Burgerrechtenvereniging VRIJBIT

www.vrijbit.nl

Inhoudsopgave

Inleiding 3

Algemene ontwikkelingen in 2020 4

Werkzaamheden Vrijbit 2020 8

- Intern functioneren 8
- Werkverslagen 9
- Bijeenkomsten 9
- Lopende dossiers 10
  - Stagnatie juridische procedures tegen de Paspoortwet 10
  - Stagnatie juridische procedures tegen schendingen van de Privacy en het medisch beroepsgeheim 11
  - Gedragscode Zorgverzekeraars Nederland 11
  - EPD-LSP 12
  - Mitz 13
  - Donorregistratie 14
  - Actie tegen toestemmingsvraag aanmeldzuilen Tergooi-ziekenhuis 16
  - De actie Kies-Keurig 16
  - ACTIE Wijvertrouwenslimmemetersniet 17
  - Betalingsverkeer 18
  - Acties tegen digi drang-en dwang 18
  - Praktisch 20

Websites 21

Ledenbestand 21

Financieel jaaroverzicht 22

- Specificatie inkomsten 2020 23
- Specificatie Uitgaven 2020 23

Beleidsvoornemens Burgerrechtenvereniging Vrijbit 2021- 2022 24

Acties 24

Informatie voorziening 25

Advisering en hulpverlening 25

Samenwerking 25

Websites 25

Intern 25

Slotwoord 26

Inleiding

Dit jaarverslag over 2020 staat onvermijdelijk in het teken van de, dit jaar ook in Nederland, losgebarsten Covid-19 virus pandemie. Dit geldt voor de informatie over de stand van zaken, aangaande de privacy in het algemeen, het intern functioneren en de werkzaamheden van Burgerrechtenvereniging Vrijbit.

shutterstock.com · 1742199671

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 2020

Door de uitbraak begin 2020 in Nederland van Covid-19 mogen we stellen dat het een bizar jaar werd. Ondanks het feit dat er door wetenschappers al jaren gewaarschuwd wordt voor een pandemie werden de meeste burgers, overheden op alle niveaus en medische instellingen totaal overrompeld.

Door tal van redenen liep de bestrijding van het coronacrisis qua overheidsbeleid niet altijd even soepel en zorgvuldig. Grote bezuinigingen binnen de GGD's en afhankelijkheid van landen als China en India met betrekking tot medicijnfabricage bleken nu een direct probleem.

Ook door de marktwerking in de zorg, waardoor de medische zorg zodanig werd gedwongen tot minutieuze prestatieverantwoording dat effectieve zorgverlening en samenwerking tussen zorginstellingen werd tegengegaan, werd de bestrijding van het virus logistiek binnen de zorgsector eveneens een chaos. Zo moesten binnen de zorgsector ziekenhuizen, zorginstellingen, thuiszorgorganisaties, huisartsen en de 25 verschillende Gemeentelijke Gezondheids Diensten enerzijds volgens eigen plan zien om te gaan met het testen van mensen, regelen van beschermingsmiddelen, zoeken van opvangplekken enz. en kregen anderzijds vanuit de politiek opdrachten waartoe men helemaal niet was voorbereid.

Het kabinet nam formeel al snel de politieke verantwoordelijkheid om op te treden als hoeder van de volksgezondheid. In de paniek werd soms totaal voorbij gegaan aan grondwettelijke bepalingen en werd er een, volgens ons, ongerechtvaardigd vertrouwen gesteld in technologische oplossingen voor een besmettings-detectiesysteem.

Het beleid leunde zwaar op de invloed van de discussies in tv-praatprogramma's en de rol van de Tweede Kamer was mede bepalend voor het hapsnapbeleid. Door onder andere kennisgebrek werd er bijvoorbeeld geëist dat er meer IC-bedden moesten komen zonder dat daar voldoende personeel voor was en werd er ingestemd met noodmaatregelen waarvan de juridische basis niet deugde.

Zelfs tijdens de crisis bleef voor sommige politici de partijpolitiek prevaleren boven het collectief belang zoals het bewust tegenwerken van maatregelen voor eigen gewin, denk aan; afstand houden tot mensen hoeft niet, mondkapjes zijn onzin, het is een complot, het is maar een (zware) griep etc.

