Privacy en Politie

Door: Mariska Temming en Isa Verkruyssen
Begeleider: meneer Janssen
Vak: maatschappijleer
Datum: 10 januari 2017

Inhoudsopgave

Hoofdstuk 1 Voorwoord

Wij hebben hard gewerkt aan het profielwerkstuk en zijn zeer tevreden over het eindresultaat. Wij willen graag een aantal mensen bedanken voor hun hulp. Als eerste bedanken we de mensen die wij hebben geïnterviewd, met dank aan Remco Verhoef (data-analist) en Ingrid de Vries (rechercheur).
In het bijzonder willen we Bas Eikelenboom (teamchef onderzoeken landelijke recherche) bedanken, hij heeft ons veel informatie geven en geholpen met complexe onderwerpen zoals datamining; hoe dat in zijn werk gaat. Bas heeft zijn datavisualisatietool (middel) aan ons laten zien, hoe je met behulp van Big Data data van bijvoorbeeld telefoons kunt analyseren. Hierdoor kregen wij een goed overzicht van hoe de theorie in praktijk te werk gaat.

Criminaliteit is een actueel onderwerp dat goed bij ons past. We wilden graag iets kiezen wat we allebei interessant vonden en dat past bij ons vervolgstudie. Mariska wil graag Forensisch-ICT studeren in Leiden en Isa weet het nog niet precies, maar heeft belangstelling voor maatschappelijke problemen. In dit onderwerp komen onze beide interesses samen, waardoor we dus allebei met veel plezier aan het profielwerkstuk kunnen werken.

Criminaliteit speelt een grote rol in onze samenleving en nieuwe vormen zoals cybercrime groeit momenteel explosief[1]. Als je veel leest op het internet over criminaliteit, vind je een groot dilemma. Hoe moet de politie veiligheid, in een maatschappij die al meer digitaal wordt, garanderen en tegelijkertijd er voor zorgen dat onze privacy zo min mogelijk wordt geschonden. Het dilemma vonden we best wel moeilijk en leek het ons leuk om dit te onderzoeken.

In ons profielwerkstuk gaan wij in sommige hoofdstukken ook in op misbruik van kinderen en dus ook kinderporno. Dit doen we omdat wij zelf kindermisbruik de ergste vorm van criminaliteit vinden. Na gesproken te hebben met Bas Eikelenboom en andere rechercheurs op dat gebied, kregen wij een beter beeld van hoeveel kinderporno er op het internet is verspreid en hoe erg de kinderen kunnen worden misbruikt. De kinderen waar we het dan over hebben, zijn minderjarig van 0 tot en met 16 jaar.
Wij vonden het leuk en interessant onderwerp en wilden graag jullie onze kennis delen. Wij hopen met ons profielwerkstuk jullie iets te kunnen leren over hoe veiligheid en privacy samen in z’n werk gaan.

---

[1] https://rejo.zenger.nl/files/20090000-criminaliteitsbeeldanalyse-2009-high-tech-crime.pdf

1.1 Inleiding

Actueel zijn vele berichten over aanslagen en bij ieder onderzoek zijn er linken naar georganiseerde criminaliteit[2][3]. Telkens als er kinderporno opduikt of als er na een aanlag een onderzoek plaatsvindt, ontstaat de vraag waar de dader geweest- en waarom hij niet tegengehouden is. Zeker als blijkt dat hij al eerder opgevallen was bij onderzoeken naar kinderporno, wapen- of drugshandel. Het probleem blijkt dan vaak te zijn dat de politie geen bevoegdheden had om heel veel data op te vragen of om mensen structureel te monitoren omdat onder andere privacywetgeving dan in de weg lijkt te zitten. Ons leek dit een belangrijk gegeven en wij stelden ons de vraag of onze privacy van een groter belang was dan onze veiligheid. Maar ook hoe dat dan zit binnen ons land.

Het lijkt wel of de (cyber)criminaliteit op de wereld steeds heftiger wordt. Er vinden liquidaties plaats op klaarlichte dag, banken worden gehackt, er wordt gehandeld in drugs en kinderporno wordt verspreid alsof het niets is. De overheid wilt dit natuurlijk oplossen maar stuit dan op een probleem, want als ze iets willen ondernemen moeten ze de privacy van de burgers schenden. Maar als ze niets ondernemen zullen grote (cyber)criminelen nooit worden opgepakt. In ons profielwerkstuk zullen we stap voor stap uitleggen hoe dit allemaal in elkaar zit en of dit opgelost kan worden. Het vermogen om misdrijven op te lossen wordt door veel mensen gekoppeld aan hun veiligheidsgevoel. Hoe beter de politie zaken aanpakt en oplost hoe veiliger mensen zich voelen. De hoofdvraag die we uiteindelijk zullen beantwoorden is: *hoe zorgt de politie voor de veiligheid van burgers en wordt schending van privacy voorkomen?*

Om deze hoofdvraag te beantwoorden, hebben wij een aantal deelvragen opgesteld. Als eerste zullen we uitleggen wat het dilemma van de rechtstaat precies inhoud, dit doen we aan de hand van theorie en een aantal praktische voorbeelden om je zo een helder beeld te geven. Vervolgens zullen we ingaan op een aantal belangrijke begrippen die belangrijk zijn in het profielwerkstuk. Als laatste zullen we een eindconclusie geven.

---

[2] http://www.dagelijksestandaard.nl/2016/07/isis-aanslag-in-parijs-nog-veel-erger-dan-gedacht-terroristen-martelden-hun-slachtoffers-in-bataclan/

[3] http://nieuws.tpo.nl/2017/01/28/efficient-criminelen-en-terroristen-werken-steeds-meer-samen/

Na het literatuuronderzoek, wilden wij nog meer weten en nuttige vragen stellen aan de professionals. Hiervoor hebben we een aantal specialisten gesproken en geïnterviewd. We hebben gesproken met Bas Eikelenboom, teamleider bij de landelijke recherche. Met Bas hebben we goede contacten (hij speelt in het orkest waar Mariska ook in zit). Daarna zijn we op bezoek geweest bij een data-analist, een jurist, een advocaat, en een rechercheur, die we ook geïnterviewd hebben. Ook vonden we de mening van de burgers belangrijk en hebben dit verwerkt in het profielwerkstuk aan de hand van een enquête. Verder hebben wij ons verdiept in de verschillende standpunten van de politieke partijen.
Onze veiligheid vinden wij het meest belangrijk en wij hebben daar best een stuk van onze privacy voor over. Niet al onze privacy want ieder mens heeft zeker recht om dingen voor zichzelf te bewaren.
Een belangrijk onderdeel was dat in ons land gelukkig veel is geregeld via Wetgeving. Dat komt omdat wij leven in een rechtsstaat. Het is belangrijk dat mensen grondrechten hebben. En dat de rechtsstaat zorgt voor veiligheid maar ook privacy van de burgers. En daar zit eigenlijk een probleem wat wij tegenkwamen, namelijk het dilemma van de rechtsstaat. Privacy versus Veiligheid.

Hoofstuk 2 Wat is het dilemma van de rechtsstaat?

2.1 Wat is een rechtsstaat?

We leven in Nederland in een rechtsstaat. Dat betekent dat iedereen, dus alle inwoners van Nederland, maar ook de overheid (zoals de Eerste en de Tweede Kamer, het Koninklijk Huis, de politie en het Openbaar Ministerie), zich moeten houden aan de wetten en regels die we in Nederland met elkaar afgesproken hebben.

Een doel van de rechtsstaat is om voor de veiligheid van de burgers te zorgen. Doordat de macht van de overheid wordt beperkt door wetten, regels en gewoonten worden de burgers beschermd tegen machtsmisbruik van de overheid. Ook zorgt de rechtsstaat dat de burgers gelijk worden behandeld en dat ze in vrijheid kunnen leven. Om deze waarden[4] te garanderen zijn er hiervoor vier grondbeginselen die in de rechtsstaat belangrijk zijn: grondrechten, de scheiding van de machten (in een wetgevende, uitvoerende en rechterlijke macht), de onafhankelijke rechtspraak en het legaliteitsbeginsel.

Zonder rechtsstaat kan er geen democratie bestaan, want alleen in een rechtsstaat kunnen burgers gebruik maken van politieke grondrechten. De rechtsstaat is dus een voorwaarde voor een democratie. In landen waar geen onafhankelijke rechtspraak bestaat, komen burgerrechten in het gedrang en ligt machtsmisbruik op de loer. “Een rechtsstaat is een staat waarin vrijheid, rechtszekerheid en rechtsgelijkheid voor de burger heel belangrijk zijn. Bovendien geniet de burger bescherming van zijn rechten en vrijheden, tegen medeburgers én tegen de overheid”.[5]

[4] Een waarde is een uitgangspunt of principe dat belangrijk is in je leven. Boek maatschappij-leer Havo 4/5.

[5] https://www.prodemos.nl/leer/informatie-over-politiek/wat-is-een-rechtsstaat/

2.2 Wat is een grondrecht?

In de rechtsstaat worden de burgers door middel van grondrechten beschermd tegen machtsmisbruik van de overheid. In Nederland bestaat de rechtsstaat uit diverse rechten welke in een juridisch stelsel gecontroleerd en verdedigd worden. Zo doet de politie door middel van onderzoeken aan ‘waarheidsvinding’; dat wil zeggen dat ze de feiten en omstandigheden uitzoeken waaronder een vermoed strafbaar feit heeft plaatsgevonden. Het Openbaar Ministerie, met behulp van de Officier van Justitie, toetst de rechtmatigheid van de onderzoekshandelingen van de politie en brengt de verdachte, om deze te vervolgen, voor de rechtbank. De rechters bepalen uiteindelijk of iemand veroordeeld wordt, zij controleren de totale procesgang. Belangrijk daarin zijn ook de advocaten die de verdediging van de verdachte doen. Tenslotte is ook heel erg belangrijk dat een verdachte niet hoeft mee te werken aan zijn eigen veroordeling, hij heeft bijvoorbeeld zwijgrecht. Zwijgrecht is een grondrecht. Politie moet dus waarheidsvinding doen met gebruik van bepaalde bevoegdheden. Een voorbeeld is dat een Officier van Justitie geen zware bevoegdheden afgeeft voordat de politie voldoende de redenen van wetenschap omschreven hebben waarom iemand verdachte is in het kader van artikel 27 Wetboek van Strafrecht[6].
Grondrechten worden ook wel fundamentele rechten of mensenrechten genoemd, deze zijn opgenomen in hoofdstuk 1 van de Nederlandse Grondwet. De grondwet bevat de regels voor de inrichting van de staat.

2.3 Waaruit bestaat de inrichting van de staat met de grondwet?

1. Grondrechten: Grondrechten worden ook wel fundamentele rechten of mensenrechten genoemd. Ze zijn opgenomen in hoofdstuk 1 van de Nederlandse Grondwet. De grondwet bevat de regels voor de inrichting van de staat.

   Er zijn twee soorten grondrechten: klassieke- en sociale grondrechten.

   - Bij klassieke grondrechten gaat het over de vrijheidsrechten die in artikel 1 tot en met 17 in de Grondwet staan, zoals: recht op gelijke behandeling (artikel 1), kiesrecht (artikel 4), vrijheid van meningsuiting (artikel 7), en recht op privacy (artikel 10). De overheid moet deze grondrechten ook echt garanderen en als ze dit niet goed doen, dan kan je naar de rechter gaan.

[6] http://www.wetboek-online.nl/wet/Sr/27.html

- Bij sociale grondrechten moet de overheid zich actief opstellen, de overheid moet haar best doen om bijvoorbeeld iedereen werk te geven, maar als jij geen werk hebt kun je niet naar de rechter stappen en eisen dat je een baan krijgt, zo werkt dat niet. Een ander voorbeeld van sociale grondrechten is het recht op gezondheidszorg en het recht op woongelegenheid (artikel 22).

2. De rechterlijke macht is in een rechtsstaat de macht waaraan de rechtspraak is opgedragen. De andere machten zijn de wetgevende macht en de uitvoerende macht. Een van de kenmerken van een rechtsstaat is een scheiding tussen de drie machten. Dit is om onafhankelijkheid van de rechterlijke macht te waarborgen. Daarin is scheiding der machten belangrijk. De scheiding der machten wordt ook wel trias politica genoemd. Dat betekent dat de scheiding van de politieke macht gesplitst wordt in drie onderdelen die elkaar kunnen controleren en verbeteren. Dit zijn de wetgevende macht, de uitvoerende macht en de rechterlijke macht.
    - De wetgevende macht bestaat uit het parlement (de Eerste Kamer en de Tweede Kamer) en de regering. De regering komt met wetsvoorstellen waarbij het parlement moet instemmen, anders kan het geen wet worden.
    - De uitvoerende macht bestaat uit de regering. Dit omdat de regering leiding geeft aan hun ministeries en ambtenaren. Deze houden zich bezig met de uitvoering van wetten en moet verantwoording afleggen aan de wetgevende macht.
    - De rechterlijke macht in Nederland bestaat uit de rechters en de Officieren van Justitie. Deze Officieren van Justitie vormen het Openbaar Ministerie (OM). De rechters spreken recht op basis van wetten, verdragen, gewoonten en eerdere rechterlijke uitspraken (jurisprudentie). Het OM vervolgt verdachten van een strafbaar feit.

3. Legaliteitsbeginsel: Het legaliteitsbeginsel gaat over twee zaken: ten eerste moet alles wat de overheid doet, gebaseerd zijn op de wet. Ten tweede mag je pas gestraft worden als hetgeen eerst strafbaar is gesteld.

4. Onafhankelijke rechtspraak*:* In een rechtsstaat komen rechters op een onafhankelijke en onpartijdige manier tot hun oordeel. Om dat zo te houden is er afgesproken dat rechters niet ontslagen kunnen worden, rechters mogen niet zomaar allerlei bijbanen of nevenfuncties hebben en rechters moeten mogen niet hun eigen persoonlijke overtuigingen laten meespelen.

De rechtstaat heeft meer belangen dan opsporing en vervolging. Doordat data toeneemt is er al meer te vinden over mensen en door verschillende soorten data met elkaar te combineren kunnen er heel veel gegevens over mensen gevonden worden, en vaak over een enorme lange periode. Dit heeft ervoor gezorgd dat behalve de normale grondrechten het recht om bijvoorbeeld vergeten te worden is vastgelegd. Het vastleggen van deze beschermende maatregelen wordt in de privacywetgeving geregeld. Door de privacy van mensen te beschermen worden de opsporingskansen mogelijk minder en daarover zijn flinke discussies ontstaan[7][8].

[7] https://www.privacybarometer.nl/maatregel/37/Bewaarplicht_telecomgegevens

[8] https://www.privacynieuws.nl/internet-en-telecom/bewaarplicht.html

Hoofdstuk 3 Dilemma: privacy versus opsporing

3.1 Opsporing

Het Openbaar Ministerie (OM), middels Officieren van Justitie, vervolgt verdachten van strafbaar feiten. Deze strafbare feiten zijn benoemd in het Wetboek van Strafrecht. Eerst moet de politie genoeg bewijsmateriaal verzamelen en verwoorden in dossiers. Dossiers zijn bijvoorbeeld persoonsdossiers; die geven aan per persoon wat deze precies gedaan heeft, maar er zijn ook zaakdossiers, daarin wordt omgeschreven wat de rol van iedere persoon binnen een onderzoek was. Die dossiers bestaat uit meerdere processen-verbaal. Het verzamelen van bewijs gebeurt met behulp van bevoegdheden gegeven in het Wetboek van Strafvordering en moet terug te vinden zijn in de processen-verbaal en dossiers.

Het OM valt onder de verantwoordelijkheid van de Uitvoerende Macht namelijk de minister van Veiligheid en Justitie. De minister geeft aan hoe het OM moet werken. Daarom is de minister politiek verantwoordelijk als het OM fouten maakt. De verdachten moeten bij een vervolging voor de rechters verschijnen. De rechter bepaalt uiteindelijk als laatste in de rechtszaal of de gebruikte opsporingsmethodieken gerechtvaardigd waren en of de verdachten schuldig of onschuldig waren. Binnen een strafrechtelijk onderzoek worden gedurende de tijd veel gegevens verzameld; deze gegevens moeten wel rechtmatig verkregen zijn. Op basis van die gegevens worden gedurende een onderzoek al beslissingen genomen, bijvoorbeeld beslissingen die een behoorlijk zware impact op de persoonlijke levenssfeer van een verachte kunnen hebben. Hierbij moet gedacht worden aan het iedere dag volgen van mensen, hun gesprekken afluisteren of het plaatsen van camera’s . Al deze middelen leveren gegevens op die gebruikt kunnen worden om te bewijzen dat iemand een strafbaar feit heeft begaan. Dat daarmee de verdachten de wet overtreden hebben, valt terug te lezen in een vonnis.

Het dilemma van de rechtsstaat komt dan tot uiting in de botsende belangen (waarden) van de rechtsbescherming en rechtshandhaving. Dit heeft te maken met subsidiariteit en proportionaliteit.[9] Dat wil zeggen dat we aan de ene kant beschermd willen worden tegen criminaliteit, maar aan de andere kant ook willen dat we tegen de overheid beschermt worden in verband met onze vrijheden en privacy. En er moet een goede balans ontstaan tussen hoever de politie mag gaan voor een onderzoek, en in hoeverre de privacy van de burgers daarbij mag worden geschonden.

