JAARGANG 9
EDITIE 1
2022/2023

OVERHEID & IT

E-MAGAZINE

LISA Law & ICT Students' Association

INHOUDSOPGAVE

- 01 Overheid verantwoordelijk voor grootste datalek uit de Nederlandse geschiedenis 4
- 02 Toeslagenaffaire: ‘Ongekend onrecht’ 10
- 03 Interview met dr. Ritsema van Eck 14
- 04 Twitter als politiek instrument 21

NORD Brinkhof

VOORWOORD

Beste lezer,

De nieuwe redactiecommissie heeft de afgelopen tijd hard gewerkt, met als resultaat het eerste E-magazine van dit collegejaar! Ik wil bij deze mijn commissie bedanken voor hun inzet de afgelopen weken en met trots presenteren wij u het E-magazine met de titel 'Overheid&IT'.

De overheid staat niet bepaald bekend om haar brede ICT-kennis. In februari 2021 noemt Arjen Lubach Nederland een digibetocratie. Dat betekent dat Nederland een land is waarvan de economie sterk leunt op digitale technieken en vaardigheden, terwijl het land bestuurd wordt door digibeten.

De afgelopen jaren hebben we dat vaak mis zien gaan. In de coronaperiode is veel gebruik gemaakt van ICT voor testsystemen en om de besmettingen in kaart te brengen. Het is ongelofelijk hoe we door de digitalisering de besmettingen hebben kunnen beperken, maar er is ook veel misgegaan. Hierbij heeft namelijk het grootste datalek in de Nederlandse geschiedenis tot dusverre plaatsgevonden. Daarnaast is het gebrek aan IT-kennis bij de overheid een oorzaak van de Toeslagenaffaire. De Belastingdienst voerde in 2013 een algoritmisch besluitvormingssysteem in voor de opsporing van onjuiste aanvragen en fraude, waardoor er etnisch profileren door algoritmen mogelijk werd. Duizenden ouders die kinderopvangtoeslag ontvingen werden door de Belastingdienst onterecht aangewezen als fraudeur. Ook politiek wordt tegenwoordig via sociale media bedreven en dat komt met belangrijke vragen. Want wat doet bijvoorbeeld Twitter tegen 'fake news' en misleidende politici en moeten we willen dat grote machthebbers bepalen welke politici een podium krijgen? Daarentegen is digitalisering bij de overheid ook zeker positief. Politici staan door het gebruik van sociale media platformen dichter bij de kiezer dan ooit. Al met al een onderwerp waar ontzettend veel over te vertellen valt. Dat belooft dus een interessant E-magazine.

Ik wens u dan ook veel leesplezier en ik hoop dat deze stof u aan het denken zet!

Namens de redactiecommissie,

Anniek Bos
Hoofdredacteur

- **Hoofdredacteur**
  Anniek Bos
- **Redacteur/Secretaris**
  Yong Hui Zhou
- **Redacteur**
  Resa van Westering
- **Redacteur/Vormgever**
  Kirsten Brandsma

NORD Brinkhof

Overheid verantwoordelijk voor grootste datalek uit de Nederlandse geschiedenis

De inzet van technologie door de overheid leidt doorgaans tot het gebruik van persoonsgegevens, daarvoor is de overheid de verwerkingsverantwoordelijke. Recente datalek-affaires onderstrepen dat de overheid nog steeds geen goede cybersecuritysystemen kent. Een relatief recent en vooral erg bekend voorbeeld is het datalek van de GGD. Het gaat daarbij om handel in data uit twee coronasystemen van de GGD: CoronIT, waar de privégegevens van Nederlanders die een coronatest hebben gedaan in staan, en HPZone Lite, het systeem voor het bron- en contactonderzoek. Dit datalek is bijzonder ernstig, omdat er ook medische gegevens in de systemen staan. Verder bestaat de gestolen data uit naam, adres, telefoonnummer, e-mailadres, Burgerservicenummer en nationaliteit. RTL Nieuws meldt op 25 januari 2021 dat privégegevens van miljoenen Nederlanders uit systemen van de GGD illegaal op het internet worden verhandeld. Enkele dagen eerder meldt de journalist Daniël Verlaan dit als eerste bij de GGD, diezelfde dag nog doet de GGD aangifte van computervredebreuk.[1] Het nieuwsbericht van RTL zorgde voor veel onrust onder de Nederlanders. De Autoriteit Persoonsgegevens (hierna: AP) brengt op 27 januari zelfs een persbericht naar buiten dat zij slecht bereikbaar zijn, vanwege de vele telefoontjes van ongeruste mensen.[2]

Mensen zijn meestal verplicht om hun gegevens aan de overheid af te staan. Daarom moet iedereen erop kunnen vertrouwen dat overheidsorganisaties uiterst zorgvuldig met hun gegevens omgaan. Na het nieuwsbericht van RTL daalde gelijk het aantal mensen dat zich liet testen, dit bewijst dat het vertrouwen in de overheidssystemen daalde. Recentelijk is er nog een datalek geweest bij het Kadaster, waardoor geheime woonadressen tijdelijk zichtbaar zijn geweest. Dit datalek is het gevolg geweest van een systeemupdate waarbij de koppeling met de BRP die de afscherming mogelijk maakt "helaas tijdelijk niet juist gelegd" is.[3] Het is dus zeker niet een eenmalig incident.

De vraag luidt of de overheid verantwoordelijkheid draagt voor een datalek in een overheidssysteem. Daarbij zal specifiek worden gekeken naar het GGD-datalek. Dit artikel bespreekt eerst de strafrechtelijke vervolging van GGD-medewerkers. Vervolgens worden de AVG-plichten van overheidsinstanties uiteengezet. Daarna zullen de kansen van de collectieve schadeclaim van Stichting ICAM tegenover de staat besproken worden. Ten slotte bespreekt dit artikel de stappen die de overheid heeft genomen sinds het GGD-datalek om volgende datalekken te voorkomen.

Strafrechtelijke vervolging GGD-medewerkers

Allereerst kijken we naar de personen die letterlijk het datalek hebben veroorzaakt. Zij worden verantwoordelijk gehouden doordat zij strafrechtelijk zijn vervolgd. Een 19-jarige man uit Den Haag heeft persoonsgegevens van de GGD gestolen en verhandeld. Hij maakte in totaal 795 foto's van dossiers in het CoronIT-systeem.[4] Hij heeft gebruik gemaakt van een rechtmatig verkregen wachtwoord met een ander doel dan het uitvoeren van de aan hem toebedeelde werkzaamheden. In andere woorden, de man heeft gebruikt gemaakt van een valse sleutel in de zin van artikel 138a Wetboek van Strafrecht. Het moge duidelijk zijn

1 'Celstraf geëist voor diefstal en verkoop van gegevens van de GGD', om.nl.
2 'AP slecht bereikbaar door vragen datadiefstal GGD', autoriteitpersoonsgegevens.nl.
3 'Kamerbrief over datalek kadaster', open.overheid.nl.
4 'Celstraf geëist voor diefstal en verkoop van gegevens van de GGD', om.nl.

dat dit volledig de schuld is van de werknemer. Voor zijn werk heeft hij een geheimhoudingsverklaring getekend. Daarnaast heeft hij een securitytraining moeten behalen, waarin hij onder meer over de AVG leerde.[1] Hij wist dan ook dat hij strafbaar bezig was en hij is uiteindelijk veroordeeld. De Officier van Justitie in de zaak benadrukte hoezeer de verdachte door zijn handelen inbreuk heeft gemaakt op de privacy van mensen en het vertrouwen in de GGD en de overheid heeft geschaad.[2]

Echter werd het misbruikers wel erg makkelijk gemaakt in HPZone, daarin zat namelijk een downloadknop voor alle gebruikers.[3] Deze knop gaf de mogelijkheid om grote databestanden te exporteren. Ondanks dat dit nog steeds diefstal is, zou men zich kunnen voorstellen dat de overheid hier als verwerkingsverantwoordelijke ook een schuld en verantwoordelijkheid heeft.

AVG-plichten van de overheid

De Algemene verordening gegevensbescherming (hierna: AVG) gaat over het rechtmatig omgaan met persoonsgegevens. Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de wet en mogen alleen verzameld worden met een gerechtvaardigd doel. Belangrijk is dat gegevensverwerking op een passende manier moet worden beveiligd, daarbij gelden voor bijzondere gegevens in de zin van artikel 9 lid 1 AVG, zoals over gezondheid en ras of etnische afkomst, extra strenge regels.