Het beleid omvatte tal van inperkende maatregelen zoals we allemaal weten; mensen werden verplicht afstand tot elkaar te houden, samenkomsten werden verboden, werkplekken en scholen werden gesloten, invoering van de avondklok, mondkapjesplicht etc. Allen uiteraard immense inperking van de persoonlijke vrijheid. Maar wel met dien verstande dat daarmee op zich nog geen inbreuk werd gemaakt op het recht op bescherming van de persoonlijke levenssfeer. Waar de persoonlijke vrijheid van de een, om de meest elementaire hygiënemaatregelen en voorkomen van besmettingsgevaar te willen negeren, ziekte en dood van anderen tot gevolg heeft, stuit het recht op privacy immers op de grens van het toelaatbare in een sociale samenleving.

Het uitgangspunt van Vrijbit is dat voor het recht op bescherming van de persoonlijke vrijheid geldt dat het gaat om een fundamenteel burgerrecht. Voor zover dat niet schadelijk is voor anderen.

Wel zijn wij van mening dat tal van noodverordeningen veel te lang van kracht waren zonder dat daar een wettige basis voor was. Na de vele kritiek op de spoedwetgevingsvoorstellen medio 2020 die een grondslag beoogde te creëren om per decreet te kunnen regeren en controles achter de voordeur mogelijk te maken, werd het voorstel ingrijpend gewijzigd. Op 1 december werd vervolgens de 'tijdelijke wet maatregelen Covid-19' van kracht, en daarmee de wettelijke grondslag verankerd. Vrijbit is evengoed van mening dat de juridische basis voor de coronawetgeving op veel vlakken onvoldoende is voor de verregaande maatregelen omdat het systematisch ontbreekt aan voldoende onderbouwing met betrekking tot de noodzakelijkheid qua effectiviteit, proportionaliteit en mogelijke alternatieven. Wat betekent dat waar niet voldaan werd aan de formele randvoorwaarden qua doelbinding, subsidiariteit en proportionaliteit, waaraan overheidsingrepen op de persoonlijke vrijheid dient te voldoen, er alsnog af te dingen viel op de rechtmatigheid van de maatregelen, ook toen deze in formele wetgeving waren vastgelegd.

Deze kwestie speelt uiteraard niet alleen op landelijk niveau. Vandaar dat we het statement van Privacy International op 2 april publiceerde van harte steunen. Samen met meer dan 100 Burgerrechtenorganisaties die via deze weg op acht concrete punten regeringen opriepen om (ook) bij de bestrijding van Corona de mensenrechten te blijven respecteren.

We willen tegelijkertijd aangeven dat Vrijbit met bovenstaande statements en mening niets te kort wil doen aan de gigantische inspanningen van medisch- en zorg personeel, wetenschappers en tal van politici om de beste maatregelen te treffen om patiënten zo goed mogelijk te kunnen verzorgen en de verspreiding van het virus zo veel mogelijk te beperken. In het bijzonder voor directe hulpverleners die vaak, met gevaar voor eigen leven en gezondheid van hun naasten, aan het werk bleven. Zij werden extra zwaarbelast werden door het ontbreken van een duidelijk rampenplan en helderheid over wie verantwoordelijk was voor allerhande regelingen en beslissingen.

Als voorbeelden voor dit laatste kennen we allemaal de drama's die zich afspeelden in de verzorgingshuizen en thuiszorg zonder dat deze sectoren zelfs maar deel konden nemen aan het beleidsbepalende Outbreak Management Team (OMT) waardoor personeel maandenlang verstoken bleef van elementaire beschermingsmiddelen, heel veel corona diagnoses gemist- en niet meegeteld zijn, iedere organisatie maar zelf moest uitzoeken hoe om te gaan met besmettingsgevaar van bewoners en bezoekers etc. Chaos qua test- en vaccinatiebeleid werden mede veroorzaakt door de versnippering van verantwoordelijkheden, uitvoeringsorganisaties, gebrek aan correcte registratiesystemen en inconsistente overheidsopdrachten.