[9] http://juribus.eu/proportionaliteit-en-subsidiariteit/

Het is onmogelijk om de veiligheid te garanderen en tegelijkertijd te zorgen voor honderd procent privacy. De politie moet bijvoorbeeld om aan informatie te komen iemands huis binnen gaan, en in de persoonlijke spullen van de bewoners zoeken. Ook luistert de politie (onschuldige) burgers/criminelen af en worden voortdurend beelden van ze gemaakt. Vanwege de enorme impact op de persoonlijke levenssfeer zijn bepaalde bevoegdheden apart verwoord als bijzondere opsporingsbevoegdheden.[10]

Deze zogenoemde BOB wetgeving is gekomen nadat de IRT-affaire in Nederland gespeeld heeft. Deze affaire is gekomen nadat de politie zware opsporingsmethodieken in het verleden zonder goed wettelijk kader gebruikt heeft waardoor de privacy van mensen zwaar geschonden werd. De politie werkte toen in een interregionaal verband. Dat was een recherche-samenwerking tussen de korpsen Amsterdam, Noord-Holland, Kennemerland, Utrecht en Zaanstreek-Waterland. De politie besloot diep te infiltreren in de criminele-wereld en daardoor was het mogelijk dat de politie de criminelen voorzag van bijvoorbeeld vrachtauto's met chauffeur om verdovende middelen te vervoeren. Hierbij waren de afspraken tussen de politie en het Openbaar Ministerie te onduidelijk zodat het voor rechters niet meer te toetsen was of de informatie rechtmatig was verkregen. De BOB wetgeving eist dat er een verdenking moet zijn van bepaalde ernstige misdrijven, er moet een redelijk vermoeden zijn dat in georganiseerd verband misdrijven worden gepleegd die een ernstige inbreuk op de rechtsorde opleveren of er moeten aanwijzingen zijn dat een terroristisch misdrijf wordt gepleegd. Dit laatste is geregeld door de wet Verruiming mogelijkheden tot opsporing en vervolging van terroristische misdrijven.

[10] http://wetten.overheid.nl/BWBR0021581/2004-12-01

3.2 Dillemma's

Niemand vindt het leuk als zijn of haar privacy geschonden wordt, maar wat nu als de politie hierdoor een terrorist kan oppakken, of een pedofiel? Is het dan nog steeds een probleem als de politie daarvoor een huis binnen is gegaan of gesprekken afgeluisterd heeft?

Ook is de vraag wat er eigenlijk van de politie verwacht wordt? Dat de politie repressief opspoort of ook moet voorkomen en tegenhouden? Repressief opsporen is gericht op iets wat al gebeurd is en daarmee op mogelijk bekende verdachten en daarvoor zijn er artikelen in het Wetboek van Strafvordering die kaders geven voor de te gebruiken bevoegdheden. Die kaders dienen onder andere voor de bescherming van de rechten van de burgers.

> Ingrid de Vries
> "Dat je wel steeds weer aan de voorkant ter voorkoming van het misdrijf wil komen. Dus preventief handelen door de politie, dit verwacht je ook als samenleving en houdt in dat je waarschijnlijk wetgeving moet veranderen. Bijvoorbeeld de politie voorkomt een liquidatie is gelijk aan 20 jaar celstraf. Ter vergelijk: in 26 koper werd een voorbereiding liquidatie bestraft met 8 jaar".

Als bovenstaande uitgelegd wordt, dan is er bij voorkomen en tegenhouden een andere situatie dan bij het opsporen van een mogelijk gekende verdachte. Er is namelijk meer sprake van een vermoeden tot bijvoorbeeld het voornemen hebben een misdrijf te plegen. Het misdrijf is dus nog niet gepleegd. Het is moeilijk om behoorlijke ingrijpende bevoegdheden af te geven op basis van het vermoeden dat iemand een strafbaarheid wil plegen, hij heeft immers nog niets gedaan. Maar het afwachten van hetgeen waar hij mee bezig is voor te bereiden kan andere mensen in groot gevaar brengen. Dit kan concreet uitgelegd worden aan de hand van de recente recherchezaken in verband met de Knokkestraat in Amsterdam[11] en de wapenvangst in Nieuwegein[12]. Iemand kan dan wel verdacht zijn, maar is dan nog geen verdachte in het kader van artikel 27 Wetboek van Strafrecht.[13] Er zijn dan onvoldoende feiten of omstandigheden die dit rechtvaardigen en daardoor kan een Officier van Justitie dan minder vaak toestemming geven voor het inzetten van bepaalde methodieken.

---

[11] https://www.youtube.com/watch?v=bolSSjDAVEo

[12] http://www.parool.nl/amsterdam/tot-acht-jaar-cel-in-megaproces-26koper~a4423772/

[13] http://www.wetboek-online.nl/wet/Sv/27.html

Daarvoor zijn er ook wel wetsartikelen, maar bij lichtere misdrijven kan het al snel een grove inbreuk op de privacy van iemand betekenen. Het gaat dus om de proportionaliteit en de subsidiariteit. Dus of het (voorgenomen) misdrijf de inzet van bepaalde opsporingsmiddelen kan rechtvaardigen, en de opsporingsmiddelen noodzakelijk zijn. In de hierboven genoemde zaak in de Knokkestraat in Amsterdam wordt dat ook duidelijk wat proportionaliteit dan eigenlijk is. Want in die zaak werden zware automatische vuurwapens aangetroffen in een gestolen auto maar de politie besloot de auto niet in beslag te nemen en maakte de wapens onklaar. Toen de auto uiteindelijk ging rijden en de politie het mogelijke slachtoffer van een liquidatie in veiligheid had gebracht, ontstond er een aanhoudingssituatie waarbij de auto van de verdachten door de politie opzettelijk aangereden werd en uiteindelijk werd ook een verdachte neergeschoten. Hierbij is dan het vraagstuk of het door de politie gebruikte geweld wel proportioneel was ten opzichte van de verdachte met een onklaar gemaakt wapen. Uit interviews met de politie, te zien in het YouTube filmpje, blijkt dat de politie van mening is dat dit proportioneel was omdat onbekend welke andere wapens de mensen bij zich konden hebben en dat de verdachten bereid waren geweld tegen de politie te gebruiken.

3.3 Privacy en inbreng van de burger

De privacy van mensen kan in het gedrang komen bij een justitieel onderzoek. Artikel 10 (recht op privacy) luidt:

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

In een rechtsstaat kunnen burgers die het niet eens zijn met de wetten en regels die afgesproken zijn, naar een onafhankelijke persoon (de rechter) toegaan om te vragen hoe het precies zit en rechterlijke uitspraak te vragen (recht te spreken). De rechter bepaalt dan op een eerlijke, onafhankelijke en onpartijdige manier wat wel en niet mag. Hij zorgt er zo voor dat voor iedereen dezelfde regels gelden. Als je voor de rechter moet komen, is het in veel gevallen verstandig (en soms verplicht) om een advocaat te nemen. Advocaten kosten veel geld. In een rechtsstaat is rechtsgelijkheid (wat in de grondwet staat) een voorwaarde.

Als je weinig geld hebt, dan kan je een beroep doen op gratis rechtsbijstand, een pro-deo advocaat. Deze advocaat is niet gratis, maar de verdediging wordt vanuit de staat betaald. Dit is belangrijk omdat anders alleen rijke mensen een advocaat kunnen nemen om zich te verdedigen en dat is dan niet rechtsgelijk. De rechtsstaat zorgt dus ook iedereen een goede verdediging kan krijgen.

3.4 Privacy, opsporing en mening van de burger

Als burgers de wetten en regels overtreden hebben, dan kan de politie verdachten opsporen en arresteren. Met behulp van allerlei onderzoeken doet de politie aan 'waarheidsbevinding'. Ze zoeken de feiten en omstandigheden uit waaronder een vermoedelijk strafbaar feit heeft plaatsgevonden. Het Openbaar Ministerie, de Officier van Justitie, toetst dan de rechtmatigheid van de onderzoekshandelingen van de politie en brengt de verdachte voor de rechtbank. In de rechtbank wordt een verdediging gevoerd door advocaten en uiteindelijk doet een onafhankelijke rechter uitspraak of iemand schuldig is of niet. In Nederland hoeft een verdachte niet mee te werken aan zijn eigen veroordeling. Hij heeft zwijgrecht, dat weer een grondrecht is.

Doordat de rechter onafhankelijk is, kan niemand de rechter dwingen om bepaalde beslissingen te nemen; zelfs de overheid kan dat niet. Hierdoor kunnen we beter op de rechter en zo dus op de rechterlijke macht vertrouwen. En dit geeft weer vertrouwen in de samenleving. Wie het niet eens is met de uitspraak van de rechter, kan in hoger beroep gaan bij het gerechtshof en daarna zelfs bij de Hoge Raad of het Europees Gerechtshof. Een hogere rechter kijkt dan opnieuw en dus met een frisse blik naar de zaak.

"Zeker in een samenleving die snel verandert, is duurzame steun voor de rechtsstaat geen overbodige luxe. Uit onderzoek blijkt weliswaar dat in Nederland, zeker in vergelijking met andere landen, het vertrouwen in de rechtsstaat tamelijk groot is. Maar ook blijkt die steun steeds minder vanzelfsprekend. Op onderdelen - politiek en strafrecht - is het vertrouwen zelfs broos, soms zelfs aan het afnemen en blijkt het niet erg stabiel, mede onder invloed van kwesties die veel publiciteit trekken."[14]

Geert Wilders van de PVV heeft 25 augustus 2016 het concept van zijn verkiezingsprogramma gepresenteerd. Hierin doet hij door voorstellen op een verbod op de koran, het sluiten van moskeeën en islamitische scholen, preventief opsluiten van "radicale moslims" en totale asielstop.

---

[14] https://www.rijksoverheid.nl/actueel/nieuws/2008/02/14/een-duurzame-rechtsstaat-vraagt-om-gezaghebbende-instituties-en-betrokken-burgers

Dit programma is onder andere in strijd met de vrijheid van godsdienst en de uitingsvrijheid en recht op een eerlijk proces. Met deze voorstellen gaat hij tegen in op de waarden van de Nederlandse rechtsstaat.

Voor ons profielwerkstuk hebben wij (Isa en Mariska) een enquête gehouden onder de bevolking. Honderd mensen hebben hier aan meegedaan, en er zijn een paar resultaten uitgekomen die vragen oproepen. Zo vind 66% het niet kunnen dat de politie de online gegevens van burgers aftapt en bewaart, maar vindt 42% ook dat de politie niet genoeg doet om criminelen op te sporen. Dit geeft dan ook perfect het dilemma weer. Want aan de ene kant willen we dat de politie meer doet om criminelen op te sporen, maar aan de andere kant willen we daar zelf geen stukje privacy voor opgeven. Toch zegt 50% van de mensen wel weer dat ze hun veiligheid belangrijker vinden dan hun privacy. Waarbij de andere 50% zegt dat ze hun veiligheid en privacy even belangrijk vinden, of zelfs hun privacy belangrijker vinden.

Hoofdstuk 4 Wat betekent de privacyschending voor het opsporen van criminelen?

De politie schendt natuurlijk niet zomaar de privacy van mensen. Ze zullen altijd een reden hebben, en een reden nodig hebben om een actie te ondernemen. Het is voor de politie onmogelijk om criminelen op te sporen en zaken op te lossen als ze geen informatie hebben. Deze informatie vinden ze bijvoorbeeld door het huis van een verdachte te doorzoeken of door zijn telefoon af te luisteren of uit te peilen. Hierbij schenden ze de privacy van deze persoon op een behoorlijke manier, en het zou kunnen zijn dat deze verdachte onschuldig blijkt te zijn, maar het zou ook kunnen dat hij een aanslag had gepland en dat hij nu op tijd wordt gestopt. Het schenden van privacy is dus van groot belang voor het opsporen van criminelen.

Bevoegdheden die de politie in kan zetten om aan informatie te komen kunnen zijn[15]: een huis doorzoeken, een telefoon uitpeilen of een foto of filmpje van de verdachte in de media verspreiden. Natuurlijk mag de politie dit niet zomaar doen en heeft zij hiervoor toestemming nodig van de officier van justitie, de Officier van Justitie (ook wel OvJ) heeft de leiding over het opsporingsonderzoek. De Officier van Justitie mag dus alleen toestemming geven voor inzet van bepaalde methodieken als er concrete aanwijzingen zijn dat er sprake is van een (ernstig) strafbaar feit. Een belangrijke maatstaf is of er voorlopige hechtenis[16] toegelaten is in relatie tot het strafbare feit. De strafbaarstelling is dan meestal vier jaar of meer gevangenisstraf. Voorbeelden van deze specifieke strafbare feiten zijn:

- computervredebreuk (hacking)
- bedreiging
- mishandeling
- verduistering
- witwassen
- het telen, bereiden, bewerken, verwerken, verkopen, afleveren, verstrekken of vervoeren van softdrugs / harddrugs
- invoer van bepaalde wapens en munitie

---

[15] https://www.politie.nl/themas/bevoegdheden-politie.html

[16] https://www.om.nl/onderwerpen/verdachte/voorlopige-hechtenis/

Deze verdenking kan aanleiding zijn om een strafrechtelijk onderzoek te starten. De bevoegdheden van de politie worden dus afgeleid van de strafbaarstelling op het feit. Hoe zwaarder de strafbaarstelling op een misdrijf, hoe zwaarder de inzet van bevoegdheden kan zijn. Een voorbeeld is dat als iemand verdacht wordt van diefstal van een fiets dat hier bijvoorbeeld geen toestemming gegeven zal worden om zijn telefoon af te luisteren. Op diefstal staat maximaal 4 jaar[17] maar voor diefstal van fiets wordt meestal door een rechter geen gevangenisstraf opgelegd. Daardoor zou het inzetten van het middel interceptie te zwaar zijn. Maar bij iemand die verdacht wordt van moord (artikel 289 Wetboek van Strafrecht) kan levenslange gevangenisstraf krijgen. Dan is interceptie niet zo'n zwaar middel.

De politie kan dan dus bijzondere opsporingsbevoegdheden (BOB) gebruiken om de nodige informatie te verkrijgen. Een voorbeeld waar Bas Eikelenboom Teamleider Landelijke Recherche ons over verteld heeft, is bijvoorbeeld het opvragen van paalgegevens. Paalgegevens hebben de gegevens van telefoons die gebruik maken van een bepaalde GSM-mast. De politie kan deze gegevens verkrijgen, en kan dan zien welke telefoons er allemaal binnen een bepaalde tijd in de buurt van zo'n GSM-mast zijn geweest. Dit zal gedaan worden als ze een zaak hebben waarbij nog niet exact bekend is wie de verdachte is. Dit gebeurt bij bijvoorbeeld onderzoek op een plaats delict bij liquidaties. Iemand is doodgeschoten, een verdachte is bij hem in de buurt geweest; echter onbekend is welke verdachte. Uit vergelijkingen met andere telecomgegevens kan dan een verdachte gevonden worden. Een voorbeeld hiervan is het onderzoek dat plaatsvond naar aanleiding van de zogenaamde aanslag op de koningin in 2009. [18] Dit heet BigData onderzoek. Bij BigData worden grote hoeveelheden en verschillende soorten digitale informatie met elkaar gecombineerd. Bijvoorbeeld telecomgegevens met kentekenplaat herkenning (ANPR) met Internet gegevens (Social Media). Hier zijn veel vragen over en ook bezwaren tegen en daardoor zijn er ook al uitspraken door het Hof over gedaan. Dat gaat dan over het heel erg lang bewaren van bijvoorbeeld telecomgegevens, dataretentie genoemd. [19] Niemand heeft door dat dit gebeurt, je zou dus kunnen zeggen dat niemand hier "last" van heeft. Toch is dit ook een manier van privacyschending, want de politie ziet

---

[17] http://maxius.nl/wetboek-van-strafrecht/artikel310

[18] https://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0ahUKEwj-k7Kz9rzPAhVDzRQKHTpKA8k4ChAWCFUwCQ&url=https%3A%2F%2Fwww.ivenj.nl%2FImages%2Fkon-dag-rapport-nationale-recherche_tcm131-481666.pdf&usg=AFQjC-NEM_RBT_cqlSzWgmYYP4fGD2F19bw

[19] https://www.rijksoverheid.nl/actueel/nieuws/2014/11/18/kabinet-wijzigt-regels-dataretentie-na-uitspraak-hof

en bewaart jouw persoonlijke gegevens en daar heb jij geen toestemming voor gegeven. Zo kan de politie precies zien waar jij je bevindt op een bepaalde tijdstip. Ze kunnen bijvoorbeeld zien dat jij elke dag van 9 tot 3 verbonden bent met de GSM mast in de buurt van jouw school. Als de politie wil, kan ze jou telefoongegevens natrekken, en zien zo precies waar jij bijvoorbeeld afgelopen week allemaal bent geweest. Dit past de politie vaak toe bij het opsporen van criminelen. De politie ziet door de paalgegevens op te vragen bijvoorbeeld dat een crimineel om 2 uur ’s middags op het industrieterrein staat. Ook ziet de politie dat er een andere telefoon aanwezig is; door de telefoons na te trekken ziet de politie dat de twee personen meerdere keren met elkaar hebben gebeld. Er speelt dan een groot vermoeden dat deze twee personen op het industrieterrein aan het dealen zijn.

Remco Verhoef
“Politie moet informatie verzamelen, maar wel op de privacy van de burgers letten. Dus niet meer data verzamelen dan nodig is en met de data die de politie heeft moet slim worden omgegaan”.

Zonder dat je het door hebt, wordt jouw privacy elke dag geschonden. Eigenlijk is dat ook niet gek, want mensen willen heel graag informatie op maat. Dus willen weten waar ze lopen zodat ze via GPS hun lokatie kunnen sturen naar iemand die naar ze toe moet lopen voor een ontmoeting, of ze twitteren over wat ze van een product vinden en willen graag via WhatsApp en Facebook van alles met andere mensen delen. En zo spelen bedrijven daar ook op in door advertenties op maat aan te bieden. En eigenlijk willen mensen dat, steeds weer meer informatie waar ze belangstelling voor hebben. En daarmee geven wij al meer van onze privacy zelf prijs. Maar mensen willen ook graag veiligheid en vragen dan om meer toezicht. Zo word je bijvoorbeeld gefilmd als je door het winkelcentrum loopt. Al deze informatie kan ervoor zorgen dat menselijke handelingen al beter te volgen zijn door techniek. Dat wordt dus gebruikt voor marketing, hetgeen mensen graag van een product verwachten, maar ook door de overheid om voor meer veiligheid te zorgen. Maar dat heeft wel grote invloed op je privacy. Toch is deze privacyschending nodig, want zo kan er gezien worden wie er bijvoorbeeld dinsdagnacht jouw moeder in elkaar heeft geslagen, of wie er ingebroken heeft in jouw winkel. Dit is een heel goed voorbeeld van hoe privacyschending en veiligheid bij elkaar komen. Jouw privacy zou anders nooit zoveel geschonden worden, als er geen reden achter zou zitten. Behalve dat jij wordt gefilmd als je in de stad loopt, wordt ook die ene inbreker gefilmd.
En behalve dat jouw paalgegevens bekeken worden, komt de politie ook achter welke telefoon wordt gebruikt door die ene drugsdealer. Met cybercriminaliteit wordt het complex, want cybercriminelen gebruiken de informatie ook maar dan

bijvoorbeeld om jouw indentiteit te stelen. Of om jouw foto's die op Facebook staan aan te passen en op porno-sites te zetten. Zij verdienen dus aan de gegevens die wij zelf op het internet achterlaten en misbruiken deze gegevens om zichzelf voor te doen als een ander.