De overheid is een van de grootste verwerkers van persoonsgegevens. De overheid besteedt de verwerking van de persoonsgegevens uit, maar als verwerkingsverantwoordelijke blijft zij wel altijd verantwoordelijk voor de persoonsgegevens die zij verwerkt. Immers, burgers zijn in de veronderstelling dat zij hun gegevens delen met de overheid, niet met de opdrachtnemer. De overheid heeft daarbij ook een voorbeeldfunctie als het gaat om het voldoen aan de wet. Daarom is het in het bijzonder voor overheidsorganisaties belangrijk om uiterst zorgvuldig met persoonsgegevens om te gaan. Sinds de AVG zijn alle overheidsorganisaties verplicht om een functionaris gegevensbescherming aan te stellen.[4] Daarnaast kan een overheidsorganisatie verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Daarmee worden de privacyrisico's van een gegevensverwerking vooraf in kaart gebracht, waardoor preventief maatregelen genomen kunnen worden om de risico's te verkleinen.[5] Een DPIA zou door de overheid in geval van de GGD-systemen in ieder geval moeten worden uitgevoerd, omdat zij op grote schaal bijzondere persoonsgegevens verwerkt. Uit het feitenrelaas inzake gebeurtenissen omtrent het coronatest-IT-systeem blijkt dat de DPIA een van de onderwerpen is die zich op het "kritische pad" bevond. Waar eerst gezegd wordt dat de DPIA 30 oktober klaar moest zijn, zijn er nog steeds vragen over het op tijd vaststellen van de DPIA op 15 december dat jaar.[6]

1 Rb. Midden-Nederland 14 september 2021, ECLI:NLRBMNE:2021:4434, r.o. 7.
2 'Celstraf geëist voor diefstal en verkoop van gegevens van de GGD', om.nl.
3 'Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD', zoek.officielebekendmakingen.nl.
4 'Functionaris gegevensbescherming (FG)', autoriteitpersoonsgegevens.nl.
5 'Data protection impact assessment (DPIA)', autoriteitpersoonsgegevens.nl.
6 'Feitenrelaas inzake gebeurtenissen omtrent coronatest-IT-systeem van de GGD', zoek.officielebekendmakingen.nl.

Daarnaast heeft de organisatie een verantwoordingsplicht om aan te tonen dat zij aan de privacyregels voldoet.[1] Voorbeelden zijn dat aangetoond moet worden dat een verwerking voldoet aan rechtmatigheid, transparantie, doelbinding en juistheid. Ook moet de verwerkingsverantwoordelijke kunnen laten zien dat zij de juiste technische en organisatorische maatregelen heeft genomen om de persoonsgegevens te beveiligen. Na het RTL bericht van januari 2021 intensiveerde de AP het toezicht op de GGD en startte zij een onderzoek. In november 2021 rondde de AP het onderzoek af en daaruit bleek dat nog steeds wezenlijke risico's bestonden voor de bescherming van persoonsgegevens bij testen, vaccineren en het bron- en contactonderzoek tijdens de coronapandemie.[2] Dit betekent dat de overheid op dat moment niet voldeed aan de eis dat gegevensverwerking op een passende manier wordt beveiligd op grond van artikelen 25 en 32 AVG. De overheid lijkt niet in staat snel genoeg adequaat maatregelen te kunnen nemen bij datalekken van deze schaal. Daarom waren veel Nederlanders bezorgd. Stichting ICAM komt voor de gedupeerden op en start een collectieve actie tegen het Ministerie van Volksgezondheid, Welzijn en Sport (hierna: Ministerie van VWS).

Collectieve schadeclaim Stichting ICAM

Afgelopen mei 2022 boden de GGD'en ongeveer 1250 mensen van wie de gegevens uit de computersystemen zijn gestolen een schadevergoeding van 500 euro.[3] Zowel volgens RTL Nieuws als volgens Stichting Initiatieven Collectieve Acties Massaschade (hierna: ICAM) ligt het aantal gedupeerden veel hoger.

Stichting ICAM is een onafhankelijke organisatie die met collectieve acties opkomt voor personen die schade lijden door toedoen van grote organisaties.[4] De stichting stelt het Ministerie van VWS verantwoordelijk voor de IT-systemen van de GGD. Daarmee willen zij dat het Ministerie verantwoordelijkheid neemt voor het grootste datalek uit de Nederlandse geschiedenis in de vorm van schadevergoeding aan de gedupeerden. Met de collectieve actie hopen zij op zijn minst de overheid te dwingen zorgvuldiger om te gaan met persoonsgegevens en privacy van burgers. De stichting eist 500 euro voor iedereen waarvan persoonsgegevens toegankelijk zijn geweest en mogelijk zijn gestolen. Voor iedereen waarvan werkelijk blijkt dat de gegevens gestolen zijn, wordt 1500 euro per persoon geëist. Erg kansrijk acht ik de eerste helft van de claim niet nu de privéinformatie van ruim 6,5 miljoen Nederlanders in de systemen stond. Voor iedereen waarvan werkelijk bewezen kan worden dat hun persoonsgegevens gestolen zijn moet een schadevergoeding reëel zijn met het oog op de door de GGD geboden 500 euro aan 1250 mensen. Wellicht zal 1500 euro niet slagen, maar ik acht een schadevergoeding wel realistisch. Daarbij is het positief dat de GGD'en al schadevergoeding hebben geboden, daarmee laten zij naar mijn mening zien dat zij zichzelf als verantwoordelijke zien.

Wat heeft de Nederlandse overheid geleerd?

Minister de Jonge en het Ministerie van VWS grepen snel in met kortetermijnacties bij het GGD-lek. Het gebruik van HPZone werd gelijk beperkt tot een selecte groep in infectiebestrijding en de exportfunctie van HPZone werd snel uitgeschakeld.[5] Er is echter weinig te vinden over de acties van overheidsorganisaties op de lange termijn. De AP heeft in november 2021 een onderzoek gedaan naar de beleving van de

1 'Verantwoordingsplicht', autoriteitpersoonsgegevens.nl.
2 'GGD moet persoonsgegevens beter beschermen', autoriteitpersoonsgegevens.nl.
3 'GGD biedt 1250 gedupeerden datadiefstal schadevergoeding van 500 euro', rtlnieuws.nl.
4 datalek-ggd.nl.
5 'Kamerbrief inzake de stand van zaken datalek GGD', open.overheid.nl.

privacywetgeving bij de GGD. De AP ziet verbeteringen, maar ook nog veel verbeterpunten. Daarbij noemt de AP dat een groot aantal partijen betrokken is bij de verwerking van persoonsgegevens waardoor het lastiger is om een verantwoordelijke aan te wijzen die maatregelen moet treffen. Men mag verwachten dat heel Nederland geschrokken is van dit gigantische datalek en daarvan heeft geleerd. Echter, we hebben kunnen zien dat na het GGD-datalek nog vele datalekken volgden. Gelijk in maart 2021 lekte de Zwijndrechtse gemeente data.[1] Een recenter voorbeeld is het datalek bij het Kadaster, waardoor geheime adressen van 18 september tot 11 oktober 2022 zichtbaar zijn geweest.[2] Begin december heeft RTL Nieuws ook een datalek bij Forum voor Democratie aan het licht gebracht. De privégegevens van 92.901 leden en oud-leden zijn gelekt als gevolg van een lek in de koppeling tussen de website van de FVD en de ForumApp. Het gaat hier om bijzondere persoonsgegevens in de zin van artikel 9 AVG, want het gaat hier om politieke opvattingen. Zelfs de partijleider, Baudet, zijn privémail, telefoonnummer, adres en IBAN staan in het lek.[3]

Geconcludeerd kan worden dat de overheid een zekere verantwoordelijkheid heeft voor de beveiliging van IT-systemen die zij gebruikt. Allereerst is de overheid verantwoordelijk voor de beveiliging van de systemen, zodat het niet te gemakkelijk is voor criminelen om data te lekken. Zoals je ziet in het voorbeeld van de 19-jarige jongen uit Den Haag was het lekken van data erg laagdrempelig. Daarnaast is de overheid als verwerkingsverantwoordelijke in de zin van de AVG verantwoordelijk bij het verwerken van persoonsgegevens. De overheid wordt nu ook daadwerkelijk verantwoordelijk gehouden door Stichting ICAM. Ik ben erg benieuwd naar de uitspraak in de tweede rechtszaak die de Stichting afgelopen december aanspande, waarin zij een beroep doet op de Wet Open Overheid om meer informatie over het datalek boven tafel te krijgen. Uiteindelijk zijn dit soort datalekken een ernstige inbreuk op het recht op privacy van de burgers dat beschermd wordt door artikel 10 van de Grondwet, dus de overheid moet verantwoordelijk gehouden kunnen worden voor het schenden van dit recht.

Namens de redactiecommissie,

Anniek Bos

1 'Excuses gemeente: Zwijndrechtse wethouder en ambtenaar lekten data', ad.nl.
2 'Kamerbrief over datalek kadaster', open.overheid.nl.
3 'Nieuwe app Forum lek: privégegevens alle 92.000 (oud-)leden op straat', rtlnieuws.nl.


Stibbe
Connect to grow.
STBB2N
8 t/m 13 maart 2023
MELD JE UITERLIJK 18 JANUARI 2023 A
STUDENT.WERKENBIJSTIBBE.NL

STBB2NY 2023

Ben jij een ondernemende student Nederlands, Fiscaal of Notarieel recht en ben jij klaar voor een unieke ervaring? Wil jij in vijf dagen tijd ondergedompeld worden in de wereld van de internationale rechtspraktijk en kan jij niet wachten om erachter te komen hoe het is om bij Stibbe te werken? Ben jij minimaal derdejaars student en klaar voor een uitdaging?
Meld je dan aan voor STBB2NY 2023!

Houd alvast de volgende data vrij in je agenda:
- aanmelden kan t/m woensdag 18 januari;
- in de week van 23 januari hoor je of je bent geselecteerd voor een selectiegesprek en assessment, die plaatsvinden in de week van 6 februari;
- op woensdag 1 maart vindt de kick-off dag plaats op ons kantoor in Amsterdam;
- op dinsdag 21 maart organiseren wij een feestelijk Reüniediner in Amsterdam.
Wil je ervaren of jij de klik hebt met Stibbe? Register now!

