presentatie moeten zijn, wel het bedrag om de gegevens aan te kopen.⁴²⁵ In dat geval zou er dan een forfaitair bedrag kunnen worden betaald voor bepaalde gegevens, per keer dat gegevens doorgegeven worden. In mijns inziens zou het beter zijn dat in de plaats van een forfaitair bedrag per gegevensoverdracht, een forfaitair bedrag betaald wordt per jaar, voor de aankoop van alle gegevens in dat jaar. Hierbij kan er mijns inziens in uitzonderingen worden voorzien, waarbij er voor bepaalde gegevens, wel een forfaitair bedrag betaald wordt. Bovendien kan het bedrag voor de aankoop van persoonsgegevens mijns inziens worden vastgesteld in de tariefbesluiten en jaarlijks worden geïndexeerd.⁴²⁶ Daardoor zullen de dataverzamelingsbedrijven mijns inziens niet bevoegd zijn, om het bedrag te bepalen. Bijgevolg zal de procureur des Konings, respectievelijk de onderzoeksrechter, niet zelf de persoonsgegevens aankopen of betalen voor de aankoop van deze gegevens. De procureur des Konings of de onderzoeksrechter zullen de aankoop van persoonsgegevens bij dataverzamelingsbedrijven slechts bevelen.

⁴²⁵ *Supra* nr. 291.

⁴²⁶ *Supra* nr. 299.

Afdeling III. Budget FOD Justitie

298. **Jaarlijks budget** - Daarnaast kan de FOD Justitie per jaar slechts beschikken over een beperkt budget. Dit bedrag wordt vastgesteld in de begroting, deze begroting wordt jaarlijks vastgesteld door de federale regering. De begroting is bovendien een inschatting van de te verwachten inkomsten en uitgaven van de federale overheid voor het volgende jaar. Iedere minister, waaronder deze van de FOD Justitie, stelt een begrotingsvoorstel op. Daarna bepaalt de regering, het budget dat het volgende jaar beschikbaar zal zijn. Nadien moet de begroting besproken worden in het federaal parlement. Uiteindelijk moet het federaal parlement de begroting goedkeuren. Bovendien wordt de begroting, in de loop van het begrotingsjaar geëvalueerd en indien nodig aangepast. Er wordt jaarlijks een begroting opgesteld op federaal niveau en op het Vlaams niveau. Op Vlaams niveau stelt de Vlaamse regering de begroting op en moet deze worden goedgekeurd in het Vlaams parlement.⁴²⁷
299. **Budget FOD Justitie** - De FOD Justitie heeft jaarlijks een bepaald bedrag ter beschikking, dat bepaald wordt in de begroting. Daarboven moet er binnen de FOD Justitie bepaald worden, aan welke zaken het budget wordt besteed. Bijgevolg stelt het Directoraat-generaal Budget en Beheerscontrole de begroting van justitie op. Andere taken van dit directoraat-generaal zijn het beheren van de comptabiliteit, het verstrekken van relevante beheersinformatie voor een doeltreffend en efficiënt gebruik van de middelen. Daarnaast oefent het directoraat controle uit op de doeltreffendheid en efficiëntie van de middelen. Daarboven heeft het directoraat nog andere taken, zoals het vastleggen van uitgavendossiers, vereffenen van facturen en invorderen van ontvangsten, het beheer van masterdata, voeren van de dubbele boekhouding voor heel justitie, het boekhoudkundig beheer van de vaste activa, analytische boekhouding en de opmaak van de jaarrekening.⁴²⁸
300. **Aankoop persoonsgegevens** – Mijns inziens zou het bedrag dat besteed zou worden aan de aankoop van persoonsgegevens bij dataverzamelingsbedrijven moeten worden betaald uit het bedrag dat in de begroting werd toegekend aan de FOD Justitie. Binnen de FOD Justitie moet dan de specifieke kostenposten bepaald worden, door het Directoraat-generaal Budget en Beheerscontrole.

⁴²⁷BLOCKMANS, T. en MORTIER, T., *Begrotingswetgeving anno 2024: Ontstaan, structuur en recente ontwikkelingen in de Belgische budgettaire wet- en regelgeving*, Intersentia, 2024, 1-200.

⁴²⁸FOD Justitie, 'Budget: missie en visie', *Federale Overheidsdienst Justitie*, https://justitie.belgium.be/nl/overheidsdienst_justitie/organisatie/stafdiensten/budget_en_beheerscontrole (geraadpleegd op 22 juli 2025).

Deel VII. Conclusie

301. **Inleiding** – In deze conclusie zal er een antwoord geformuleerd worden op de centrale onderzoeksvraag: 'Op welke manier kan de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de Belgische overheid in het kader van het strafonderzoek worden toegepast en in hoeverre kunnen procedurele waarborgen de grondrechtsbescherming, met inbegrip van het gegevensbeschermingsrecht waarborgen?'.
302. **Vergelijkbare onderzoekshandelingen** - In dit onderzoek werd de aankoop van persoonsgegevens vergeleken met een aantal vergelijkbare onderzoekshandelingen, zoals het opvragen van gegevens op basis van wettelijke regels, het klassiek beslag en het databeslag, het DNA-onderzoek, de huiszoeking, het opsporen van communicatie, de zoeking in het communicatie- en informaticasysteem en het opsporen van de elektronische communicatie. De onderzoeksrechter kan een zoeking in het communicatie- en informaticasysteem bevelen. Indien in de betrokken informaticasystemen opgeslagen gegevens aangetroffen worden die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is, kan er een beslag worden gelegd op deze gegevens. In dat geval worden de gegevens gekopieerd op een drager, deze handeling kadert in het databeslag.
303. **Nut handeling** – Mijns inziens kunnen bepaalde gegevens, die kunnen worden aangekocht door dataverzamelingsbedrijven, ook worden verkregen door middel van de zoeking in het informatica- en communicatiesysteem en het beslag op deze data of door middel van andere onderzoekshandelingen. Het verschil tussen de aankoop van persoonsgegevens bij dataverzamelingsbedrijven en andere middelen, is mijns inziens dat de overheid bij deze handeling gegevens aankoopt in de plaats van de gegevens zelf te zoeken. Daarnaast is het grootste verschil de hoeveelheid van informatie die kan worden verkregen en de korte tijdspanne, waarin deze informatie kan worden verkregen. Bovendien is het mogelijk dat bepaalde gegevens enkel kunnen worden verkregen door de aankoop van persoonsgegevens en niet door toepassing van andere middelen. Bijvoorbeeld historische gegevens die niet meer terug te vinden zijn in het communicatie- en informaticasysteem of niet meer kunnen worden opgevraagd bij telecomoperatoren door de kortere bewaringstermijnen. Bovendien moet erop worden gewezen dat de aankoop van persoonsgegevens bij dataverzamelingsbedrijven ethische gevaren met zich mee kan brengen, de overheid betaalt immers voor informatie, in de plaats van deze zelf te zoeken. Daarnaast kan er een belangenconflict bestaan, in hoofde van de overheid. De overheid zou er immers belang bij kunnen hebben dat dataverzamelingsbedrijven de regels, die het gegevensbeschermingsrecht waarborgen niet strikt toepassen.
304. **Proactieve en reactieve recherche** – Mijns inziens zou de aankoop van persoonsgegevens bij dataverzamelingsbedrijven zowel kunnen worden toegepast in het kader van proactieve, als reactieve recherche. De handeling zou kunnen worden uitgevoerd met toestemming van de verdachte, in dat geval moet er een wettelijke basis bestaan, of

zonder toestemming van de verdachte. Daarboven kunnen de gegevens van een individueel persoon, meerdere persoon of een groep personen worden aangekocht.