Dat het in een rijk klein land als Nederland, met een (formeel) hoogopgeleide bevolking, een fijnmazige computer- en internetinfrastructuur, niet mogelijk bleek te zijn om adequaat bij te houden welke mensen getest, dan wel gevaccineerd zijn zonder dat hun persoonsgegevens op straat komen te liggen, zou onmogelijk dienen te zijn. Hetgeen ook geldt voor het totaal onderschatten van de technologische oplossingen als corona meldingsapplicaties voor het in kaart kunnen brengen van de verspreiding van het virus en fraudegevoelige, ondoordachte, ad hoc ontwikkelde toegangssystemen voor reis- en bezoek mogelijkheden.

Dat de persoonsgegevens uit twee GGD coronasystemen werden verkocht is onvergeeflijk. Dat er tussen neus en lippen door geregeld werd dat de medische gegevens van iedereen, die niet uitdrukkelijk had aangegeven niet in het landelijk uitwisselingssysteem EPD-LSP opgenomen te willen worden, werden opengesteld voor inzage van alle professionele zorgverleners is ten principale strijdig met de uitdrukkelijke bepaling dat niemand in dit (particuliere) systeem wordt opgenomen ténzij men daar uitdrukkelijk vooraf en welgeïnformeerd toestemming voor verleent. We gaan hier later in dit jaarverslag verder op in.

De regering heeft van deze periode gebruik gemaakt om verregaande wetgeving, inzake het ongelimiteerd mogen uitwisselen van ieders persoonlijke gegevens, door te zetten. Niet gehinderd door het feit dat de rechter het risicoprofileringssysteem SyRI op 5-2-2020 in strijd met de mensenrechten verklaarde. Zonder zich ook maar iets aan te trekken van het Toeslagenrampscenario poogde de regering de wet SYRI-2.0 (formeel wet Gegevensverwerking door Samenwerkingsverbanden) door de Kamer te loodsen.

Een ander voorbeeld zijn de inspanningen van staatssecretaris van Arkel (VWS) om de coronacrisis te gebruiken als argument om de al zolang gewenste doorbreking van het recht op privacy van patiënten en het medisch beroepsgeheim om zeep te helpen(Kamerstuk spoedhulpverlening 27 529, nr. 230).

De jacht op het verzamelen van gedragsgegevens van de burger door gemeentes ging onverdroten voort. Defensie richtte zelfs een nieuwe eenheid op – het LIMC- om onder het motto van ‘beeldopbouw van de coronacrisis’, zonder de bevoegdheid daartoe te hebben en zonder toezicht, privégegevens van burgers te gaan verzamelen.

Ook het extra toezicht van de TIB (toetsingscommissie Inzet Bevoegdheden) op de toepassing van de wet op de inlichtingen- en veiligheidsdiensten, op het verzamelen van bulk informatie via internet, dreigde alsnog te verdwijnen. De burgers die dit toezicht hadden afgedwongen door het referendum tegen de Wiv-2017 (wet op inlichtingen- en veiligheidsdiensten) bleven goeddeels onkundig hierover door de lawine van chaotische overheidsvoorlichting die totaal gedomineerd werd door de coronaberichtgeving.

De coronacrisis had ook grote gevolgen voor de verdere digitalisering van de samenleving. Grote opgang maakte het beeldbellen, het digitaal vergaderen en thuiswerken, het digitaal boodschappen bestellen en het volgen van online onderwijs en afleggen van ‘thuisexamens’. Negatieve uitwassen zijn veelvuldig in de media geweest zoals privacyinbreuken door het in beeld brengen van de privéwoonruimte van studenten en werknemers tot cybercriminaliteit van identiteitsfraude tot afpersing.

De Autoriteit Persoonsgegevens noteerde in 2020 25.590 klachten over privacyschendingen en 23.976 datalekmeldingen met een toename van 30% gevallen van hacking, malwareof phishing-incidenten in 2020.

