Burgerrechtenvereniging VRIJBIT

www.vrijbit.nl





Maar om dat zo te houden gaat niet vanzelf.

Jaarverslag 2019 Burgerrechtenvereniging Vrijbit 29 april 2020

Inhoudsopgave

Inhoudsopgave	pagina 1
Inleiding	pagina 2
Algemene ontwikkelingen in 2019	pagina 3
Actuele kwesties	pagina 6
Privacynieuwsdienst	pagina 10
Doorlopende kwesties waar Vrijbit in verwikkeld was	pagina 11
Intern functioneren 2019	pagina 22
Financieel jaaroverzicht 2019	pagina 26

Inleiding

In dit jaarverslag geeft Burgerrechtenvereniging Vrijbit een schets van de ontwikkelingen op het gebied van de privacybescherming, een overzicht van verrichte werkzaamheden, een blik op het intern functioneren van de vereniging en de financiële verantwoording over het jaar 2019. Door middel van dit jaarverslag legt het bestuur verantwoording af tegenover de leden en donateurs.

Tevens verschaft het verslag informatie over de stand van zaken aangaande de strijd om het behoud van het recht op persoonlijke vrijheid in 2019 en de rol die Vrijbit daarin speelde. Het jaarverslag zal, na goedkeuringdoor de leden, op de website www.vrijbit.nl worden gepubliceerd. Op aanvraag is een papieren versie verkrijgbaar.

Algemene ontwikkelingen in 2019

2019 ging, net als voorgaande jaren, de geschiedenis in als een jaar waarin we geconfronteerd werden met een gigantische hoeveelheid nieuwe berichten en ontwikkelingen in het kader van de Privacy.



Zoals, bijna dagelijks, nieuwe informatie over datalekken en misbruik van persoonsgegevens.

Over nieuwe ontwikkelingen voor het systematisch en grootschalig kunnen verzamelen van persoonlijke data via sensoren en tot de persoon te herleiden analyses via gezichtsherkenningstechnologie.

Over nieuwe en recent ontdekte, gevaren (zoals gijzelsoftware) van online communicatie die een bedreiging vormen voor de bescherming van personen en het functioneren van instanties, bedrijven en zelfs vitale sectoren van de samenleving.

Over het toenemende aantal mensen dat buitengesloten dreigt te raken van de steeds intensiever gedigitaliseerde maatschappij. Inmiddels zijn er namelijk volgens cijfers van de overheid in februari 2019 rond de 2,5 miljoen Nederlanders die het 'moeilijk vinden om te werken met digitale apparaten, zoals een computer, smartphone of tablet en 1,2 miljoen Nederlanders nog nooit internet hebben gebruikt'.

Informatie over de falende inzet van informatie- en communicatietechnologie (ICT-systemen) voor publieke diensten. Waardoor bijvoorbeeld, wegens een stroomstoring bij KPN op 24 juni 2019, zelfs het alarmnummer 112 onbereikbaar was.

Een nauwelijks bij te benen berichtenstroom over de voortgang van *(nieuwe, aangepaste, voorgenomen of afgeschoten)* wet-en regelgeving met impact op de bescherming van het recht op persoonlijke vrijheid.

Informatie in zake juridische procedures tegen privacy-aantastingen en inbreuken op het recht op een privéleven.

Waarbij zich eveneens de trend voortzette:

- Dat veel kwesties direct te maken hadden met de nog alsmaar toenemende macht die de kleine groep mondiale internetbedrijven uitoefent op allerlei sectoren van de samenleving.
- De decentralisatie en vermarkten van de zorgsector leidde tot een verdere kaalslag van de verzorgingsstaat. Zodanig dat het voor zorgverleners nauwelijks meer mogelijk is om hun werk naar behoren te kunnen doen en cliënten/patiënten van hulp verstoken blijven. Met alle gevolgen van dien in de Jeugdzorg, ouderenzorg, reguliere ziekenzorg en Geestelijke Gezondheids Zorg. En niet te vergeten voor het disfunctioneren van de Immigratie- en Naturalisatie Dienst (IND) en de Belastingdienst.
- Steeds schrijnender voorbeelden zich opdrongen over de gevolgen van een overheidsbeleid waarbij de burger als potentieel verdachte van fraude wordt bejegend.

- Steeds duidelijker werd hoe de inrichting van het onderwijs en de beoordeling van de ontwikkeling van kinderen en jongeren wordt geïnfiltreerd en gedicteerd door commerciële bedrijven.
- Dat er meer oog kwam voor de onoverzienbare gevolgen van de mogelijkheden voor de toepassing van kunstmatige intelligentie (AI). Op gebied van grootschalige verzameling en verwerking van persoonsgegevens voor data analyse en (risico)profilering.



Begin 2019, op 28 januari de 'dag van de Privacy' om precies te zijn, maakte de Autoriteit Persoonsgegevens bekend dat uit het Motivaction onderzoek dat zij hadden laten doen, gebleken was dat maar liefst 94% van de bevolking zich zorgen maakt over de veiligheid van zijn of haar persoonsgegevens en een op drie mensen zelfs veel of zeer veel zorgen.

Dat ongekend hoge percentage heeft natuurlijk alles te maken met het feit dat inmiddels bijna iedereen ofwel uit eigen ervaring, via bekenden en/of uit de media begrepen heeft hoeveel persoonsgegevens er constant van iedereen worden vastgelegd. Op welke manier dat gebeurt en hoe dat het risico met zich meebrengt dat iemands gegevens worden misbruikt door kwaadwillenden. Met alle gevolgen voor mogelijkheden tot identiteitsfraude, chantage en manipulering van dien. Evenals hoe dat gebeurt door de eigen overheid. Waardoor persoonsgegevens bijvoorbeeld ook volkomen onterecht kunnen worden gebruikt om burgers te brandmerken als fraudeur of te classificeren als potentieel risico voor het plegen van fraude.

> De drama's, bijvoorbeeld ten gevolge van de terugvorderingen en opgelegde boetes voor vermeend onterecht uitgekeerde toeslagen voor kinderopvang, kunnen haast niemand ontgaan zijn. Waarbij, naast het leed wat dit veroorzaakte, vooral ook duidelijk werd hoe machteloos een burger in dergelijke gevallen is en hoe halsstarrig een overheidsdienst- gedekt door het ministerie- kan volharden in het handelen op grond van onjuiste data.

Daarnaast had het van kracht worden van de nieuwe Wet Bescherming Persoonsgegevens (AVG of GDPR) op 25 mei 2018 ervoor gezorgd dat binnen heel veel bedrijven, instanties en organisaties (eindelijk) überhaupt het besef doordrong dat men vaak data gebruikte die als persoonsgegevens beschouwd moeten worden. En dat de bescherming van persoonsgegevens enerzijds een fundamenteel recht is van de betrokken persoon en anderzijds een plicht daarvoor zorg te dragen door de verwerker.

Dat nieuwe inzicht in met name de onderwijssector, kleine- en middelgrote bedrijven, stichtingen en verenigingen, ontstond weliswaar vooral omdat er onder de nieuwe wet boetes konden worden uitgedeeld voor overtredingen. Maar leverde in elk geval op dat nu op veel grotere schaal

bekend werd dat persoonsgegevens niet alleen data zijn die rechtstreeks deel uit maken van iemands identiteit maar ook alle informatie betreft over een ' *geïdentificeerde of identificeerbare natuurlijke persoon*'. *Alle gegevens dus die ofwel direct over iemand gaan, ofwel naar deze persoon te herleiden is.*

In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

- U heeft toestemming van de persoon om wie het gaat.
- Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
- Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
- Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
- Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen.
- Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

We mogen dus wel concluderen dat er in de afgelopen tien jaar een grote verschuiving heeft plaatsgevonden ten aanzien van het belang van privacy en van de bescherming van persoonsgegevens. **Waarbij we er vanuit Vrijbit altijd eraan hechten om helder aan te geven dat privacy, het fundamentele recht op de bescherming van het privéleven, geen doel op zich vormt maar wel de voorwaarde is voor de mens om in vrijheid te kunnen leven.**

Met de nadruk op het fundamentéle karakter van dit recht, zoals dat is vastgelegd in de Universele Verklaring van de Rechten van de Mens en voor heel Europa als 'afdwingbaar recht met directe werking' in de Europese Verklaring voor de Rechten van de Mens (EVRM)

art. 1: Verplichting van lidstaten zich te houden aan de rechten en toe te passen op iedereen binnen hun rechtsmacht.
art. 2: recht op leven
art. 3: verbod op martelen
art. 4: verbod op slavernij en dwangarbeid
art. 5: recht op vrijheid en veiligheid
art. 6: recht op een eerlijk proces en toegang tot de rechter
art. 7: geen straf zonder wet: legaliteitsbeginsel
art. 8: recht op bescherming van de privésfeer, waaronder valt: privacy en bescherming van het gezin (voluit: recht op eerbiediging van privé-, familie- en gezinsleven)
art. 9: vrijheid van gedachte, geweten en godsdienst
art. 10: vrijheid van meningsuiting
art. 11: vrijheid van vergadering
art. 12: recht op huwelijk
art. 13: recht op daadwerkelijk rechtsmiddel
art. 14: verbod op discriminatie
art. 15: afwijkingen indien ten tijde van oorlog of noodsituatie
art. 16: beperkingen op politieke activiteiten van vreemdelingen
art. 17: rechten in het verdrag mogen niet beperkt worden in naam van ander recht
art. 18: rechten mogen alleen gebruikt worden waarvoor ze bedoeld zijn: verbod op détournement de pouvoir



Als reden waarom, in tegenstelling tot aan het begin van deze eeuw, steeds grotere delen van de bevolking zich bewust zijn geraakt van het belang van Privacy en de bescherming van persoonsgegevens is tevens de maatschappelijke onrust aan te wijzen. Zoals in 2019 zichtbaar werd doordat zorg- en onderwijspersoneel massaal in opstand kwamen tegen het doorgeschoten systeem van regelzucht en controledrift.