AANMELDEN

Aanmelden kan door jouw CV, officiële cijferlijst(en) van de universiteit en eventuele stagebeoordelingen te uploaden in PDF-format. In plaats van een reguliere motivatiebrief, ontvangen wij daarnaast graag de antwoorden op onderstaande genummerde vragen:

1. Waarom solliciteer jij voor STBB2NY?
2. Heb jij al eerder kennisgemaakt met Stibbe? Zo ja: waar en wanneer was dit, en wat was naar aanleiding daarvan jouw indruk van Stibbe als kantoor?
3. Wanneer verwacht jij je bachelor/master af te ronden?
4. Naar welke praktijkgroep(en) gaat jouw voorkeur uit op dit moment en waarom?
5. Wat zullen we jou nooit zien doen?
6. Overige opmerkingen waarvan jij denkt dat het goed is dat wij dit weten.

Dit document kan je vervolgens (wederom in PDF-format) uploaden onder de button ‘motivatiebrief’.

Vanzelfsprekend vindt de masterclass plaats volgens de op dat moment geldende maatregelen.

Past STBB2NY helaas niet in jouw studieschema, maar wil je wel graag op een andere manier kennismaken met Stibbe? Kom dan naar één van onze aankomende events, zoals Stibbe Talks of onze praktijkdagen. Check het overzicht van onze eerstvolgende evenementen op www.student.werken-bijstibbe.nl/events

Toeslagenaffaire: 'ongekend onrecht'

De Autoriteit Persoonsgegevens (hierna: AP) legt de Belastingdienst een boete op van €3,7 miljoen, de hoogste boete die de AP ooit oplegde. AP-voorzitter Aleid Wolfsen: 'De Belastingdienst heeft levens overhoop gehaald.'[1] Een headline van de krant Trouw: "Gedupeerde ouders: 'We zijn moe, kwaad en uitgeput'".[2] 'De overheid speelt balletje-balletje met gegevens van burgers', aldus AP-voorzitter Aleid Wolfsen tijdens de presentatie van het onderzoek naar de Belastingdienst.[3] Het is niemand in Nederland ontgaan, de Toeslagenaffaire. Jarenlang, van 2004 tot 2019, werden duizenden ouders die kinderopvangtoeslag ontvingen door de Belastingdienst onterecht aangewezen als fraudeur. Deze ouders moesten het ontvangen bedrag aan toeslagen, dat wel op kon lopen tot tienduizenden euro's, vaak in één keer terugbetalen. Zij belandden hierdoor in de schulden met alle gevolgen van dien.[4] Naast financiële schade leden ouders ook aan psychische problemen. Zo vertelt Tamara, een gedupeerde ouder, dat zij zich schaamde en depressieve periodes had.[5] De vraag rijst hoe dit heeft kunnen gebeuren. Eerst wordt in dit artikel achtergrondinformatie gegeven over de harde aanpak bij fraudebestrijding. Vervolgens wordt in dit artikel gekeken of sprake was van etnische profilering bij de Belastingdienst. Daarna komt het onrechtmatig verwerken van persoonsgegevens door de Belastingdienst aan de orde.

Bulgarenfraude

Het begon allemaal met de Bulgarenfraude: Bulgaren schrijven zich bij de gemeente in als inwoner, openen een bankrekening en ontvangen tienduizenden euro's aan Nederlandse toeslagen.[6] Op gegeven moment blijkt dat zelfs dode Polen toeslagen ontvingen.[7] De Tweede Kamer eist meer antifraudemaatregelen, dus toenmalig staatssecretaris Weekers kondigt aan dat de Belastingdienst voortaan met 'risicoprofielen' zal werken. Daarbij zegt hij wel meteen dat 'de goeden onder de kwaden zullen lijden'.[8] Later zal blijken dat dit ook het geval is. De nadruk lag toentertijd dus erg op fraudebestrijding; 'alles op alles' moest worden gezet om misbruik te stoppen. De strengere handhaving kwam er met de Wet aanpak fraude toeslagen en fiscaliteit. De Tweede Kamer lijkt echter over het hoofd te hebben gezien dat de bestaande wet al heel streng was. . Al jaren voor de Bulgarenfraude ondervonden ouders ellende van die wet en al jaren voor de Bulgarenfraude werd gewaarschuwd voor verstrekkende consequenties.[9]

1 'Boete Belastingdienst voor zwarte lijst FSV', autoriteitpersoonsgegevens.nl, 12 april 2022.
2 J. Kleinnijenhuis, 'Gedupeerde ouders toeslagenaffaire luiden noodklok in open brief: 'We zijn moe, kwaad en uitgeput'', trouw.nl, 6 mei 2022.
3 J. Kleinnijenhuis, "De overheid speelt balletje-balletje met gegevens van burgers", trouw.nl, 29 oktober 2021.
4 J. Kleinnijenhuis en C. Verlouw, 'De toeslagenaffaire uitgelegd: zo kwam het 'ongekende onrecht' tot stand', trouw.nl, 31 mei 2022.
5 W. Hilhorst, 'Depressief en bang door toeslagenaffaire: 'Ik sloot me af van de buitenwereld'', commen.nl.
6 J. Frederik, 'Zo hadden we het niet bedoeld: de tragedie achter de toeslagenaffaire', decorrespondent.nl.
7 'Dode Polen kregen toeslagen', rtlnieuws.nl, 12 juli 2013.
8 Handelingen II 2012/13, nr. 81, item 13, p. 81-86.
9 J. Frederik, 'Zo hadden we het niet bedoeld: de tragedie achter de toeslagenaffaire', decorrespondent.nl.

Geen hardheidsclausule: 'alles of niets'

In artikel 1.8 lid 2 Wet kinderopvang staat dat ouders een eigen bijdrage moeten betalen. Artikel 26 lid 1 Algemene wet inkomensafhankelijke regelingen bepaalt dat indien een herziening van een tegemoetkoming of een herziening van een voorschot leidt tot een terug te vorderen bedrag dan wel een verrekening van een voorschot met een tegemoetkoming daartoe leidt, de belanghebbende het bedrag van de terugvordering in zijn geheel is verschuldigd.[1] Oftewel, als een ouder een paar honderd euro aan eigen bijdrage is vergeten te betalen, moet het gehele jaar aan kinderopvangtoeslag van ruim €10.000 worden terugbetaald. Niet alleen het niet betalen van de eigen bijdrage leidt tot enorme terugvordering, maar ook kleine fouten kunnen aanleiding zijn om het gehele bedrag terug te vorderen. Dit kan dus grote gevolgen hebben voor gezinnen en dan vooral voor armere ouders, omdat zij de meeste kinderopvangtoeslag ontvangen. In tegenstelling tot de meeste socialezekerheidswetten is in de toeslagen wetgeving geen 'algemene hardheidsclausule' opgenomen. Op grond van zo'n clausule kan een bepaling geheel of gedeeltelijk buiten toepassing worden gelaten als de toepassing ervan zou leiden tot onbillijke gevolgen.[2]

Etnische profilering door algoritmen

Overheidsinstanties wereldwijd maken steeds vaker gebruik van algoritmen om risico's in te schatten. Vaak gebeurt dit in de trant van fraudebestrijding, waaronder bij de Belastingdienst. In 2013 voerde de Belastingdienst een algoritmisch besluitvormingssysteem in voor de opsporing van onjuiste aanvragen en fraude: het 'risico-classificatiemodel'.[3] Op 25 oktober 2021 brachten Nederlandse Amnesty-onderzoekers het rapport 'Xenofobe machines – Discriminatie door ongereguleerd gebruik van algoritmen in het Nederlandse toeslagenschandaal' uit, waarin etnisch profileren door middel van het risico-classificatiemodel centraal staat. Uit het rapport blijkt dat de Belastingdienst informatie met betrekking tot de nationaliteit van de aanvrager als een risicofactor gebruikte in het algoritmische systeem. Volgens Amnesty onthult het gebruik van de nationaliteit in het risico-classificatiemodel de veronderstelling van de ontwerper, ontwikkelaar en/of gebruiker van het systeem dat mensen van bepaalde nationaliteiten meer geneigd zouden zijn fraude te plegen dan mensen van andere nationaliteiten. Ook is het volgens Amnesty een aanwijzing dat de Belastingdienst meende dat een verband bestaat tussen etniciteit en criminaliteit.[4] Amnesty International komt hier tot harde conclusies.

Ook de AP is een onderzoek begonnen naar 'de verwerking van de tweede nationaliteit'. Jarenlang stond de dubbele nationaliteit van burgers in de Gemeentelijke Basisadministratie (hierna: GBA) vermeld. Vanaf 6 januari 2014 is de GBA in de Basisregistratie Personen (hierna: BRP) overgegaan, waarin de dubbele nationaliteit niet meer mag worden opgenomen. De AP constateerde dat de gegevens van de oude GBA nog in de systemen van de Belastingdienst stonden, onder andere vanwege de ICT-problemen bij de Belastingdienst. In 2020 staan de gegevens nog steeds gedeeltelijk in de systemen, terwijl deze volgens de wet verwijderd moeten worden.[5]

---

1 Sinds 1 januari 2021 is deze bepaling gewijzigd: lid 2 is toegevoegd waarin staat dat de Belastingdienst in bepaalde gevallen een lager bedrag kan terugvorderen (Stb. 2020, 543).