305. **Opsporingsonderzoek vs. gerechtelijk onderzoek** - In het kader van het strafonderzoek kunnen het opsporingsonderzoek, onder leiding van de procureur des Konings en het gerechtelijk onderzoek, onder leiding van de onderzoeksrechter onderscheiden worden. Het gemeenschappelijk doel van beide soorten onderzoek is het opsporen van misdrijven en hun daders en het verzamelen van bewijs. De onderzoekshandelingen die de procureur des Konings in het kader van het opsporingsonderzoek kan toepassen, mogen in principe geen significante inbreuk op de individuele rechten en vrijheden uitmaken. Aangezien de procureur des Konings in principe geen dwangmaatregelen mag uitvoeren. Niettegenstaande kan de onderzoeksrechter in het kader van het gerechtelijk onderzoek, wel dwangmaatregelen uitvoeren, deze kunnen bijgevolg inbreuk maken op de fundamentele rechten. Uitzonderlijk kan de procureur des Konings bij het vaststellen van bepaalde misdrijven op heterdaad, wel gebruik maken van dwangmaatregelen. Daarnaast kan de procureur des Konings onderzoekshandelingen die dwang inhouden, uitvoeren met toestemming van de betrokkene persoon.
306. **Mini-instructie** - In het kader van een mini-instructie kan de procureur des Konings tijdens het opsporingsonderzoek, de onderzoeksrechter vorderen om een bepaalde onderzoekshandeling te verrichten, waarvoor de procureur des Konings zelf niet bevoegd is. In het kader van de mini-instructie kan de procureur des Konings bijgevolg wel dwangmaatregelen uitvoeren. Hierbij wordt geen gerechtelijk onderzoek ingesteld. Na het uitvoeren van deze onderzoekshandeling kan de onderzoeksrechter beslissen om het onderzoek verder te laten uitvoeren door de procureur des Konings of om het onderzoek naar zich toe te trekken en zelf het onderzoek voort te zetten. Echter zijn een aantal onderzoekshandelingen van het toepassingsgebied van de mini-instructie uitgesloten, waaronder het bevel tot aanhouding, de zoeking in een informatica- en communicatiesysteem, de huiszoeking, de observatie met technische hulpmiddelen om zich te verwerven in een woning en de inblikoperatie in de woning.
307. **Indeling persoonsgegevens** - Een dwangmaatregel is een maatregel die de inbreuk van de fundamentele rechten van een persoon tot gevolg kan hebben. De aankoop van persoonsgegevens zou naargelang de aard van de informatie een dwangmaatregel kunnen uitmaken. Persoonsgegevens kunnen worden ingedeeld in verschillende categorieën, naar gelang de informatie. Bijgevolg kunnen persoonsgegevens worden ingedeeld in niet-gevoelige gegevens, ook wel 'gewone' gegevens genoemd en in gevoelige gegevens, ook wel bijzondere gegevens genoemd. Daarbij zijn gevoelige gegevens, gegevens die naar hun aard gevoelig zijn en grotere risico's met zich meebrengen met betrekking tot de grondrechten en fundamentele vrijheden. Bovendien behoeven gevoelige gegevens een grotere, specifieke bescherming. Hierbij zijn gevoelige gegevens, gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, en de verwerking van genetische gegevens,

biometrische gegevens met het oog op de unieke identificatie van een persoon of gegevens over gezondheid of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

308. **Bevelen aankoop niet-gevoelige gegevens** – Mijns inziens zal de aankoop van niet-gevoelige gegevens, de fundamentele rechten niet schenden. Daarom maakt de aankoop van niet-gevoelige gegevens volgens mij geen dwangmaatregel uit. Bijgevolg is naar mijn bescheiden mening, de procureur des Konings bevoegd om de aankoop van niet-gevoelige gegevens te bevelen. Aangezien er dan geen sprake is van een dwangmaatregel. De onderzoeksrechter kan bevelen om niet-gevoelige gegevens aan te kopen, indien er een gerechtelijk onderzoek werd ingesteld.
309. **Bevelen aankoop gevoelige gegevens** - In tegenstelling tot niet-gevoelige gegevens, zou de aankoop van gevoelige gegevens mijns inziens wel de fundamentele rechten kunnen schenden en bijgevolg een dwangmaatregel uitmaken. Bijgevolg zou in principe uitsluitend de onderzoeksrechter kunnen bevelen om gevoelige gegevens aan te kopen. Eventueel zou er kunnen worden voorzien dat de procureur des Konings, kan bevelen om gevoelige gegevens aan te kopen, indien er een heterdaadsituatie bestaat, vergelijkbaar met andere onderzoekshandelingen. Zo kan bijvoorbeeld de procureur des Konings een huiszoeking bevelen wanneer er sprake is van een heterdaadssituatie. Bijgevolg kan er bijvoorbeeld worden beslist, dat de procureurs des Konings de handeling kan bevelen bij een ontdekking op heterdaad van een gijzeling, een wederrechtelijke vrijheidsbeneming, afpersing, bij het plegen van een terroristisch misdrijf of wanneer er gedreigd wordt met het plegen van een terroristisch misdrijf. Dit zou vergelijkbaar zijn met de situaties op heterdaad, waarbij de procureur des Konings een zoeking in het informatica-en communicatiesysteem kan bevelen. De procureur des Konings zou de handeling kunnen bevelen indien er toestemming werd verkregen van de betrokkene.
310. **Mini-instructie** - Daarboven zou deze handeling mijns inziens kunnen worden uitgevoerd door middel van een mini-instructie. De handeling is immers niet opgenomen in de lijst van onderzoekshandelingen, waarbij een mini-instructie is uitgesloten. Echter zou de handeling ook kunnen worden uitgesloten van de mini-instructie, aangezien de handeling zo ingrijpend is. De gegevens die verkregen worden door de zoeking in een informatica-en communicatiesysteem zijn vergelijkbaar met de gegevens die verkregen worden door middel van de aankoop van gegevens bij dataverzamelingsbedrijven. Aangezien deze onderzoekshandeling werd uitgesloten van de mini-instructie, zou het naar mijn bescheiden mening een logisch gevolg zijn dat de aankoop van persoonsgegevens bij dataverzamelingsbedrijven ook wordt uitgesloten van de mini-instructie.
311. **Inmenging fundamenteel recht** - Eventueel zou de aankoop van persoonsgegevens bij dataverzamelingsbedrijven in het kader van het strafonderzoek, fundamentele rechten kunnen schenden. Zo zou eventueel het recht op een eerlijk proces, het recht op privacy, met inbegrip van het recht op eerbiediging van het privéleven en het recht op bescherming