Maar ook de verschuivende internationale verhoudingen veroorzaakten een groter besef van de kwetsbaarheden waaraan de inwoners van Nederland en Europa komen bloot te staan.

> Waarbij van invloed was dat de hoogoplopende Brexitperikelen in Groot-Brittannië en het opereren van de V.S. regering onder president Trump, duidelijk maakten wat bijvoorbeeld de gevolgen zijn van de macht van databedrijven die, zoals Cambridge Analytica, datamining, data-analyse en direct marketing zodanig kunnen inzetten dat zij de uitslag van verkiezingen kunnen gaan bepalen. En waarbij in 2019 steeds meer bekend werd hoe de Chinese regering haar eigen bevolking onderwerpt aan een totaalsurveillance systeem en internationaal ongekende invloed verwerft via monopolisering van de geneesmiddelen industrie t/m die van de wereldwijd toegepaste apparaten voor telecommunicatie technologie (waaronder de afluistermogelijkheden via Huawai).

Tot slot vermelden we dat begin 2019 uit het Motivaction onderzoek ook naar voren kwam dat mensen weliswaar aangeven bezorgd zijn, maar slechts 12% wel eens gebruik bleek te hebben gemaakt van een privacyrecht. ‘Dit omdat mensen niet weten hoe ze dat moeten doen, het (te veel) gedoe vinden of niet belangrijk genoeg. Waarbij ook nog eens komt dat rechten, zoals het recht op dataportabiliteit en het recht op een menselijke blik bij geautomatiseerde besluiten, velen ook onbekend bleken te zijn’.

Cijfers die bij Vrijbit niet echt verbazing opleverden omdat ook vanuit onze organisatie nog steeds geconstateerd wordt dat het maar een klein aantal mensen is dat zich actief inzet voor het behoud van het recht op privacy en lichamelijke integriteit en in actie komt als er misbruik wordt gemaakt van hun persoonsgegevens.

Actuele kwesties

EU nieuwe wet-en regelgeving

Omdat de Europese Unie op veel gebieden dwingend de invoering van EU wetgeving kan voorschrijven, lichten we hier enkele van de belangrijke wetgevingstrajecten toe.

Vingerafdrukken alsnog verplicht in ID-kaart

Na jaren actie werd, niet in de laatste plaats door de inzet van Vrijbit, de verplichte vingerafdruk voor de Nederlandse ID-kaart (die in 2009 werd ingevoerd) in 2014 afgeschaft. Niet omdat de vingerafdrukken een te grote inbreuk maakten op iemands lichamelijke integriteit, niet omdat ze

zo ondeugdelijk waren dat ze totaal ongeschikt bleken voor het doel waarvoor ze afgegeven dienden te worden, niet omdat het burgers in gevaar kon brengen maar formeel alleen omdat het geen verplichting vanuit de EU betrof zoals de regering jarenlang had doen voorkomen. Maar zoals wel vaker het geval bleek als het onrechtmatige inbreuken op de privacy betreft: als de overheid na jaren procederen bakzeil moet halen en het maatschappelijke protest niet gesmoord kan worden, dan probeert men via een omweg alsnog vast te houden aan de eenmaal ingeslagen weg. In dit geval van de route om alle burgers te persen in een dwangbuis van biometrische identificatie die gestoeld is op de uitgifte van biometrische paspoorten en ID-kaarten waarvan de persoonsgegevens worden opgeslagen in een op afstand uitleesbare RFID-chip van het document en in een overheidsregister wat gekoppeld is aan het unieke persoonsregistratienummer (BSN) dat aan iedere Nederlander bij de aangifte van geboorte wordt toegekend.

Hoewel de Europese Commissie voorheen, enkel om redenen van harmonisatie ter beveiliging van de buitengrenzen van het Schengengebied, biometrische paspoorten had voorgeschreven, heeft men nu alsnog een wet ingevoerd die de lidstaten verplicht om ook de nationale identiteitskaarten *(waarmee men binnen het Schengengebied gebruik kan maken van het recht op vrij verkeer van personen)* van vingerafdrukken te laten voorzien. Het Europees Parlement stemde op 4 april 2019 met 335 stemmen tegen 269 stemmen in met deze nieuwe wetgeving.
Voor stemden: VVD, CDA, CU, SGP, D66 (1 persoon).
Tegen: PvdA, PVV, GL, SP, PvdD, D66 (3 personen)

Daarmee zijn mensen die weigeren om vingerafdrukken af te geven aan de Staat- zodra deze wetgeving in nationaal recht is geïmplementeerd- weer terug bij af. En wordt totaal voorbij gegaan aan het feit dat het EU Hof voor de Rechten van de Mens(EHRM) nog geen uitspraak heeft gedaan in de diverse aanklachten die daar zijn ingediend om een oordeel te vragen of onschuldige burgers in hun recht staan als zij weigeren om hun automatisch herkenbare lichaamskenmerken voor het verkrijgen van een paspoort- of ID-kaart af te staan.

Reden genoeg voor de nationale regeringen- zeker die van Nederland waartegen bij het EHRM minimaal 6 van dergelijke procedures lopen- om de implementatie van deze EU wet op te houden…..Maar aangezien Nederland van meet af aan de motor vormde achter de ontwikkeling van biometrische identificatie, en van de invoering van de vingerafdrukken in het bijzonder, is daar weinig zicht op. Het laat zich zelfs raden op instigatie van welke lidstaat de invoering van de verplichte vingerafdruk via EU wetgeving alsnog is gepusht. Immers als de Nederlandse Staat door het EHRM uiteindelijk (na inmiddels meer dan 10 jaar juridische strijd)verboden zou worden om een grootschalige biometrische dataverzameling van onschuldige burgers aan te leggen, dan kan men de verantwoordelijkheid proberen buiten zichzelf te leggen en te beleggen bij de EU Commissie die niet is toegetreden tot het EVRM .

<u>Registratie passagiersgegevens vliegreizen (PNR)</u>

Passenger Name Record (PNR) betreft een veelheid aan gegevens over reizigers in de luchtvaart. Het gaat dan bijvoorbeeld om naam, adres, woonplaats, e-mailadres, telefoonnummer, paspoortnummer, nationaliteit, geslacht, reisgenoten en geplande reisdata en reisroute. De gegevens worden gekoppeld met andere bestanden en desgevraagd ook uitgewisseld met andere landen binnen de EU. Nadat deze gegevens eerst werden vastgelegd voor buiten-continentaal vliegverkeer stelde de Europese Commissie later in de Richtlijn (EU)2016/681 dat dit ook nodig

was voor de veiligheid binnen Europa en in de strijd tegen terrorisme en ernstige misdrijven. Op 4 juni 2019 werd deze wet door de Eerste Kamer aangenomen. Ondanks de bezwaren aangaande de noodzaak en proportionaliteit van het wetsvoorstel en de zorgen over de waarborgen van grondrechten met betrekking tot de werking en (discriminatoire) gevolgen van (semi)geautomatiseerde besluitvorming.

Een Europese database met vingerafdrukken en foto's.

Op 16 april 2019 stemde het EU Parlement in met de nieuwe wetgeving 'JD - Interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration'. Opzet van deze wet is dat de nationale systemen met biometrische gegevens gekoppeld worden aan vergelijkbare systemen in andere EU landen waardoor er in de praktijk een enorme database ontstaat met vingerafdrukken en pasfoto opnames die gebruikt mogen worden voor asiel- en migratiezaken, maar ook voor het opsporen en vervolgen van mensen.

Ook de systemen voor grensbewaking worden op eenzelfde manier gekoppeld aan vergelijkbare systemen in de andere landen van de EU, waardoor politie en douane met één druk op de knop informatie over een persoon uit alle 28 EU-landen tegelijk kunnen opvragen. Het gaat dan bijvoorbeeld om naam, geboortedatum, paspoortgegevens, vingerafdrukken en een gezichtsopname van de pasfoto.

Betaalgegevens openstellen voor bedrijven

Vanaf begin 2019 werd in Nederland de Payment Service Directive 2 (PSD2) van kracht. Dit is een nieuwe Europese wet voor het betalingsverkeer die het bankgeheim heeft opengebroken. Sinds het van kracht worden van deze wet zijn banken verplicht om, als u hen daar opdracht en toestemming voor geeft, uw betaalgegevens door te leveren aan commerciële partijen met een vergunning in heel Europa.