Als er over privacyschending door politie wordt gepraat, is het eerste dat bij veel mensen opkomt dat politie mensen jouw huis binnenvallen. Je zou zeggen als je niks hebt gedaan, zal dit nooit gebeuren, maar bedenk wel dat er meer mensen in het huis wonen dan alleen degene die verdacht wordt van een strafbaar feit. Het kan zelfs een hele familie uit elkaar laten vallen. Nadat wij met Bas Eikelenboom hebben gesproken, gaf hij ons hier een voorbeeld van. De ouders van een gezin komen erachter dat hun pasgeboren kindje is verkracht[20]. Natuurlijk doen ze gelijk aangifte bij de politie. De politie gaat op onderzoek uit, en komt er dan via een computer uit het gezin erachter dat er kinderporno aanwezig was en dat een andere vader uit een ander gezin vermoedelijk in het bezit was van kinderporno. Ten eerste is de vader van het gezin dat aangifte deed nu een verdachte, en de politie valt ook het andere huis, van de andere vader, binnen. De politie moet dus onderzoeken wat de rol van beide vaders was. Ze nemen alle computers in beslag en arresteren beide vaders. De eerste vader werd later veroordeeld voor bezit van kinderporno. Maar niet voor het verkrachten van de baby; dat had de oppas gedaan. De tweede vader bleek onschuldig, iemand anders had namelijk gebruik gemaakt van zijn computer. Niet alleen is de privacy van de onschuldige vrouw geschonden, maar de gedachten dat haar man misschien toch hun baby heeft verkracht omdat hij kinderporno had, was voldoende voor haar om een echtscheiding aan te vragen. Dat gezin is totaal ontwricht, maar van het andere gezin is de vader onterecht aangehouden en dat werkt natuurlijk ook enorm door op het totale gezin. Zeker als de pers daar dan ook nog veel aandacht aangeeft. Privacy en zorgvuldigheid in omgang met gegevens door de politie is dus van zeer groot belang.

[20] http://www.nu.nl/zedenzaak-amsterdam

Dit voorbeeld laat zien dat privacyschending en het opsporen van criminelen ook enorme nare gevolgen kan hebben, en hele gezinnen kan verwoesten. Dit is dan ook een reden voor de politie om dit soort zaken heel rustig en vooral zorgvuldig aan te pakken. Gevallen zoals deze komen gelukkig niet al te vaak voor, maar kunnen wel een reden zijn waardoor mensen fel tegen privacymisbruik van de politie zijn. Natuurlijk zijn gevallen zoals deze verschrikkelijk, maar we moeten kijken naar het grotere plaatje. Zonder de camera's, invallen, paalgegevens en alle andere manieren van privacyschending zouden er nu een stuk meer criminelen op straat rondlopen en zouden cybercriminelen enorme kansen hebben op het misbruiken van onze gegevens.

De politie kan haar werk dus niet doen zonder informatie. Maar informatie kan heel erg gevoelig zijn en een grote impact hebben op het leven van mensen. Een belangrijke vraag is dan: welke garanties of controle-middelen kan de burger van de overheid verwachten om het juiste gebruik van de gegevens te bevorderen?

Een belangrijk deel daarvan wordt geregeld in wet en regelgeving. Hieronder gaan wij daarom meer in op de Wet Bescherming Persoonsgegevens (WBP). Daarnaast kunnen mensen op grond van de Wet Openbaarheid van Bestuur (WOB) ook opvragen wat er van het bekend is en hoe ermee omgegaan wordt[21].

[21] https://www.om.nl/onderwerpen/wet-openbaarheid/

4.1 De Wet Bescherming Persoonsgegevens (WBP)

Welke garanties of controle-middelen kan de burger van de overheid verwachten om het juiste gebruik van de gegevens te bevorderen? Hiervoor is onder andere specifieke wetgeving gemaakt. De Wet Bescherming Persoonsgegevens (WBP) bepaalt wat er wel en niet mag met de persoonsgegevens van de burgers. Ook regelt de WBP op welke wijze een organisatie de persoonsgegevens mag verwerken voor een bepaald doel. De organisatie mag deze gegevens niet zomaar weer gebruiken voor een ander doel en de organisaties hebben de verplichting om deze persoonsgegevens goed te beveiligen. Het verwerken van persoonsgegevens heeft betrekking op het verzamelen, vastleggen, verspreiden, bijwerken of wijzigen van persoonsgegevens. Het begrip 'persoonsgegevens' wordt in artikel 2, onder a, van de richtlijn omschreven als 'alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'[22]. Dit houdt in dat de informatie over een persoon gaat of te herleiden is dat het om die gene gaat. Dat het alleen om natuurlijke personen gaat, houdt in dat van een overleden persoon of een organisatie geen persoonsgegevens zijn. Voorbeelden van persoonsgegevens zijn bijvoorbeeld het adres, telefoonnummer, e-mail adressen, IP-adressen, pasfoto's en vingerafdrukken. Er zijn ook gevoelige persoonsgegevens zoals iemands godsdienst, ras, gezondheid en strafrechtelijk verleden. Deze gegevens worden ook wel bijzondere persoonsgegevens genoemd en het kan je privacy ernstig beïnvloeden. De gegevens van de burgers worden bewaard in computers van bedrijven.

De gegevens over personen in bijvoorbeeld een digitaal of papieren dossier bevat uiteraard veel informatie. Voor bedrijven is het belangrijk om te zorgen voor een goede administratie. Op grond van de WBP zijn er geen specifieke bewaartermijnen voor persoonsgegevens, de bedrijven bepalen zelf hoelang zij de gegevens in beslag willen houden. Toch kunnen organisaties dit niet eindeloos houden en zijn er wetten waar organisaties zich aan moeten houden. Bijvoorbeeld als je gefilmd bent in een winkelcentrum, heeft de Kruitvat camerabeelden van jou. De camerabeelden van openbare ruimtes mogen volgens de Wet maximaal vier weken bewaard worden.

---

[22] https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-wbp

Maar als er een crimineel de Kruitvat heeft overvallen, dan is er sprake van een strafbaar feit en kan de bewaartermijn worden verlengd. Dit komt omdat deze videobeelden dan als bewijsmateriaal kunnen worden gebruikt in een strafprocedure.

De WBP kent verschillende partijen die deel uit kunnen maken van de verwerking van persoonsgegevens. Deze partijen zijn de verantwoordelijke, de betrokkene en de ontvanger. De verantwoordelijke[23] heeft zeggenschap over de gegevensverwerking en stelt bijvoorbeeld vast op welke wijze en doeleinde de gegevens worden verwerkt. De private partij die gegevens wil of moet verstrekken is de verantwoordelijke, omdat deze het doel en de middelen bepaalt voor de gegevensverwerking. De betrokkene is degene op wie de persoonsgegevens betrekking heeft. De betrokkene is in de meeste gevallen degene die een mogelijk strafbaar feit heeft begaan. Bijvoorbeeld in de situatie dat de betrokkene herkenbaar in beeld komt op camerabeelden waarop is te zien is dat hij een overval heeft gepleegd. De betrokkene is natuurlijk geen partij bij de keuze om de gegevens te verstrekken, maar is relevant en heeft bepaalde rechten bij een verstrekking van zijn persoonsgegevens. Van de betrokkene worden de persoonsgegevens verwerkt. Hij moet tenminste op de hoogte zijn van de identiteit van de organisatie of persoon (dus de verantwoordelijke) die zijn persoonsgegevens verwerkt en van het doel van de gegevensverwerking, dus wat de verantwoordelijke met de gegevens wil bereiken. De ontvanger[24] speelt ook een rol. De ontvanger is degene die persoonsgegevens ontvangt bij een gegevensverstrekking. Dit kan iemand zijn van de verantwoordelijke maar dit kan ook een andere organisatie zijn zoals de politie of het OM.

Een bedrijf heeft concluderend bepaalde data. Deze data kunnen afkomstig van camera’s zijn, of bijvoorbeeld een salarisadministratie. Het bedrijf moet vaststellen hoe zij met deze gegevens omgaat, waar deze opgeslagen worden en waarom deze verwerkt worden. En daarmee is het bedrijf de verantwoordelijke voor de data. In feite is dit gegevensverwerking. Vaak wordt dit vastgelegd in een bewerkersovereenkomst. Data die dan over een bepaalde persoon bekend zijn, kunnen worden verstrekt aan anderen. Die persoon is dan een betrokkene. De ontvanger, bijvoorbeeld politie kan dan data / gegevens krijgen van de betrokkene via de verantwoordelijke.

---

[23] https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-d-wbp

[24] https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-h-wbp

Het gebruik van gegevens moet wel in overeenstemming zijn met de reden waarom en er moet uitgelegd kunnen worden dat het gebruikte middel niet te zwaar is. Het opslaan van alle gezichten in een database bij een fietsenstalling is te zwaar als dit fietsendiefstal tegen moet gaan. Meer algemene beelden die na een incident terug gekeken kunnen worden, is dan minder ingrijpend op de privacy van mensen. De Hoge Raad heeft bepaald dat bij elke verwerkingsgrondslag uit artikel 8 WBP het proportionaliteit en subsidiariteitsbeginsel in acht moet worden genomen. Het proportionaliteitsbeginsel houdt in dat de belangen van de betrokkene niet evenredig mogen zijn in verhouding met het doel van de gegevensverwerking. Het subsidiariteitsbeginsel houdt in dat het doel waarvoor de persoonsgegevens worden verwerkt niet op een andere minder ingrijpende wijze kunnen worden verwerkelijkt. Belangrijk is dus dat er doelstelling is voor het opslaan van gegevens. Een voorbeeld is de IKEA in Delft. Hierbij werd vastgelegd met behulp van WiFi waar de klanten van de IKEA liepen. Dit werd gebruikt om te zien voor welke goederen de klanten het meeste belangstelling hadden en welke advertenties (marketing) het beste werkte. Dit mag niet zomaar. Een bedrijf moet dit duidelijk aankondigen zodat klanten kunnen besluiten hun WiFi uit te zetten. Als het volgen van de klant de doelbinding is, dan mag er niet nog meer gedaan worden, bijvoorbeeld het identificeren van de klant en daaraan het aankoopgedrag koppelen. Middels profileren kunnen dan immers mensen een financiële ‘waarde’ krijgen en dan duurdere goederen op maat aangeboden worden (direct marketing). Dit geldt ook voor de politie. Als interceptie (tappen) bedoeld is om een gesprek te kunnen afluisteren dan is het niet zonder extra machting van de Officier van Justitie toegestaan om ook de verdachte te volgen via de telecompalen die er zijn. De doelbinding was het afluisteren van gesprekken en niet het stelselmatig observeren (volgen) van de verdachte.

Hierdoor wordt dus duidelijk dat er wetgeving buiten het Wetboek van Strafvordering is die zich specifiek bezig houdt met de rechten van de mens, waaronder het recht op privacy. Dit wordt sterker doordat het opslaan en verwerken van gegevens aan een bepaald doel gebonden worden. Deze doelbinding zorgt ervoor dat niet zomaar van alles over iedereen onbeperkt opgeslagen mag worden.

Op grond van artikel 9 WBP dient het principe doelbinding in acht te worden genomen, dit houdt in dat persoonsgegevens niet verder worden verwerkt voor doeleinden die onverenigbaar zijn met het oorspronkelijke doel. Daarnaast dient de gegevensverwerking ingevolge artikel 11 WBP[25] toereikend, ter zake dienend, juist, nauwkeurig en niet bovenmatig te zijn.

---

[25] http://maxius.nl/wet-bescherming-persoonsgegevens/artikel11

Verder mogen persoonsgegevens op grond van artikel 10 WBP niet langer bewaard worden dan noodzakelijk voor het te dienen doel en de verantwoordelijke dient technische en organisatorische maatregelen te nemen om de persoonsgegevens te beveiligen op grond van artikel 12 WBP jo artikel 13 WBP jo artikel 14 WBP. Op grond van artikel 27 WBP dient elke gegevensverwerking, waaronder de verstrekking van persoonsgegevens aan de Nationale Politie, te worden gemeld aan de AP. Ten slotte dient rekening te worden gehouden met de rechten van de betrokkene. Zo moet de betrokkene op grond van artikel 33 WBP of artikel 34 WBP geïnformeerd worden door de verantwoordelijke over de gegevensverwerking, zoals het verstrekken van persoonsgegevens aan de Nationale Politie.

Op grond van artikel 35 WBP heeft de betrokkene het recht op inzage. De informatieplicht en het recht op inzage vervallen wanneer dit noodzakelijk is ter voorkoming, opsporing en vervolging van strafbare feiten conform artikel 43 sub b WBP. Verder heeft de betrokkene op grond van artikel 36 WBP het recht op correctie en ten slotte kan de betrokkene op grond van artikel 40 WBP verzet aantekenen wanneer de verwerking is gebaseerd artikel 8 sub e WBP of artikel 8 sub f WBP. De laatste twee rechten kan de betrokkene niet uitoefenen wanneer de informatieplicht en het recht op inzage vervallen op grond van artikel 43 sub b WBP. Deze artikelen bieden dus een extra bescherming voor privacy, naast wat er in het Wetboek van Strafvordering geregeld is.

Een voorbeeld hiervan is dat als er op iemand bijvoorbeeld interceptie is aangevraagd dat het doel dan is om zijn telefoongesprekken af te kunnen luisteren. De doelbinding is dan afluisteren. Maar als de politie dezelfde tap wil gebruiken om vooral te zien waar iemand zich bevindt, dus zijn telefoon gebruikt als een soort van GPS-baken (volgen via de telecommunicatie masten), dan schiet dat het oorspronkelijke doel voorbij. De politie zal dan bijvoorbeeld aanvullend een bevel stelselmatig observeren aan moeten vragen via de Officier van Justitie.

Ook mag de politie de telecomgegevens ook niet onbeperkt bewaren. Na het afsluiten van een onderzoek (via de rechter) moeten de opgeslagen gegevens dan ook binnen een termijn van vijf jaar uit de systemen verwijderd worden. Deze termijn is niet altijd vijf jaar, maar kan ook langer zijn als er sprake was van bepaalde zwaardere misdrijven of als niet iedere verdachte uit het onderzoek aangehouden was en er dus nog onderzoekshandelingen verwacht kunnen worden.

Bas Eikelenboom

“Ik vind dat mensen recht hebben op een hele goede opsporing en voorkomen van misdrijven en dus dat ook bedrijven vrijwillig aan mee moeten werken en dus dat die dataretentie zo lang mogelijk moet zijn”.

Een deelconclusie is dat bescherming van de burger tegen het verkeerd gebruik van hun data door de overheid geregeld moet zijn in de Wet, maar ook controleerbaar moet zijn. In een rechtsstaat is transparantie door de overheid van groot belang en daarmee toetsbaarheid door de rechterlijke macht. Dit is met name van belang omdat je wel een verdachte kunt zijn, maar je bent pas schuldig als een rechter dat ook zo in een vonnis vertelt. Als er geen controle is op het juiste gebruik dan kan het zijn dat de middelen die gebruikt zijn te zwaar waren in verhouding met hetgeen iemand verdachte van was en dat er onrechtmatig gebruik is gemaakt van zware bevoegdheden. Dit dient dus als bescherming van de rechtsstaat.

Hoofdstuk 5 Dilemma's

5.1 Wat betekenen nieuwe datamogelijkheden voor de wijze van opsporen?

Net als andere sectoren in de Nederlandse maatschappij is het werk van de politie de laatste decennia steeds complexer geworden. De politie is dan ook genoodzaakt om steeds slimmer te werk te gaan. Één van de nieuwe opsporingsmogelijkheden is datamining, waarvan de politie al veel gebruik maakt.

De hoeveelheid data groeit explosief, elke dag wordt er informatie digitaal opgeslagen in computers. Data kunnen van alles zijn zoals: documenten, software, foto's, video's, maar ook gegevens over waar iemand zich bevindt en met wie iemand belt. De nieuwe manier voor de wijze van opsporen is bijvoorbeeld datamining. Datamining[26] is een relatief nieuw proces waarbij techniek waarin concepten uit de marketing, database management, statistiek en computerwetenschappen met elkaar worden gecombineerd. Voor de politie heeft dit het doel om criminelen op te sporen.
Bij datamining worden nieuwe vormen van data gevormd met behulp van gegevens in de bestaande data, dus de data die je hebt, worden vanuit verschillende perspectieven geanalyseerd om zo nieuwe bruikbare informatie te verkrijgen. Dus er wordt naar belangrijke patronen en verbanden gezocht in de bestandsgegevens van mensen, bijvoorbeeld de telefoongegevens van iemand met wie, wanneer en waar diegene heeft gebeld.

Om met een overzichtelijker voorbeeld te beginnen, datamining wordt ook gebruikt in bijvoorbeeld supermarkten. Denk dan bijvoorbeeld aan de bonuskaart waarmee Albert Heijn bepaalde gegevens binnen haalt van haar klanten. De Albert Heijn ziet door middel van datamining verbanden. Namelijk, Albert Heijn heeft ontdekt dat er bijvoorbeeld elke vrijdag vlak voor sluitingstijd vooral jonge mannen luiers, bier en chips halen.
Deze gegevens zorgen ervoor dat de supermarkten niet alleen aanbiedingen toe kunnen passen, maar leren ook over de situaties binnen het gezin, inkomen, sociale

[26] http://www.mkbservicedesk.nl/9966/datamining-wat-hoe-werkt.htm

klasse, en andere informatie van de klant. Zo wist bijvoorbeeld een supermarkt uit Amerika eerder dan de ouders dat een meisje zwanger was. Uit Big Data analyseerde de winkel dat zwangere vrouwen onder meer minder geurende shampoos en lotions kopen. Het meisje kocht een andere shampoo dan gewoonlijk en hierdoor wist de supermarkt met 70 procent zekerheid dat het meisje zwanger was[27].