van persoonsgegevens, het recht op gelijkheid en non-discriminatie en het recht op vrije meningsuiting kunnen worden geschonden. Er bestaat een grotere grondrechtsbescherming wanneer de inbreuk op het fundamentele recht bij wet is vastgelegd, er een legitiem doel wordt nagestreefd en de inbreuk noodzakelijk, proportioneel en subsidiair is. Bijgevolg moeten deze voorwaarden worden nageleefd, bij de aankoop van gevoelige gegevens.

312. **GDPR en privacyrichtlijn politie-justitie** - Daarboven moeten ook de regels met betrekking tot het gegevensbeschermingsrecht, die het recht op privacy waarborgen, worden nageleefd indien persoonsgegevens worden aangekocht worden bij dataverzamelingsbedrijven. De instrumenten die het gegevensbeschermingsrecht waarborgen, zijn de GDPR, deze richtlijn werd omgezet in Titel I Wet Verwerking Persoonsgegevens en de privacyrichtlijn politie-justitie, deze werd omgezet in Titel II Wet Verwerking Persoonsgegevens. Echter bleek uit het onderzoek dat de GDPR niet van toepassing is, indien persoonsgegevens door de bevoegde overheden worden verwerkt met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen met inbegrip van de bescherming tegen en de voorkoming van gebaren voor de openbare veiligheid. In dat geval is bijgevolg de privacyrichtlijn politie-justitie van toepassing. Deze regelgeving bepaalt de regels, die moeten worden nageleefd, indien gegevens worden verwerkt in het kader van het strafonderzoek. Deze regels moeten zowel worden nageleefd bij de verwerking van gevoelige gegevens, als bij de verwerking van niet-gevoelige gegevens.
313. **Rechtmatige verwerking** - De privacyrichtlijn politie-justitie en Titel II Wet Verwerking Persoonsgegevens bepalen dat een verwerking van persoonsgegevens slechts rechtmatig is indien er een wet is vastgelegd, er een legitiem doel, dit doel moet de verwerking van gegevens zijn met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen met inbegrip van de bescherming tegen en de voorkoming van gebaren voor de openbare veiligheid, wordt nagestreefd en de inbreuk noodzakelijk, proportioneel en subsidiair is.
314. **Gelijkaardige voorwaarden** - Hierbij valt op dat zowel een gerechtvaardigde inmenging in een fundamenteel recht, als een rechtmatige verwerking van persoonsgegevens slechts mogelijk is indien wordt voldaan aan bepaalde voorwaarden. Zo moet er een wettelijke basis bestaan, er moet een legitiem doel worden nagestreefd en de inbreuk moet noodzakelijk, proportioneel en subsidiair zijn. In de volgende alinea's zullen bijgevolg criteria worden aangereikt, die het mogelijk maken, om te bepalen of er aan deze voorwaarden werd voldaan.
315. **Wettelijke basis** - Op dit moment bestaat er geen specifiek, duidelijk regelgevend kader omtrent de aankoop van persoonsgegevens in het kader van het strafonderzoek. Echter vormt dit geen probleem, aangezien andere bestaande regelgeving, zoals het wetboek van strafvordering of andere regels, mijns inziens een voldoende wettelijke basis zijn. Wel zou

naar mijn bescheiden mening een grotere grondrechtsbescherming bestaan, indien er een duidelijk wetgevend kader bestaat, dan wanneer er geen duidelijk wetgevend kader bestaat. In deze regelgeving zouden passende waarborgen kunnen worden opgenomen, bijvoorbeeld welke persoonsgegevens kunnen worden aangekocht, voor welke doeleinden deze gegevens mogen worden verwerkt, wie bevoegd is om deze gegevens op te vragen... Het is belangrijk dat de wet, bijvoorbeeld het wetboek van strafvordering toegankelijk wordt gemaakt voor de burgers. Daarnaast moet de wet duidelijk opgesteld zijn, zodat burgers de rechtsgevolgen van hun handelen kunnen inschatten. Met betrekking tot de transparantie, kan de overheid meedelen aan de burger dat de overheid persoonsgegevens kan aankopen bij dataverzamelingsbedrijven in het kader van het strafonderzoek en welke gegevens er kunnen worden aangekocht.

316. **Legitiem doel** – Daarnaast moet er een legitiem doel worden nagestreefd. Met betrekking tot de inmenging in fundamentele rechten zou dit doel mijns inziens in het kader van het strafonderzoek, bijvoorbeeld de veiligheid van het land, de openbare veiligheid en de bescherming van de openbare orde of de verwerking of de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid kunnen zijn. Hierbij moet worden benadrukt dat bij een rechtmatige verwerking van persoonsgegevens dit doel de verwerking de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid moet zijn. Volgens mij is aan deze voorwaarde voldaan, indien gegevens worden aangekocht, met als doel de opsporing en het onderzoek naar strafbare feiten.
317. **Noodzakelijkheid** – Opdat de handeling noodzakelijk zou zijn, moet de handeling voldoen aan de vereisten van subsidiariteit en proportionaliteit. De handeling is noodzakelijk, indien de handeling nodig is om onderzoek te doen naar strafbare feiten. Met betrekking tot de noodzakelijkheid, mogen er niet meer gegevens bewaard worden dan nodig.
318. **Subsidiariteit** – Om te voldoen aan de vereiste van subsidiariteit, mogen er geen minder ingrijpende maatregelen voorhanden zijn, dan de aankoop van persoonsgegevens bij dataverzamelingsbedrijven. Bijgevolg moet indien er een minder ingrijpende maatregel bestaat, geopteerd worden voor de minst ingrijpende maatregel. Bijgevolg zal de vereiste van subsidiariteit niet voldaan zijn, indien er gekozen werd voor de aankoop van gegevens, terwijl er andere minder ingrijpende maatregelen voorhanden waren. Indien bijvoorbeeld de gegevens kunnen verkregen worden door de geldige toestemming van een betrokkene of door een gewone opzoeking, moet voor deze minder ingrijpende maatregelen worden gekozen.
319. **Proportionaliteit** – Daarnaast mag de onderzoekshandeling niet verder reiken dan nodig is om een bepaald doel te bereiken, om aan de vereiste van proportionaliteit te voldoen. Bijgevolg moet de handeling in verhouding zijn tot het doel. Het doel dat nagestreefd wordt