Het probleem is echter dat als iemand ánders die toestemming aan de bank geeft in diens datapakket ook betaalgegevens kunnen zitten van mensen die dat niet willen. Gegevens die op deze manier in handen komen van bedrijven zonder dat de betrokkene daar toestemming voor gaf, zonder dat deze daarvan op de hoogte wordt gesteld en zonder dat die persoon enig zicht heeft op wat er vervolgens met zijn of haar financiële gegevens kan gebeuren.

Auteursrecht/vrij internet

Op 26 maart 2019 stemde het EU parlement in met de nieuwe auteursrechtwetgeving. Inclusief het omstreden artikel 13 dat regelt dat internetplatforms verantwoordelijk worden voor wat iemand uploadt en uploadfilters gaan plaatsen om (de verspreiding van) ongewenste publicaties te voorkomen. Hiermee heeft de wetgever het maatschappelijk belang van een open internet ondergeschikt gemaakt aan de belangen van grote bedrijven en tussenpartijen. Omdat uploadfilters veel fouten maken en ook veel content onterecht blokkeren.

NL nieuwe wet-en regelgeving

Op 1 januari kregen de bijzondere opsporingsambtenaren (weer) ruimere bevoegdheden voor het aantal overtredingen waarvoor zij boetes mogen uitschrijven. Ook komt het bewapenen van de BOA's(vooralsnog met wapenstok en pepperspray) steeds dichterbij, via de route *'optimalisering van de operationele samenwerking tussen de BOA's en politiediensten'.*

Op 19 februari 2019 heeft de Eerste Kamer het wetsvoorstel 'register onderwijsdeelnemers' (43.878), ter bevordering van flexibeler gebruik van data uit leerlingvolgsystemen aangenomen. In het wetsvoorstel is de mogelijkheid opgenomen dat de minister zelfstandig bepaalt welke gegevens verzameld mogen worden en met wie die gedeeld mogen worden. Tot die invoering was wettelijk verankerd welke gegevens verzameld moeten worden en wie toegang tot de gegevens heeft. Dat kon niet zomaar worden aangepast. Maar met deze nieuwe wet kan de minister dat op elk moment zelfstandig aanpassen als deze dat nodig acht.

Op 1 maart 2019 trad De Wet computercriminaliteit III in werking. Met de nieuwe wet heeft de politie een hackbevoegdheid gekregen. De politie mag op afstand geautomatiseerde werken, waaronder dus smartphones, routers en computers, binnendringen voor de opsporing van ernstige delicten. Positief voor de bescherming van de privacy is dat de wet tevens regelde dat het onrechtmatig overnemen of 'helen' van niet-openbare gegevens uit een geautomatiseerd werk strafbaar werd gesteld.

Op 26 maart 2019 verleende de Eerste Kamer goedkeuring aan de wetswijziging 35.044 van de *'Zorgverzekeringswet, de Wet Langdurige Zorg en enige andere wetten in verband met het controleren van de verzekeringsplicht voor de zorgverzekering en het regelen van de verwerking van gepseudonimiseerde persoonsgegevens door de minister voor medische zorg, het Zorginstituut Nederland en het RIVM(Stb.2019, 140)'*

Op 18 juli 2019 werd het wetswijzigingvoorstel modernisering elektronisch bestuurlijk verkeer (35.261) ingediend. Waarmee o.a. het recht van burgers/bedrijven vergroot werd op elektronische communicatie en de verlaging van de drempel voor de bijzondere wetgever om elektronische communicatie verplicht te stellen voor ondernemingen en rechtspersonen.

In september 2019 laat de minister van V&J de Tweede Kamer weten dat hij het stroomstootwapen (Taser) als standaarduitrusting van politieagenten wil invoeren. Nadat hiermee was proefgedraaid, concludeerde de regering dat de gezondheidsrisico's van het gebruik niet op zouden wegen tegen het machtsmiddel voor de handhaving. Voor de komende jaren werd er daarom budget beschikbaar gesteld om 17.000 agenten te leren om het stroomstootwapen te gebruiken.

Op 29 november 2019 viel het besluit tot inwerkingtreding per 1-1-2020 van wet betreffende regels voor het kunnen verlenen van verplichte zorg aan een persoon met een psychische stoornis (Wet verplichte geestelijke gezondheidszorg- Wvggz 33. 399).

Conclusie

Deze opsomming is niet volledig maar geeft wel aan dat er via de Nederlandse regering systematisch bleef worden ingezet op het verder digitaliseren van de communicatie tussen de overheid en de burger.

Opvallend was dat, naarmate er in 2019 steeds meer bekend werd dat Nederland een spilfunctie vervult in de internationaal georganiseerde misdaad, het belang van zoveel mogelijk data verzamelen van de burger iets minder expliciet als voornamelijk bedoeld voor terrorisme bestrijding werd gemotiveerd.

De datagulzige overheid bleef daarbij onverminderd burgers allemaal als potentieel verdachten van crimineel gedrag bejegenen. Waarmee de inzet op, vooral preventief, fraudebeleid als grondslag werd aangedragen. En de verruiming van bevoegdheden en afdekken van onrechtmatige praktijken van overheid- en semi overheidsinstellingen als gerechtvaardigd belang voor de openbare orde en veiligheid werden gepresenteerd.



Ter aanvulling van een goed begrip over wat er in 2019 allemaal ‘speelde’ op het gebied van privacy publiceren we onderstaand overzicht van de door Vrijbits Privacynieuwsdienst gepubliceerde digitale nieuwsbrieven geeft een overzicht van de veelheid en verscheidenheid aan wekelijkse berichten.

Het overzicht geeft links naar deze weekoverzichten. Berichten die op de website zelf niet alleen chronologisch, maar ook op onderwerp te doorzoeken zijn.

Privacynieuws weekbrief - 52 Verzonden op 27 december 2019
Privacynieuws weekbrief - 51 Verzonden op 20 december 2019
Privacynieuws weekbrief - 50 Verzonden op 13 december 2019
Privacynieuws weekbrief - 49 Verzonden op 06 december 2019
Privacynieuws weekbrief - 48 Verzonden op 29 november 2019
Privacynieuws weekbrief - 47 Verzonden op 22 november 2019
Privacynieuws weekbrief - 46 Verzonden op 15 november 2019
Privacynieuws weekbrief - 45 Verzonden op 08 november 2019
Privacynieuws weekbrief - 44 Verzonden op 01 november 2019
Privacynieuws weekbrief - 43 Verzonden op 25 oktober 2019
Privacynieuws weekbrief - 42 Verzonden op 18 oktober 2019
Privacynieuws weekbrief - 41 Verzonden op 11 oktober 2019
Privacynieuws weekbrief - 40 Verzonden op 04 oktober 2019
Privacynieuws weekbrief - 39 Verzonden op 27 september 2019
Privacynieuws weekbrief - 37/38 Verzonden op 20 september 2019
Privacynieuws weekbrief - 37 Verzonden op 17 september 2019
Privacynieuws weekbrief - 36 Verzonden op 06 september 2019
Privacynieuws weekbrief - 35 Verzonden op 30 augustus 2019
Privacynieuws weekbrief - 34 Verzonden op 23 augustus 2019

Privacynieuws weekbrief - 33 Verzonden op 16 augustus 2019
Privacynieuws weekbrief - 32 Verzonden op 09 augustus 2019
Privacynieuws weekbrief - 31 Verzonden op 02 augustus 2019
Privacynieuws weekbrief - 30 Verzonden op 26 juli 2019
Privacynieuws weekbrief - 29 Verzonden op 19 juli 2019
Privacynieuws weekbrief - 28 Verzonden op 12 juli 2019
Privacynieuws weekbrief - 27 Verzonden op 05 juli 2019
Privacynieuws weekbrief - 26 Verzonden op 28 juni 2019
Privacynieuws weekbrief - 25 Verzonden op 21 juni 2019
Privacynieuws weekbrief - 24 Verzonden op 14 juni 2019
Privacynieuws weekbrief - 23 Verzonden op 07 juni 2019
Privacynieuws weekbrief - 22 Verzonden op 31 mei 2019
Privacynieuws weekbrief - 21 Verzonden op 25 mei 2019
Privacynieuws weekbrief - 20 Verzonden op 17 mei 2019
Privacynieuws weekbrief - 19 Verzonden op 11 mei 2019
Privacynieuws weekbrief - 18 Verzonden op 03 mei 2019
Privacynieuws weekbrief - 17 Verzonden op 26 april 2019
Privacynieuws weekbrief -16 Verzonden op 22 april 2019
Privacynieuws weekbrief - 15 Verzonden op 13 april 2019
Privacynieuws weekbrief - 14 Verzonden op 05 april 2019
Privacynieuws weekbrief - 13 Verzonden op 29 maart 2019
Privacynieuws weekbrief - 12 Verzonden op 22 maart 2019
Privacynieuws weekbrief - 11 Verzonden op 15 maart 2019
Privacynieuws weekbrief - 10 Verzonden op 09 maart 2019
Privacynieuws weekbrief - 9 Verzonden op 01 maart 2019
Privacynieuws weekbrief - 8 Verzonden op 22 februari 2019
Privacynieuws weekbrief - 7 Verzonden op 16 februari 2019
Privacynieuws weekbrief - 6 Verzonden op 08 februari 2019
Privacynieuws weekbrief - 5 Verzonden op 02 februari 2019
Privacynieuws weekbrief - 4 Verzonden op 25 januari 2019
Privacynieuws weekbrief - 3 Verzonden op 18 januari 2019
Privacynieuws weekbrief - 2 Verzonden op 11 januari 2019
Privacynieuws weekbrief - 1 Verzonden op 05 januari 2019

Doorlopende kwesties waar Vrijbit in verwikkeld was

Actie BSN-BTW-ZZP-WEG ERMEE

Om met het positieve bericht te beginnen: de actie BSN-BTW-ZZP-WEG ERMEE werd in 2019 succesvol afgerond. In oktober 2019 stuurde de Belastingdienst eindelijk aan iedere ZZPer een brief met een nieuw BTW nummer waarin het unieke persoonsregistratie nummer BSN niet meer is verwerkt. Zo werd na 12 jaar strijd, waarin Vrijbit een grote rol speelde, bereikt dat deze ondernemers vanaf 1 januari 2020 niet langer automatisch hun unieke persoonsregistratienummer prijsgaven aan derden via hun website en facturen voorzien van het BTW nummer.