De gevolgen van uitsluiting en achterstelling van grote groepen in de samenleving die niet mee kunnen of willen komen met een verregaande gedigitaliseerde samenleving blijven substantieel. Alleen al de gevolgen voor de 2 ½ miljoen Nederlanders die als ‘laaggeletterd’ te boek staan maken duidelijk dat zij buiten de boot vallen bij online informatievoorziening en dienstverlening. Bron: Feiten en cijfers digitale inclusie 2020 file:///C:/Users/vrijbit/AppData/Local/Temp/boekje-feiten-en-cijfers-digitale-inclusie-2019-2020.pdf

Intussen stonden daarentegen de ontwikkelingen niet stil om via de Europese Unie meer grip te krijgen op de macht van de grote internetgiganten. De regelgeving uit 2000 voldeed niet meer omdat geen van de nu door de commissie als ‘zeer groot’ (meer dan 45 miljoen Europese gebruikers) aangeduide platformen toen al bestonden, en problemen als datamacht, desinformatie, filterbubbels en online radicalisering nog nauwelijks speelden. De Digital Services Act (DSA) beoogt de ‘fundamentele rechten’ van de Europese burger beschermen, terwijl de Digital Markets Act (DMA) ervoor moet zorgen dat machtige techbedrijven niet nog machtiger worden. Beide voorstellen werden eind 2020 door de Europese Commissie gepresenteerd. Zie: https://www.volkskrant.nl/nieuws-achtergrond/nieuwe-europese-wetten-moeten-grip-op-big-tech-krijgen~b4712e0d/?referrer=https%3A%2F%2Fwww.startpage.com%2F

Anderzijds werden via de EU de ontwikkeling van een e-ID en het gebruik van biometrie daarvoor wel doorgezet. Zo werd op 19 oktober 2020 het EU-id initiatief door de EU Commissie opgenomen in het werkprogramma 2021. Zie https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-eid.

Op nationaal niveau zagen we een toename van bewustzijn ten aanzien van de mogelijkheden tot het digitaal volgen van burgers en de uitsluiting van mensen die geen gebruik kunnen en/of willen maken van elektronische communicatie via internet. Deels te wijten aan bijvoorbeeld berichtgeving over de cononameldingsapp en de aanhoudende berichten over datalekken en nieuwe gevallen van gijzelsoftware, die een bedreiging vormden voor de bescherming van personen en het functioneren van instanties, bedrijven en vitale sectoren van de samenleving.

Uit onderzoek bleek dat negentig procent van Nederlanders in 2020 op de een of andere manier maatregelen had genomen om persoonsgegevens op internet te beschermen. Bron: CBS
Zie https://www.cbs.nl/nl-nl/nieuws/2021/06/9-op-de-10-internetgebruikers-beschermen-persoonsgegevens

We constateerden een toenemende algemene kennis in de maatschappij over wat men zich moet voorstellen bij de, tot voor kort, als zeer abstract ervaren begrippen als het gebruik van algoritmes en kunstmatige intelligentie (AI).

Werkzaamheden Vrijbit 2020

Ter aanvulling op wat er in 2020 allemaal 'speelde' op het gebied van privacy verwijzen we naar de Privacynieuwsdienst. De dagelijkse berichten op deze Vrijbit-website geven een overzicht van de veelheid en verscheidenheid aan actuele privacy kwesties. Berichten die op de website zelf niet alleen chronologisch, maar ook op onderwerp te doorzoeken zijn. Daarnaast verzorgt onze onvolprezen privacynieuws-redacteur ook wekelijks een overzicht via de digitale nieuwsbrieven waarop men een (gratis) abonnement kan nemen.

Intern functioneren

Ter voorkoming van besmettingsgevaar werden de maandelijkse ledenvergaderingen dit jaar sinds maart afgelast. Alle communicatie tussen de leden vond daardoor plaats via e-mail, telefonisch of per papierpost. Ook aan de statutaire verplichting tot het jaarlijks organiseren van een Algemene Ledenvergadering werd op alternatieve wijze voldaan.

Het aantal directe hulpvragen bleef beperkt. De gevraagde hulp en informatieverzoeken betroffen onder andere:

- De aanhoudende druk van de netwerkbeheerders om (toch) tot de installatie van een 'slimme' energiemeters over te gaan en tegenwerking door netwerkbeheerders bij verwijderverzoeken.
- Eisen van particuliere instellingen, banken, bedrijven en onderwijsinstellingen, om voor dienstverlening onnodige persoonsgegevens beschikbaar te stellen.
- Algemene informatieverzoeken om toelichting op nieuwe betalingsverkeer-systemen als PSD2, op onze websites gepubliceerde informatie, en over nieuwe voorstellen voor wet- en regelgeving.
- Vragen om alternatieven waar uitsluitend digitale communicatiemogelijkheden werden geboden.
- Hulpverzoeken ter ondersteuning van juridische studies.
- Bijdrage voor onderzoek van het Montaigne Centrum voor Rechtsstaat en Rechtspleging van het departement Rechtsgeleerdheid en het Utrecht Institute of Linguistics van het departement Geesteswetenschappen van de Universiteit Utrecht, om inzicht te krijgen in hoe verschillende procespartijen rechterlijke uitspraken als tekst ervaren.
- Praktische adviesvragen over hoe rechtsgeldige verzoeken en klachten in te dienen en juridische procedures op te starten.
- Vragen over de nieuwe donorregistratie en zoekraken van de data uit het oude donorsysteem.
- Verzoeken tot ondersteuning van getroffenen van onrechtmatige bejegening door de Belastingdienst, politieagenten en gemeenteambtenaren.
- De nodige onbetamelijke verzoeken om geld en ondersteuning van viruswaanzinprojecten.

Werkverslagen

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

Bijeenkomsten

Door de coronacrisis kwam ook begin 2020 een eind aan het bijwonen van privacy bijeenkomsten. Voor die periode, in Januari , leverde twee medewerkers van Vrijbit inbreng op de EU Privacy conferentie in Brussel. Met name tijdens de sessies over 'data protection and artificial intelligence' over de ontwikkelingen qua gezichtsherkenning.

Op 8 januari namen we actief deel aan de bijeenkomst van Privacy First over de onderwerpen blockchain, Witwasrecherche en PSD2. Met als resultaat een vervolgoverleg om te kijken hoe we gezamenlijk het PSD2 systeem konden attaqueren.

Op 28 januari namen we deel aan de Nationale Privacy Conferentie in Den Haag

Op 1 en 2 februari namen we met een informatiekraam van Vrijbit deel aan het 2DH5 festival 'Defeating Distropia' in Utrecht. alwaar we succesvol actie voerden tegen ongevraagde video/foto registratie.

Op 10 maart gingen we voor het laatst op pad. Dit keer voor een vervolgoverleg met de Autoriteit Persoonsgegevens (AP), die ons in opdracht van de rechter voor dit reguliere overleg uitnodigde om te komen overleggen over de privacy kwesties waar Vrijbit tegenaan loopt,en de voorstellen die wij hebben ter verbetering van het toezicht op de bescherming van het recht op privacy.

Waar tot voor kort het optreden van AP als contraproductief werd ondervonden bleek in dit gesprek, met afdelingshoofd systeembeheer en 11 inspecteurs, dat de AP duidelijk op weg was om daadkrachtiger te gaan opereren.
Vrijbit hamerde op het feit dat de architectuur niet deugt van zowel de wijze waarop overheid met persoonsgegevens omgaat als hoe zaken in de zorg geregeld worden. Met als voornaamste signaal naar AP dat het van het grootste belang is dat AP gezien de grote complexiteit van de problemen men het toezicht zodanig vorm gaat geven dat het gericht wordt op de juiste richting waarin het beleid zich zal moeten omvormen naar een te bereiken veiliger en privacy vriendelijkere invulling.
Waarbij volgens ons de volgende als uitgangspunten dienen te gelden:

- AP moet gaan opereren vanuit een **kennis onderbouwde visie** *(i.t.t. tot aanpak via geïsoleerde binnenkomende deelproblemen/klachten en met name ook veel meer ICT expertise noodzakelijk is).*
- Dat AP- in tegenstelling tot haar houding tot nu toe altijd **principieel als uitgangspunt neemt dat men tot taak heeft om de burger te (helpen) beschermen**.
- Dat het gegeven dat het om de **bescherming van fundamentele rechten** gaat veel meer leidinggevend moet worden.
- Dat men **pro actief moet** gaan werken.

Vrijbit was aanwezig met 2 leden en Dhr. Vos als deskundige van Voswiz die creatieve en innovatieve '*out of de box*' oplossingen verzint voor (geo)data-infrastructuur en organisatieversterking en innovatie volgens *privacy-by-design* voor de (eerstelijns)zorg.