in het kader van het strafonderzoek, is het achterhalen van de waarheid. Mijns inziens zal de onderzoekshandeling bijvoorbeeld niet proportioneel zijn, indien de handeling wordt toegepast bij het onderzoeken van minder ernstige misdrijven, bijvoorbeeld een diefstal zonder braak. Daarentegen zal de handeling wel proportioneel zijn, indien er onderzoek wordt gevoerd naar ernstige criminele feiten. Om deze proportionaliteit te beoordelen kan er verwezen worden naar de misdrijven opgenomen in artikel 90ter, §2-4 Sv.. Aangezien deze misdrijven meerdere keren worden gebruikt in het wetboek van strafvordering, als drempel voor de proportionaliteitsvereiste voor wat betreft de opsporingsmethoden die het meest ingrijpend zijn in de persoonlijke levenssfeer. Bijgevolg kan er worden beslist dat de aankoop van gevoelige gegevens slechts mogelijk is, indien er onderzoek wordt gevoerd naar ernstige misdrijven. Met betrekking tot niet-gevoelige gegevens zou er eventueel kunnen worden beslist dat de gegevens, slechts kunnen worden aangekocht, indien er ernstige aanwijzingen bestaan, dat de gepleegde misdrijven kunnen worden gestraft met een correctionele hoofdgevangenisstraf van één jaar of een zwaardere straf.

320. **Doelmatigheid** - Hierbij zullen er enkele parameters aangereikt worden die naar mijn bescheiden mening, kunnen worden gehanteerd om de proportionaliteit te beoordelen. Vooreerst kan de doelmatigheid van de handeling worden gebruikt als criterium. Hierbij verwijst doelmatigheid naar de vraag of de handeling of inbreuk op het fundamentele recht daadwerkelijk bijdraagt aan het beoogde doel. Bijvoorbeeld, wanneer verzamelde gegevens niet bruikbaar zijn of niet kunnen bijdragen aan het gestelde doel, kan de handeling als disproportioneel worden beschouwd. Bijgevolg moeten gegevens effectief kunnen bijdragen aan het strafonderzoek. Ook wanneer er gegevens worden verzameld die niet relevant zijn voor het onderzoek of overmatig veel gegevens worden verzameld, kan de handeling als disproportioneel worden beschouwd. Stel bijvoorbeeld dat er in de loop der tijd meer onderzoek wordt gevoerd naar de effectiviteit van het gebruik van gegevens, verkregen uit informatie die dataverzamelingsbedrijven opslaan en hieruit blijkt dat de informatie niet of slechts in beperkte mate kan bijdragen aan het doel van het strafonderzoek. Dan zou de handeling, mijns inziens niet langer proportioneel kunnen zijn. Tenzij de effectiviteit kan worden verbeterd.
321. **Belangenafweging** - Daarnaast kan er een belangenafweging worden gemaakt, om de proportionaliteit te beoordelen. Hierbij wordt de mate van schade voor de betrokkene afgewogen tegen het beoogde doel. Zo kan het bijvoorbeeld gerechtvaardigd zijn om meer ingrijpende maatregelen te nemen in onderzoeken naar zwaardere criminaliteit, terwijl dit minder proportioneel zou zijn bij lichtere misdrijven. Het nadeel voor de betrokkene moet dus in verhouding staan tot het beoogde doel, waarbij moet worden beoordeeld of het nadeel groot of gering is.
322. **Aard gegevens en hoeveelheid** – Bovendien spelen de aard van de gegevens en de hoeveelheid van de verzamelde gegevens een rol bij de beoordeling van de proportionaliteit. Hoe gevoeliger de informatie is of hoe groter de hoeveelheid gegevens, des te sterker moet de rechtvaardiging voor het ingrijpen zijn. Aangezien de

proportionaliteitsvereiste misschien minder snel voldaan is, indien er zeer veel gegevens of bijzonder gevoelige gegevens worden verzameld. De proportionaliteit moet bijgevolg zorgvuldig worden beoordeeld door de mate van inbreuk op de rechten van de betrokkene, de verwachte effectiviteit en noodzakelijkheid van de handeling.

323. **Bevelschrift** – Naar mijn bescheiden mening zal de procureur des Konings of de onderzoeksrechter, afhankelijk van wie bevoegd is om de handeling te bevelen, de noodzakelijk, subsidiariteit en proportionaliteit moeten controleren. Bijgevolg kan de procureur des Konings of de onderzoeksrechter, de handeling bevelen in een met redenen omkleed bevelschrift. Hierbij moeten de feitelijke omstandigheden van de zaak worden uiteengezet. Daarnaast moet worden aangetoond, dat er voldaan is aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.
324. **Grondrechtsbescherming** - De aankoop van gevoelige gegevens, moet met betrekking tot de inmenging in een grondrecht aan bovenstaande vereisten voldoen om de grondrechtsbescherming te waarborgen. Indien niet werd voldaan aan deze vereisten, kan de grondrechtsbescherming niet langer gewaarborgd worden. Dit heeft tot gevolg dat bepaalde fundamentele rechten kunnen worden geschonden. Echter, zullen zowel niet-gevoelige gegevens als gevoelige gegevens aan deze vereisten moeten voldoen, aangezien deze vereisten moeten worden nageleefd om gegevens op een rechtmatige manier te verwerken. Indien deze gegevens niet op een rechtmatige manier worden verwerkt, zullen de privacyregels worden geschonden. Bijgevolg zal dan ook de grondrechtsbescherming niet langer kunnen worden gewaarborgd, aangezien het recht op privacy een fundamenteel recht is.
325. **Waarborgen privacyrichtlijn** - Daarnaast moeten zowel niet-gevoelige, als gevoelige gegevens volgens de privacyrichtlijn politie-justitie toereikend en ter zake dienend zijn. Bovendien mogen de gegevens niet bovenmatig zijn in verhouding met de doeleinden, waarvoor de gegevens worden verwerkt. Voorts moeten de gegevens correct zijn en indien nodig moeten de gegevens worden geactualiseerd. Daarnaast moeten de gegevens bewaard worden in een vorm, die het mogelijk maakt om de betrokkene niet langer te laten identificeren dan noodzakelijk is voor het verwerkingsdoel. Bovendien moet er gebruik worden gemaakt van passende technische of organisatorische maatregelen, op een manier die de beveiliging waarborgt. Zo moeten de gegevens beschermd zijn tegen een ongeoorloofde of onrechtmatige verwerking, tegen opzettelijk verlies, vernietiging en beschadiging. Bovendien moeten er bewaartermijnen worden vastgesteld.
326. **Waarborgen gevoelige gegevens** - Met betrekking tot gevoelige gegevens bepaalt de wet bovendien dat, voor de verwerking van gevoelige gegevens, passende waarborgen moeten worden genomen. Zo moet er voor de verwerking ten minste worden voorzien, dat de bevoegde overheid of de verwerkingsverantwoordelijke een lijst van de categorieën van personen die toegang hebben tot de persoonsgegevens opstelt. Daarboven moet een beschrijving worden opgesteld, van de hoedanigheid van deze personen, ten opzichte van