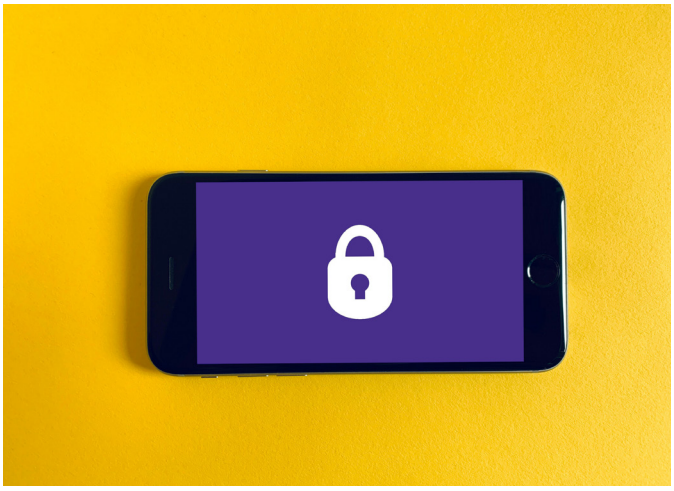
2 J. Frederik, 'Zo hadden we het niet bedoeld: de tragedie achter de toeslagenaffaire', decorrespondent.nl.

3 Onderzoeksrapport van de Autoriteit Persoonsgegevens inzake de Belastingdienst/Toeslagen: De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, bijlage bij Kamerstukken II 2019/20, 31066, nr. 683.

4 Xenofobe machines – Discriminatie door ongereguleerd gebruik van algoritmen in het Nederlandse toeslagenschandaal (Amnesty International), 25 oktober 2021.

5 Onderzoeksrapport van de Autoriteit Persoonsgegevens inzake de Belastingdienst/Toeslagen: De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, bijlage bij Kamerstukken II 2019/20, 31066, nr. 683.

De vraag luidt of de gegevens over de dubbele nationaliteit niet alleen beschikbaar waren, maar of er ook op werd geselecteerd. AP-voorzitter Aleid Wolfsen beweert van wel: 'De tweede nationaliteit werd gebruikt voor het bouwen van risicotaxatie-instrument: wie gaan we extra controleren en wie niet?'[1] In het rapport van de AP staat echter het tegenovergestelde: een eventuele dubbele nationaliteit werd niet gebruikt als indicator in het risico-classificatiemodel. Nederlanderschap/niet-Nederlanderschap was een indicator in het risico-classificatiemodel en de nationaliteit van aanvragers is alleen gebruikt om te bepalen of sprake is van wel of geen Nederlanderschap. Toch concludeert de AP dat het gebruik van de nationaliteit van aanvragers voor de indicator Nederlanderschap/niet-Nederlanderschap in het risico-classificatiemodel is aan te merken als een discriminerende verwerking en daarmee onbehoorlijk is in de zin van art. 5 lid 1 sub a Algemene verordening gegevensbescherming (hierna: AVG). Het niet hebben van de Nederlandse nationaliteit droeg bij aan de uiteindelijke risicoscore, wat in combinatie met scores op andere indicatoren kon leiden tot een hoge risicoscore. Het onderscheid tussen het wel of niet bezitten van de Nederlandse nationaliteit heeft geleid tot nadeel in de behandeling voor aanvragers zonder de Nederlandse nationaliteit. Het onderscheid dat werd gemaakt is niet redelijk en objectief gerechtvaardigd.[2] De AP legt de Belastingdienst uiteindelijk een boete op van €2,75 miljoen vanwege het op onrechtmatige, discriminerende en daarmee onbehoorlijke wijze verwerken van de (dubbele) nationaliteit van aanvragers van kinderopvangtoeslag.[3] De AP concludeert dat het opvragen van de nationaliteit van aanvragers geen daadwerkelijke betekenis heeft gehad.[4] Het is dus onduidelijk waarom de gegevens überhaupt werden opgevraagd. De AP doet geen uitspraak over de gevolgen van het opvragen van die gegevens en vindt geen aanwijzingen dat de beschikbaarheid van de gegevens bij de Belastingdienst daadwerkelijk tot een selectie op (tweede) nationaliteit heeft geleid. Dit is dan ook niet gek; racisme wordt niet snel op papier vastgelegd. Wat zich in de hoofden van de ambtenaren heeft afgespeeld, is niet achter te komen. Hoe dan ook is het onacceptabel dat de tweede nationaliteit nog zichtbaar was in de systemen.[5]



Gegevensbescherming

Naast het overtreden van het discriminatieverbod heeft de Belastingdienst ook op onrechtmatige wijze persoonsgegevens verwerkt door niet de gegevens van de dubbele nationaliteit te verwijderen. Bovendien heeft de Belastingdienst jarenlang de Fraude Signalering Voorziening (FSV) gebruikt, een zwarte lijst waarop signalen van fraude werden bijgehouden. De Belastingdienst had nooit persoonsgegevens mogen verwerken in de FSV; uit een onderzoek van de AP blijkt dat veel van de kernbeginselen van de AVG op ernstige wijze werden geschonden. De belangrijkste overtreding is dat geen wettelijke grondslag bestond voor FSV en zonder grondslag is het verwerken van persoonsgegevens verboden.

1 'Werkwijze Belastingdienst 'discriminerend en onrechtmatig'', nporadio1.nl, 17 juli 2020.

2 Onderzoeksrapport van de Autoriteit Persoonsgegevens inzake de Belastingdienst/Toeslagen: De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, bijlage bij Kamerstukken II 2019/20, 31066, nr. 683.

3 'Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze', autoriteitpersoonsgegevens.nl, 7 december 2021.

4 Onderzoeksrapport van de Autoriteit Persoonsgegevens inzake de Belastingdienst/Toeslagen: De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, bijlage bij Kamerstukken II 2019/20, 31066, nr. 683.

5 J. Frederik, 'Zo hadden we het niet bedoeld: de tragedie achter de toeslagenaffaire', decorrespondent.nl.

Andere overtredingen waren onder andere dat de signalen van fraude te lang in FSV werden bewaard en dat de gegevens in bepaalde gevallen onjuist en niet actueel waren. Soms kreeg een persoon het label 'fraudeur' zonder dat dit volgde uit gedegen onderzoek. En zelfs nadat bleek dat de informatie niet actueel was of dat geen sprake was van fraude, werd dit vaak niet in FSV genoteerd, waardoor mensen onterecht als vermeend fraudeur in het systeem bleven staan.[1] In april 2022 heeft de AP de Belastingdienst naar aanleiding hiervan een boete opgelegd van €3,7 miljoen, de hoogste boete die de AP ooit oplegde.[2]

Al met al kan geconcludeerd worden dat de Belastingdienst er nogal een potje van heeft gemaakt. De manier waarop persoonsgegevens werden verwerkt, was discriminerend en onrechtmatig. Dit had grote gevolgen voor burgers; mensen werden vaak onterecht als fraudeur bestempeld, waardoor sommigen geen betalingsregeling kregen of niet in aanmerking kwamen voor schuldsanering. AP-voorzitter Wolfsen concludeert: 'De Belastingdienst is meerdere keren in de fout gegaan. Terwijl juist de Belastingdienst een zeer grote verantwoordelijkheid heeft tegenover de mensen in Nederland. (…) Mensen moeten erop kunnen vertrouwen dat de Belastingdienst zorgvuldig met hun gegevens omgaat.'[3] Naast het feit dat de Belastingdienst een grote rol had in de Toeslagenaffaire moet ook niet vergeten worden wat de rol van de wetgever hierin was. Deze heeft willens en wetens een onevenredig harde regel gemaakt. Nog even een lichtpuntje in dit artikel: de gedupeerde ouders hebben recht op compensatie. Al kan aan die compensatieregeling ook een geheel artikel gewijd worden, want nu blijkt dat de helft van de mensen die zich melden als 'toeslagenouders' geen gedupeerde blijkt te zijn van het toeslagenschandaal. Leert de overheid dan nooit? Nederland zal in ieder geval niet in de nabije toekomst afkomen van de problemen rondom de Toeslagenaffaire.

Namens de redactiecommissie,

Resa van Westering

1 Onderzoeksrapport van de Autoriteit Persoonsgegevens inzake de Belastingdienst: Verwerkingen van persoonsgegevens in de Fraude Signalering Voorziening (FSV), bijlage bij Kamerstukken II 2021/22, 31066, nr. 911.
2 'Boete Belastingdienst voor zwarte lijst FSV', autoriteitpersoonsgegevens.nl, 12 april 2022.
3 'Helft melders is volgens overheid toch geen gedupeerde in toeslagenschandaal', rtlnieuws.nl, 21 oktober 2022.