Lopende dossiers

Al jaren is Vrijbit verwikkeld in een aantal slepende procedures zoals:

- De acties tegen de opslag van biometrische gegevens door de overheid voor het verkrijgen van een ID-kaart of paspoort.
- Acties tegen toepassing van digitale gezichtsherkenningssoftware.
- De jacht op de medische persoonsgegevens door het pact van de Nederlandse Zorgverzekeraars en de overheid.
    - Zoals via het Diagnose Informatiesysteem van de Nederlandse Zorg autoriteit (NZa)(dossier DIS).
    - Middels de gedragscode Zorgverzekeraars die indruist tegen het EU Verdrag van de Rechten van de mens.
    - Via het Landelijk Schakelpunt (EPD-LSP)
    - Door uitbreiding bevoegdheden tot gebruik van DNA voor onderzoeksdoeleinden.
- Acties tegen ongebreidelde verzameling en uitwisseling van persoonsgegevens van onschuldige burgers door AIVD-MIVD, politiediensten, gemeentelijke overheden en hulpinstanties.
- Acties tegen risicoprofilering van burgers door overheids-en semi overheidsinstellingen middels het koppelen van data die voor verscheidene doeleinden werden verzameld en analysering daarvan door rekenkundige systemen waar de betrokkenen geen weet van heeft.
- Procedures tegen het opdringen aan de burger van 'slimme' systemen. Zoals voor energiebemetering, surveillance via trackingcookies op internet, (bel- en) camerasystemen, 'slimme' afvalcontainers t/m inzet van drones.
- Strijd tegen digitaliserings drang-en dwang.

Wat betreft de juridische procedures kunnen we stellen dat er in 2020 domweg geen enkele vordering te melden is omdat alle behandelingen daarvan werden uitgesteld.

Stagnatie juridische procedures tegen de Paspoortwet

Er staan sinds 2016 nog steeds 6 procedures in de wacht bij het EU Hof voor de Rechten van de Mens (EHRM) tegen de verplichte afname en opslag van vingerafdrukken en een digitale gezichtsopname voor het aanvragen en afgeven van een paspoort of ID-bewijs. Zaken die daar pas konden worden aangekaart nadat de nationale rechtsgang was uitgeput. Wat van 2009 tot 2016 heeft geduurd.

Sindsdien komt er al jaren taal nog teken van het EHRM in Straatsburg, behoudens af en toe een afkeurende brief dat betrokkenen niet naar de voortgang mogen informeren.
Extra schrijnend omdat de EU intussen de afgifte van vingerafdrukken, die met dank aan de Vrijbitacties in Nederland werd afgeschaft, alsnog aan de lidstaten verplicht om in te voeren (in Nederland wil men dit vanaf 2 augustus 2021 laten gelden).

Waardoor principiële vingerafdruk-weigeraars, zich na 13 jaar, zonder dat ze in die tijd een finaal oordeel van de rechter hebben kunnen krijgen, opnieuw gedwongen zien om zonder ID-bewijs te

moeten gaan leven. Waarmee we toch wel definitief moeten vaststellen dat het recht op faire beoordeling en toegang tot de rechter een absolute farce is. Ook al is dat als een van de fundamentele grondrechten vastgelegd in artikel 6 van het Europees verdrag voor de Rechten van de mens (EVRM).

Dat geldt ook voor de tweede procedure van voorzitster Wijnberg van Vrijbit inzake haar verzoek om tenminste ná afgifte van een ID-bewijs haar digitale gezichtsopname te verwijderen uit de overheidsdatabase en de op afstand uitleesbare chip van het document. Een procedure die inmiddels ook alweer jaren in beslag heeft genomen en waarvan als enige nieuwe ontwikkeling in 2020 gemeld kan worden dat de Raad van State geprobeerd heeft om het Hoger beroep hierover niet ontvankelijk te verklaren.

Ook de ontdekking dat een van de Nederlandse paspoortzaken bij het EHRM werd ondersteund door een hoogleraar staats- en bestuursrecht aan de Universiteit Leiden die als advocaat optreedt als partner van het grote advocatenkantoor Stibbe maar datzelfde advocatenkantoor in België de overheid als verweerder, in de rechtszaak 'stop de vingerafdruk', bijstaat is weinig bemoedigend.