Een ander voorbeeld: datamining wordt bij de politie gebruikt en hier worden wiskundige berekeningen (algoritmes) bij gebruikt. Om criminelen op te sporen maak je gebruik van algoritmes; met algoritmes maak je berekeningen om zo gebruikslijke patronen te vinden. Bijvoorbeeld waar en wanneer een crimineel zich bevindt en met wie. Als de crimineel elke dinsdag in een café zit, kun je voorspellen dat zij volgende week dinsdag daar ook weer is. De politie zou dan een observatieteam neer kunnen zetten (predictive analyses). Met predictive analyses zal de percentage inbraken dalen. Stel dat Amsterdam bijvoorbeeld is onderverdeeld in blokjes door datamining, kan de politie zien in welke wijken er veel wordt ingebroken en voorspellen in welke wijken de volgende inbraken kunnen plaatsvinden[28]. Met deze nieuwe data heeft de politie inzicht waar ze het blauw extra kunnen inzetten. Hierdoor zal het percentage inbraken dalen.

Deze data krijgt de politie natuurlijk niet zomaar. Eerst moet zij toestemming krijgen van de Officier van Justitie en geld wetgeving, als de politie toestemming krijgt, wordt

[27] http://www.mkbservicedesk.nl/9966/datamining-wat-hoe-werkt.htm

[28] https://beveiligingnieuws.nl/nieuws/productnieuws/vier-steden-gaan-criminaliteits-anticipa-tie-systeem-testen

de bestaande data opgeslagen in een datawarehouse[29]. Datamining wordt ook wel eens aangeduid als business intelligence. Ook bij datamining kan de privacy van burgers worden geschonden.

OSINT (Open Source Intelligence) is een andere techniek om criminelen op te sporen. Met tooling (hulpmiddelen) wordt onder andere virtuele ontmoetingsplaatsen op Internet in de gaten gehouden. Virtuele ontmoetingsplaatsen zijn bijvoorbeeld Twitter, Facebook, Websites en forums. Mensen 'spreken' daar met elkaar, delen foto's en geven hun mening.

Bas, Ingrid en Remco
"Zakelijk vind ik dat het voorkomen van een aanslag belangrijker is dan welke privacy dan ook".

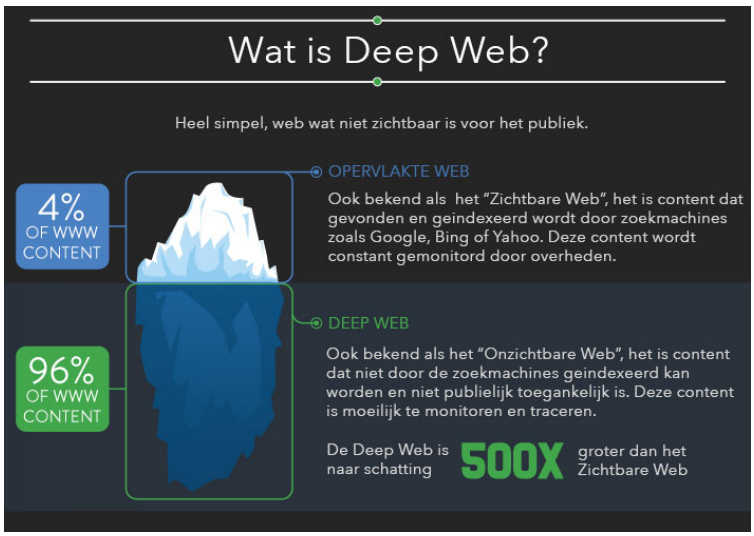
Het verzamelen van deze data gaat door middel van geautomatiseerde web-crawlers en rechercheurs die handmatig veel verzamelen. Dit mag overigens in veel gevallen niet zomaar, een Officier van Justitie moet dan wel een bevel stelselmatig observeren afgeven. Door deze data te verzamelen en te analyseren, is de politie in staat een sociale netwerkanalyse te maken of sentimentanalyse te doen. Uit de sociale netwerkanalyse wordt zichtbaar hoe mensen in verhouding met elkaar staan, bijvoorbeeld familie, maar ook wie leiding over wie heeft enzovoorts. Uit sentiment-analyse worden bijvoorbeeld dreigingen zichtbaar. Een voorbeeld kan zijn OSINT op voetbalwedstrijden om te bepalen of er extra inzet van politie noodzakelijk is op basis van dreiging tot geweld. Sociale netwerkanalyse kan dan inzichtelijk maken welke bekende mensen die veelvuldig geweld plegen, samen naar een wedstrijd gaan en sentimentanalyse kan dan meer over de sfeer zeggen. Het hoeft namelijk niet zo te zijn dat als geweldplegers bij elkaar komen dat er dan ook geweld plaats gaat vinden, maar als dit uit ruzies en teksten blijkt is het verstandiger op basis van die informatie dan extra mensen in te zetten. Dit wordt ook wel Informatie Gestuurde Politie (IGP) genoemd en is onderdeel van Business Intelligence (BI).

[29] Een datawarehouse zijn meerdere databases bij elkaar, waarbij de databases met elkaar worden vergeleken.

Hoofdstuk 6 Wat is de invloed van DarkWeb op de privacy en veiligheid?

Het internet heeft overal in de wereld heel veel invloed. In twee klikken kan je zo in contact komen met iemand van de andere kant van de wereld. En alle informatie die je maar wilt, kan je zo opzoeken. Op deze manier komen we steeds meer te weten over van alles en nog wat. We leren over de cultuur van andere mensen en krijgen een algemener beeld van wat er allemaal in de wereld gebeurt. Dit is natuurlijk geweldig dat we dit hebben, maar het internet heeft ook een donkere kant. We hebben namelijk ook te maken met het DarkWeb. Het DarkWeb is een illegaal netwerk waar je de meest gruwelijke dingen tegenkomt. Je kunt het zien als online shoppen voor criminelen want je kunt er wapens, drugs en nog veel meer illegale producten kopen.

Het DarkWeb is, in tegenstelling van wat de meeste mensen denken een klein onderdeel van het DeepWeb. Het is zeker niet hetzelfde. Het DeepWeb is namelijk bedoeld voor bijvoorbeeld advocaten of journalisten zodat zij anoniem over het internet kunnen surfen. Het grote verschil is dat je bij het DeepWeb nog steeds op het reguliere internet zit, alleen surf je er anoniem. Terwijl je bij het DarkWeb geheel onzichtbaar bent, en je komt in de ´onderwereld´ van het internet. Geschat wordt dat slechts 4 procent van alle gegevens op het reguliere internet staat. Je bent op het DarkWeb onzichtbaar door het programma TOR, die je moet downloaden voordat je op het DarkWeb kunt. Dingen die je op het DarkWeb kunt vinden zijn wapens, drugs, kinderporno en nog veel meer illegale en gruwelijke dingen. Wij vroegen ons af wat voor invloed van het DarkWeb nu eigenlijk heeft op de veiligheid en privacy van de mensen.



6.1 Het DarkWeb

Het DarkWeb is slechts een klein onderdeel van het DeepWeb. Veel mensen denken dat het DeepWeb en het DarkWeb hetzelfde zijn, maar dit klopt niet. Het grootste verschil is dat het DeepWeb niet gelijk al illegaal is, maar het DarkWeb wel.

Het DarkWeb is erg gevaarlijk omdat iedereen er anoniem is. De politie heeft dan ook heel veel moeite met het achterhalen van deze mensen, mede door het programma TOR[30]. Hierdoor kunnen criminelen ongestoord hun gang gaan. Het gevolg hiervan is dat het DarkWeb ongelofelijk uitgebreid en divers is. Je kunt er letterlijk alles vinden, ook dingen waarvan je niet eens van had gedacht dat het bestond. Er zijn natuurlijk ook een hele boel vrij onschuldige zaken op het DarkWeb, als een goedkoop Spotify account of gratis Netflix.[31] Maar je kunt er ook voor een paar duizend euro een moordenaar huren, of je koopt er een wapen.[32] Er bestaan zelfs sites over hoe je het beste zelfmoord kunt plegen, en je vindt er filmpjes van mensen die gemarteld en langzaam vermoord worden. Andere grote problemen van het DarkWeb zijn onder andere het drugsverkoop en de kinderporno.

Of het DarkWeb ooit opgeheven kan worden? Het is te hopen van wel. Toch wordt dit heel lastig omdat het zo ongelofelijk groot is. Je kan het vergelijken met het proberen op te heffen van het internet. Het wordt zeker wel geprobeerd en op z'n tijd worden er ook wel grote sites uit de lucht gehaald, maar er komen twee keer zo snel ook weer nieuwe sites bij. Het is dus op het moment bijna onmogelijk om het op te heffen. Gelukkig zit er wel in elk software ergens een lek waardoor de politie naar binnen kan gaan, en ook daadwerkelijk achter de identiteit van deze personen kunnen komen.

---

[30] TOR is een programma dat ervoor zorgt dat je anoniem blijft

[31] http://www.esquire.nl/the-good-life/news/a416/ik-bestelde-drugs-op-het-dark-web-zo-ging-dat/

[32] http://www.crimesite.nl/zoekmachine-laat-je-zoeken-naar-drugs-en-wapens/

Bas Eikelenboom vertelt over zijn ervaringen tijdens het opheffen van kinderporno sites, hij vertelde hierbij dat sommige mensen zelfmoord hebben gepleegd alleen al omdat ze bang waren dat hun identiteit boven water zou komen. Want hoe ga je je vrouw uitleggen dat je naam is opgedoken bij een illegale kinderporno site.

Dit is een afbeelding die gemaakt is op het DarkWeb, je ziet hier een site waar je een moordenaar kan huren.

6.2 TOR

In verband met grote militaire geheimen die de Amerikaanse marine wilde beschermen[33], is er jaren geleden een soort van privé netwerk over het internet heen gebouwd. De gedachte daarachter was dat het Internet voor iedereen op de wereld bereikbaar moest zijn en daardoor dus een enorme connectiviteit (verbindingen) opleverde. Echter het internet was als netwerk niet veilig genoeg voor vertrouwelijke data. Daarom is er een privé netwerk gebouwd wat volledige [34]encryptie had via verschillende schillen. Deze schillen worden visueel als een 'UI' uitgebeeld. Om het dataverkeer te kunnen transporteren is een nieuwe routing methode gemaakt, hier uit is The Onion Router (TOR) als netwerk ontstaan. TOR moest anonimiteit en privacy kunnen garanderen. Juist doordat TOR niet als normale webservers gezien kon worden, werd al snel de naam DarkWeb geïntroduceerd.

Voordat je op het DarkWeb terecht kunt, moet je eerst bepaalde software downloaden, namelijk TOR. Met deze software kun je geheel anoniem op het DarkWeb surfen. Gek genoeg is dit programma bedacht door de Amerikaanse marine, met als doel de burgers meer privacy te schenken. En terwijl de ene helft van de Amerikaanse veiligheidsdiensten bezig is met het ontmaskeren van DarkWeb gebruikers, financiert de andere helft juist weer het programma TOR.

TOR is de afkorting van The Onion Router, vandaar de ui in het logo. Ook heeft TOR zijn eigen netwerk met webadressen die eindigen op .onion. Deze websites zijn dus alleen te bereiken als je dit programma hebt gedownload, en is dus onderdeel van het DeepWeb.

TOR is zo succesvol omdat de internetgebruiker zijn echte IP-adres kan verbergen. Een IP-adres is eigenlijk een soort postcode van de technologie. Normaal kan bijvoorbeeld de politie precies zien welk IP-adres op een bepaalde website is geweest, maar TOR zorgt ervoor dat het echte IP-adres van de gebruiker wordt verborgen en er een ander IP-adres aankoppelt. Nu is TOR niet alleen maar negatief er is ook heel veel profijt van dit programma. Zo kunnen bijvoorbeeld rechercheurs, politici of journalisten rustig anoniem surfen en wordt hun identiteit verborgen gehouden. En ook landen als China of Syrië en Noord-Korea hebben veel baat bij TOR.

---

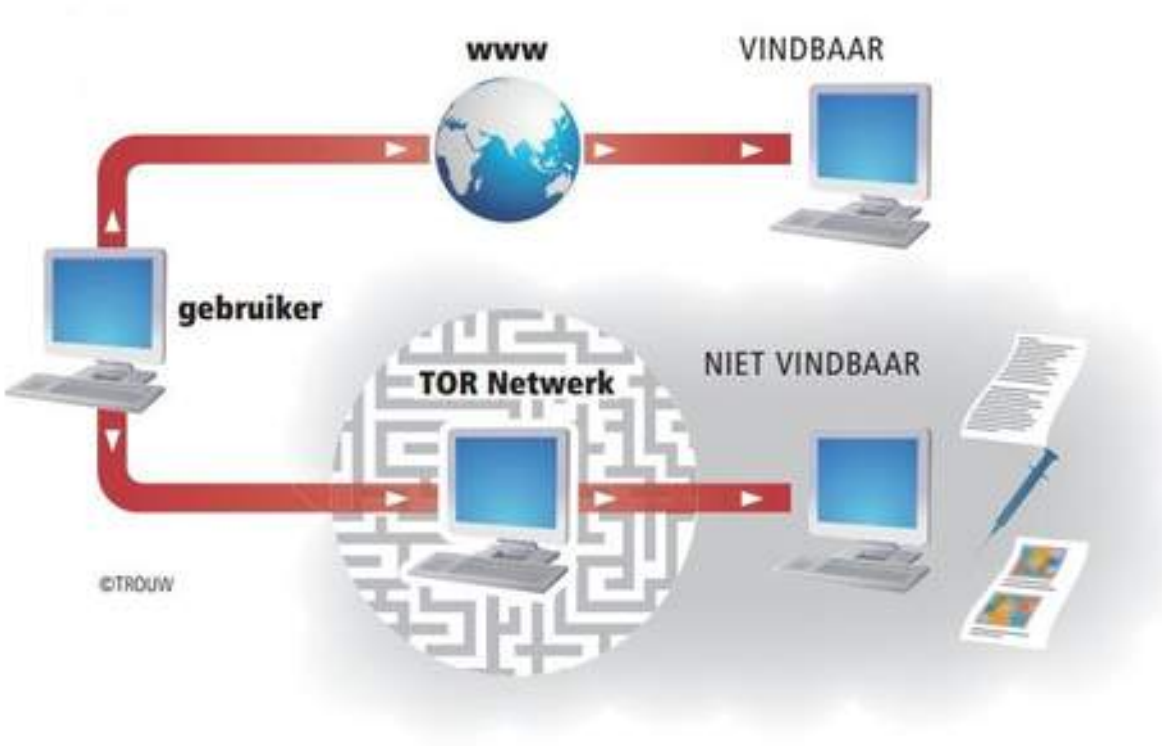
[33] http://www.winmagpro.nl/content/tor-en-het-donkere-web

[34] De omzetting van data naar een geheime code. De nog niet versleutelde data heet gewone tekst of `plain text` en de versleutelde data noemt men vercijferde tekst of `cipher text`.

Het is in deze landen namelijk verboden om internet te gebruiken of sommige sites worden geblokkeerd. Zo bestaat het internet van Noord-Korea uit slechts 21 pagina's. De mensen kunnen in deze landen worden vervolgd als ze op bepaalde sites op het internet zitten en door TOR kunnen deze mensen rustig en anoniem gebruik maken van het internet. Door TOR kunnen ze de firewall van hun overheid ontzeilen en komen ze terecht op het internet dat wij kennen.

TOR kan niet honderd procent veiligheid garanderen. Niet alleen proberen veiligheidsdiensten het netwerk te kraken, ook de software is niet altijd waterdicht. Zo zijn de veiligheidsdiensten ook op zoek naar deze gaatjes, om zo de gebruikers van TOR te kunnen volgen. Wel blijft het heel moeilijk om dan ook deze gebruikers te pakken te krijgen.

Het gevaarlijke van TOR is natuurlijk dat het verbergen van je identiteit perfect is voor criminelen. Zo kunnen pedofielen anoniem hele websites oprichten met foto's en filmpjes van kinderen die misbruikt worden. Er bestaan zelfs websites waar je voor een paar duizend euro iemand kan laten vermoorden. Het enige dat je daarvoor hoeft te doen, is een foto van diegene te sturen en binnen een paar weken wordt deze persoon vermoord. En er is niemand die hier wat tegen kan doen want het is immers allemaal anoniem[35].



[35] http://www.volkskrant.nl/archief/de-digitale-onderwereld~a3223214/

6.3 Wat is de invloed van DarkWeb op de privacy en veiligheid?

Wat is de invloed van het DarkWeb op de veiligheid en privacy van de mensen? Met privacy heeft het niet zo veel te maken. De privacy van de onschuldige burgers wordt niet of nauwelijks geschonden, ook niet op het DarkWeb.

Dit gebeurt niet vrijwillig omdat het door TOR heel moeilijk is om de identiteit van DarkWeb gebruikers te achterhalen. De politie probeert wel om lekken te vinden. Zo kunnen ze de daders oppakken, maar dit gaat allemaal heel stroef. Omdat de privacy zo wordt beschermd, gaat het van kwaad tot erger. [36] Er zijn nu zelfs filmpjes te vinden van mensen die doodgemarteld worden. Ook zijn er duizenden filmpjes van hoe kleine kindjes verkracht worden, en vind je er automatische wapens. Zo vertelt Bas Eikelenboom.

Wel heeft het DarkWeb enorme invloed op de veiligheid. Doordat de DarkWeb-gebruikers onzichtbaar zijn, kan de politie heel weinig doen. Grote hoeveelheden wapens en drugs worden ongemerkt ingekocht. Het gevaar is hiervan natuurlijk dat bijvoorbeeld de buurman waar je vorige week enorme ruzie mee hebt gehad, zomaar zonder wapenvergunning een pistool kan kopen. En dat bijvoorbeeld je kind van 16 drugs koopt zonder dat je daar iets van weet. Criminelen kunnen ongestoord hun gang gaan. De kans bestaat zelfs dat er een foto of filmpje van jou op het DarkWeb te vinden is, en de kans dat je die er af kan halen is heel erg klein. Verder is het natuurlijk heel gevaarlijk dat je al deze verboden producten op het internet kan kopen, alsof je online aan het shoppen bent.