de verwerking van de beoogde gegevens. Voorts moet deze lijst ter beschikking worden gehouden van de bevoegde toezichthoudende autoriteit. Daarboven moet de bevoegde overheid erover waken, dat de aangewezen personen door een wettelijke of statutaire verplichting of door een evenwaardige contractuele bepaling ertoe gehouden zijn, het vertrouwelijke karakter van de betrokken gegevens in acht te nemen.

327. **Voorbeelden** - Voorbeelden van passende waarborgen die kunnen worden ingevoerd, zijn dat de gevoelige gegevens enkel mogen worden verzameld in samenhang met andere gegevens over de natuurlijke persoon in kwestie. Bovendien moeten de verzamelde gegevens afdoende kunnen worden beveiligd. Bijgevolg kunnen er strengere regels gelden, voor de toegang van het personeel van de bevoegde overheid tot de gegevens. Eveneens moet de doorzending van die gegevens worden verboden.
328. **Grondrechtbescherming** - Dit heeft tot gevolg dat, wanneer de waarborgen met betrekking tot niet-gevoelige gegevens en gevoelige gegevens, niet worden nageleefd, dit een schending van de regels met betrekking tot het gegevensbeschermingsrecht met zich mee kan brengen. Bijgevolg kan dit ervoor zorgen dat de grondrechtbescherming niet langer kan worden gewaarborgd. Waardoor fundamentele rechten, zoals het recht op privacy, kunnen worden geschonden.
329. **Controle** – De Gegevensbeschermingsautoriteit oefent toezicht uit op de verwerking van persoonsgegevens door dataverzamelingsbedrijven. Echter bestaat er geen toezichtsorgaan dat toezicht uitoefent op de verwerking van persoonsgegevens door de procureur des Konings of de onderzoeksrechter. Een persoon die van mening is dat zijn fundamentele rechten werden geschonden, door het gebruik van gegevens die werden aangekocht bij dataverzamelingsbedrijven in het kader van het strafonderzoek, kan in eerste aanleg en in hoger beroep opwerpen dat zijn rechten werden geschonden. Wanneer een persoon alle mogelijke rechtsmiddelen in België heeft doorlopen en nog steeds de mening is toegedaan, dat zijn fundamentele rechten werden geschonden, kan deze persoon een zaak aanhangig maken bij het Hof voor de Rechten van de Mens. In dat geval moeten de belangen van de betrokkene, rechtsreeks en persoonlijk zijn geschonden.
330. **Betalingsprocedure kosten** – Mijns inziens zou met betrekking tot de aankoop van persoonsgegevens bij dataverzamelingsbedrijven door de overheid, de betaling kunnen verlopen conform dezelfde regels, als de regels die van toepassing zijn op alle prestatieverleners. Dit wil zeggen dat dataverzamelingsbedrijven een kostenstaat opmaken van hun geleverde diensten en deze bezorgen aan het taxatiebureau. Na registratie, verificatie en een eventuele vermindering van de kosten, bezorgt het taxatiebureau, de kostenstaat aan het vereffeningsbureau. Wanneer aan de nodige voorwaarden is voldaan, kan het vereffeningsbureau over gaan tot betaling. Met betrekking tot de onderzochte handeling, zou het mijns inziens, evenwel logischer zijn, indien dataverzamelingsbedrijven niet worden vergoed voor het verlenen van een prestatie, maar dat er betaald wordt voor de gegevens die door de overheid worden

verkregen, in dat geval zou er wel sprake zijn van de aankoop van persoonsgegevens. De aankoop van persoonsgegevens zou naar mijns inziens kunnen worden beschouwd als een gerechtskost, aangezien de aankoop van persoonsgegevens door de FOD Justitie kan worden betaald of worden voorgeschoten, met het oog op de terugvordering van deze kosten. Bovendien kunnen deze gerechtskosten achteraf worden verhaald van de in de strafzaak veroordeelde, van de schuldig verklaarde of van de burgerrechtelijk aansprakelijke betrokken partij of van de in het ongelijk gestelde burgerlijke partij.

331. **Forfaitair bedrag** - Bovendien zou er mijns inziens kunnen worden geopteerd om een forfaitair bedrag per geleverde dienst of per jaar te betalen. Zo kunnen er, vergelijkbaar met de regeling met betrekking tot telecomoperatoren, bepaalde diensten worden opgenomen waarvoor een forfaitair bedrag per dienst wordt betaald. Voor de andere diensten kan dan een forfaitair bedrag per jaar worden betaald. Indien dataverzamelingsbedrijven daarentegen worden betaald, voor de gegevens die deze bedrijven aan de overheid 'verkopen', zou er een forfaitair bedrag kunnen worden betaald voor bepaalde gegevens, per keer dat gegevens doorgegeven worden. In mijns inziens zou het beter zijn dat in de plaats van een forfaitair bedrag per gegevensoverdracht, een forfaitair bedrag betaald wordt per jaar, voor de aankoop van alle gegevens in dat jaar.
332. **Vaststelling tarieven** - De Koning bepaalt, bij besluit vastgesteld na overleg in de ministerraad, de lijsten van de gerechtskosten en hun tarifiering, tariefbesluiten genaamd. De bedragen die moeten worden betaald voor de aankoop van gegevens, zou mijns inziens kunnen worden vastgesteld in deze tariefbesluiten. Daarboven worden de bedragen, die werden opgenomen in de tariefbesluiten, elk jaar op 1 januari aangepast aan de afgevlakte gezondheidsindex van de voorgaande maand december. De minister van Justitie maakt na elke indexatie van de tarieven overzichtslijsten daarvan, schalen genaamd, bekend in het Belgisch Staatsblad.
333. **Aankoop persoonsgegevens** - Bijgevolg zal de procureur des Konings, respectievelijk de onderzoeksrechter, niet zelf de persoonsgegevens aankopen of betalen voor de aankoop van deze gegevens. De procureur des Konings of de onderzoeksrechter zullen de aankoop van persoonsgegevens bij dataverzamelingsbedrijven slechts bevelen.

Deel VIII. Bibliografie

Wetgeving

Europees Verdrag voor de Rechten van de Mens 4 november 1950, *BS* 19 augustus 1955.