De actie Kies-Keurig

In 2019 vonden 2 verkiezingen plaats. Namelijk die voor de Provinciale Staten en Waterschappen op 20 maart en die voor het EU parlement op 23 mei. Bij beide verkiezingen voerde Vrijbit opnieuw actie tegen de aanvullende identiteitsplicht bij verkiezingen. Door middel van voorbeeld protestbrieven en uitleg hoe zulke protesten verplicht verwerkt moeten worden in de proces-verbalen van de kieslokalen en zo indirect terecht komen bij de burgermeester als voorzitter van het hoofdstembureau en bij de Kiesraad. De Kiesraad had inmiddels laten weten formeel geen stappen te mogen zetten tot initiatief van het afschaffen. Daarom verzocht Vrijbit de minister en de Tweede Kamer om hiertoe het initiatief te nemen. We deden dit symbolisch op 27 september, de dag dat op de kop af 100 jaar geleden vrouwen kiesrecht kregen. Onder het motto ‘100 jaar vrouwenkiesrecht- maar nu wordt niemand meer vertrouwd door de overheid’

Stand van zaken eind 2019 was dat de minister een ondermaatse afwijzing stuurde waarop Vrijbit op 3-11-2019 een 'bezwaar op besluit' heeft ingediend en de vaste Kamercommissie van de Tweede Kamer liet weten dat men verzoek nu in een algemeen overleg in een openbare zitting aan de orde zou stellen.

Onderwijs/ registratie leerling gegevens

Vrijbit heeft in 2019 een start gemaakt met het aanleggen van een dossier over de gigantische hoeveelheid persoonsgegevens die wordt vastgelegd (en 25 jaar bewaard) en welke ontwikkelingen zich op dit gebied voordoen.

Met als belangrijke opzet om zicht te krijgen op wat er allemaal wordt vastgelegd in het basisregister onderwijs (BRON), het meldingsregister relatief verzuim, het diplomaregister en het register vrijstellingen en vervangende leerplicht. Hoe deze data beheerd worden door de Dienst Uitvoering Onderwijs (DUO) en (deels onrechtmatig) verzameld via o.a. onderwijsinstellingen- en koepels. Wat het wetsvoorstel ‘flexibeler gebruik leerling-gegevens, behelsde en hoe de toezichthouder AP onder de verschuilende aanduiding ‘Advies Algemene wet onderwijs’ als enige kanttekening aanbevelingen deed om het wetsvoorstel inhoudelijk ongewijzigd in te dienen *(na aanvulling van de motivaties om de grondslag juridisch te verankeren via vermelding dat het allemaal zou voldoen aan de eisen van doelmatigheid en proportionaliteit).* En wat er via het gebruik van de technologie door commerciële partijen wordt vastgelegd van kinderen en jongeren.

Naast dit onderzoek heeft Vrijbit ook concrete hulp geboden aan mensen die bezwaar maakten tegen de verplichting van de opleiding(o.a. In Holland) om hun privé onderwijsprestaties tot in detail op social media te posten en hulpvragers die in verzet kwamen tegen de praktijken van universiteiten en hogescholen om via het platform Studielink te doen voorkomen of men zich uitsluitend via internet kan inschrijven voor een opleiding.

Ook de hele digitaliseringsdwang binnen het onderwijs had onze aandacht. Zowel qua impact van bedrijven als Google op de lesstof en het effect van digitaal aanbieden van lesstof als van de communicatie met ouders via software applicaties op de computer/i-Pad.

Rechtszaken Vrijbit inzake verzoeken tot inzage vooraf van te vernietigen dossiers bij AIVD en MIVD

Op 15 januari 2019 diende voor de rechtbank Den Haag de beroepszaak van Vrijbit tegen de afwijzing van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) om inzage te geven in per dienst 10 aangevraagde inzage van dossiers die op de nominatie staan om als archief vernietigd te worden. De verzoeken werden op 31 maart 2017 gedaan toen via onderzoeksburo Jansen en Janssen bekend werd dat de dossiers voor historisch onderzoek verloren zouden gaan.

Op 13 september volgde de uitspraken [SGR18/2614 en SRG 18/2992] . Deze luidden dat het *beroep niet-ontvankelijk werd verklaard aangezien de rechtbank van oordeel was gekomen dat eiseres de bevoegdheid voor een ander doel had gebruikt dan waarvoor het bedoeld is en er derhalve sprake zou zijn van 'misbruik van recht'. Reden waarom de rechtbank niet aan een inhoudelijke behandeling was toegekomen.*

Wel werd nog specifiek vermeld dat de uitspraak de vereniging Vrijbit betrof. En de bestuursleden niet, zoals tijdens de procedure gepoogd was door de MIVD, op persoonlijke titel van misbruik werden beschuldigd. Proceskosten hoefden ook niet vergoed te worden.

Omdat de Raad van State als hoogste beroepsrechter in een andere, deels vergelijkbare zaak, al had aangegeven dat alle inzageverzoeken betreffende de te vernietigen dossiers beschouwd werden als misbruik (omdat ze de werking van de archiefwet te niet zouden doen als er van vernietigde archieven toch gegevens bewaard werden) heeft Vrijbit er van afgezien om tegen de uitspraak in eerste aanleg Hoger beroep aan te tekenen.



Rechtszaken onrechtmatige aanmeldingen EPD-LSP

In juli 2017 diende Vrijbit een handhavingsverzoek in bij de toezichthouder AP om op te treden tegen het feit dat de beheerder van het EPD-LSP (VZVZ) geen verantwoordelijkheid wenste te nemen dat er mensen in het systeem werden aangemeld die daar niet de vereiste toestemming voor hadden gegeven. Toestemming die voor de particuliere doorstart van het EPD als ultieme voorwaarde was gesteld. Toen duidelijk werd dat er, met name via apothekers, veel mensen werden aangemeld die daar geen toestemming voor hadden gegeven, diende Vrijbit enkele maanden later ook een

handhavingsverzoek over deze kwestie in om de apothekers aan te pakken. Na de inmiddels standaard reactie van AP om de zaak zoveel mogelijk te traineren was in februari 2019 het hele voortraject van afwijzing verzoek, bezwaar op besluit en besluit op bezwaar doorlopen. Daarop werd beroep aangetekend bij de rechtbank Midden-Nederland en vond op 15 oktober 2019 behandeling van de zaak op zitting plaats.

Voor de duidelijkheid dient vermeld te worden dat Vrijbit niet alleen eiste dat er een eind zou worden gemaakt aan de mogelijkheden om mensen aan te melden die daar bezwaar tegen hebben, die op grond van onjuiste informatie toestemming gaven, onder druk waren gezet om in te stemmen of onkundig waren van het feit dat de apotheek waar ze al jaren geen contact mee hadden hen had aangemeld. Vrijbit deed er alles aan om duidelijk te maken dat een uitwisselingsysteem met de meest gevoelige medische persoonsgegevens, dat deze data in principe toegankelijk maakt voor alle professionele zorgverleners en zorgverlenende instanties in Nederland ten minste van een deugdelijke logging–systeem zou moeten zijn voorzien waarbij direct inzichtelijk en controleerbaar zou moeten zijn wanneer wie op grond van welke informatie toestemming verleend zou hebben.

Citaat uit onze pleitnota 15-10-2019

Gelet op het grote belang van correcte verlening van specifieke geïnformeerde toestemming, voor de uitwisseling van medische persoonsgegevens via het Landelijk Schakel Punt(LSP), dient de procedure voor aanmeldingen, registratie van deze toestemming, zodanig te zijn geregeld binnen het LSP-informatiesysteem dat dit, wanneer daar aanleiding toe is effectief kan worden gecontroleerd en geverifieerd.

Het grote belang van een correcte en verifieerbare registratie van toestemming wordt ook expliciet onderschreven in de uitspraak van de Hoge Raad (d.d. 01-12-2017 ECLI NLHR 2017 3053) waarin wordt gesteld dat het LSP als veilig wordt beoordeeld indien en voor zover NIEMAND zonder toestemming in dit systeem kan worden opgenomen.