Interview met dr. Ritsema van Eck

Kunt u misschien wat over uzelf vertellen en over hoe u terecht bent gekomen bij de universiteit?
Ik ben bij de universiteit terechtgekomen als student want ik heb hier ook gewoon gestudeerd. Ik heb internationale betrekkingen gestudeerd, geen rechten, en daarna een master Europese cultuurgeschiedenis. Ik ben wel indertijd student-assistent geweest bij rechten, bij Europees recht. En dus via Europees recht een beetje het privacyrecht ingerold. Toen ik was afgestudeerd, was er een vacature voor onderzoeksassistent. Ik ben onderzoeksassistent geworden en toen ben ik gepromoveerd. Als je internationale betrekkingen studeert, heb je ook een aantal rechtenvakken; Europees en internationaal recht. Dat vond ik wel de leukste vakken in de studie. Achteraf gezien was het dus heel logisch.

Waarom ging u in Groningen studeren?
Het was de enige plek waar je internationale betrekkingen kon studeren. Dus het was eigenlijk meer een keuze voor de studie dan voor de stad. Ik heb een jaar gestudeerd in Middelburg bij de Roosevelt Academy. Dat is een dependant van de Universiteit van Utrecht, de campus Fryslân van Utrecht. Ik heb ook een half jaar in Duitsland gestudeerd. In Göttingen, dat ligt een uurtje met de trein onder Hannover. Tegenwoordig heet de studie Euroculture, dus een soort Europese cultuurstudies.

U dacht niet 'ik wil Europarlementariër worden'?
Oh nee, alsjeblieft niet. Nee, de bubbel in Brussel is heel interessant van buitenaf maar ik ben als onderzoeksassistent best vaak in Brussel geweest. Het zijn een heleboel grijze gebouwen en een heleboel mensen die zich met hele specifieke dingen bezighouden. Ik ben heel blij dat ze het doen hoor, dat er mensen zijn die zich bezighouden met importtarieven op suikerbieten. Ja, fijn dat iemand het doet, ik hoef het niet zelf te zijn. Zet mij maar in een collegezaal, dat vind ik veel leuker.

Wat vindt u daar dan leuk aan, college geven?
Waarom doe ik het? Omdat het leuk is. Voor een groep staan en een beetje proberen om het leerproces aan te jagen. Je bent geen basisschooldocent die de informatie aanreikt, maar je probeert een beetje te enthousiasmeren en extra context te geven zodat het wat beter landt. Je hoopt dan dat studenten dat zelf kunnen gebruiken om er iets moois van te maken. Het is soms lastig, maar dat maakt het ook uitdagend. Ik kan er niet zomaar een beetje gaan staan en dan gaat het wel. Het lesgeven ziet er soms wel wat geïmproviseerd uit, maar daar zitten uren voorbereiding in. Je moet altijd de best voorbereide student van de groep zijn. Als jij het college het best van iedereen hebt voorbereid, dan zit je goed. En dan scheelt het wel dat je natuurlijk het vak vaak meerdere jaren geeft.

Heeft u ook online lesgegeven en hoe vond u dat?
Afschuwelijk. Als docent is online onderwijs echt heel zwaar. Ik weet dat het voor studenten ook niks is, maar ook voor de docent niet. Je krijgt veel minder reactie, dus je kan veel minder makkelijk zien van 'oh volgens mij heb ik hier genoeg van uitgelegd, want iedereen lijkt het te begrijpen.' Of: 'Ik moet toch even door want er kijken wel veel studenten moeilijk naar hun aantekeningen'. Het zijn van die dingen die je moet aanvoelen in een groep en dat gaat online niet. In een lokaal heb je een bepaalde sfeer in de groep, er is een spanning of ontspanning en daar kan je op inspelen. Dat mis je online.

Dan nu wat meer inhoudelijk over het onderwerp van dit e-magazine 'Overheid en IT'. In hoeverre gebruikt de overheid surveillance?
Er zijn heel veel overheidsorganisaties die surveillance toepassen. Surveillance, als heel breed begrip, is het toezicht houden op mensen met als doel hun gedrag te beïnvloeden. En dan heb je het dus echt over heel simpele dingen als camera's ophangen door bijvoorbeeld de politie. Maar je hebt het ook over bijvoorbeeld het bijhouden van basisregistratie personen. Kijken of dat wel klopt en dat checken met andere bronnen. Dat is ook een vorm van surveillance. Alles wat de overheid doet, daar heb je surveillance bij nodig om te kijken of het wel klopt, of het wel werkt. Ook dingen als onderzoek doen naar hoe goed het gaat met de onderwijskwaliteit in Nederland is een vorm van surveillance. Surveillance is een breed begrip en bijna alles wat de overheid doet, heeft er wel mee te maken. De overheid moet dingen weten om te kunnen functioneren.

Kijken naar gedrag en hoe je daarop reageert?
Ja, bijvoorbeeld de DUO: als je je lening moet terugbetalen, moet DUO ook weten hoeveel inkomsten je hebt en op basis daarvan moet je meer of minder terugbetalen. Dat is ook een vorm van surveillance. Dat is maar een heel klein deeltje van je leven dat gesurveilleerd wordt door een specifieke overheidsorganisatie. En de meeste surveillance zit echt op dat niveau: één organisatie die een specifiek dingetje moet weten over jou om te kunnen functioneren. Daar zit helemaal geen Big Brother-achtig idee achter, maar we hebben nou eenmaal veel regeltjes en dingetjes. Dan heb je informatie nodig om dat uit te kunnen voeren en dat is allemaal surveillance. Dat is allemaal informatie over menselijk gedrag waarmee je dan iets kan doen en iemands gedrag kan sturen daarop. De universiteit die in de gaten houdt of je je vakken wel haalt, is ook een vorm van surveillance.

"Het is een oplossing op zoek naar een probleem"

De RUG wil een grote data-analyse doen om de kwaliteit van het onderwijs te verbeteren. Op Brightspace kun je veel informatie zien van studenten: wanneer we hebben ingelogd en hoelang we op een onderwerp zijn blijven hangen. Wat vindt u daarvan?
Ik heb ervan gehoord, maar ik weet er het fijne niet van. Meer in zijn algemeen ben ik wel bekend met learning analytics: dan kan je kijken naar welke student kijkt hoelang naar wat etc. Dat kan je dan vervolgens correleren aan tentamenuitslagen bijvoorbeeld. Ik zie zelf niet helemaal in waarom het nodig is. Ik denk dan: je surveilleert het tentamen en dan lijkt het mij aan de studenten zelf hoe je je voorbereidt op het tentamen. En wat hebben we er met z'n allen aan wie wanneer waar op klikt. Je maakt een hele grote datastroom over wat iedereen aan het doen is. Dan ga je in de pot zitten roeren en hopen dat daar een correlatie uitkomt. Het is een oplossing op zoek naar een probleem. Al die data is er en daar kun je in principe in zitten roeren. Daar zullen dan ongetwijfeld correlaties uit komen. Ja, en dan? Ga je dan tegen studenten zeggen 'jullie moeten vaker op Brightspace klikken want studenten die gemiddeld vaker op Brightspace klikken die halen hogere cijfers'. Die correlatie kan ik je nu al geven, dat zal ongetwijfeld zo zijn. Studenten die actiever met hun studie bezig zijn, halen hogere cijfers dan studenten die dat niet zijn, wat een verrassing jongens. Je genereert heel veel data maar die data heeft niet per se een hele hoge informatiedichtheid. Je moet veel moeite doen om van informatie data te maken. Dat ga je dan proberen te doen door algoritmen en correlaties zoeken, maar als je lang genoeg zoekt, dan vind je altijd wel iets.

Hoeveel een student op Brightspace zit, is toch niet privacygevoelig?
Hoeveel maakt het inderdaad uit dat je van een specifiek ding iets weet? Eigenlijk niet zo heel veel. Maar een beetje hetzelfde als met de overheid: er zijn een heleboel overheidsorganisaties die een klein dingetje weten. Het wordt problematisch op het moment dat je alle dingen gaat samenvoegen. En dan weet je ineens heel veel over iemand. Dat wordt in de literatuur, prachtige term, 'turnkey totalitarianism' genoemd. 'Turnkey' is een term uit de technologiewereld. Als je een product turnkey oplevert, is het compleet klaar voor gebruik. En dan geef je op een gegeven moment de sleutel aan de koper, en die kan dan het serverpark binnenlopen en dan werkt alles. De gedachte achter turnkey totalitarianism is als je alles gaat opslaan, weet je nooit wat voor regering er straks komt, of wie die data allemaal krijgt. Die kunnen er ook van alles mee gaan doen. Als zij de sleutel van je afpakken, dan heb je een probleem. Een goed voorbeeld is de machtsovername van de Taliban in Afghanistan na het vertrek van de Amerikanen. Amerikanen gebruikten gezichtsherkenningstechnologie om lokale medewerkers te kunnen identificeren, een soort eigen toegangscontrole. Toen nam de Taliban het over, die apparaatjes, en liepen ermee over straat: 'hallo wie heeft hier allemaal voor de Amerikanen gewerkt?'. Want dat apparaat weet niet wie aan de knoppen zit, dus dan kan je nog steeds mensen makkelijk herkennen. Als je dat soort technologieën gebruikt, wees dan bewust dat iemand dat kan overnemen en voor iets kan gebruiken wat jij niet bedacht hebt. Je kan nooit helemaal voorkomen dat het in de verkeerde handen terechtkomt. Dan denk ik: doe het maar niet, dan kan het ook niet fout gaan. Als je er niks aan hebt, waarom zou je het dan doen? Dan ben je een risico aan het creëren om niks.