Verordening (EU) 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.

Handvest van de grondrechten van de Europese Unie van 26 oktober 2012, *Pb. L.* 26 oktober 2012.

De Gecoördineerde Grondwet van 17 februari 1994, *BS* 17 februari 1994.

Gerechtigd Wetboek van 10 oktober 1967, *BS* 31 oktober 1967.

Wetboek van strafvordering van 19 november 1808, *BS* 29 november 1808.

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 23 maart 2019 betreffende de gerechtskosten in strafzaken en gelijkgestelde kosten en tot invoeging van een artikel 648 in het Wetboek van strafvorderingen, *BS* 19 april 2019.

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

Wet 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, *BS* 10 januari 2018.

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

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

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

Wet 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, *BS* 4 september 2002.

KB 15 december 2019 tot vaststelling van de organisatie van de arrondissementale bureaus gerechtskosten en de procedure volgens dewelke gerechtskosten in strafzaken en gelijkgestelde kosten worden toegekend, geverifieerd, betaald en teruggevorderd, *BS* 27 december 2019.

KB 8 november 2016 tot wijziging van het koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie, betreffende de tarieven voor de vergoeding van de medewerking, *BS* 22 december 2016.

KB 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 8 oktober 2013.

KB 6 januari 2011 tot bepaling van de werkingsregels van de nationale en lokale informantenbeheerders en van de contactambtenaren, *BS* 18 januari 2011.

KB 12 oktober 2010 houdende de nadere regels voor de wettelijke medewerkingsplicht bij vorderingen door de inlichtingen- en veiligheidsdiensten met betrekking tot elektronische communicatie, *BS* 8 november 2010.

KB 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 109ter, E, § 2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *BS* 10 februari 2003.

Omz. 131/12 over de indexering van de tarieven van de gerechtskosten in strafzaken en de gelijkgestelde kosten, *BS* 9 januari 2025.

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. 55-2572/001.

Wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, KAMER, 2017-2018, 11 juni 2018, nr. 54-3126/001.

Wetsontwerp houdende wijziging van het Wetboek van Strafvordering en van de wet van 22 maart 1999 betreffende de identificatieprocedure via DNA-onderzoek in strafzaken, KAMER, 2010-2011, 26 mei 2011, nr. 53-1504/001.

Wetsontwerp tot verbetering van de strafrechtspleging in het stadium van het opsporingsonderzoek en het gerechtelijk onderzoek, KAMER, 1996-1997, 19 december 1996, nr. 857/1-96/97.

Wetgeving Amerika

U.S. Const. amend. IV. (1789).

Vermont General Assembly. (n.d.). *Vermont Consumer Protection Act*, 9 V.S.A. § 2451 et seq.

California State Legislature. (2018). *California Consumer Privacy Act of 2018*, Cal. Civ. Code § 1798.100 et seq.

U.S. Congress. (2018). *Clarifying Lawful Overseas Use of Data Act* (H.R. 4943).

Rechtsleer

Boeken

BAILLIEUX, A., *Afstand van recht in de strafprocedure: Zelfbeschikking bij een traditionele afhandeling van een strafprocedure*, Intersentia, 2019.

BENICHIU, B., KINDT, E. en BEUDELS, M., *Informatie en recht: Informatieverplichtingen in het gegevensbeschermingsrecht: much ado about nothing?*, Intersentia, 2021.

BENSOUSSAN, A., HENROTTE, J., GALLARDO, M. en FANTI, S., *[General Data Protection Regulation] Annexes*, Wolters Kluwer, 2018.

BERBUTO, S., THEVISSEN, P. en MONVILLE, P., *Droits de la défense – L'article 6 de la Convention Européenne des Droits de l'Homme*, Wolters Kluwer, 2025.

BERKMOES, H., *Identificatie van (gebruikers van) elektronische communicatie*, Wolters Kluwer, 2023.

BERKMOES, H., *Informatenwerking (bijzondere opsporingsmethoden)*, Wolters Kluwer, 2022.

BERKMOES, H., *Interceptie van privécommunicatie en gegevens van een informaticasysteem*, Wolters Kluwer, 2022.

BERKMOES, H., *Inkijkoperatie ('klassiek' en in 'IT-systemen')*, Wolters Kluwer, 2023.

BLOCKMANS, T. en MORTIER, T., *Begrotingswetgeving anno 2024: Ontstaan, structuur en recente ontwikkelingen in de Belgische budgettaire wet- en regelgeving*, Intersentia, 2024.

BRULOOT, D., DE GROOTE, B. en DE CORTE, R., *Privaatrecht in hoofdlijnen: Strafrecht en strafrechtspleging*, LeA Uitgevers, 2022.

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

CONINGS, C., *Infiltratie op het internet*, Wolters Kluwer, 2022.

DE BOT, D., *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Wolters Kluwer, 2020.

DEBRUYNE, N. *Commerciële exploitatie de menselijke afbeelding, naam en stem: Deel I: Normatief kader en commercialisering*, die Keure, 2021.

DE POORTER, I., *Financiële regulering: een dwarsdoorsnede: De 'GDPR' of Algemene Verordening Gegevensbescherming (AVG)*, Intersentia, 2019.

DEPREZ, S., FOCQUET, A. en MANNEKENS, J., *Gegevensbescherming: Bos door de bomen*, LeA, Uitgevers, 2022.

DESTERBECK, F. en VAN DROOGBROECK, J., *De inbeslagneming en verbeurdverklaring in strafzaken in België: De inbeslagneming*, Wolters Kluwer, 2017.

DE BOIS, A., *Commercieel gebruik van persoonsgegevens*, Intersentia, 2017.

DE BRUYNE, J., VALCKE, P., HENDRICKX, V. en GIELEN, G., *Technologie en recht, online privacy*, Owl Press Legal, 2025.

DE SMEDT, B., *Handboek deskundigenonderzoek*, Wolters Kluwer, 2024.

DE SMET, B., *Registratie en lokalisatie van elektronische communicatie*, Wolters Kluwer, 2019.

DE SMEDT, J., *De complexe verhouding tussen het Openbaar Ministerie en de fiscale administratie: Bescherming van persoonsgegevens bij gegevensuitwisseling*, Intersentia, 2024.

DELBROUCK, I., *Aanranding van de eerbaarheid en verkrachting: Enige aspecten van strafprocesrecht*, die Keure, 2015.

DERUYCK, F., *Overzicht van het Belgisch Strafprocesrecht*, die Keure, 2024.

DE WOLF, T., *Zakboekje strafprocesrecht: (Het gerechtelijk onderzoek): De onderzoeksdaden binnen het gerechtelijk onderzoek*, Wolters Kluwer, 2023.

DELFORGE, A., *La jurisprudence de l'APD en matière de marketing direct*, Intersentia, 2024.