Het is aan VZVZ als systeemverantwoordelijke om vooraf erop toe te zien dat zorgverleners controleerbare en verifieerbare procedures hebben voor aanmelding en registratie van toestemming.

Om een lang verhaal kort te maken: in de rechtszaal werd bevestigd dat verweerder het niet bezwaarlijk vond dat de apothekers tot november 2018 mensen als informatie de VZVZ folders met gemankeerde informatie hadden verstrekt. Evenmin dat men de apothekers hard viel waarvan was aangetoond dat zij helemaal niet hadden aangegeven dat toestemming voor het LSP werd gevraagd, en het niet nodig had gevonden andere praktijken hierop te onderzoeken. Ook dat zelfs de Haarlemse apotheek, die glashard patiënten had aangemeld als zij daar niet voor een bepaalde datum bezwaar tegen hadden gemaakt, met fluwelen handschoenen door AP werd aangepakt en (zonder boeteoplegging) weg kwam met de belofte om de opt-in aanmeldingen gedeeltelijk terug te draaien. Ook voor de rechter bleef VZVZ volharden in haar stellingname dat het niet onder hun verantwoordelijkheid van de systeembeheerder zou vallen, maar de schuld van huisartsen en apothekers was, als mensen niet correct werden aangemeld.

Dat het simpel invoeren van een notificatieplicht al veel zou ondervangen, daar wilde men niet aan. En zo ontstond de enge situatie dat het weliswaar voor de rechter helder was dat mensen tegen hun wil konden/ waren aangemeld ondanks de vereiste expliciete toestemming. Maar dat hij daarin geen soelaas kon bieden omdat 'de wet geen schriftelijke toestemming verplicht stelt en het bij mondelinge aanmeldingen altijd een kwestie van welles nietes zal blijven als mensen aangeven dat ze geen toestemming gaven en toch werden aangemeld'. Ook het argument dat mensen zo geen enkele rechtszekerheid hebben omdat wie niet in het systeem wil worden opgenomen dan feitelijk dagelijks moet controleren om er van verzekerd te zijn dat men niet (niet weer) toch staat aangemeld, zette geen zoden aan de dijk.

Het resultaat van alle inspanningen was wel dat de rechter er op zitting voor gezorgd heeft dat de AP de signalen en argumenten van Vrijbit voortaan serieus dient te nemen, in plaats van per definitie de loopgraven in te duiken als er een beroep op hen wordt gedaan om in te grijpen bij evidente aantastingen van de wet bescherming persoonsgegevens. Op instigatie van de rechtbank nodigt AP Vrijbit voortaan regelmatig uit voor regulier overleg om, in plaats van tegen elkaar, samen te werken aan een betere bescherming van de privacyrechten.

De uitspraak begin 2020 liet zich raden. Maar zoals wel vaker het geval is bij langdurige juridische trajecten, had de praktijk bij voorbaat de hele uitkomst van de rechtsgang al achterhaald. In 2019 had onderzoek namelijk uitgewezen dat zorginfo uitwisseling op grond van 'specifieke toestemmingen' sowieso totaal onwerkbaar was. Waarop de minister aan de Kamer liet weten dat er niet langer ingezet zou worden op het invoeren van het wetsvoorstel 'Cliëntenrechten bij elektronische verwerking van gegevens' (33 509) maar voortaan gestreefd zou worden naar gegevensuitwisseling in de zorg binnen de behandelrelatie en niet met beschikbaarstelling vooraf. Zoals de EPD-LSP zorginfrastructuur waarbij gegevens niet binnen een behandelrelatie worden uitgewisseld maar gegevens vooraf opvraagbaar worden gemaakt voor nog onbekend later gebruik.

Dit wetsvoorstel waar o.a. Vrijbit zich vanaf de lancering in 2012 actief tegen heeft verzet blokkeerde een zorginfo uitwisseling gebaseerd op de behandelrelatie. Een basisprincipe waar Vrijbit altijd voor gepleit heeft. Met de ommekeer kwam eindelijk de erkenning voor de veiliger manier van zorginfo uitwisseling zoals via de Whitebox waarbij via push autorisatie zorgaanbieders of patiënten actief andere behandelende zorgverleners autorisatie verlenen voor het delen van patiëntgegevens.

Het dossier is daarmee beslist nog niet af te ronden, want VZVZ ging onverdroten voort met het verder uitbouwen van het LSP.

Rechtzaak DIS

Het DBc-informatiesysteem (DIS) van de NZa ontvangt en beheert informatie over alle behandeltrajecten in de medisch-specialistische, GGZ, forensische zorg en revalidatiezorg. Zorgaanbieders in deze sectoren hebben de wettelijke plicht om deze gegevens aan te leveren.

Op 23 juli 2019 deed de rechter in eerste aanleg uitspraak over de Vrijbit zaak tegen de AP wegens de weigering van de toezichthouder om een eind te maken aan de onrechtmatige

verzameling en verwerking van medische gegevens door Nederlandse Zorgautoriteit (NZA) via de het Diagnose Informatie Systeem(DIS). En de verstrekking hiervan aan derde partijen. Op 30 augustus tekende Vrijbit tegen deze uitspraak Hoger Beroep aan.

Eind 2019 was onbekend wanneer de Raad van State hierover een zitting zou plannen en duurde de juridische procedure tegen het DIS inmiddels al 4 ½ jaar. De rechtsgang heeft evengoed er inmiddels wel toe geleid dat de Nza veel minder data aan derde partijen verstrekt en sinds april 2019 ook de dataset die zorgverleners diende aan te leveren iets heeft ingeperkt.

Rechtzaak Gedragscode Zorgverzekeraar

Al sinds de oprichting van Vrijbit werden we gewaarschuwd dat de Zorgverzekeraars de hand lichtten met hun plicht om volgens een goedgekeurde gedragscode te werken bij het verwerken van persoonsgegevens (waaronder medische gegevens). Eerst weigerde de verzekeraars en hun samenwerkingsorganisatie ZN om zo'n gedragscode op te stellen. Men bleef gewoon doorwerken onder de gedragscode voor financiële instellingen zoals die gold voordat de overheid hen in 2006 de regie van de zorg in handen had gelegd. Vervolgens zag men zich, met name door actie van de KDVP, gedwongen om alsnog een eigen gedragscode op te stellen. waarop de rechtbank Amsterdam in 2013 oordeelde dat deze strijdig was met de fundamentele mensenrechten. De toezichthouder AP, die de gedragscode had goedgekeurd moest deze goedkeuring daarop intrekken, maar weigert tot op heden om de zorgverzekeraars te dwingen om zich aan een gedragscode te conformeren die wel de toets van EVRM kan doorstaan.

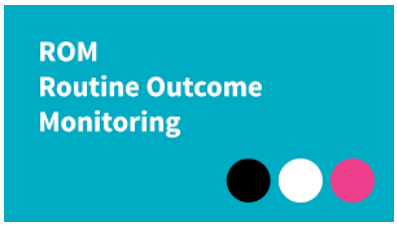
Op 23 juli deed de rechtbank Midden-Nederland in onze zaak tegen AP hierover uitspraak. Op 30 augustus tekende Vrijbit hiertegen Hoger beroep aan. Ook in deze zaak was eind 2019 onbekend wanneer de Raad van State het Hoger beroep [201906616/1/A3] zou gaan behandelen. Wel was, net als in eerste aanleg, het hele circus van geheimhouding van stukken van de zorgverzekeraars *(waaronder de cruciale onderzoeksvragen)* weer van start gegaan. En schakelde AP wederom de grootste zorgverzekeraars, waartegen zij moet optreden, in als mede verweerderende procespartijen.

De hele gang van zaken heeft tot nu toe enkel opgeleverd dat AP onderzoek uitwees dat medewerkers van Menzis en VGZ voor commerciële doeleinden onrechtmatig gebruik maakten van patiëntgegevens. Dat leverde Menzis in april 2019 een boete op van € 50.000, maar deed verder niet af aan het feit dat AP zich ten onrechte er vanaf had gemaakt met een ondermaats onderzoek naar alleen dit aspect van het overtreden van privacyrechten.

Intussen draaide Zorgverzekeraars Nederland de minister en de toezichthouder een rad voor ogen door op 17 april 2019 in een brief *(over het wetsvoorstel inzake marktwerking in de zorg (34 445)* te schrijven 'bezig te zijn met een herziening van de Gedragscode Verwerking Persoonsgegevens Zorgverzekeraars'.

Op 13 mei 2019 ging het wetsvoorstel 33 980, waarmee zorgverzekeraars zonder toestemming in medische dossiers mogen kijken bij een vermoeden van fraude, in elk geval van tafel. Dit wetsvoorstel dateerde uit 2012 en werd door de minister vlak voor de behandeling in de Eerste

Kamer ingetrokken. Een voorlopig succes ten gevolge van de actie die o.a. Vrijbit, in samenwerking met de Privacybarometer en KDVP, tegen dit wetsvoorstel hadden gevoerd.