Wat kunnen criminelen met onze data van Brightspace?
Je cijfers publiceren bijvoorbeeld. Ze weten dat je een student rechten bent hier in Groningen, dat is op zich niet heel interessant. Maar er zijn genoeg revoluties in de geschiedenis geweest waarbij universiteiten en studenten het zwaar hebben moeten ontgelden. Denk aan de culturele revolutie in China waar het feit dat je studeerde aan de universiteit je een klassenvijand maakte. Dan kon je dus in de cel belanden, puur omdat je aan de universiteit studeerde. Als je dat in je achterhoofd houdt: hoeveel sporen op het internet wil je hebben dat je op de universiteit studeert? En dan blijkt uit je Brightspace dat je een hele actieve student was. Dan hang je, misschien letterlijk. Het is onschuldige data, totdat er iets raars gebeurt, en dan is het geen onschuldige data.

Zo ver als China is Nederland nog niet toch?
Nee dat zeker niet, het is nog niet zo ver in Nederland. Maar het feit dat het nu zo is, wil niet zeggen dat het altijd zo blijft. Er zijn genoeg voorbeelden van landen waar het fout is gegaan. Je weet nooit wanneer iets afglijdt. Misschien een pessimistisch wereldbeeld maar je moet altijd voorbereid zijn op de val van de democratische rechtsstaat. Dat zit er wel voor een deel achter.

"Je moet altijd voorbereid zijn op de val van de democratische rechtsstaat."

Vaak hoor je dat ze in China op straat allemaal camera's hebben waar ze je mee filmen. Is dat in Nederland ook zo, dat je best vaak wordt gefilmd zonder dat je het weet?
Je wordt in Nederland best vaak gefilmd, als je een beetje oplet heb je het vaak wel door. Op straat valt het wel mee met de beveiligingscamera's, tenminste in Groningen. Het verschilt per stad, want camera's ophangen in de openbare ruimte mag de burgemeester alleen. In Groningen zijn het er ook een stuk of vijftien of twintig, uit mijn hoofd. In Rotterdam hangen er bijvoorbeeld honderden. In zijn algemeenheid is dat nog steeds wel beperkt. Als je in winkels of op een treinstation komt, dus semipublieke ruimtes, zijn het er heel veel. Er zijn daar weinig plekken waar je niet gefilmd wordt.

Maakt dat dan inbreuk op je privacy of ga je eigenlijk automatisch akkoord met het feit dat je wordt gefilmd wanneer je je begeeft in een winkel of op een treinstation bijvoorbeeld?
Ja, je bent dan in principe in de ruimte van iemand anders, dus je moet je dan gedragen naar de regels die de ander maakt. En dat mag ook allemaal, maar het hangt ervan af wat iemand vervolgens doet met die opname. De overgrote meerderheid doet niks met die opnames. Pas als er iets gebeurt, gaat men het terugkijken. Maar als jij 20 camera's hebt hangen die 24/7 aanstaan, de hoeveelheid data die dat maakt is niet bij te houden. Dat zijn eindeloze gigabytes aan data, dus je moet het meestal wel verwijderen anders staat de harde schijf vol. Meestal wordt het voor een bepaalde termijn opgeslagen en daarna automatisch verwijderd. Dan is er niks aan de hand, maar op het moment dat je dat gaat combineren met bijvoorbeeld gezichtsherkenning zoals in China, specifiek over de Oeigoerengebieden waar inderdaad camera's hangen met gezichtsherkenning die bijhouden waar iemand op dat moment is, dan is het een ander verhaal.

Denkt u dat de Nederlandse overheid verantwoord met camera's kan omgaan?
Als het gaat om biometrische herkenning, gaat de Nederlandse overheid daar heel verantwoord mee om. Camera's op straat hebben dat niet, nog niet… De politie heeft bijvoorbeeld wel de CATCH-database waarin ze van alle verdachten een foto hebben voor biometrische herkenning. Maar de meeste verdachten worden nooit veroordeeld, dus die zouden eigenlijk uit de database moeten. Dat blijkt dan technisch heel moeilijk te zijn en binnen de politie is weinig animo om daar veel moeite voor te doen. Dus er staan tienduizenden, misschien wel honderdduizenden, mensen in die database die er eigenlijk niet in horen. Dat is natuurlijk een twijfelachtig gebeuren. Zo zie je wel vaker dat iemand zo'n systeem begint met de beste bedoelingen. Soms wordt er goed nagedacht over de checks & balances die erin moeten zitten en in de uitvoering blijkt het dan toch lastig om ervoor te zorgen dat het goed gaat. Zeker bij

de politie, waarom zou je als politieman moeite doen om gegevens te verwijderen? Misschien komen ze later van pas bij andere arrestaties.

Je kan eventueel zelf ook zoeken in die database of je verdachte bent.
Ja, en inzageverzoeken doen bij de politie is heel lastig. Ze hebben een heleboel verschillende databases die eigenlijk met duct tape en tie wraps aan elkaar vastzitten, dus dat werkt niet super. Het is als buitenstaander dus moeilijk om daar goed zicht op te krijgen. Amnesty International heeft het ook wel eens geprobeerd en zij gingen dan als privépersonen naar de politie om een inzageverzoek te doen. Als ze als Amnesty kwamen, kregen ze een heel algemene verwijzing naar de website. Maar als privépersonen duurt het ook allemaal heel lang en krijg je ook niet veel meer informatie dan 'je staat in dit systeem en in dat systeem'. 'En in dat systeem dan?' 'Ja, weet ik niet, moet ik dat ook nog opzoeken? Vast niet.' Er ligt een heleboel data waarvan je denkt 'moet de overheid dat nou allemaal opslaan?'

De Toeslagenaffaire is misschien een goed voorbeeld daarvan. Daar is ook veel data opgeslagen van personen die eigenlijk verwijderd moest worden in 2014, en in 2018 bleek dat die data nog steeds in de systemen stond. Dus bij de overheid gaat het ook niet altijd helemaal goed.
De Toeslagenaffaire is een heel duidelijk voorbeeld van hoe het mis kan gaan als je al die data opslaat en dan kan iets heel makkelijk uit de hand lopen. Dan blijkt ook hoe moeilijk het is om van die data af te komen als het in allerlei systemen is

verspreid die aan elkaar vastgeknoopt zitten. En dan gaat het niet eens om heel veel data. Bij de meeste mensen ging het om een aantekening van 'verhoogd risico', twee regeltjes data. Maar daar kan zoveel uit voortvloeien. Het hoeft niet eens expres te gebeuren, maar het kan fout geïnterpreteerd worden en voor je het weet ga je diep de shit in. Dan werd je een 'verhoogd risico' voor fraude omdat je bijvoorbeeld je kinderen had gestuurd naar een kinderopvang waar fraude was gepleegd en dan was ineens elke klant automatisch eenverhoogd risico. Vervolgens werd elk jaar je volledige belastingaangifte doorgelicht door de Belastingdienst en moest je voor elke cent een bonnetje hebben. Het ene probleem veroorzaakt het andere probleem en dan word je een vicieuze cirkel in getrokken. Ik heb zelf ook twee kinderen en, nou, het aanvragen van kinderopvangtoeslag… Ik hoop ook altijd maar dat ik het goed gedaan heb, want je moet van tevoren opgeven op de cent nauwkeurig hoeveel je in een jaar gaat verdienen, en hoeveel uur je kinderen naar de kinderopvang gaan. Dus elke keer als de kinderen een extra middagje naar de kinderopvang moeten, moet je dat doorgeven aan de Belastingdienst. De hoeveelheid informatie die je moet aanleveren is zo groot en gevarieerd, waardoor je heel makkelijk een foutje maakt. En dan vorderen ze al het geld terug wanneer je een klein foutje hebt gemaakt. Als je kijkt naar proportionaliteit en subsidiariteit, heb je al die data niet nodig om kinderopvang betaalbaar te houden. Maar er is dan een systeem opgetuigd dat al die data nodig heeft. Soms is de oplossing waarbij je de minste data nodig hebt de beste oplossing.

"Het ene probleem veroorzaakt het andere probleem en dan word je een vicieuze cirkel in getrokken."

We hebben het vooral gehad over de inbreuk die surveillance maakt op de privacy, maar maakt het ook inbreuk op andere grondrechten?