Conclusie: het DarkWeb heeft niet heel veel invloed op de privacy van de burgers. Het is namelijk gebouwd om privacy te garanderen. De privacy van de mensen op het DarkWeb wordt dus beschermd. Het DarkWeb heeft veel invloed op de veiligheid van de mensen, want er kunnen veel illegale producten worden aangeschaft. Het zou dan ook veel beter zijn als het DarkWeb beter in de gaten gehouden kan worden, daarom krijgt de politie dan ook zwaardere bevoegdheden. Zoals de zogenaamde ‘terug hack wet’. Hierop is heel veel commentaar [37] maar inmiddels is de wet eind december 2016 aangenomen.

---

[36] Bron: Bas Eikelenboom, baas landelijke recherche

[37] https://www.bof.nl/2012/10/16/terughacken-is-risico-voor-cybersecurity/#donationOverlay

6.4 Bevoegdheden politie en mogelijkheden bedrijfsleven

De politie is middels wetgeving gebonden aan regelgeving die betrekking heeft op bijvoorbeeld het stelselmatig observeren van mensen of groepen. Het dagelijks monitoren van deze mensen via het internet / DeepWeb en/of DarkWeb mag dus niet zonder meer en is ook tijdsgebonden. Toch is deze informatie vaak van groot belang. Het bedrijfsleven doet dit vaak bedrijfsmatig. Bijvoorbeeld als Threat Intelligence (bedreigingsinformatie) en gebruiken dit om de ICT systemen te beschermen. Er zijn mogelijkheden voor de politie om deze data te vorderen, maar bedrijven kunnen ook een structurele samenwerking met de politie aangaan en gevonden informatie verzamelen, veredelen met bedrijfsinformatie en ter analyse aan de politie aanbieden. Dat is een publiek-private samenwerking.

Bas Eikelenboom
"Beveiligen van data in verband met privacy is voor de overheid een verplichting, namelijk uitvoeren van een autorisatiemodel waarin vast gelegd wordt wie welke informatie mag zien en waarom. Voor bedrijven zou datamining verplicht gesteld moeten worden om te controleren en bij de politie melden of criminelen misbruik maken van de ICT systemen".

Er is namelijk een groot economisch belang voor bedrijven om samen te werken met de politie. Criminaliteit, zoals fraude, kost bedrijven enorm veel geld. Misbruik van ICT systemen, bijvoorbeeld het verspreiden van kinderporno via een foto-site, kost reputatie en daarmee adverteerders en kost het dus enorm veel geld. Opvragen van gegevens of zelfs inbeslagname van servers door de politie kost heel veel menskracht en geeft kosten voor uitvallende ICT systemen. Bedrijven hebben dus een belang om ook zelf onderzoek te doen en de gegevens snel te delen met de overheid.

Hoofdstuk 7 Wat betekent publiek-private samenwerking voor de privacyschending?

De politie heeft heel veel data; deze data komt voort uit opsporingsbevoegdheden of uit handhaving. Door samenwerking met het bedrijfsleven krijgt de politie de mogelijkheid om veel meer data te verkrijgen dan zij zelf al in bezit hebben. Het gaat hier om data van bedrijven die data van veel personen hebben, maar het delen van deze data met politie kan wel, maar hoeft dan niet specifiek van de verdachte te zijn. Thematisch kan veel data gedeeld worden, die inzicht geven in criminele fenomenen maar daar zit dan ook data tussen van onschuldige burgers. Dat komt omdat een bedrijf geen goed onderscheid kan maken tussen normale gedragingen en criminele gedragingen. De politie ziet dan dus ook informatie van onschuldige burgers.

Een voorbeeld is dat rond Kerst veel mensen cadeaus kopen via Marktplaats. Criminelen maken daar ook gebruik van door valse advertenties te plaatsen. Als bekend is dat er veel belangstelling is voor fototoestellen en dat de meeste fraude uit bijvoorbeeld Eindhoven komt, dan kan Marktplaats alle advertenties met meta-data (zoals naam, adres, telefoonnummers, rekeningnummers) aan de politie kunnen verstrekken ter controle. De politie krijgt dan alle verkopers, maar slechts een of twee zijn dan bekende criminelen. Vraag is of een provider (bedrijf) alle persoonsgegevens wil delen met de politie? Of zou het kunnen dat bijvoorbeeld iemand van Team High Tech Crime een tweede baan neemt en gaat werken bij bijvoorbeeld Ziggo als security expert. Zo kan hij vanuit Ziggo zicht krijgen op bepaalde misdrijven, waar hij bij de politie mee bezig is. Wij kunnen ons voorstellen dat de politie de IP-adressen van de bekende loverboys wil vergelijken met bijvoorbeeld de IP-adressen van gezinnen met meisjes in de leeftijdscategorie 11 tot en met 17, om zo te voorkomen dat ze in de prostitutie komen. Uiteraard is dit een schending van de wetgeving, bedrijfsvoorwaarden en in principe zal dit niet voorkomen. Hiervoor is een aparte regeling: Werken onder Dekmantel. Dat heeft te maken met infiltratie door de politie en is aan zeer zware voorwaarden verbonden.

De politie heeft in veel gevallen deze data nodig van de bedrijven. Bij de opsporing kunnen deze data gevorderd worden of in beslag worden genomen. De vraag is wat de politie proactief mag doen, dus wat zij mogen doen om bijvoorbeeld kindermisbruik of zware criminaliteit te voorkomen? Hierdoor zal de politie met deze bedrijven samen moeten werken. Een voorbeeld van dit soort bedrijven zijn providers.

De wet maakt onderscheid tussen twee soorten providers: de access provider en hosting provider. De access provider is bijvoorbeeld Ziggo, die zorgt ervoor dat je toegang krijgt op het internet door informatie door te geven. De hosting provider geeft niet alleen informatie door maar slaat het ook op. Het zijn niet alleen webhosting diensten zoals gmail en hotmail die jouw gegevens opslaan en doorgeven. Ook zijn het webforums en soms zelfs weblogs.

Het doorgeven of publiceren van informatie kan stafbaar zijn. Als een provider samenwerkt met de politie, kan het gebeuren dat de provider aansprakelijk gesteld kan worden of strafbaar kan zijn. Internetproviders, zowel access providers als hosting providers, kunnen hiervoor vervolgd worden. Maar wat moet je doen als je geconfronteerd wordt met kruisende ethische belangen? Het hosten van bijvoorbeeld een foto-site waar mensen privéfoto's uploaden, kan ook betekenen dat er bijvoorbeeld kinderporno of terrorisme faciliterende afbeeldingen via die site verspreid worden. In Nederland is het kijken naar kinderporno strafbaar, dus als je als bedrijf het een en ander waarneemt, ga je dan die foto's aan de politie (vrijwillig) verstrekken? Met het risico dat je kinderporno verspreidt of dat je strafbaar bent omdat je ernaar gekeken hebt.

Een ander geval kan zijn dat de provider (het bedrijfsleven) beelden tegenkomt welke mogelijk te maken hebben met terrorisme. Ga je die beelden dan (vrijwillig) verstrekken? Een oplossing is dan een vordering vanuit de politie aan de provider, dus werken ze samen. In feite wordt de provider dan gedwongen om mee te werken en dan vervalt eigenlijk de aansprakelijkheid of strafbaarheid.

Het bedrijfsleven (de provider) heeft diverse vormen van data en met behulp van deze data kan er voor de politie waardevolle informatie verkregen worden. De servers die deze informatie hebben en door de bedrijven gebruikt worden heeft de politie niet ter beschikking. Het bedrijf gmail kan bijvoorbeeld zien dat er in een bepaalde server een persoon veel spam mailt naar e-mailadressen. Dit kan het bedrijf melden aan de politie om zo de spammer op te pakken.

7.1 Informatie-gestuurd werken

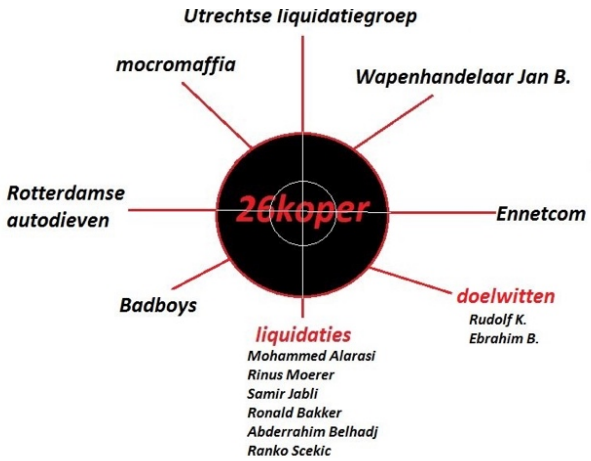
De politie kan dan de informatie van verschillende bedrijven verzamelen en deze vervolgens verbinden en daarmee een beeld vormen waardoor de politie op basis van informatie gaat werken waardoor de maatschappij gericht veiliger wordt. Dat is noodzakelijk om grote schades voor de bedrijven zelf te voorkomen maar ook voor de economie van een land. Dus dat middels deze technieken lover-boys, criminelen, terroristen al snel met big-data, data-mining, machine learning en data-science effectief geïdentificeerd kunnen worden. Dit is dan het verwerken van operationele data waarop tactische beslissingen genomen worden en die weer leiden tot het veranderen van beslissingen en regelgeving op strategisch niveau. Maar dat is op basis van strategische analyses die gebaseerd zijn op politiedata. Dit was voor ons lastig om te begrijpen, maar ons is uitgelegd dat onderzoeken op een operationeel niveau gedaan worden en dat dit reden is om op tactisch niveau te bepalen welke groep onderzoeken gedaan gaan worden; een voorbeeld is thematisch rechercheren op bijvoorbeeld liquidaties en dat het tactisch niveau weer informatie geeft voor het strategisch niveau. Dus als illegale wapens het grote probleem binnen alle liquidaties zijn dat dan wetgeving aangepast kan worden of dat de politie opdracht krijgt extra capaciteit vrij te maken voor wapenonderzoeken in plaats van liquidatie onderzoeken. Omdat als er minder wapens te krijgen zijn ook de liquidaties minder zullen worden of de pakkans groter wordt.

Het bedrijfsleven kan op basis van haar eigen beschikbare data ook analyses maken. De reden dat dit goed kan, is omdat het bedrijfsleven vaak geconfronteerd wordt met politie verzoeken (vorderen van data) en dus weet het bedrijfsleven waar de politie-opsporing belangstelling voor heeft. Dus een telecomprovider weet prima voor welke soort abonnementen de politie belangstelling heeft of welke wijken in een bepaalde stad de meeste criminelen wonen omdat de politie daar het meeste opvraagt of interceptie aansluitingen aanvraagt. Middels profielen kan een provider dan zelfs aangeven welke achtergronden mensen hebben, uit welke landen deze komen enzovoorts. In principe doen de providers dit niet. De ethische vraag is dan of als er niet naar deze data gekeken wordt of het bedrijfsleven dan bewust of onbewust facilitair is aan georganiseerde criminaliteit en terrorisme ten behoeve van de eigen winst / groei. Tevens is een ethische vraag of het gerechtvaardigd is dat de politie over al deze data beschikt en daar Big-data onderzoek mee doet. Immers doordat de politie opsporing data met bedrijfsdata kan combineren en dan dus meer data dan bedrijven heeft, wordt de privacyschending groter.
Én is de controle op wat er met de data van de betrokkene gebeurt vanuit de verantwoordelijke (het bedrijf) minder groot. Criminelen hebben dus middelen nodig

om hun criminele activiteiten te ondersteunen. Dus telecom, vervoer, vastgoed en bijvoorbeeld financiën. Het bedrijfsleven vervult dan een faciliterende rol.

7.2 Wat wordt er precies met facilitaire rollen bedoeld?

De politie heeft onder andere als doel liquidaties aan te pakken in de maatschappij. Het onderzoek 26tear[38] en 26koper[39] gaan hierover. De politie heeft een nieuwe manier bedacht om liquidaties te voorkomen. De criminele organisaties zoeken naar criminelen die de faciliterende rollen kunnen uitvoeren. Om een liquidatie te plegen, moet er namelijk eerst een aantal zaken van tevoren worden geregeld. Er zijn faciliterende werkzaamheden nodig, of te wel “ondersteunende rollen”. Er zijn mensen nodig om bijvoorbeeld wapens te regelen, mensen in de gaten houden, de gebruikten spullen opruimen/verbranden en er moet iemand zijn om een vluchtauto te regelen voor de “moordenaars” zodat ze snel weg kunnen vluchten na het plegen van de liquidaties. Dit zijn voorbeelden van facilitaire rollen. Dus facilitator zijn mensen of organisaties die criminelen helpen bij het voorbereiden, uitvoeren of verhullen van illegale activiteiten, soms willens en wetens, soms tegen wil en dank en soms zonder dat zij zich dat bewust zijn. In de digitale wereld spelen facilitators hierbij een sleutelrol. Tijdens een onderzoek van de politie in 2014 is er een Audi gestolen. Deze ‘Rotterdamse autodieven’, die de Audi hebben gestolen speelden hier een facilitaire rol, een ondersteunende rol. Door het volgen van deze auto wist de politie uiteindelijk wie de Utrechtse liquidatiegroep was. Deze nieuwe manier van opsporen is een groot succes geworden om liquidaties te voorkomen. Op het plaatje 26koper, een onderzoek van de politie, staat wat er allemaal nodig was om de liquidaties te plegen.



Je ziet bijvoorbeeld op het plaatje de facilitaire rollen: Rotterdamse autodieven, wapenhandelaar Jan B. en badboys. Ook zie je dat er een macromaffia en Ennetcom aanwezig waren. Ennetcom was bijvoorbeeld leverancier van gecrypte telefoons, waardoor de politie niet de telefoons kon doorzoeken naar gegevens.

[38] https://www.om.nl/onderwerpen/ondermijnende/verhalen/meerdere-liquidaties/

[39] http://www.boevennieuws.nl/nieuws/26koper-onderzoek/

7.3 LeaseWeb

LeaseWeb is een enorm grote Nederlandse provider. Door het aantal klanten uit heel Europa is LeaseWeb een knooppunt van data. Daarin zit legale data maar ook enorm veel illegale data. LeaseWeb is belangrijk bij aanpak van bijvoorbeeld kinderporno.

“LeaseWeb heeft meer dan 2 miljoen websites in beheer, is de grootste website hostingprovider in Nederland en een van de grootste hostingaanbieders in Europa,” zegt Alex de Joode, Security Officer (beveiligingsspecialist) van LeaseWeb. “Het aantal meldingen van kinderpornoplaatjes op websites bij LeaseWeb is dus een aardige indicatie voor het algehele probleem van kinderporno op internet in Nederland. Helaas zien wij op dit moment zelfs een stijging van het aantal meldingen van kinderpornoafbeeldingen op websites in ons hostingnetwerk. Het kinderpornofilter kan daar verandering in brengen. LeaseWeb wil als grootste hostingprovider in Nederland graag een maatschappelijke verantwoordelijkheid nemen, maar we hebben hiervoor wel de medewerking nodig van het KPLD.”[40]

Zoals hierboven omschreven is het voor de politie door middel van publiek private samenwerking mogelijk om meer gegevens te zien dan als alleen de standaard bevoegdheden gebruikt worden. In het geval van LeaseWeb zou de politie eerst een verdenking moeten hebben tegen een persoon voordat er een vordering om persoonsgegevens gemaakt kan worden. Doordat LeaseWeb zelf verantwoordelijkheid neemt, worden verdachte personen eerder zichtbaar en kan de politie dus andere verdachte personen vinden dan normaal gezien via een aangifte bekend zouden worden. Maar…. de publiek private samenwerking moet dan ook wel twee kanten opwerken. Dus moet de politie ook wel wat doen met door het bedrijfsleven aangeleverde data. Of moet de politie aan het bedrijfsleven data geven waarmee het bedrijfsleven kan zoeken in de systemen. Dit laatste ligt best wel gevoelig omdat het privacy van mensen gaat, deze mensen misschien wel verdacht maar nog geen verdachte zijn.

[40] http://www.ocom.com/nl/pers/kinderpornofilter-leaseweb-technologisch-gereed-politie-nog-niet

7.4 Verdacht of verdachte zijn?

Een verdachte is iemand waar artikel 27 Wetboek van Strafvordering op van toepassing is. [41] Als er dus nog geen feiten of omstandigheden zijn waaruit een redelijk vermoeden van schuld zou voortvloeien dan zijn er weinig rechtmatige mogelijkheden. Dat kan soms heel raar zijn. Als in Nederland iemand chat over wat hij of zij met kleine kinderen op misbruik gericht zou willen doen, dan is dat niet strafbaar. En daarom kan iemand op alleen chat-text niet als verdachte aangemerkt worden. Het kijken naar kinderporno is wel strafbaar. Dus als van iemand zijn ip-adres (dit is een persoonsgegeven) bekend is uit chats EN LeaseWeb heeft kinderporno afbeeldingen waar hetzelfde ip-adres bij gevonden wordt, bijvoorbeeld omdat een afbeelding geklikt is, dan is er wel een redelijk vermoeden van schuld en kan de eigenaar van het ip-adres aangemerkt worden als verdachte.

Maar: een ip-adres kan door een heel gezin, studentenhuis of bedrijf gebruikt worden. Daarom moet de politie dan uitzoeken wie de abonnee is, wie er verder wonen of werken en of de namen die daarbij horen al eerder in beeld zijn geweest bij soortgelijke strafbare feiten. Daarnaast zal de politie ook onderzoek doen naar welk beroep deze mensen hebben, omdat bijvoorbeeld bekend is dat veel pedofielen leraar, fotograaf of sportbegeleider zijn. De combinatie tussen plaats, tijd, beroep (gelegenheid) maakt dan of iemand verdachte is.

Om dat verder uit te zoeken (waarheidsvinding) zal de politie soms verregaande middelen in moeten zetten. Dat zijn dan vaak de Bijzondere Opsporings Bevoegdheden (BOB-wetgeving) zoals interceptie (tappen), observeren en soms direct afluisteren (microfoons in een huis plaatsen).

---

[41] Artikel 27

1.
Als verdachte wordt vóórdat de vervolging is aangevangen, aangemerkt degene te wiens aanzien uit feiten of omstandigheden een redelijk vermoeden van schuld aan een strafbaar feit voortvloeit.