Actie Stop Benchmark met ROM

ROM – Routine Outcome Monitoring-gegevens zijn door patiënten ingevulde vragenlijsten. Dat invullen gebeurt voor, tijdens en na therapie in de GGZ om daarmee het verloop van de behandeling met de therapeut te evalueren. Deze ROM-data werden door de Stichting Benchmark GGZ (SBG), een organisatie betaald door de zorgverzekeraars, verzameld om te analyseren en zorgaanbieders in te GGZ te vergelijken (benchmarking). Ook om er zorginkoop door zorgverzekeraars op te baseren.

Begin 2017 riep een groep patiënten, psychiaters, verpleegkundigen en psychologen op een eind te maken aan het verplicht moeten aanleveren van allerlei gegevens van patiënten aan SBG. Ze hadden zich verenigd onder de naam Comité Stop Benchmark met ROM. Vrijbit heeft dit comité van meet af aan gesteund omdat de gegevens veelal zonder toestemming van de patiënt naar SBG werden doorgezonden. Onrechtmatig dus omdat toestemming ondanks de pseudonimisering van deze bijzondere persoonsgegevens bij wet verplicht is.

Lange tijd heeft SBG volgehouden dat er niets onrechtmatigs gebeurde maar uiteindelijk kwamen er langzaam barsten in het SBG-bolwerk en beëindigde SBG de werkzaamheden.

Als opvolger nam Akwa GGZ, de werkwijze van SBG over en kwamen de gegevens die SBG verzameld had in de vorm van een “verarmde” database in handen van deze nieuwe organisatie. Maar uiteindelijk maakte men op 8 augustus 2019 bekend dat de historische ROM-database zou worden vernietigd.

Biometrische paspoort- en IDkaarten dossier

De rechtszaken tegen de vingerafdrukplicht voor paspoorten, de digitale gezichtsopname voor paspoorten- en ID-kaarten en de opslag van de biometrische gegevens in de RFID-chip van de documenten staan nog steeds in de wacht om behandeld te worden door het Europese Hof voor de Rechten van de Mens (EHRM). Dat betekent dat de 6 mensen die al vanaf 2009 verwikkeld zijn in een juridische procedure over dit aspect van de Paspoortwet, na doorlopen van de jarenlange nationale rechtsgang nu eindelijk hun zaak hebben kunnen voorleggen aan het hoogste mensenrechtenhof. Om een finaal oordeel te kunnen vragen over het feit dat de Staat zich systematisch en grootschalig meester maakt van de biometrische lichaamskenmerken van al haar burgers.

Tot nog toe heeft het EHRM meermalen zich al uitgesproken tegen het disproportioneel toe-eigenen van biometrische kenmerken door de overheid, in gevallen waarin het ging om personen die ooit veroordeeld waren voor strafbare feiten. Nooit eerder werd de principiële kwestie beoordeeld of een onschuldige burger zich terecht op het EVRM kan beroepen als men het onacceptabel acht dat lichaamskenmerken, die een onlosmakelijk deel van zijn of haar persoon uitmaken, moeten worden afgestaan aan de Staat.

Het Hof zit duidelijk met de zaken omhoog, volgens juridische experts, gezien het feit dat de indieners afgezien van een dossiernummer taal nog teken horen uit Straatsburg. Geen van de aanklachten is in elk geval niet ontvankelijk verklaard en geduld geldt als een schone zaak.

De urgentie voor de dossiers daarentegen neemt alsmaar verder toe. Met name waar het gaat om de opslag van de digitale gezichtsopname van de pasfoto in de overheidsdatabase dringt zich meer en meer op hoe indringende gevolgen een dergelijke database kan vormen voor het ontwikkelen van een totaal-surveillance systeem gebaseerd op digitale gezichtsherkenning.

Vrijbit, die de rechtszaken helpt coördineren, is dan ook volop in de weer om alle ontwikkelingen qua digitale gezichtsherkenning te blijven volgen en archiveren om bij behandeling van het EHRM te kunnen inbrengen.

Intussen speelde er een nieuwe zaak, die niet insteekt op de principiële weigering om biometrische data af te staan bij aanvraag van een identiteitsdocument, maar inzet op de eis dat de gegevens na aanmaak van het document zouden moeten worden verwijderd uit de database en onuitleesbaar zouden moeten worden gemaakt in de op afstand uitleesbare chip van het document. Ook hier begon het hele juridische steekspel weer met een besluit van de burgemeester, een bezwaar op besluit en besluit op bezwaar. Gevolgd op 11 oktober 2019 door een beroep op de rechter en zitting op 24 december 2019.

Intussen is, zoals hierboven al uitgelegd, er vanuit Europa de verplichting aan de lidstaten opgelegd om ook voor de ID-kaart verplicht vingerafdrukken in het document te gaan verwerken. Dat betekent dat vingerafdrukweigeraars- die na het afschaffen van de verplichting in 2014 in ieder geval weer over een geldig identiteitsdocument konden beschikken, nu terug bij af zijn als hun document verloopt (zolang het EHRM geen uitspraak heeft gedaan die dit verbiedt).

Waarbij, ter verduidelijking, de EU de verwerking ín het document verlangt en de Nederlandse regering zelf de discretionaire bevoegdheid heeft om te beslissen of ze de vingerafdrukken al dan niet in een eigen database gaan bewaren. met de vermelding dat actie voeren tegen de opslag in de nationale registers de vorige keer in elk geval er toe heeft geleid dat de vingerafdrukken, *die voor de paspoorten nog steeds worden opgeëist*, na uitgifte van de documenten worden verwijderd uit de databases en enkel in het document zelf geacht worden te blijven opgeslagen.

Vrijbit blijft onverminderd de personen steunen die de kwestie hebben aangekaart bij het EHRM evenals initiatieven tot verzet in het buitenland. Met name de actie stop de vingerafdruk van ‘het Ministry of Privacy’ in België, en oproepen via het actieplatform Freedom Not Fear om in verzet te komen.

Wordt vervolgd

Wijvertrouwenslimmemetersniet

Zowel de uitrol van de ‘slimme’meters als het verzet van mensen die deze meters niet accepteren bleef onveranderd doorgaan.

Dit jaar kreeg Vrijbit vooral hulpvragen van weigeraars die in een nieuwbouwhuis gingen wonen en stuitten op tegenwerking van de huiseigenaar om het recht van de bewoners op weigeren te

respecteren. Ook in gezamenlijk wonen complexen was dat het geval. De netbeheerders bleven mensen onder druk zetten met argumenten als: We kunnen geen analoge meters meer leveren en drogredenen dat de 'slimme' meter onontkoombaar was bij vervanging van een oude meter of een alternatief de bewoner geld zou gaan kosten. Veelvuldig kwam ook weer het argument langs dat een 'slimme' meter de enige optie zou bieden aan mensen die zelf energie opwekken om de overtollige energie te kunnen terugleveren.

Dat de installatie van de 'slimme'meters niet bedoeld was om de klant te helpen energie te besparen (zoals dat van oorsprong aan de man werden gebracht), heeft Vrijbit van meet af aan duidelijk proberen te maken. Nu in 2019, in het kader van de aanstaande energietransitie en de inzet op uitbouw van het elektrisch autoverkeer en Internet of Things (IoT), werd in steeds grotere kring bekend dat de 'slimme' bemetering van het energiegebruik tot inzet heeft om het gedrag van klanten te kunnen monitoren. *Dit om zowel de piekbelasting die energiemaatschappijen moeten kunnen leveren af te vlakken als om het beprijzen van het terugleveren van (zonne- en wind) energie te kunnen gaan vermarkten.*

Qua internationale wetgeving zag Vrijbit zich gedwongen om wederom de uiterst gecompliceerde wetswijziging te gaan bestuderen waarmee de EU de lidstaten verplicht om de wijzigingen in de Elektriciteitswet en de Gaswet te implementeren. *Formeel genaamd 'Richtlijn over gemeenschappelijke regels voor de interne markt voor aardgas, en over verordeningen over de oprichting van een Agentschap van de Europese Unie voor de samenwerking tussen energieregulators, over risicoparaatheid in de elektriciteitssector, over de interne markt voor elektriciteit, en over maatregelen om de gasleveringszekerheid veilig te stellen.'* Het wetsvoorstel voor implementatie werd op 10 september 2019 bij de Tweede Kamer ingediend en was eind 2019 daar na vele wijzigingen en amendementen nog steeds in behandeling.

Wel kwam er versterking voor het Vrijbit standpunt dat er grote gevaren en bezwaren kleven aan het op afstand kunnen volgen van het energieverbruik van kleine huishouders 'achter de voordeur'. En wel in de vorm van een publicatie op 18 oktober 2019 van de Europese dataprotectie toezichthouders(European Data Protection Supervisor-EDPS). In een technisch rapport waarschuwde de EDPS namelijk snoeihard dat ' een netwerk van slimme meters kan worden gebruikt voor massasurveillance van burgers' en ook dat 'het profileren en volgen van personen in hun dagelijks leven behoort tot de mogelijkheden'.

Systeem Risico indicatie(SyRI)

In september 2014 was Vrijbit de eerste organisatie die bij het Platform Bescherming Burgerrechten aan de bel trok over het, zonder discussie door het parlement aangenomen wetsvoorstel SyRI.