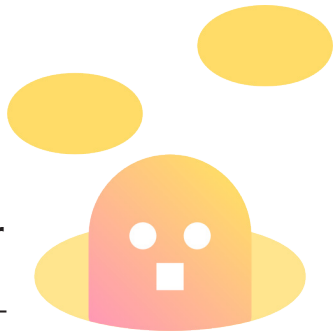
Het maakt ook een heel grote inbreuk op het recht van vrijheid van meningsuiting. Gek voorbeeld: toen in, uit mijn hoofd, 2013 Snowden met zijn onthullingen kwam over de NSA en de GCHQ stond dat over de hele wereld een aantal weken op de voorpagina's. Dit ging dan vooral over de monitoring van internetgebruik. Wikipedia houdt de populaire pagina's bij en hoeveel gebruikers naar een pagina hebben gekeken. Je zou denken dat de Wikipediapagina voor NSA heel veel bezocht werd, omdat het veel in het nieuws was en niet veel mensen de NSA kennen. Maar je ziet juist dat het inzakt op dat moment. Dus op het moment dat in het nieuws komt dat de NSA je internetverkeer in de gaten houdt, worden mensen blijkbaar bang om op Wikipedia over de NSA te lezen. Misschien zoeken ze daar wel iets achter, denken mensen dan. Dat is dus een heel idioot effect, maar daardoor kunnen mensen wel minder goed een mening vormen over iets. Het recht op vrijheid van meningsuiting betekent ook informatie kunnen vergaren. Als mensen dus bij het vergaren van informatie bang zijn dat een veiligheidsdienst meekijkt, gaan ze dat minder snel doen. Dat heet het 'chilling effect'. Op het moment dat wordt gesurveilleerd bij een protest en de politie alles opneemt, kunnen mensen denken 'laat ik maar niet protesteren'. Daardoor worden mensen voorzichtiger in het uiten van hun mening, maar dat is veel moeilijker kwantificeerbaar te maken. Je kan veel minder duidelijk zeggen: doordat er surveillance is, is er zoveel minder vrijheid van meningsuiting. We weten dat het minder is en er zijn veel aanwijzingen dat het zo is, maar het is moeilijk om er de vinger op te leggen hoeveel het precies is. Het is dus een hele wazige inbreuk en je kan er niet mee naar de rechter. Je kan niet zeggen: doordat de staat surveillance doet, durf ik niet naar de Wikipediapagina van de NSA te kijken. Je kan moeilijk naar de rechter voor iets dat je niet hebt durven doen. Uiteindelijk zijn we met z'n allen wel slechter af als mensen niet meer naar een Wikipediapagina durven te kijken.

Soms is de oplossing waarbij je de minste data nodig hebt de beste oplossing.

Op YouTube heb je bijvoorbeeld een eigen account, maar dat hoeft niet op jouw naam te staan en dan kan je alles over iedereen zeggen in de comments. Er zijn mensen die hiervan af willen, omdat er best lelijke dingen worden gezegd op het internet door random namen waarvan je niet weet wie het is. Dan zou een oplossing bijvoorbeeld zijn dat je alleen door middel van je paspoort of BSN een account aan zou kunnen maken. Dat maakt dan wel een inbreuk op het 'recht om anoniem te blijven'.

Dat is een heel ingewikkelde afweging. Je kan veel nare of eventueel illegale dingen posten op sociale media of bijvoorbeeld oproepen tot haat en geweld. Mensen vinden dat dit alleen zou moeten mogen als je je kan identificeren. Ik denk wel dat dat op zekere hoogte leidt tot iets geciviliseerder internet, maar dat hoeft ook niet altijd waar te zijn. Facebook is daar een voorbeeld van: dit is een plek waar in principe geacht wordt dat je je eigen naam gebruikt, maar dit leidt niet altijd tot geciviliseerde acties. Er zijn ook een heleboel mensen die afhankelijk zijn van anonimiteit om dingen te doen die we heel goed vinden als maatschappij. Mensen die in een regime wonen met een stuk minder vrijheid van meningsuiting ontneem je daarmee de mogelijkheid om zich te uiten en informatie te delen zonder te worden opgepakt. Daar zit wel een balans in; aan de ene kant maak je het de criminelen makkelijker, maar aan de andere kant maak je het een heleboel mensen die goeds in de zin hebben moeilijker. Ik zie veel meer in een moderatieplicht van dat soort platformen. Op het moment dat iemand iets illegaals post, moet je het er gewoon af knallen. Ik denk dat je zeker een bepaalde verantwoordelijkheid hebt als je een website maakt waar mensen dingen op kunnen gooien, dan moet je dat ook onderhouden. Twitter loopt meer de andere kant op. Het is nog maar de vraag of Twitter straks nog wel aan alle regelgeving voldoet. Ik denk ondertussen niet meer en dat ze daardoor wel tegen problemen aan gaan lopen. Daarnaast kun je technologisch altijd anoniem zijn. Er zijn altijd handige jongens die weer een nieuwe manier bedenken om anoniem te zijn op het internet. Je kan dit soort dingen eindeloos proberen te verbieden en uit te bannen, maar de decentrale architectuur van het internet zorgt ervoor dat altijd wel weer iemand iets bedenkt waardoor het toch anoniem kan. Ik denk dat het weinig zin heeft, want als mensen echt anoniem willen zijn dan lukt dat ze wel. Denk maar aan illegale handelsplaatsen voor wapens en drugs. Daar investeert Interpol heel veel geld in om die elke keer uit de lucht te halen. En dat lukt na een paar jaar ook wel, maar dat zijn hele complexe operaties en vaak komt er meteen weer een nieuwe website.

Er zijn ook websites waar je gratis series en films kan kijken, dan weet ik ook dat er steeds weer een nieuwe komt. Je kan er weinig tegen doen



Je bent altijd whack-a-mole aan het spelen met dat soort sites. Je haalt de ene uit de lucht en dan komt de ander. Zo lang mensen gemotiveerd genoeg zijn om het te doen, blijft het bestaan. Je kan het alleen maar lastiger maken. Het is eigenlijk niet te voorkomen dat iemand weer een weg vindt. Bij anonimiteit moet je eerst nog de vraag stellen of je het überhaupt wel moet willen. Dat je de handel in wapens aan banden wil leggen, die begrijp ik, maar bij de anonimiteit kun je daar nog een fundamentele discussie over voeren waarbij ik vind dat je het eigenlijk niet moet willen.

Heeft u nog tips over hoe je de IT-Recht studie kan halen?

Nou, als je je studie IT-recht wil halen, denk ik dat het goed zou zijn als meer studenten een beetje zouden leren programmeren. Er zijn genoeg dingen op het internet of websites waar je gratis de basis van het programmeren kunt leren en verschillende programmeertalen kunt uitproberen. Het helpt heel erg om te weten hoe een computer denkt. Als je een paar regeltjes code kunt schrijven helpt het al. Het hoeft echt niet ingewikkeld te zijn, je hoeft echt niet je eigen operating system te bouwen.

Programmeer eens een klein spelletje voor jezelf. Er zijn genoeg websites te vinden waar je codes erin gooit en die website gaat het dan compilen en runnen. Dan zie je heel duidelijk: als ik dit erin typ, komt er dit uit en als ik dit erin typ, komt er dat uit. Dat helpt heel erg als je IT-recht studeert om dat IT-stukje extra in de vingers te krijgen. In het boek van het vak IT in de context van het recht staan wel twee hoofdstukken over programmeren maar die behandelen we gewoon niet. Dus je kan het wel gebruiken om te kijken hoe programmeren werkt en hoe je praat tegen een computer. Eigenlijk alles wat je doet op een computer, daar zit code achter. Misschien ook een tip: ik heb mijn apparaten altijd op Engels staan, zodat ik makkelijk kan Googelen op bijvoorbeeld tutorials en how-to's. Zet je apparaat op Engelstalig, dan kan je makkelijker Googelen.

De Spotify Wrapped is laatst uitgekomen. Heeft u Spotify en hoeveel minuten heeft u geluisterd?
Ik heb inderdaad Spotify. Mijn meest beluisterde artiest is Bach, want dat is fijn om te luisteren tijdens werk, en daarna Taylor Swift. Ik heb 39.653 minuten geluisterd.
Ja, ik luister veel Spotify tijdens werken. Veel Bach.

Namens de redactiecommissie,

Resa van Westering en Kirsten Brandsma

Twitter als politiek instrument

Mark Rutte: 1,3 miljoen, Emmanuel Macron: 8,9 miljoen en Barack Obama: 133 miljoen. Tegenwoordig hebben politici over de hele wereld miljoenen aan Twitter- volgers. Dit gaat niet zonder meer gepaard met een enorme impact in de politieke wereld. Door de ontwikkeling van sociale media is communicatie onder de mensen interactiever geworden. Vroeger werd een politicus geïnterviewd door een journalist en vervolgens werd dit gesprek via hun media gepubliceerd. Tegenwoordig is dit hele proces versneld, een politicus kan onverwijld en ogenblikkelijk communiceren met de ontvangende partij. Enkel een paar simpele handelingen zijn nodig om een tweet te versturen die vervolgens door 1,3 miljard Twitter-gebruikers gezien kan worden. Politieke partijen, specifiek individuele politici, kunnen op deze manier zichzelf positief karakteriseren en geven eventuele aanhangers de mogelijkheid om vragen te stellen. Derhalve is het niet vreemd dat bijna alle politici in dit huidig tijdperk gebruik maken van Twitter. In dit artikel wordt de reikwijdte van Twitter in de politiek behandeld door middel van de volgende twee onderwerpen. Ten eerste wordt het gebruik van Twitter door Trump behandeld. En ten tweede worden de maatregelen besproken die worden genomen om foutieve informatie tegen te gaan. Hierbij wordt ook kort gesproken over de overname van Elon Musk van Twitter.