2.
Daarna wordt als verdachte aangemerkt degene tegen wie de vervolging is gericht.

3.
De aan de verdachte toekomende rechten komen tevens toe aan de veroordeelde tegen wie een strafrechtelijk financieel onderzoek is ingesteld of te wiens aanzien op een vordering van het openbaar ministerie als bedoeld in artikel 36e van het Wetboek van Strafrecht niet onherroepelijk is beslist.

4.
De verdachte die de Nederlandse taal niet of onvoldoende beheerst, is bevoegd zich te laten bijstaan door een tolk.

In het geval van kinderporno maakt de politie ook al snel verschil in verschillende fases: het downloaden en bekijken van kinderporno (minder ernstig), het uploaded en verspreiden van kinderporno (ernstiger) en het maken van kinderporno (heel ernstig).

7.5 Dilemma van publiek-privaat samenwerken

Het Korps Landelijke Politiediensten (KLPD) werkt sinds 2009 samen met LeaseWeb voor bestrijden van seksueel kindermisbruik. LeaseWeb is het grootste website hostingbedrijf van Nederland en is in nauw overleg met het ministerie van Justitie en Meldpunt Kinderporno. Het KLPD heeft zijn hash-databases hiervoor beschikbaar gesteld, om zo met deze filtering oplossing, kinderporno gevoelige websites in Nederland proactief te controleren op kinderporno plaatjes.

LeaseWeb maakt gebruik van MD5 hash-technologie. Deze hash-technologie wordt ook al gebruikt door het KLPD. Het algoritme dat LeaseWeb toepast, werd in 1991 ontwikkeld door de Amerikaanse wiskundige en informaticus Ron Rivest. MD5 (Message Digest Algorithm 5) wordt gebruikt in vele veiligheidstoepassingen, in dit geval gaat het hier om beschrijden van kindermisbruik. Met deze techniek worden digitale ‘vingerafdrukken’ (hashes) genomen van de afbeeldingen die zich op het internet bevinden. Een hashwaarde van een afbeelding is een unieke code/rekensom die gebruik maakt van hexadecimale karakters (0 t/m 9 en A t/m F). De hashwaarde verschilt al gelijk bij een verandering van één pixel van het plaatje, zo hebben alle plaatjes een unieke code, hashwaarde.

De technologie bespaart de politie veel tijd en psychische klachten. ‘Een computer kan in tweeënhalf uur vijftig- tot zestigduizend plaatjes op de computer van een verdachte bekijken’, zegt Frans Kolkman, leider van het IBDE Oost-Nederland en een veteraan in de strijd tegen kinderporno[42]. De landelijke database bevat tussen de vier en vijf miljoen strafbare plaatjes. De computer verlicht het werk van zedenrechercheurs, die hebben veel schokkende beelden gezien van onder andere kinderporno. Sommige van hen hebben trauma’s opgelopen. Ze schikken bijvoorbeeld wakker in bed en kunnen moeilijk slapen, ook moesten ze psychische hulp zoeken.

[42] http://www.volkskrant.nl/recensies/kinderporno-laat-verdachte-vingerafdrukken-achter~a323354/

De beelden vergelijken gebeurt op een even eenvoudige als ingenieuze wijze, zegt Alex de Joode, Security Officer van Leaseweb[43]. ‘Wat we doen, is de beelden die bij onze klant worden geüpload, afzetten tegen een database met beelden die door de politie zijn verzameld en zijn gekenmerkt als strafbaar. Als een gebruiker een foto neerzet die overeenkomt met eentje uit de database, wordt dat beeld geweerd.’ De computer doet dus het werk. Hij zoekt in de database met de vingerafdrukken van ongewenste afbeeldingen en zoekt vervolgens naar gelijke foto’s op het internet. Wanneer de hash van twee bestanden overeenkomen dan is er sprake van een ‘match’. De betreffende foto wordt geblokkeerd en van het internet verwijderd.

Concluderend, wanneer er te zien is dat het overduidelijk om kindermisbruik gaat, dan wordt de desbetreffende website op zwart gezet voor Leaseweb, de website wordt eruit gegooid. De politie wordt dan gelijk geïnformeerd, zodat ze actie kunnen ondernemen en criminelen oppakken. Maar als het een onduidelijk geval is, het plaatje komt eigenlijk niet overeen met de kinderpornoplaatjes, dan beoordeelt eerst een gespecialiseerde afdeling van het KLPD of iets strafbaar is of niet. Als het dan toch nog strafbaar is, wordt de website op de zwarte lijst gezet. De hashwaarde kunnen ook niet overeenkomen, dan betekent dat de politie de privacy schendt van onschuldige burgers. Als jij bijvoorbeeld foto’s van jezelf op een blog zet, waarin jij in bikini ligt op het strand, dan controleert de computer ook deze hashwaarde na en kan de politie jouw foto’s zien; dit wil je natuurlijk niet want het is jouw privacy.

Maar er ontstond ook een dilemma:
De Joode wil dat de KLPD meer vaart maakt. "Wij vinden het jammer dat het zo lang moet duren voordat er bij het KLPD een beslissing wordt genomen over het beschikbaar stellen van hun kinderpornodatabases. Welke politieke of organisatorische oorzaken er ook aan ten grondslag liggen, het gaat om de bescherming van kinderen.” In reactie op het bericht van LeaseWeb liet een woordvoerder van de KLPD weten het initiatief van LeaseWeb 'sympathiek' te vinden en er niet onwelwillend tegenover te staan. "Het gaat wel om een politiedatabase die we niet zonder meer voor gebruik door derden beschikbaar stellen. We werken eraan en bekijken welke veiligheden we daarvoor moeten inbouwen. In principe werken we eraan mee, maar het is nog niet zover.” Duidelijk was dus dat bedrijfsleven graag wilde maar dat de overheid ook zorgvuldig met de politiedata om moest gaan. en dat kan de samenwerking heel erg veel moeilijker maken.

---

[43] http://www.volkskrant.nl/recensies/kinderporno-laat-verdachte-vingerafdrukken-achter~a323354/

7.6 Publiek-private samenwerking en invloed op de politiek

Informatie gestuurd werken dus vindt z'n oorsprong in data en hoe deze data verwerkt wordt op verschillende niveaus. Door het samenvoegen van strategische analyses van de politie wordt een criminaliteitsbeeldanalyse gevormd[44]. Deze analyses zijn dan wel een beeld dat gevormd wordt vanuit de politie. Dat is uiteraard nog niet het beeld dat ook bedrijven of burgers hebben. Die ervaren criminaliteit vaak anders. Door samenwerking te zoeken tussen de verschillende partijen en verschillende analyses op strategisch niveau goed samen te brengen kan er dan een bestuurlijk criminaliteitsbeeld analyse gemaakt worden[45].

Een bestuurlijk criminaliteitsbeeld-analyse heeft dus invloed op bestuurlijke maatregelen en beslissingen. Deze vinden plaats op lokaal niveau, bijvoorbeeld de burgemeester. Maar ze hebben ook grote invloed op verkiezingsprogramma's en de daarmee de politiek. Tenslotte kan hierdoor ook wetgeving aangepast gaan worden.

Ingrid de Vries
"De opsporing van zware delicten heeft naar mijn mening niets te maken het het schenden van privacy. Er zijn namelijk wetten waar de politie zich aan houdt en daarmee is het in de wet geregeld en wordt dus niet iets geschonden".

De politiek kijkt vanuit haar verantwoordelijkheden zoals veiligheidsvraagstukken maar ook bescherming van de burger naar het privacy domein. Het is dus een schaakspel tussen veiligheid en bescherming van de burger op meerdere domeinen.

[44] http://www.openbaarministerie.org/images/stories/Persberichten/Curacao/Start%20Criminaliteitsbeeldanalyse%20Curaao%202013%20NL.pdf

[45] https://www.riec.nl/index/thema

Hoofdstuk 8 Hoe denkt de Tweede Kamer over privacyschending?

In Nederland leven wij in een indirecte democratie. Dit houdt in dat dat wij als volk niet zelf beslissingen nemen, maar dit overlaten aan de zelfgekozen vertegenwoordiger. Hierdoor hebben wij dus wel nog indirect invloed op de politieke besluitvorming. [46]De Tweede Kamer heeft 150 leden, en verschillende partijen zoals de Partij van de Dieren, het CDA en GroenLinks. Elke vier jaar mogen alle Nederlanders van 18 of ouder stemmen op een partij naar keuze. Als alle stemmen zijn uitgebracht wordt er gewerkt met zetels. Er zijn 150 zetels te verdelen, en één zetel staat gelijk aan het aantal uitgebrachte stemmen gedeeld door 150. Daarna krijgen de partijen het aantal zetels dat ze hebben verdiend. Om het kabinet te kunnen vormen is wel de meerderheid van de zetels nodig, namelijk 76. Dit wordt nooit gehaald door één partij en dus moeten er partijen gaan samenwerken. Dus stel dat de VVD 33 zetels heeft en de PvdA heeft 43 zetels én beide partijen willen met elkaar samenwerken, kan het kabinet gevormd worden. Een aantal taken die de Tweede Kamer heeft zijn onder andere debatteren over actuele en/of belangrijke zaken, ook kunnen er wetsvoorstellen goedgekeurd of verworpen worden én kunnen er wetsvoorstellen worden gedaan.

Het begrip privacyschending is de Tweede Kamer zeker niet ontgaan. Meerdere malen is er stevig over gedebatteerd, en de meningen lopen ook erg uit elkaar. De punten waar ze vooral op botsen zijn hoever de politie mag gaan met het schenden van privacy. [47]Vorig jaar in 2015 heeft de minister van veiligheid en justitie, Ard van der Steur, nog een rapport uitgebracht over privacy-onderzoeken van de politie. Uit dit rapport bleek onder andere dat de politie zich op belangrijke punten zich nog onvoldoende aan de wet politiegegevens (WPG) houdt. In de WPG staat dat de politie zorgvuldig moet omgegaan met de privacy van burgers. Zo wordt er volgens Steur te laks omgegaan met de persoonsgegevens en worden deze veel langer in het systeem bewaard dan eigenlijk de bedoeling is. Ook zegt hij dat er onvoldoende gecontroleerd wordt, en dat de politie niet voldoet aan de eisen van de WPG over het op orde hebben van verstrekken, tussentijds controleren en intrekken van autorisaties[48].

---

46 https://www.parlement.com/id/vhnnmt7ih7yh/tweede_kamer

47 file:///C:/Users/isave/Downloads/tk-beleidsreactie-wodc-onderzoek-privacy-slachtoffers.pdf

48 Het proces waarbij een persoon inzicht kan krijgen in een document.

Wat verder ook veel ter sprake is gekomen in de Tweede Kamer zijn de hackbevoegdheden van de politie. [49]Toen staatssecretaris Dijkhoff van de VVD een wetsvoorstel deed om de politie de bevoegdheid te geven om in computers en telefoons in te breken, waren het de D66, GroenLinks, SP en Partij voor de Dieren de partijen die hier zeer kritisch over waren. De VVD en het CDA zagen deze wet dan weer wel zitten. Het grote argument van de partijen die tegen zijn, is dat zij vinden dat de samenleving juist onveiliger wordt als de politie computers en telefoons zou gaan hacken. Zo zegt D66: ”*het is erg tegenstrijdig als de politie juist cybercriminaliteit wil bestrijden door kwetsbaarheden in de software niet de dichten, maar juist open te houden en zelf te misbruiken.”* Verder vinden de tegenpartijen ook dat dit een te grote inbreuk op de privacy zou hebben. En zegt de SP: “*via software volgen van gegevensstromen is niet veel anders dan het permanent waarnemen wat zich in een woning afspeelt. Dat laatste is niet toegestaan en dat eerste wordt geregeld met dit wetsvoorstel.”* De voorstanders, de VVD en het CDA hebben een hele andere mening. Zo vindt de VVD dat door de snelle ontwikkelingen ook de wetten mee moeten met de tijd, en dat deze wet noodzakelijk is. Het CDA gaat nog een stapje verder, en vindt dat dit wetsvoorstel nog uitgebreider moet. Ze vinden onder andere dat het ook weer verplicht moet worden de mensen om hun gegevens te laten zien aan de politie.

Aan de ene kant wil de overheid bepaalde bevoegdheden om in computersystemen te kunnen kijken en aan de andere kant stelt de overheid eisen aan bedrijven om data van klanten te beveiligen. De tegenstrijdigheid zit in het niet bekend maken van lekken ins software, die lekken zouden namelijk ook door cyber criminelen misbruikt kunnen worden en dat is nu juist waar de politie onderzoek naar doet.

[49] https://www.privacybarometer.nl/maatregel/86/Inbraakbevoegdheid_voor_politie

Hoofdstuk 9 Eindconclusie

Wij hebben ons profielwerkstuk geschreven over veiligheid en privacy in relatie tot opsporing. Door te praten met deskundigen afkomstig uit de opsporing en veel research te doen, hebben wij genoeg informatie om tot begrijpelijke conclusies te komen. Voordat wij dat doen willen we eerst onze twee belangrijkste deelvragen beantwoorden.

- Wat betekent de privacyschending voor het opsporen van criminelen?

De mogelijkheid tot schenden van privacy is voor de politie heel belangrijk. De politie heeft deze informatie namelijk nodig om criminelen op te kunnen sporen. Je kunt hierbij denken aan het doorzoeken van woningen of het aftappen van telefoons, maar ook aan dingen zoals het verspreiden van videobeelden van de verdachten of het bekijken van jouw telecomgegevens en zo zien waar jij je bevindt. Dit zijn slechts vier manieren waarop de politie jouw privacy kan schenden. Dit zijn overigens wel manieren die een behoorlijke inbreuk maken op je privacy, en daarom moet de politie hiervoor toestemming hebben van een rechter. Dit zijn daarom bijzondere opsporingsbevoegdheden. Maar door deze acties krijgt de politie wel veel informatie wat misschien wel doorslaggevend kan zijn voor een aanhouding. Kortom: privacy schending is noodzakelijk voor de politie om criminelen te kunnen opsporen.

- Wat betekenen nieuwe datamogelijkheden voor de wijze van opsporen?

De afgelopen jaren is de technologie enorm vooruitgegaan. Vooral als je kijkt naar de technologische ontwikkelingen om beter en sneller te communiceren zoals bijvoorbeeld met de computer, en de mobiele telefoons. Het is daarom ook voor de politie enorm belangrijk om bij te blijven met deze technologie, zodat ze criminelen altijd een stapje voor kunnen zijn. Op dit moment heeft de politie bijvoorbeeld geavanceerde techniek waarmee gezien kan worden waar verdachten afgelopen week zijn geweest. Of kunnen ze met behulp van een WiFi scanner kijken met welke WiFi-accesspoints jouw telefoon verbonden is geweest en zo locaties vaststellen waar mensen elkaar ontmoet hebben. Dit is een klein voorbeeld van de vele manieren waarop de politie informatie van iemand kan verkrijgen met behulp van veel data. Kortom: voor de politie zijn de nieuwe techieken met data heel belangrijk, omdat ze zo veel sneller criminelen kunnen opsporen maar ook tegenhouden.

Het vinden van antwoorden op de hoofdvraag was enorm ingewikkeld. Er was heel veel informatie maar de meeste informatie bleek te gaan over meningen van mensen en veel was niet op feiten gebaseerd. De interviews bleken ook ingewikkeld. Mensen die gevraagd werden naar de onderwerpen gaven ook aan dat ze er als burger anders naar keken dan vanuit hun beroep. Het is ons wel vrij duidelijk geworden dat het niet mogelijk is om en voor de veiligheid van burgers te zorgen, en tegelijkertijd honderd procent privacy te garanderen. Je kunt dus beter vragen hoe de politie zo min mogelijk privacy schend van burgers, en tegelijkertijd ook voor de veiligheid kan zorgen. Daarnaast is het belangrijk te weten waar de prioriteit van privacy ligt voor de burger als het gaat om de veiligheid. Dit blijkt ook afhankelijk van de actualiteit. Mensen vinden de privacy minder belangrijk als het gaat om het voorkomen van terroristische aanslagen, zeker als die enorm in het nieuws zijn. Maar als daar geen dreiging op is dan vinden ze de privacy wel weer heel erg belangrijk, want ze zijn voor hun gevoel veilig.

Wat ons is opgevallen tijdens het schrijven van ons profielwerkstuk is dat veel privacyschending gebeurt zonder dat we dit doorhebben: we rijden op de snelweg, en daar worden we gefilmd, we verbinden met onze mobiel met een gratis wifi netwerk, en we worden geregistreerd. Dit zijn twee voorbeelden van hoe onze privacy bijna dagelijks wordt geschonden. Gewone burgers, die wij gesproken hebben en die geen expert zijn op gebied van politie en justitie, hadden geen flauw idee dat dit gebeurt.

We kunnen dit ook zo houden, en niets zeggen over de mate waarin en de manieren waarop hun privacy geschonden wordt. Hierdoor weten de mensen niet dat hun privacy geschonden wordt en kunnen ze er dus ook niet hierover klagen. Het gevolg is dat de politie en justitie rustig hun gang kunnen gaan, zonder gestoord te worden door mensen die boos zijn dat hun privacy steeds wordt geschonden. Deze oplossing heeft zeker niet onze voorkeur.

Wat waarschijnlijk het belangrijkste is, is dat de burgers goed ingelicht moeten worden dat hun privacy geschonden wordt, maar vooral ook waarom. Dit omdat wij leven in een rechtsstaat en daarmee burgers ook een democratische inspraak moeten hebben over hoe er met hun gegevens omgegaan wordt. Dit kan bijvoorbeeld met behulp van flyers en natuurlijk via social media. Ons lijkt het verstandig om hierin deze mensen te vertellen waarom het schenden van privacy zo belangrijk is. Wij denken dat dit als gevolg heeft dat een grote groep mensen heel anders tegen het schenden van privacy aan zal kijken dan dat ze daarvoor deden. Ze zullen er minder problemen mee hebben, omdat ze weten dat het voor een beter doel is. Waar ook rekening mee gehouden moet worden, is dat de mensen

bijvoorbeeld wel de camera's in de winkelstraten zien hangen, en wel doorhebben dat hun privacy daarmee geschonden wordt. Ook denken wij dat het verstandig is om de burgers de gevaren van het internet uit te leggen, zodat ze hier voorzichtiger mee omgaan. Hierdoor zullen er veel minder mensen slachtoffer worden van de gevaren op het internet. Denk hierbij bijvoorbeeld dat hackers je webcam kunnen hacken, en zo alles kunnen zien wat jij doet. Door mensen hierover voor te lichten, weten ze dat je dit bijvoorbeeld heel simpel kunt verhelpen door een stickertje op de webcam te plakken.