In 2019 diende voor de rechtbank den Haag de bodemprocedure van een coalitie van maatschappelijke organisaties tegen de Nederlandse Staat. Teneinde het risicoprofileringssysteem SyRI te doen stopzetten en een halt toe te roepen aan de risicoprofilering van onverdachte burgers door overheidsinstanties.

Hoewel Vrijbit geen deel uitmaakte van de coalitie van eisende procespartijen die de rechtszaak voerde, waren wij op de achtergrond wel één van de partijen die vanaf de start actief bij dit

initiatief betrokken was. De zaak werd op zitting behandeld in oktober 2019. Naarmate de tegenstanders zelfs ondersteuning kregen vanuit de hoogste commissaris voor de mensenrechten van de VN, en bekende Nederlanders in de pers veel aandacht voor het systeem wisten te genereren, werden de vooruitzichten voor een positieve uitspraak (voorzien in februari 2010). optimistisch. Terwijl de tegenstand tegen het systeem al zodanig gegroeid was dat gemeentes bij voorbaat het gebruik van SyRI al hadden stopgezet.

Omdat de overheid al een tweede wetsvoorstel op stapel had staan, om uitwisseling van persoonsgegevens van de burger op grote schaal wettelijk te legitimeren, bleef Vrijbit er steeds op hameren dat waakzaamheid geboden was om niet enkel op SyRI te focussen waarbij de aandacht zou verslappen voor de voortgang van het wetgevingsproces van het conceptwetsvoorstel 'gegevensverwerking door samenwerkinsverbanden-WGS) alias' SyRI-PLUS of 'overheid mag alles'.

Mini acties

Identificatieperikelen

Opnieuw hielp Vrijbit personen die in verzet kwamen tegen onrechtmatige identiteitscontrole. Zoals tegen bedrijven die onrechtmatige eisen stelden aan het moeten aanleveren van een identiteitsbewijs, geen kopietje paspoort accepteerden waarop het BSN onleesbaar was gemaakt of een gezichtsscan als voorwaarde voor toegang stelden.

In het verlengde hiervan voerde Vrijbit ook constant actie tegen allerlei praktijken van particulieren en bedrijven om via camera opnames identificeerbare opnames te maken waarvan dit niet is toegestaan. Van registraties door particuliere camera's in de publieke ruimte, ongevraagde opnames tijdens bijeenkomsten, posten van foto's op internet door particulieren.

Actie ticketverkoop en digi aanmeldingen

Zowel vanuit de vereniging zelf als door een aantal van onze leden werd consequent bezwaar aangetekend bij organisaties die geen mogelijkheid boden voor alternatieven voor digitale aanmeldingen of ticket verkoop. Waarna vaak bleek dat men zich helemaal niet gerealiseerd had dat dit mensen buiten sluit of dat er wel degelijk een andere mogelijkheid was (maar men die voor het gemak liever niet vermeldde). In tegenstelling tot de oplossing die vanuit Bits of Freedom gepromoot werd om domweg geen correcte gegevens door te geven in dergelijke gevallen, koos Vrijbit ervoor om altijd de discussie aan te gaan met de betreffende organisatie en daar aan te dringen op het wel realiseren en vermelden van andere mogelijkheden. Vaak met succes tot gevolg.

Cookie beleid

In meerdere gevallen heeft Vrijbit organisaties aangepakt die zich schuldig maakten aan praktijken waarbij men wettelijke voorschriften overtrad door geen melding te maken van het gebruik van tracking cookies(die informatie doorspelen aan derde partijen) of enkel toegang verleende tot informatie op de website als de bezoeker integraal toestemming geeft voor het gebruik van noodzakelijke bestanden voor het onderhouden van een website en bestandjes die het internet gedrag van personen door de tijd kunnen volgen.

Met name onze actie hierover tegen het bestuur van ECP het Platform, dat zich ten doel stelt om een betrouwbare digitale samenleving op te bouwen, kreeg de wind van voren. Deze organisatie dacht de cookiewetgeving te kunnen omzeilen met een systeem waarbij mensen uitsluitend gebruik konden maken van hun informatievoorziening als men vooraf akkoord ging met alle geplaatste cookies die men dan (op ECP aanwijzing) achteraf op omslachtige wijze en via andere websites weer van de computer zou kunnen verwijderen. ECP beloofde hierop het systeem aan te passen. Wat tevens doorwerking had op alle organisaties en bedrijven waar ECP op dubieuze wijze een voorbeeld aan had voorgeschoteld om de wettelijke cookievoorschriften te omzeilen.

Contante betaling

Op de Algemene ledenvergadering 2018 werd er op aan gedrongen om het verzet niet op te geven tegen de druk om het cash geld af te schaffen. Dat gebeurde dit jaar voornamelijk in de vorm van prikacties van een deel van onze leden die in winkels en horeca de moeite bleven nemen om bezwaar te maken als er enkel pinbetalingen worden geaccepteerd. Ook door onvermoeibaar aan mensen te blijven uitleggen dat elektronisch betalen direct gevolg heeft voor het minutieus kunnen volgen van iemands gedrag. Wat inhoudt dat het vastleggen van iemands financiële digitale sporen niet alleen door commerciële bedrijven kunnen worden gebruikt voor het aanleggen van te exploiteren klantprofielen, maar via opvraag ook beschikbaar zijn voor opsporingsdiensten als politie en sociale recherche en integraal voor de geheime diensten.

Ook naar de gemeente Utrecht werd actie ondernomen waardoor deze haar formulieren moest aanpassen voor het aanvragen van een paspoort of ID-kaart. Formulieren waarbij via de zinsnede ’vergeet niet uw pinpas mee te nemen’ gesuggereerd werd dat uitsluitend per pin betaald konden worden.

Vrijbit zelf blijft in elk geval principieel vasthouden aan de mogelijkheid om donaties en contributies contant te betalen, ook al levert dat niet de meest efficiënte manier van boekhouden op.





te bestellen Vrijbit Stickers

Actie tegen digitale gezichtsherkenning

Actie tegen het ongevraagd fotograferen en filmen bleef onverminderd belangrijk. Zowel door de inzet van leden en andere geestverwanten die hier niet van gediend zijn om voortdurend alert te zijn en bezwaar te maken als mensen zonder toestemming digitale opnames maken en deze (willen) gebruiken voor het posten op internet.

Als vereniging zijn we inmiddels bekend als de bonte hond die bij iedere bijeenkomst waar we aan deelnemen er op toeziet dat het expliciet vermeld moet worden als men personen herkenbaar gaat fotograferen of filmen. En aangeeft dat er een alternatief dient te worden geboden aan personen die hier bezwaar tegen hebben.

Waar dit enkele jaren terug nog vaak op negatieve reacties stuitte bleek in 2019 dat Vrijbit in gezelschappen steeds vaker bijval kreeg van personen die ook bezwaar maakten (en dat doorgaans niet uit eigen beweging hadden durven aankaarten). Gelukkig bleek ook dat er steeds vaker organisaties en debatgelegenheden zijn waar men vooraf gezorgd heeft voor een alternatief zoals het dragen van een button, bepaalde hoek van een zaal niet filmen of enkel het publiek onherkenbaar in kaart brengen.

De stickers 'houd u er rekening mee… ' vonden in beide talen grote aftrek.

Actie tegen PSD2

In 2019 begon met het opzetten van een bronnenarchief over de nieuwe betaalwetgeving en discussie hoe dit het beste aan te pakken, de actie PSD2-niet-zonder-mijn-toestemming.

Intern functioneren

Informatie-Documentatie

Intern bestond het werk van de vereniging weer voor een belangrijk deel uit het verzamelen en verwerken van de gigantische hoeveelheid informatie op het gebied van privacybeperking die dag na dag beschikbaar kwam via publicaties, media, presentaties, symposia, debatten etc.

Dit verzamelen en verwerken van informatie is nodig om op de hoogte te blijven van actuele ontwikkelingen om ons informatie/advieswerk, hulpverlening, politieke lobby en juridische procedures te kunnen onderbouwen met relevante informatie.



Wekelijks werd zowel het digitale als het knipselarchief bijgewerkt.

Dagelijks publiceerde onze medewerker van de Privacynieuwsdienst artikelen met relevante actuele informatie. Waarvan ook wekelijks een nieuwsbrief gemaakt werd.

Op individuele basis verzorgden we daarnaast via mail en 'life' gesprekken informatie over tal van privacyonderwerpen:



- Via inbreng bij tal van debatten en bijeenkomsten over de Privacy. Waaronder het EU Privacy Platform, ECP/Nictiz bijeenkomsten over inzet van AI en ethiek in de zorg. i-Poort debatten. Pinksterlanddagen. Utrecht- in-Dialoog bijeenkomsten.
- Aan andere Privacy- en Burgerrechtenorganisaties
- Aan de pers (NRC, AD, de Correspondent, Buiten de Orde, AVRO-TROS)
- Aan de regering, Tweede en Eerste Kamer, B&W's in Nederland en leden van gemeenteraden
- Aan de Autoriteit Persoonsgegevens, het Rathenau instituut en de Kiesraad
- Aan de rechtbank
- Aan netwerkbeheerders en woningbouwverenigingen.
- Aan het UWV en de Belastingdienst.
- Aan het Nederlands Juristen Comité voor de Mensenrechten(NJCM), het Public Interest Litigation Project (PILP), Platform Bescherming Burgerrechten, Bits of Freedom en Stichting Privacy First.
- Aan de vereniging van praktijkhoudende huisartsen, de stichting KDVP, de Stichting Beroepseer en actiecomité Stop Benchmark ROM
- Aan de Stichting ondersteuning ongedocumenteerden STIL
- Aan leerlingen en studenten in verband met studieprojecten.