EVERS, F. en VAN CAUWENBERGE, K., *Op-recht-uit. Een hulde aan Alain Bloch: De onderzoeksrechter*, die Keure, 2022.

KESTEMONT, L. en SCHOUKENS, P., *Rechtswetenschappelijk schrijven*, Acco, 2020.

LINERS, A., VANDERHEYDEN, K., VAN VOLSEM, F. en DE WOLF, T. *Zakboekje strafprocesrecht*, Wolters Kluwer, 2023

MASSCHELEIN, M., *Arbeidsgerechten en sociaal procesrecht: Beginselen die de grenzen van de rechter bepalen*, Wolters Kluwer, 2018.

MEULEMAN, B. en ROOSE, H., *Kennis maken - methodologie voor sociale wetenschappers*, Gent, 2021.

ROZIE, J. en TERSAGO, P., *Ondernemingsstrafrecht: Het gegevensbeschermingsrecht vanuit strafrechtelijk perspectief. Misdrijven in de AVG en de Belgische kaderwet aangestipt*, LeA Uitgevers, 2023.

ROYER, S., *Strafrechtelijk beslag: digiproof en (multi)functioneel*, die Keure, 2020.

SAELENS, R., *De sleutel rond anonimiteit opgelicht... Identiteits-, privacy-, - en persoonsgegevensafscherming in het strafprocesrecht en politierecht: De wet op het politieambt*

na de Aanpassingswet van 22 mei 2019 in het licht van de Richtlijn Politie en Justitie: een beknopte verkenning van de verwerking van persoonsgegevens voor opdrachten van bestuurlijke en gerechtelijke politie, die Keure, 2023.

SCHRAM, F., *Handboek Privacy en Persoonsgegevens*, Politeia, 2023.

SUSTRONCK, O., *[Verwerking van persoonsgegevens] Inleiding: we hebben niets te verbergen, toch? - Het belang van een degelijk privacybeleid – Wettelijk kader*, Wolters Kluwer, 2017.

VANSWEEVELT, T. en BROECKX, N., *Handboek gezondheidsrecht: Privacy, persoonsgegevens en beroepsgeheim*, Intersentia, 2022.

VANDENHOLE, W., *Economische, sociale en culturele rechten: Verbod op discriminatie en recht op gelijke behandeling*, Wolters Kluwer, 2021.

VIANGALLI, F., *Transferts internationaux de données: entre libre circulation et impératifs sécuritaires*, Larcier, 2019.

Tijdschriften

ARNOU, L., 'Zoeking op grond van artikel 6bis Drugwet en huiszoeking bij heterdaad zijn twee verschillende zaken', *NC* 2021/1, 34.

BAILLEUX, A., 'Grootschalig DNA-onderzoek: heiligt de efficiënte strafprocedure de opoffering van de grondrechten van het individu?', *NC* 2013/44, 269.

CAREEL, S. en ROYER, S., 'Voorontwerp dataretentiewet: derde keer, goede keer?', *Juristenkrant* 2021/432, 10.

CONINGS, C. en DE KEERSMAECKER, R., 'To save but not too safe: hoogste Belgische rechters zien geen graten in het decryptiebevel voor de verdachte', *T.Strafr.* 2020/3, 163.

CONINGS, C., 'Dataretentieplicht en privacy' (noot onder GwH 11 juni 2015), *NJW* 2015, 911.

CUYKENS, S., 'Les limites de l'ingérence publique dans le domicile', *Rev.trim.D.H.* 2023/135, 803.

DE COSTER, T., 'De huiszoeking bij heterdaad en in toepassing van artikel 6bis, lid 3 van de wet van 24 februari 1921: een bron van blijvende cassatierechtspraak', *T. Strafr.* 2022/6, 325.

DEPAEPE, H. en SEYEN, K., 'Opsporing en vervolging van misdrijven. Technische overdracht van gegevens', *NJW* 2022/454, 2.

DUINSLAEGER, P., 'Het vermoeden van onschuld', *RW* 2017/17, 643.

GDNEDASJ, S., 'Visatie: artikel 15 Grondwet biedt meer bescherming dan EVRM', *Fisc.Act.* 2018/30, 10.

HERBOTS, P. en DRIESSEN, M., 'DNA-wet aangepast aan wetenschappelijke vooruitgang', *Juristenkrant* 2024/489, 3.

HUYBRECHTS, L. en ROZIE, M., 'De rechten van de verdediging bij de behandeling ten gronde', *NC* 2008/2, 109.

INCALZA, T., 'Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming', *Jura Falc.* 2011/2, 329.

KUTY, F., 'Justice pénale et procès équitable', *O.C.* 2006/1, 994.

LANCKSWEERDT, E., 'De toekomst van de mensenrechten in turbulente tijden', *Juristenkrant* 2025/506, 12.

LEESTMANS, D., 'Men moet maar eens stoppen met in vakjes te denken', *Juristenkrant* 2019/391, 10.

LIEGEOIS, Y. en BLEYEN, F., 'Na een schijnhuwelijk en een schijnscheiding thans een gedwongen opname? Of de (uitoefening van de) rechten van de natuurlijke persoon bij verwerking van diens persoonsgegevens in het strafproces', *NC* 2020/0, 1.

MORANDINI, M., HUGUES, S. en HAUSMAN, J., 'La loi ADN en pleine mutation: entre révolution spontanée et altération des droits humains?', *AJT* 2025/5, 89.

MICHAIL, N., 'Le domaine d'application du GDPR: de sa portée hors de l'Union à sa mise en œuvre dans l'Union', *TBH* 2019/1, 52.

PANZAVOLTA, M., ROYER, S. en SEVERIJNS, H., 'Algemene dataretentie: ten minste houdbaar tot...?', *T. Strafr.* 2018/1, 3.

PARREIN, F., 'Kroniek Hof van Cassatie – Rechtspraak publiek- en administratief recht 2022', *TBP* 2023/6, 367.

PYPE, L., 'De verwerking van persoonsgegevens door de pers: ook de AVG vraagt om een afweging tussen de persvrijheid en het recht op de eerbiediging van het privéleven', *TPP* 2023/2, 4.

ROYER, S. en CAREEL, S., 'Houdbaarheidsdatum voor algemene dataretentie voor criminaliteitsbestrijding is verstreken', *Juristenkrant* 2020/416, 1.

ROYER, S., 'Iedereen wordt geacht ... de toegangscode van zijn gsm te kennen', *T.Strafr.* 2023/2, 114.

ROYER, S., 'Inlichtingen over toegang tot informaticasysteem', *T.Strafr.* 2024/4, 277.

ROYER, S., 'Verbod op anonieme belkaarten blijft overeind', *Juristenkrant* 2021/438, 2.