Tegenhouden kun je het niet, maar uit onder andere de enquête blijkt dat mensen het niet erg vinden dat hun privacy wordt geschonden als ze hier maar geen last van hebben. Want op de vraag: "vindt u het erg dat de politie uw privacy schendt als u hier geen last van heeft?" zegt namelijk slechts 20% dat ze het wel erg vinden, en zegt de overige 80% dat ze dit niet erg vinden.

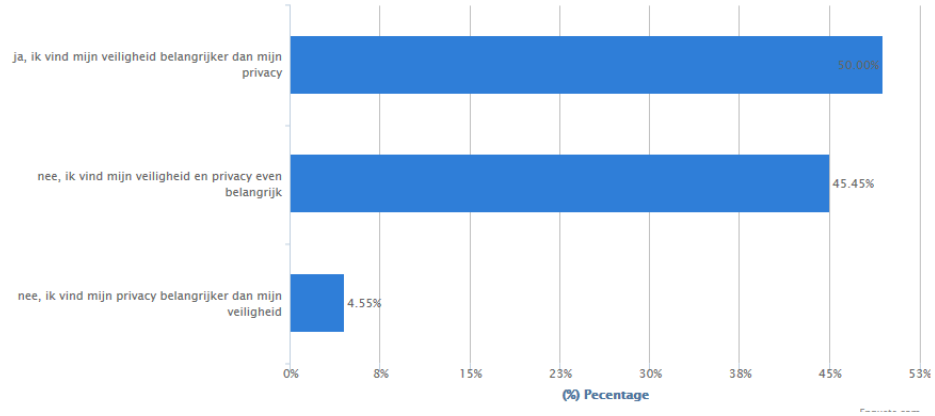
In de toekomst zal de politie meer afhankelijk zijn van grote datahoeveelheden, maar om te helpen uit al deze data de juiste informatie te halen, zal machine learning en kustmatige intelligentie noodzakelijk worden. Computers zullen gaan leren uit mensenlijk gedrag en de data die daarbij hoort. Wij denken dan ook dat het belangrijk gaat worden om te zorgen dat data goed gecontroleerd wordt tegen privacy schendingen en dat ook de algoritmes van de zelflerende systemen goed gecontroleerd moeten worden. Dit om te voorkomen dat er uit onjuiste data of verkeerde berekeningen mensen in hun privacy geschonden worden, bijvoorbeeld omdat een computer iemand onterecht als verdacht heeft aangemerkt. Wij denken dat het belangrijk is dat in de toekomst de burgers transparant ingelicht worden, over data kunnen beschikken om zelf ook onderzoek te kunnen doen en dat ze goed snappen waarom het zo belangrijk is dat politie soms privacy moet schenden[50].

Verder hopen wij dat de politie in de toekomst meer en beter zal samenwerken met bedrijven zoals Facebook, Twitter, Google en Instagram. Deze bedrijven zijn enorm goed in de analyses van de data waar ze over beschikken en kunnen heel goed per persoon aangeven waar diegene is, waar die naar zoekt, en met wie hij praat en met welke applicaties. Dit zou allemaal enorm kunnen helpen om plannen voor criminele activiteiten te voorkomen.

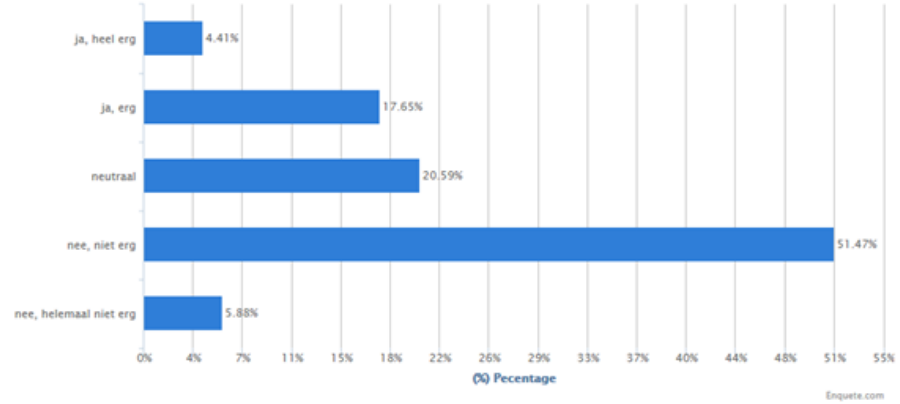
[50] https://data.overheid.nl

Bijlage 1: enquête

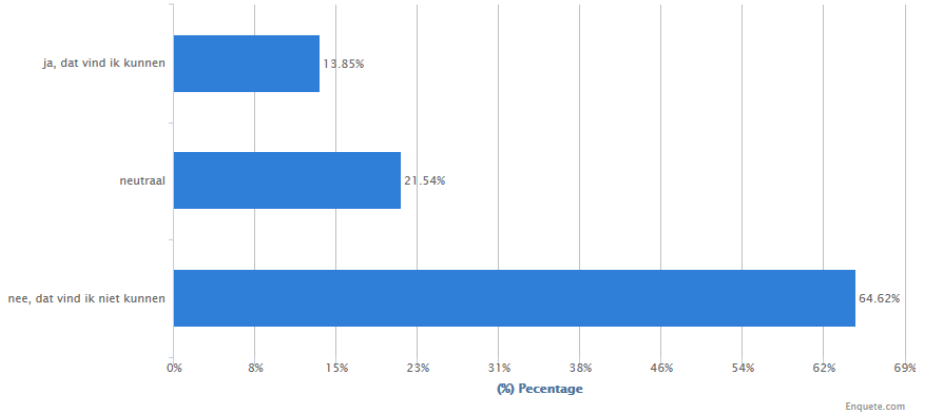
vindt u uw veiligheid belangrijker dan uw privacy?



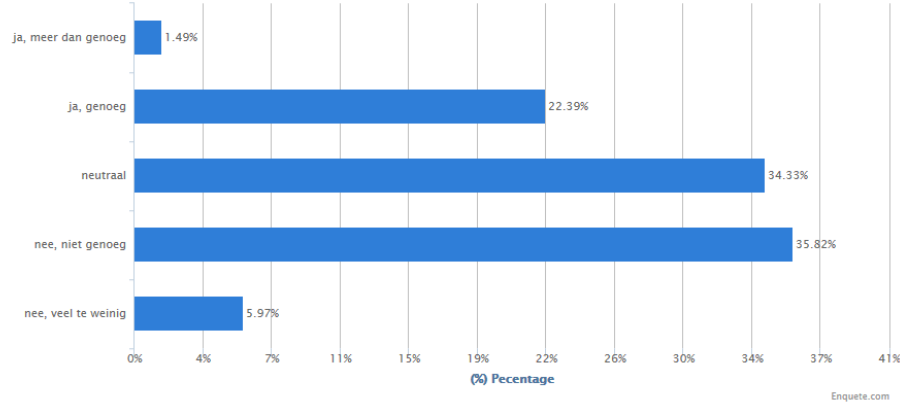
vindt u het erg dat de politie uw privacy schendt als u hier geen last van heeft?



vindt u het kunnen dat de politie uw online gegevens (internet- en telefoondata) aftapt en bewaard?



vindt u dat de politie genoeg doet om criminelen op te sporen?



Bijlage 2: interviews

Interview 1 met Remco Verhoef (data-analist)

Vraag 1:

Op welke wijze zou de overheid / de politie naar uw mening het beste voor de veiligheid van de burgers kunnen zorgen, met een zo min mogelijke schending van privacy van burgers?

- Wel informatie verzamelen, maar wel op de privacy van de burgers letten. Dus niet meer data verzamelen dan nodig is en met de data die je hebt er slim mee om te gaan.

Vraag 2:

Er wordt vaak gezegd dat de politie voornamelijk reactief is. Repressief zoals voorkomen en tegenhouden houdt in dat de politie waarschijnlijk meer privacy zal schenden omdat de aanwijzingen dan vager zijn. Wat zijn uw verwachtingen van de politie?

- Als je te vroeg bent met aanhouden dan zal de straf erg laag zijn, want er is nog geen misdaad gepleegd. Het mooiste zou zijn om het te voorkomen.

Vraag 3:

Paalgegevens hebben de gegevens van telefoons die gebruik maken van een bepaalde GSM mast. De politie kan deze gegevens verkrijgen, en kunnen dan zien welke telefoons er allemaal binnen een bepaalde tijd in de buurt van zo'n GSM mast zijn geweest. De telecom providers willen deze data maar beperkt bewaren (dataretentie) en veel voorvechters van privacy zijn het daar mee eens. Uit veel onderzoek is gebleken dat deze opgelost konden worden dankzij historische paalgegevens. Hoe denkt u over deze privacyschending in verhouding tot de mogelijkheden om zware misdrijven op te lossen of te voorkomen?

- De informatie uit palen is op dit moment heel belangrijk, je wil deze data uit palen ook nog over 20 jaar kunnen bekijken. Als dat niet kan wordt het een probleem.

Vraag 4:
Welke voorbeelden kunt u geven vanuit uw werk waarbij privacyschending door de overheid / politie een belangrijk onderwerp was. En kunt u daarbij aangeven in welke mate u hier privé anders over denkt dan zakelijk?
- Remco zit in privé heel erg op zijn privacy en vind het juist belangrijk. Maar zakelijk vind hij de informatie uit data heel belangrijk en het schenden van de privacy dan juist goed.

Vraag 5:
Bij datamining worden nieuwe vormen van data gevormd met behulp van gegevens in de bestaande data, dus de data die je hebt, wordt vanuit verschillende perspectieven geanalyseerd om zo nieuwe bruikbare informatie te verkrijgen. Data wordt daarom het nieuwe goud genoemd. Dat wil zeggen dat het voor criminelen en terrorisme veel waard is, maar ook voor de overheid / politie. Hoe kunnen we naar uw mening gebruik van data door zowel de criminele als de overheids kant zo goed mogelijk beveiligen?
- Door zo min mogelijk data op te slaan die niet nodig zijn, en dus alleen de relevante informatie opslaan.

Interview 2 met Ingrid de Vries (politie/opsporing)

Opsporing / rechercheur:

1. **In hoeverre is het schenden van privacy noodzakelijk voor het uitvoeren van de opsporing?**

- Het is voor onderzoek niet mogelijk om geen privacy te schenden. Er is informatie nodig om verder te kunnen komen met het onderzoek, en dat houdt in dat er eigenlijk altijd wel een beetje privacy van iemand geschonden moet worden.

2. Welke persoonsgegevens heeft u het meeste nodig voor de uitvoering van uw taak?

- Het belangrijkste is natuurlijk de identiteit van iemand. Deze is vaak lastig te achterhalen omdat veel criminelen valse papieren en nepnamen hebben.

3. Er is een hack-bevoegdheid voor de politie, hoe kunt u garanderen dat u de proportionaliteit kunt garanderen?

- Daar zijn regels voor. Er worden harde eisen gesteld aan wat je wel en niet mag doen.

4. In de GPDR (General Protection Data Regulation) staat dat bedrijven een datalek verplicht moeten melden, hoe staat dit in verhouding met de hack-bevoegdheid van de politie?

- Als bedrijven niet weten dat er een lek is, kun je als politie zeggen:” o ik ga wel ff het lek binnen” dat is een afweging die je als politie op dat moment maakt, en het ligt aan de situatie.

Algemeen:

Vraag 1:

Op welke wijze zou de overheid / de politie naar uw mening het beste voor de veiligheid van de burgers kunnen zorgen, met een zo min mogelijke schending van privacy van burgers?

-Door heel voorzichtig met de informatie om te gaan, en niet iemands privacy schent als dat niet persé nodig is.

Vraag 2:
Er wordt vaak gezegd dat de politie voornamelijk reactief is. Repressief zoals voorkomen en tegenhouden houdt in dat de politie waarschijnlijk meer privacy zal schenden omdat de aanwijzingen dan vager zijn. Wat zijn uw verwachtingen van de politie?
- Ik verwacht van de politie dat ze preventief te werk gaan, om zo voor de veiligheid te zorgen. Dit houdt wel in dat je de wetgeving zou moeten veranderen. Want stel dat je een liquidatie voorkomt krijgt de dader een veel lagere straf, dan wanneer de liquidatie al gebeurd is, en dat vind ik raar.

Vraag 3:
Paalgegevens hebben de gegevens van telefoons die gebruik maken van een bepaalde GSM mast. De politie kan deze gegevens verkrijgen, en kunnen dan zien welke telefoons er allemaal binnen een bepaalde tijd in de buurt van zo'n GSM mast zijn geweest. De telecom providers willen deze data maar beperkt bewaren (dataretentie) en veel voorvechters van privacy zijn het daar mee eens. Uit veel onderzoek is gebleken dat deze opgelost konden worden dankzij historische paalgegevens. Hoe denkt u over deze privacyschending in verhouding tot de mogelijkheden om zware misdrijven op te lossen of te voorkomen?
- Als je geen metagegevens meer zou hebben, zou je dezelfde informatie op een veel zwaardere en ingrijpende manier krijgen. Hierdoor zou je meer privacy schenden dan daarvoor.

Vraag 4:
Welke voorbeelden kunt u geven vanuit uw werk waarbij privacyschending door de overheid / politie een belangrijk onderwerp was. En kunt u daarbij aangeven in welke mate u hier privé anders over denkt dan zakelijk?
- Ik zou zo snel niet een voorbeeld kunnen noemen, omdat het in elke zaak een belangrijk onderwerp is. Hier denk ik dan ook privé en zakelijk precies hetzelfde over.

Vraag 5:

Bij datamining worden nieuwe vormen van data gevormd met behulp van gegevens in de bestaande data, dus de data die je hebt, wordt vanuit verschillende perspectieven geanalyseerd om zo nieuwe bruikbare informatie te verkrijgen. Data wordt daarom het nieuwe goud genoemd. Dat wil zeggen dat het voor criminelen en terrorisme veel waard is, maar ook voor de overheid / politie. Hoe kunnen we naar uw mening gebruik van data door zowel de criminele als de overheids kant zo goed mogelijk beveiligen?

- De data wordt goed beveiligd, maar je moet wel zorgen dat je bijblijft met de technologie, en dat je altijd net iets slimmer bent dan criminelen. Je moet ervoor zorgen dat je je eigen data beschermt.

Interview 3 met Bas Eikelenboom (politie/opsporing)

Opsporing / rechercheur:

1. **In hoeverre is het schenden van privacy noodzakelijk voor het uitvoeren van de opsporing?**

- Privacy schending is altijd noodzakelijk, zonder goede gegevens kun je nooit aan waarheidsvinding doen of hulp verlenen aan de mensen die dat echt nodig hebben.

2. Welke persoonsgegevens heeft u het meeste nodig voor de uitvoering van uw taak?

- Enticiteiten zoals naam, adres, woonplaats, geboortedatum, rekeningnummer, telefoonnummer en samenstelling gezin en alles wat op een bepaalde postcode te naam gesteld is zoals abonnementen, voertuigen enz.

3. Er is een hack-bevoegdheid voor de politie, hoe kunt u garanderen dat u de proportionaliteit kunt garanderen?

- Dat kan omdat dit loopt via OvJ en lagere rechter dat is bijvoorbeeld een rechtercommerisaris, deze zullen altijd waken over de inzet die gedaan wordt en als politie beseffen we ook heel goed dat als wij op een verkeerde manier gebruik maken van onze mogelijkheden dat hierdoor zaken stuk kunnen gaan en daardoor slachtoffers het nog zwager krijgen.

4. In de GPDR (General Protection Data Regulation) staat dat bedrijven een datalek verplicht moeten melden, hoe staat dit in verhouding met de hack-bevoegdheid van de politie?

- Als de politie hackt en lekken vindt in bepaalde software dan moeten zij dat zo snel mogelijk melden bij de maker van de software. Als een bedrijf gehackt wordt ook al is dit door de politie gedaan. Dan moeten zij dit melden bij de autoriteit persoonsgegevens en soms kan het ongewenst zijn.

Algemeen:

Vraag 1:

Op welke wijze zou de overheid / de politie naar uw mening het beste voor de veiligheid van de burgers kunnen zorgen, met een zo min mogelijke schending van privacy van burgers?

- Door te zorgen dat gegevens breed worden opgevraagd in plaats van alleen op een persoon en dat is om te voorkomen dat bedrijven die data aanleveren een eigen database aanleggen van mensen waarover gegevens door de politie zijn opgevraagd.

Vraag 2:

Er wordt vaak gezegd dat de politie voornamelijk reactief is. Repressief zoals voorkomen en tegenhouden houdt in dat de politie waarschijnlijk meer privacy zal schenden omdat de aanwijzingen dan vager zijn. Wat zijn uw verwachtingen van de politie?

- Zelf repressief moet zijn en dus eerder ingrijpen en niet wachten tot iets gebeurd is.

Vraag 3:

Paalgegevens hebben de gegevens van telefoons die gebruik maken van een bepaalde GSM mast. De politie kan deze gegevens verkrijgen, en kunnen dan zien welke telefoons er allemaal binnen een bepaalde tijd in de buurt van zo'n GSM mast zijn geweest. De telecom providers willen deze data maar beperkt bewaren (dataretentie) en veel voorvechters van privacy zijn het daar mee eens. Uit veel onderzoek is gebleken dat deze opgelost konden worden dankzij historische paalgegevens. Hoe denkt u over deze privacyschending in verhouding tot de mogelijkheden om zware misdrijven op te lossen of te voorkomen?

- Ik vind dat mensen recht hebben op een hele goede opsporing en voorkomen van misdrijven en dus dat ook bedrijven vrijwillig aan mee moeten werken en dus dat die dataretentie zo lang mogelijk moet zijn.