Privacynieuwsdienst 2019

Afgelopen jaar gaf weer een licht stijgende lijn te zien qua bezoekersaantallen voor privacynieuws.nl
Gemiddeld aantal dagelijkse bezoekers 5000
Gemiddeld lezen die 4 artikelen per bezoek.
Afgelopen 12 maanden bezochten 1.492.587 bezoekers onze website.
Tezamen lazen die ongeveer 8.891.189 artikelen.

Op dit moment staan er ruim 18.500 artikelen op de website. Een stijging sinds het vorige jaarverslag van bijna 1000 artikelen. De website wordt steeds drukker bezocht en bijna alle artikelen halen binnen een week na plaatsing meer dan 1000 hits. Het best bezochte artikel het afgelopen jaar haalde meer dan 4650 hits. Ook zie je dat de oude artikelen nog steeds bezoek krijgen...zelfs die uit het prille begin.

De absolute topper overall is een artikel uit 2014 over het nieuws dat IBM mag rondneuzen in pc's van ING klanten, deze heeft 23479 bezoekers gehad.

In totaal zijn de artikelen op de website bijna 21 miljoen keer bezocht sinds de oprichting.

Ook het aantal abonnees op de nieuwsbrief groeit gestaag, bij het jaarverslag 2018 was dat 916 en nu staat de teller op een geschoond aantal van 1040 abonnees. De abonnee die de nieuwsbrief het langste ontvangt sinds de website overging van Freedom-not-Fear naar PrivacyNieuws doet dat sinds 10 april van 2010. Uit deze FnF tijd zijn er nog altijd 180 abonnees !

Hulpverlening

De meeste vragen om hulp kwamen binnen via e-mail. Vaak rechtstreeks omdat mensen onze vereniging kenden of via internet ontdekten dat wij ons met bepaalde onderwerpen bezig houden. Regelmatig klopten mensen ook aan die door andere 'privacyorganisaties' waren doorverwezen. Ook kwam het regelmatig voor dat mensen die ons tegenkwamen ter plekke om hulp vroegen.

Die vragen betroffen een zeer uiteenlopend scala aan onderwerpen. We noemen in dit verband in willekeurige volgorde: de 'slimme meters', de algemene identificatieplicht, identificatieplicht banken, de vingerafdrukplicht voor paspoorten, eisen tot afgifte van biometrische persoonsgegevens door werkgevers en voor de justitiële DNA databank , ongewenst cameratoezicht en WIFI tracking in de publieke ruimte, screening door zorgverlenende instanties, plicht tot afgeven van persoonlijke gegevens voor het aanvragen sociale voorzieningen, kentekenparkeren, digi drang en dwang, problemen met ziekenhuis apotheken die weigerden om door de arts voorgeschreven medicijnen te verstrekken als mensen geen toestemming gaven voor het EPD-LSP.

De hulpverlening varieerde qua zwaarte. In een deel van de gevallen konden mensen veel zelf doen en vroegen voornamelijk om raad of om conceptbrieven na te kijken. Maar ook waren er mensen die intensievere begeleiding vroegen om bepaalde problemen op te lossen.

Websites

Om onze doelstellingen te verwezenlijken onderhouden wij de volgende 7 websites:

https:// www.vrijbit.nl

https:// www.privacynieuws.nl

https:// www.id-nee.nl (archief)

https:// www.ikgeentoestemming.nl

https:// www.wijvertrouwenslimmemetersniet.nl

https:// www.louisetegendepaspoortwet

Naast het technisch onderhoud en de beveiliging van de websites werd ook dit jaar weer verder geïnvesteerd in het publiceren van nieuwe artikelen en 'up to date ' houden van de diverse chronologische overzichten van verschillende dossiers.

Vergaderingen

Iedere eerste zondag van de maand (met uitzondering van augustus) vond er een ledenvergadering plaats van 14-16 uur op onze locatie Kruisweg 32 in Utrecht. Belangstellenden waren op aanvraag welkom.

Tijdens deze bijeenkomsten kregen aanwezigen het verslag van de werkzaamheden van de afgelopen maand uitgereikt en de notulen van de vorige vergadering. Aan de orde kwamen verder:

Toelichting op de stand van zaken van de actueel onder handen zijnde dossiers,

Privacynieuws en overzicht van komende (privacy gerelateerde) bijeenkomsten, en

De mogelijkheid om bepaalde onderwerpen uit te diepen en/of te brainstormen over aanpak en werkwijze van Vrijbit.

Daarnaast vond op 23 juni de statutair verplichtte Algemene Leden Vergadering plaats. Waar het jaarverslag, de beleidsvoornemens, bestuurswisseling en vaststelling van de kascommissie aan de leden ter stemming werden voorgelegd.

<u>Werkverslagen</u>

Voor intern gebruik werd maandelijks een nauwgezet overzicht bijgehouden van alle activiteiten.

<u>Leden</u>



Ook het bijwerken van de ledenadministratie gebeurde op maandelijkse basis. Het aantal leden stond eind 2019 op 200 Nieuwe leden meldden zich doorgaans aan via de advertentie in het ZOZ tijdschrift van stichting de Omslag.

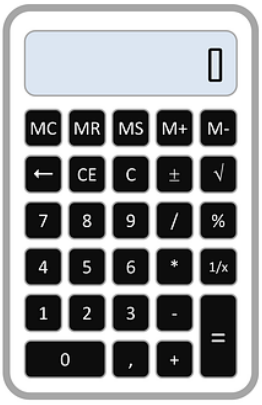
Slechts een klein deel van de leden was in de gelegenheid om zich actief in te zetten voor het Vrijbitwerk. De werkzaamheden bestonden daarbij vaak uit de inzet voor kwesties waar men persoonlijk via een aantasting van de privacy bij betrokken was geraakt. Sommige leden leverden een bijdrage op grond van hun specifieke kennis of vaardigheden op een specifiek gebied of met betrekking tot specifieke dossiers. Anderen hielpen met het verspreiden van actiemateriaal, bezoeken van bijeenkomsten en brainstormen over hoe zaken aan te pakken.



Voor de toekenning van de Vrijbit Privacy Prijs 2019 is genomineerd: Ab van Eldijk.

Wegens zijn niet aflatende inzet voor de privacy van patiënten, behoud van het medisch beroepsgeheim en doen stopzetten van het profileringssysteem SyRi.

Financieel Jaaroverzicht 2019



Saldo 1-1-2019: € 4.670,81

Saldo 31-12-2019: € 1.841,22

Totaal inkomsten 2019 € 5.506,83

Totaal uitgaven 2019 € 8.414,42

Specificatie inkomsten 2019

Contributies lidmaatschap € 610,00

Donaties …… € 3.329,35

Actiemateriaal ……. € 155,00

Restitutie griffie ……. € 1.121,00

Restitutie NS…… € 53,00

Restitutie huur locatie …… € 138,48

Aanvul fysieke kas door

opname eigen rekening ….€ 100,00

Specificatie Uitgaven 2019

Bureau artikelen…….. € 246,54

Catering ……€ 351,00

Telefoon/Internet ……..€ 751,56

Auteursrechten…… € 339,35

Vakliteratuur……. € 95,00

Kranten/tijdschriften € 1.012,00

Advertentie……. € 60,00

Webkosten…….. € 1.762,80

Reiskosten ……. € 496,24

Frankeerkosten……. € 64,10

Productie actiemateriaal € 22,41

Kosten betaalverkeer € 166,84

Griffiekosten…… € 1.728,00

Huur locatie/kramen € 1.086,08

Toegang tickets……. € 32,50

Dat er ondanks de beperkte financiële middelen zoveel werk verzet werd, is te danken aan de inzet van de vrijwilligers die zich, zonder enige onkostenvergoeding, inzetten zodat alle inkomsten voor 100% rechtstreeks aan het werk ten goede komen.

Via deze weg willen we, ook dit jaar weer, deze mensen hartelijk danken voor al hun tijd en energie. Ook alle donateurs danken we nogmaals voor hun onmisbare steun!

Steun Vrijbit door lid te worden,
u bent al lid van Vrijbit
voor een tientje per jaar.

Vrijbit opereert volledig zonder
subsidies en is afhankelijk van
donaties en de ledencontributies.

Vrijbit wordt door de Belastingdienst
aangemerkt als:
Algemeen Nut Beogende Instelling.
Giften komen voor 100%
rechtstreeks ten goede
aan het werk van Vrijbit.

Meer informatie over het lidmaatschap
vindt u op onze website
https://www.vrijbit.nl

Burgerrechtenvereniging Vrijbit
Kruisweg 32
3513 CT Utrecht
bestuur@vrijbit.nl
KvK:30242891
Banknummer Triodosbank:NL02TRIO0786722479

Namens het bestuur,

J.M.T.(Miek) Wijnberg, voorzitter