ROYER, S., '[Datagedreven onderzoeken] Cassatie verwerpt procedurele bezwaren tegen Sky ECC-onderzoek', *T.Strafr.* 2024/2, 99.

ROYER, S. en CONINGS, C., 'Verzamelen en vastleggen van digitaal bewijs in strafzaken', *NC* 2017/4, 311.

RUSHMEIER, H. 'Data Brokers and European Digital Legislation', *EDPL* 2023/1, 37.

STEVENS, D., 'Privacybescherming', *Computerr.* 2023/1, 72.

TERSAGO, P. 'Doorzoeken van smartphones en computers: Vrijwillige afgifte vereist geen mededeling zwijgrecht of bijstand van een advocaat', *Juristenkrant* 2023/468, 10.

TERSAGO, P., 'Hergebruik van telecommunicatiegegevens in strafzaken: horen, zien en zwijgen?', *Juristenkrant* 2023/475, 4.

TUTS, P., 'Het aanvechten van internationale wapenleveringen voor de rechter: wanneer de Luikse metallo's de bui reeds voelden hangen', *TBP* 2024/1, 5.

VAN DE HEYNING, C., 'Ernst van het misdrijf is een onvoldoende reden om procedurele garanties voor de zoeking in informaticasystemen te omzeilen', *T.Strafr.* 2017/6, 365.

VAN DE HEYNING, C., 'Het Mensenrechtenhof weigert een uitzonderingsregime voor versleuteld bewijs in strafzaken', *T.Strafr.* 2024/1, 33.

VAN DE HEYNING, C., 'Het gebruik van communicatiegegevens in strafzaken: hoe het Hof van Justitie het Belgische strafrecht hertekent', *T.Strafr.* 2025/2, 66.

VAN DEN BRANDE, B., 'Ook God ontsnapt niet aan de AVG', *TPP* 2018, 34.

VANDENBRUWAENE, P., 'Dataretentie: de zoektocht naar een veilige haven', *RW* 2023/9, 323.

VAN DEN BERGE, Y., 'De kamer van inbeschuldigingstelling waakt over de toepassing van de bijzondere opsporingsmethoden in proactief onderzoek', *RABG* 2012/2, 121.

VAN DE HEYNING, C., 'Not all that glitters is gold: een effectief recht op tegenspraak in tijden van bulkdata', *T.Strafr.* 2021/4, 195.

VAN DEN HENDE, T., 'Het onderscheid tussen proactief en reactief onderzoek in strafzaken', *Vigiles* 2002/4, 140.

VAN MOER, E., 'De rechten van verdediging in een efficiënt procesverloop', *T.Strafr.* 2024/4, 250

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

VAN VOLSEM, F., 'De huiszoeking op grond van artikel 6bis, derde lid Drugwet', *RABG* 2022/18, 1322.

VERNIMMEN, K., 'Verantwoordt de coronacrisis een speciale behandeling van in verdenking gestelden in voorlopige hechtenis?', *T. Strafr.* 2022/6, 315.

VROONEN, B., 'De strengere evenredigheidstoets bij het recht op bescherming van persoonsgegevens: lucky shot of kentering in de rechtspraak?', *TBP* 2024/9, 580.

YPERMAN, W., 'De bestrijding van terrorisme en strafprocesrecht: vele kleintjes maken een grote',
T.Strafr. 2019/1, 8.

Rechtspraak

EHRM 7 februari 2018, 24703/15.

EHRM 18 september 2017, 67496/10 en 52936/12.

EHRM 18 april 2013, 26419/10.

EHRM 28 november 2011, 30194/09.

EHRM 4 december 2008, 30562/04.

EHRM 4 december 2008, 30566/04.

EHRM 4 mei 2000, 28341/95.

HvJ 4 oktober 2024, C-548/21, ECLI:EU:C:2024:830.

HvJ 22 juni 2021, C-439/19.

GwH 26 september 2024, 97/2024.

GwH 12 oktober 2023, 131/2023.

GwH 22 september 2022, 110/2022.

GwH 9 december 2021, 177/2021.

GwH 22 april 2021, 57/2021.

GwH 14 januari 2021, 2/2021.

GwH 11 juni 2015, 84/2015.

Cass. 9 november 2021, P.21.1370.N.

Cass. (2e k.) 2 juni 2015, AR P.15.0263.N.

Cass. 29 april 2009, AR P090578F.

Cass. 14 oktober 2003, RW 2003/04, 814, concl. DE SWAEF, M.

Gent 30 januari 2002, *Vigiles* 2002/4, 138, noot VAN DEN HENDE, T.

Beslissing Gegevensbeschermingsautoriteit 16 januari 2024, 7/2024.

Beslissing Gegevensbeschermingsautoriteit 16 november 2022, 163/2022.

Beslissing Gegevensbeschermingsautoriteit 27 januari 2021, 04/2021.

Andere bronnen

COC, 'Bijzonder toezicht op de passagiersinformatie-eenheid door het Controleorgaan op de politionele informatie in het kader van zijn controle en toezichtbevoegdheden als bevoegde Toezienhoudende autoriteit', *Controleorgaan op de politionele informatie* 11 oktober 2022, www.controleorgaan.be/files/DAB21001-Rapport-BELPIE_Publieke-versie_nl_00069899.pdf (geraadpleegd op 27 juli 2025).

CONSTANTINESCU, E., 'What are data brokers, and how do they work?', *Proton* 20 juni 2025, [https://proton.me/blog/databrokers#:~:text=Data%20brokers%20are%20companies%20or,campaigns%20\(for%20voter%20targeting\)](https://proton.me/blog/databrokers#:~:text=Data%20brokers%20are%20companies%20or,campaigns%20(for%20voter%20targeting)) (geraadpleegd op 25 juli 2025).

FOD Justitie, 'Budget: missie en visie', *Federale Overheidsdienst Justitie*, https://justitie.belgium.be/nl/overheidsdienst_justitie/organisatie/stafdiensten/budget_en_behoerscontrole (geraadpleegd op 22 juli 2025).

Google, 'Government requests', *Google Transparency Report* 20 januari 2025, <https://transparencyreport.google.com/governmentrequests> (geraadpleegd op 18 juli 2025).

HEYMANS, P. en HIROUX, H., 'Grondwettelijk Hof vernietigt wet op bijhouden van telefoondata: wat betekent dat voor jou? En voor politie en parket?', *VRT NEWS* 22 april 2021, <https://www.vrt.be/vrtnws/nl/2021/04/07/dataretentie/> (geraadpleegd op 26 juli 2025).

WEINER, R. en HARWELL, D. 'Google location data was used to find Jan. 6 rioters. It's disappearing', *The Washington Post* 8 januari 2024, <https://www.washingtonpost.com/dc-md-va/2024/01/06/jan-6-google-location-warrants/> (geraadpleegd op 19 juli 2025).