Trump en Twitter

In 2016 vond er een presidentsverkiezing plaats in Amerika, waarbij burgers konden stemmen op Hillary Clinton of Donald Trump. Deze verkiezing kreeg te maken met veel invloed van sociale media en Trump werd in deze periode veel genoemd in samenhang met verspreiding van nep nieuws. Een uitgebreid onderzoek uit 2018 onderzocht fake en niet-fake nieuws rondom de verkiezingen op Twitter en duidde aan dat fake nieuws sneller en omvangrijker spreidt dan niet-fake nieuws, omdat fake nieuws in zekere zin 'aantrekkelijker' is en dus sneller wordt gedeeld door mensen.[1] Bij de Amerikaanse presidentsverkiezingen in 2016 ontdekte Shao dat door middel van geautomatiseerde accounts die werden beheerd door Twitterbots, desinformatie verspreid werd.[2] Een hieruit opvolgend onderzoek van het blad Nature Communications onderzocht het verspreiden van deze neptweets. Het onderzoek was hoofdzakelijk een bestudering van veertien miljoen berichten en 400.000 artikelen die tussen mei 2016 en maart 2017 op Twitter waren gedeeld. De onderzoekers hebben nadrukkelijk benoemd dat zij zowel gekeken hebben

1 S. Vosoughi, D. Roy & S. Aral, 'The spread of true and false news online', Science 2018, afl. 359, p. 1146-1151.
2 C. Shao e.a., 'The spread of low-credibility content by social bots', Nat Commun 2018, afl. 4787.

naar linkse als naar rechtse nepnieuwsberichten. Uit de analyse blijkt dat Twitterbots een grote rol hebben bij het verspreiden van fake nieuwsberichten op grote schaal. Wanneer een bericht net een paar seconden is getweet, gaan de bots gelijk te werk door dit te delen. De onderzoekers concluderen dat deze snelle verspreiding het moeilijk maakt om fake nieuws tegen te gaan. Over het algemeen geloven mensen een bericht sneller wanneer een tweet, dan wel door honderd Twitterbots, is geretweet. Desbetreffende bots wekken zo het beeld dat het bericht ontzettend populair is en mensen die dit voorbij zien komen zijn vervolgens verleid om de berichten zelf ook te retweeten. Desbetreffende bots wekken zo het beeld dat het bericht ontzettend populair is en mensen die dit voorbij zien komen zijn vervolgens verleid om de berichten zelf ook te retweeten.[1]

Trumps Twitter presidentschap

Op 2 oktober 2022 Twitterde Trump dat hij positief getest was voor COVID-19. Trump zelf stond in die tijd ongeloofwaardig tegenover de gevolgen van corona. Twitter plaatste door gebrek aan bewijs van Trump een waarschuwing bij een tweet, waar hij beweerde dat hij geen last had van het virus, en zelfs immuun zou zijn. De waarschuwing luidde als volgt: "This Tweet violated the Twitter Rules about spreading misleading and potentially harmful information related to COVID-19. However, Twitter has determined that it may be in the public's interest for the Tweet to remain accessible".[2] Tijdens de Amerikaanse verkiezingen van 2020 duidde Twitter 300.000 tweets aan als mogelijk misleidend. Opmerkelijk genoeg zaten tweets van Trump hier ook tussen. Dit speelde bij tweets waar Trump bijvoorbeeld zijn overwinning mededeelde zonder dat er resultaten waren van de stemmingen en wanneer hij twitterde dat er fraude zou zijn gepleegd door de Democraten.[3] Een onderzoek van the Times beweert dat Trump Twitter volledig had geïntegreerd in de structuur van zijn regering, wat resulteerde in een nieuwe vorm van presidentschap en presidentiële macht. Presidenten hebben vaak problemen met hun eigen bureaucratie, maar Trump gebruikte Twitter om blokkades te doorbreken door tegenstrijdige opinies terzijde te schuiven of te vernederen en zijn eigen personeel vooruit te helpen. Het is gebleken dat de voormalige president in meer dan de helft van zijn tweets iets of iemand aanvalt. Twitter is daarnaast een instrument wat Trump gebruikte voor zijn buitenlandse betrekkingen en beleid. Hij heeft meer dan honderd keer dictators geprezen, terwijl hij twee keer zoveel over de traditionele bondgenoten van Amerika klaagde.[4] Desalniettemin is het account van Trump op dit moment opgeschort na een grondige beoordeling door Twitter. Het platform onderzocht tweets van het account en de contexteromheen, met name hoe het ontvangen werd en geïnterpreteerd op en buiten Twitter. Er zou volgens Twitter een risico van aanzetten tot geweld zijn ontstaan door de tweets van Trump, en derhalve heeft het account nu een 'suspension'.[5]

1 A. Bovet & H.A. Makse, 'Influence of fake news in Twitter during the 2016 US Presidential election, Nat Commun 2018, afl 7.

2 M. den Teuling, 'Amerikaanse verkiezingen: Trump, Biden & de invloed van social media', ct.nl, 29 oktober 2020.

3 Bright, 'Twitter: '300.000 misleidende tweets tijdens verkiezingen VS', rtlnieuws.nl, 13 november 2020.

4 G. Beltran, R. Taylor & J. Huang, 'The Twitter Presidency', nytimes.com.

5 Twitter Inc, 'Permanent suspension of @realDonaldTrump', blog.twitter.com, 8 januari 2021.

Maatregelen door Twitter en de EU

Zoals genoemd, is de betrouwbaarheid op sociale media te betwisten doordat iedereen iets op een platform kan plaatsen. Wat doet Twitter tegen fake nieuws en misleidende politici? Twitter heeft in 2019 ingrijpende maatregelen genomen om mogelijke foutieve beïnvloeding van verkiezingen te vermijden. In hun beleid staat dat Twitter wereldwijd het verbiedt om politieke reclame maken. Ze hebben deze beslissing gebaseerd op de gedachte dat het bereik van politieke berichten verdiend moet worden, en niet gekocht.[1]

De Europese Unie (hierna: EU) wil dat platformen zoals Twitter meer verantwoordelijkheid nemen. De EU streeft in dit opzicht naar meer verantwoordelijkheid om de bescherming van de democratie te waarborgen. De besluiten die invloed hebben op de democratie en de gevolgen hiervoor in de toekomst zouden niet moeten genomen worden door directies van grote tech bedrijven. Derhalve is dit jaar op 5 juli een een wetsvoorstel aangenomen voor de Digital Services Act (hierna: DSA), die op 16 november daadwerkelijk in werking trad. Deze wet zou de Richtlijn voor digitale diensten moeten 'updaten'. Grote platforms moeten nu gebruikers inlichten over hoe hun algoritmes bepalen welke content zij te zien krijgen. Op deze manier zal het voor Twitter-gebruikers makkelijker zijn om te oordelen of het beeld wat het platform creëert al dan niet te vertrouwen is. Daarenboven moeten grote tech bedrijven eens in de tijd een verslag uitbrengen en de gebruikers meer informatie verstrekken over de reclameadvertenties die te zien zijn. [2] Sinds Elon Musk Twitter heeft overgekocht wordt, de handhaving van de DSA getest. Binnen enkele uren nadat Elon Musk het platform had overgenomen, nam het aantal racistische tweets toe. Zelf retweette hij berichten die onjuiste informatie bevatten over de aanval en poging tot ontvoering waarbij de echtgenoot van de voorzitter van het Amerikaanse Huis, Nancy Pelosi, ernstig gewond raakte. Tevens heeft Elon Musk het personeel gehalveerd en de meerderheid van de duizenden medewerkers ontslagen, die voornamelijk zorgen voor het toezicht op inhoud van tweets. De DSA vereist echter niet dat Twitter alle schadelijke inhoud moet verwijderen, zoals tweets die haat dragen maar wel wettelijk correct zijn. De DSA stelt enkele limieten aan wat kan worden verwijderd. Dit maakt het voor Elon Musk makkelijker om zo min mogelijk te verwijderen. Niettemin zijn platforms wel verplicht verantwoordelijk samen te werken en te handelen met vertrouwde 'flaggers' en overheidsinstanties om ervoor te zorgen dat hun diensten niet worden misbruikt voor illegale activiteiten. Elon Musk noemt zichzelf een absolutist van de vrijheid van meningsuiting. Zijn ratio om Twitter te kopen zou voor een gemeenschappelijk digitaal stadsplein zijn. Daarenboven heeft hij kritiek geuit op het inhoudsmoderatiebeleid van Twitter en zou hij zich verzetten tegen censuur die veel verder gaat dan de wet. Als Elon Musk succesvol is om het aantal gebruikers van Twitter nog meer uit te breiden, zal het platform strenger worden gecontroleerd door de DSA en zou het nodig kunnen zijn om opnieuw de afdeling voor content moderatie weer te laten bemannen.[3]

Tot slot kunnen we concluderen dat Twitter een gevaarlijk instrument kan zijn in de politieke wereld. Voor politici zoals Trump zou er meer behoedzaam gekeken moeten worden naar de inhoud van twijfelachtige tweets en de impact ervan. Deze grote verantwoordelijkheid ligt nu bij Twitter en daarom is het van groot belang dat daar wetgeving over bestaat. Gevolglijk is er dit jaar de DSA aangenomen waarin meerdere regels staan over hoe een platform zoals Twitter om zou moeten gaan. Al met al moet Twitter ervoor zorgen dat desinformatie niet verspreid kan worden op het platform.

Namens de redactiecommissie,

Yong Hui Zhou

1 Twitter Inc, 'Political content', business.twitter.com.

2 Nieuws Europees Parlement, 'Wet inzake digitale diensten: veiligere digitale platforms voor gebruikers', europarl.europa.eu, 20 januari 2022.

3 K. Gullo & C. Schmon, 'More Turbulence Ahead for Twitter as the EU's Digital Services Act Tests Musk's Vision', justsecurity.org, 23 november 2022.