Vraag 4:
Welke voorbeelden kunt u geven vanuit uw werk waarbij privacyschending door de overheid / politie een belangrijk onderwerp was. En kunt u daarbij aangeven in welke mate u hier privé anders over denkt dan zakelijk?
- Ja, met koningsdag hebben we enorm veel mensen gemonitord in hun gedrag waarvan we weten dat zei een bedreiging kunnen vormen voor de veiligheid van andere mensen. Privé vind ik dat de overheid heel voorzichtig moet zijn met het monitoren van mensen. Zakelijk vind ik dat het voorkomen van een aanslag belangrijker is dan welke privacy dan ook.

Vraag 5:
Bij datamining worden nieuwe vormen van data gevormd met behulp van gegevens in de bestaande data, dus de data die je hebt, wordt vanuit verschillende perspectieven geanalyseerd om zo nieuwe bruikbare informatie te verkrijgen. Data wordt daarom het nieuwe goud genoemd. Dat wil zeggen dat het voor criminelen en terrorisme veel waard is, maar ook voor de overheid / politie. Hoe kunnen we naar uw mening gebruik van data door zowel de criminele als de overheids kant zo goed mogelijk beveiligen?
- Voor de overheid: een autorisatiemodel waarin vast gelegd wordt wie welke informatie mag zien en waarom. Voor criminele invoeren van goederen en daarop een criptie controleren mogelijkheden en de datamelding verplicht stellen aan bedrijven.

Literatuurlijst

Filmpjes geraadpleegd over o.a. datamining en OISINT:

https://www.youtube.com/watch?v=boISSjDAVEo

https://www.youtube.com/watch?v=R-sGvh6tI04

https://www.youtube.com/watch?v=W44q6qszdqY

https://www.youtube.com/watch?v=G_0d3w0THCc

Boeken:

Schuijt, B. *Criminaliteit en rechtsstaat.* Uitgeverij Essener B.V.
Verkenning CyberCrime in Nederland (veiligheidsstudies), Boom Juridische Uitgevers
High Tech Crime Criminaliteitsbeeldanalyse, Korps Landelijke Politiediensten

internet:

Aanwijzing opsporingsbevoegdheden. (sd). Opgehaald van Overheid.nl: http://wetten.overheid.nl/BWBR0021581/2004-12-01

Admin. (2016, juni 26). *Het omvangrijke 26Koper onderzoek*. Opgehaald van Boevennieuws.nl: http://www.boevennieuws.nl/nieuws/26koper-onderzoek/

Ammelrooy, P. v. (2009, maart 21). *Kinderporno laat verdachte vingerafdrukken achter*. Opgehaald van de Volkskrant: http://www.volkskrant.nl/recensies/kinderporno-laat-verdachte-vingerafdrukken-achter~a323354/

Arikel 1 sub a Wbp. (sd). Opgehaald van Autoriteit persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-wbp

Artikel 1 sub d Wbp. (sd). Opgehaald van Autoriteit Persoonsgegevens : https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-d-wbp

Artikel 1 sub h Wbp. (sd). Opgehaald van Autoriteit Persoonsgegevens : https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wbp-naslag/hoofdstuk-1-algemene-bepalingen-art-1-tm-5/artikel-1-sub-h-wbp

Artikel 310 Wetboek van Strafrecht. (sd). Opgehaald van Maxius: http://maxius.nl/wetboek-van-strafrecht/artikel310

Bescherming persoonsgegevens. (sd). Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/inhoud/bescherming-persoonsgegevens

College van procureurs-generaal. (2014, september 1). *Aanwijzing opsporingsbevoegdheden (2014A009)*. Opgehaald van Openbaar Ministerie: https://www.om.nl/organisatie/beleidsregels/overzicht-0/opsporing-politie/@86281/aanwijzing-3/

copsincyberspace. (2013). *osint* . Opgehaald van Cops in cyberspace: https://copsincyberspace.wordpress.com/tag/osint/

Datamining:wat is het en hoe werkt het? (sd). Opgehaald van MBK servicedesk: http://www.mkbservicedesk.nl/9966/datamining-wat-hoe-werkt.htm

Een duurzame rechtsstaat vraagt om gezaghebbende instituties en betrokken burgers. (2008, februari 14). Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/actueel/nieuws/2008/02/14/een-duurzame-rechtsstaat-vraagt-om-gezaghebbende-instituties-en-betrokken-burgers

Een strafbaar feit en de gevolgen ervan. (sd). Opgehaald van Omnius: http://www.advocaatvoorstrafrecht.nl/strafbaar-feit

Grondwet. (sd). Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/grondwet-en-statuut/inhoud/grondwet

Hoofdstuk 1: Grondrechten. (sd). Opgehaald van Nederlandse Grondwet: https://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbac43qvy

Kabinet wijzigt regels dataretentie na uitspraak hof. (2014, november 18). Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/actueel/nieuws/2014/11/18/kabinet-wijzigt-regels-dataretentie-na-uitspraak-hof

Kinderpornofilter LeaseWeb technologisch gereed, politie nog niet. (sd). Opgehaald van O.com: http://www.ocom.com/nl/pers/kinderpornofilter-leaseweb-technologisch-gereed-politie-nog-niet

Normen en waarden (verschil en voorbeelden). (sd). Opgehaald van Kritischehouding: http://www.kritischehouding.nl/2013/09/normen-en-waarden.html

OSINT, cruciaal voor opsporing en veiligheid. (sd). Opgehaald van IACA: http://www.anti-crime-academy.com/osint.html

Privacy - bescherming persoonsgegevens. (sd). Opgehaald van Justitia.nl: http://www.justitia.nl/privacy/

Proportionaliteit en subsidiariteit. (2014, april 23). Opgehaald van Juribus.EU: http://juribus.eu/proportionaliteit-en-subsidiariteit/

Publiek-private samenwerking. (sd). Opgehaald van Centrum voor Criminaliteitspreventie en Veiligheid: https://hetccv.nl/certificatie-inspectie/pps/publiek-private-samenwerking/

Rouse, M. (2016, oktober). *predictive analytics* . Opgehaald van SearchBusinessAnalytics: http://searchbusinessanalytics.techtarget.com/definition/predictive-analytics

Tuil, K. v. (2011, augustus 26). *Wat is datamining?* Opgehaald van Computer World: http://computerworld.nl/business-intelligence/74941-wat-is-datamining

Valkengoed, E. v. (2016, april 19). *De kwetsbare balans tussen jouw privacy en veiligheid*. Opgehaald van One world: https://www.oneworld.nl/vrede-veiligheid/de-kwetsbare-balans-tussen-jouw-privacy-en-veiligheid

Veroordeling Robert M. definitief. (2014, september 16). Opgehaald van Nu.nl: http://www.nu.nl/zedenzaak-amsterdam/3879231/veroordeling-robert-m-definitief.html

Voorlopige hechtenis. (sd). Opgehaald van Openbaar Ministerie: https://www.om.nl/onderwerpen/verdachte/voorlopige-hechtenis/

Vugts, P. (2016, november 28). *Tot acht jaar cel in megaproces 26Koper*. Opgehaald van Het Parool: http://www.parool.nl/amsterdam/tot-acht-jaar-cel-in-megaproces-26koper~a4423772/

Wat is een rechtsstaat? (sd). Opgehaald van ProDemos: https://www.prodemos.nl/leer/informatie-over-politiek/wat-is-een-rechtsstaat/

Wat is er allemaal strafbaar online? (sd). Opgehaald van Politie: https://www.vraaghetdepolitie.nl/boetes-en-straffen/boetes-en-straffen/wat-is-er-allemaal-strafbaar-online.html

Welke bevoegdheden heeft de politie? (sd). Opgehaald van Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/politie/vraag-en-antwoord/welke-bevoegdheden-heeft-de-politie

Wet bescherming persoonsgegevens. (sd). Opgehaald van Overheid.nl: http://wetten.overheid.nl/BWBR0011468/2016-01-01

Wetboek van Strafrecht. (sd). Opgehaald van Wetboek online: http://www.wetboek-online.nl/wet/Sr/27.html

Zaak Koper: meerdere liquidaties voorkomen. (sd). Opgehaald van Openbaar Ministerie: https://www.om.nl/onderwerpen/ondermijnende/verhalen/meerdere-liquidaties/

(sd).
d66, GL, Sp en PvdD kritisch over hackbevoegdheid politie. (2016, maart 13). Opgehaald van privacy barometer: https://www.privacybarometer.nl/maatregel/86/Inbraakbevoegdheid_voor_politie

ik bestelde drukgs op het DarkWeb. zo ging dat. (2016, mei 21). Opgehaald van esquire: http://www.esquire.nl/the-good-life/news/a416/ik-bestelde-drugs-op-het-dark-web-zo-ging-dat/

Steur, G. v. (2015, december 14). *beledsreactie WODC-onderzoek privacy slachtoffers*. Opgehaald van file:///C:/Users/isave/Downloads/tk-beleidsreactie-wodc-onderzoek-privacy-slachtoffers.pdf

tot acht jaar cel in megaproces 26Koper. (2016, November 28). Opgehaald van Het Parool : http://www.parool.nl/amsterdam/tot-acht-jaar-cel-in-megaproces-26koper~a4423772/

tweede kamer. (sd). Opgehaald van parlement en politiek: https://www.parlement.com/id/vhnnmt7ih7yh/tweede_kamer

voorlopige hechtenis. (sd). Opgehaald van openvaar ministerie: https://www.om.nl/onderwerpen/verdachte/voorlopige-hechtenis/

wat is een rechsstaat? (sd). Opgehaald van prodemos: https://www.prodemos.nl/leer/informatie-over-politiek/wat-is-een-rechtsstaat/

wetboek van strafvordering. (sd). Opgehaald van wetboek online: http://www.wetboek-online.nl/wet/Sv/27.html

wet-en regelgeving. (sd). Opgehaald van overheid.nl: https://www.overheid.nl/help/wet-en-regelgeving/

zoekmachine laat je zoeken naar drugs en wapens. (2014, april 19). Opgehaald van crimesite: http://www.crimesite.nl/zoekmachine-laat-je-zoeken-naar-drugs-en-wapens/

Logboeken

Logboek Mariska Temming:

20 mei 14:10-14:50 (40 minuten)
1e gesprek met meneer Janssen

24 mei 20:15-21:15 (1 uur)
informatie zoeken voor een hoofdvraag en deelvragen

27 mei 10:50-11:05 (15 minuten)
met meneer Janssen de definitieve hoofdvraag opgesteld

30 mei 12:00-12:50 (50 minuten)
op school informatie opgezocht en bestudeerd

1 juni 16:30-17:30 (1 uur)
deelvragen + informatie besproken met Isa

2 juni 21:00-21:30 (30 minuten)
gesprek met Bas Teamleider Landelijke Recherche samen met Isa tijdens de orkest pauze

6 juni 19:00-22:00 (2 uur)
belangrijke informatie opschrijven + inlezen

1 juli 10:45-13:00 (2:15 uur)
informatie lezen op internet

5 juni 15:00-16:30 en 19:00-20:15 (2:45 uur)
het opzoeken van informatie en maken van deelvraag 1 samen met Isa

12 juli 16:00-18:30 (2:30 uur)
inlezen en werken aan deelvraag 1 met Isa

15 juli 14:00-16:00 (2 uur)
werken aan deelvraag 1 en 2 samen met Isa

16 augustus 20:30-22:15 (1:45 uur)
informatie lezen over OSINT

28 augustus 16:00-18:00 en 20:50-22:50 (4 uur)
inlezen en bestuderen over Big Data, datamining en algoritmes

29 augustus 12:00-15:00 en 19:00-21:00 (5 uur)
deelvraag maken + veel lezen

30 augustus 15:00-17:00 (2 uur)
pws doornemen en aanvullen samen met Isa

1 september 15:50-16:30 (40 minuten)
1e feedback van begeleider Janssen

9 september 18:15-20:45 (2:30 uur)
aan deelvraag werken

15 september 15:00-16:30 (1:30 uur)
werken aan nieuwe deelvraag

16 september 15:30-17:00 (1:30 uur)
bijwerken van de eerste deelvragen naar meneer Janssen verzonden

20 september 19:20-23:00 (3:40 uur)
werken aan deelvraag + informatie lezen

21 september 13:45-14:30 en 15:30-17:00 (1:30 uur)
werken aan deelvraag + informatie lezen

24 september 19:00-22:00 (3 uur)
werken aan deelvraag + informatie lezen

26 september 17:00-20:00 (3 uur)
werken aan deelvraag + informatie lezen

3 oktober 20:00-23:00 (3 uur)

inlezen: publiek-private samenwerking

5 oktober 18:00-23:00 (5 uur)
deelvraag schrijven: publiek-private samenwerking

17 oktober 19:00-21:00 (2 uur)
inlezen + deelvragen aanvullen

7 oktober 17:00-18:00 (1 uur)
1e versie van het pws in elkaar zetten

1 november 19:30-21:30 (2 uur)
deelvraag uitgebreider schrijven over Leaseweb

13 november 20:00-22:00 (2 uur)
werken aan de interview en enquête: vragen opstellen

14 november 11:10-12:00 en 19:00-22:00 (3:50 uur)
op school enquête en interview maken
deelvraag over datamining beter uitwerken + meer inlezen over datamining

15 november 17:00-19:00 (2 uur)
deelvraag verder uitwerken en ingelezen over datamining en algoritmes

16 november 12:55-13:08 (13 minuten)
2e feedback van begeleider Janssen

19 november 11:00-13:30 (4:30 uur)
feedback repareren: ‘leg uit’ + structuur pws aanpassen

20 november 15:30-20:30 (5 uur)
pws met Isa bespreken/overleg

26 november 14:00-18:30 (2:30 uur)
alle spelling verbeteren in pws + meer voorbeelden geven

2 december 16:00-19:00 (3 uur)
feedback repareren: ‘leg uit’

9 december 19:00-21:00 (2 uur)
feedback repareren + lezen op internet

10 december 10:00-13:00 (3 uur)
feedback repareren + inleiding schrijven

16 december 9:00-11:00 (2 uur)
pws verbeteren en weer in elkaar zetten, begeleider de verbeterde versie mailen

27 december 19:00-21:00 (2 uur)
feedback repareren

2 januari 9:00-16:00 (7 uur)
interviewen met Remco, Bas en Ingrid in Utrecht en Amsterdam + een soort presentatie gekregen van Bas en een Forensisch-ICT expert met wie we een liquidatie zaak hebben door lopen uit 2013

4 januari 9:00-12:00 (3 uur)
bronnen verwerken

5 januari 17:00-18:00 (1 uur) en 19:00-23:00 (4 uur)
pws controleren + inleiding, voorwoord en eindconclusie + interviews verwerken + feedback repareren

6 januari 19:00-21:00 (2 uur)
pws verbeteren

8 januari 10:00-14:00 (4 uur) + 20:00-21:30 (1,5 uur)
pws verbeteren + interview verwerken

Logboek Isa Verkruyssen:

20 mei 14:10-14:50 (40 minuten)
1e gesprek met meneer Janssen

24 mei 20:15-21:15 (1 uur)
informatie zoeken voor een hoofdvraag en deelvragen

27 mei 10:50-11:05 (15 minuten)
met meneer Janssen de definitieve hoofdvraag opgesteld

30 mei 12:00-12:50 (50 minuten)
op school informatie opgezocht en bestudeerd

1 juni 16:30-17:30 (1 uur)
deelvragen + informatie besproken met Mariska

2 juni 21:00-21:30 (30 minuten)
gesprek met Bas Teamleider Landelijke Recherche samen met Mariska tijdens de orkest pauze

6 juni 20:00-22:00 (2 uur)
Lezen over onderwerp

5 juli 15:00-16:30 en 19:00-20:15 (2:45 uur)
het opzoeken van informatie en maken van deelvraag 1 samen met Mariska

12 juli 16:00-18:30 (2:30 uur)
inlezen en werken aan deelvraag 1 met Mariska

15 juli 14:00-16:00 (2 uur)
werken aan deelvraag 1 en 2 samen met Mariska

7 augustus 16:00-18:00 en 20:00-22:00 (4 uur)
Deelvraag typen

18 augustus 20:00-22:00 (2 uur)
Lezen en typen

19 augustus 16:00-18:00 en 19:00-23:00 (6 uur)
Lezen en typen

30 augustus 15:00-17:00 (2 uur)
pws doornemen en aanvullen samen met Isa

1 september 15:50-16:30 (40 minuten)
1e feedback van begeleider Janssen

10 september 16:00-18:00 en 19:00-22:00 (5 uur)
Deelvraag typen en informatie zoeken

15 september 15:00-17:30 (2:30 uur)
werken aan nieuwe deelvraag

16 september 15:00-17:00 (2 uur)
bijwerken van de eerste deelvragen naar meneer Janssen verzonden

19 september 18:00-20:00 (2 uur)
Typen

20 september 18:00-20:00 (2 uur)
Typen

24 september 16:30-18:00 (2:30)
Typen

2 oktober 18:30-22:30 (4 uur)
Lezen en typen

5 oktober 19:00-20:30 (1:30 uur)
Lezen en typen

7 oktober 17:00-18:00 (1 uur)
1e versie van het pws in elkaar zetten

17 oktober 19:00-21:00 (2 uur)
inlezen

23 oktober 19:00-21:00 (2 uur)
Lezen en typen

3 november 20:00-22:00 (2 uur)
Typen

13 november 20:00-22:00 (2 uur)
werken aan de interview en enquête

14 november 11:10-12:00 en 19:00-22:00 (3:50 uur)
op school enquête en interview maken

16 november 12:55-13:08 (13 minuten)
2e feedback van begeleider Janssen

20 november 15:30-20:30 (5 uur)
Pws met Mariska bespreken/overleg

24 november 20:00-22:30 (2:30 uur)
Feedback repareren

4 december 21:00-22:00 (1 uur)
Feedback repareren

10 december 20:00-22:00 (2 uur)
Inlezen

15 december 19:00-23:00 (4 uur)
Repareren + enquête uitwerken

2 januari 9:00-16:00 (7 uur)
interviewen met Remco, Bas en Ingrid in Utrecht en Amsterdam + een soort presentatie gekregen van Bas en een Forensisch-ICT expert met wie we een liquidatie zaak hebben door lopen uit 2013

4 januari 13:00-16:00 (3 uur)
Feedback repareren, en uitwerken

5 januari 12:00-15:00 (3 uur)
Repareren, literatuurlijst

8 januari 18:15-20:00 (1,75 uur)
aan pws werken