Stagnatie juridische procedures tegen schendingen van de Privacy en het medisch beroepsgeheim

De Hoger beroepszaak over het Diagnose behandel Informatie Systeem (DIS) stond zonder enige voortgang in de wacht bij de Raad van State. Het gaat om het onrechtmatig verzamelen van de Nederlandse Zorgautoriteit van medische gegevens voor beleidsdoeleinden, zonder dat betrokken daar toestemming voor gaven, weet van hebben en zonder dat het medisch beroepsgeheim daarbij gerespecteerd wordt. Voor meer info zie....

Deze kwestie speelt inmiddels vanaf 2004. Op 30 augustus 2019 tekende Vrijbit Hoger beroep aan tegen de uitspraak van de rechtbank Midden-Nederland. Inmiddels is de verwachting dat de behandeling op zijn vroegst in het laatste trimester van 2021 gepland gaat worden.

Gedragscode Zorgverzekeraars Nederland

Deze rechtszaak is gericht tegen de toezichthouder (AP) omdat deze weigert in te grijpen tegen de 'Gedragscode Zorgverzekeraars' ondanks dat de procedures en bedrijfsprocessen, zoals ze zijn vastgelegd in die Gedragscode onrechtmatig zijn, en zowel het recht op privacy van patiënten als het medisch beroepsgeheim schenden. Ook deze zaak kent een lange voorgeschiedenis, omdat de gedragscode al niet deugde vanaf 2006 toen het nieuwe Zorgstelsel inging waarbij de particuliere verzekeringsmaatschappijen van de minister van VWS de regie over de Zorg kregen toebedeeld.

Nadat diverse organisaties tevergeefs gepoogd hadden om de Gedragscode wel in overeenstemming met wet- en verdrag te krijgen, heeft Vrijbit op 3 mei 2015 daartoe een handhavingverzoek ingediend bij het College Bescherming Persoonsgegevens (tegenwoordig Autoriteit

Persoonsgegevens). Na een tergend jarenlang slepend traject van tegenwerking en vertraging werd er uiteindelijk een ondeugdelijk onderzoek gedaan en geldt de Gedragscode tot op de dag van vandaag. Ook al kondigde Zorgverzekeraars Nederland bij de minister in 2019 aan dat er een nieuwe opgesteld zou worden en deze aan de AP ter goedkeuring zou worden voorgelegd. Het Hoger beroep (zaaknummer 201906616/1/A3) wat Vrijbit op 30 augustus 2019 instelde tegen de uitspraak in eerste aanleg van de rechtbank Midden-Nederland (d.d. op 23 juli 2019) wacht sindsdien op behandeling.

EPD-LSP

Vrijbit heeft ook twee rechtszaken tegen de manier waarop mensen, zonder dat ze daarvoor de vereiste toestemming hadden gegeven, in het particuliere EPD-LSP systeem konden worden geregistreerd. Één tegen het AP om op te treden tegen de beheerder van het LSP uitwisselingssysteem die weigert verantwoordelijkheid te nemen en een systeem beheert waardoor alle BIG geregistreerde zorgverleners inzage kunnen krijgen in de medische gegevens van personen die daar geen toestemming voor gaven. De andere omdat niet ingegrepen werd tegen de praktijken van veelal apothekers die mensen zonder de vereiste toestemming aan meldden.

Op 10 januari 2020 oordeelde de rechtbank dat de beroepsgronden van Vrijbit ongegrond waren, ook al was zonneklaar dat aanmelding in het EPD-LSP enkel geoorloofd is wanneer de betrokkene daar uitdrukkelijk toestemming voor heeft gegeven en de praktijk uitwijst dat het nog steeds mogelijk blijkt dat medische data van personen die géén toestemming gaven toch kunnen worden uitgewisseld via het EPD- LSP.

De Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ), beheerder van het Landelijk Schakelpunt (LSP) faciliteert de uitwisseling van medische gegevens. Toch kwam VZVZ onder haar verantwoordelijkheid weg. Met de redenering dat er inmiddels wel correcte voorlichting zou worden gegeven, men af en toe een steekproef deed en zich als beheerder van het systeem verder niet verantwoordelijk achtte. De enkele apothekers die zich apert schuldig hadden gemaakt aan onrechtmatige aanmeldingen kregen gelegenheid om bij de duizenden opt-in registraties mensen opnieuw om toestemming te vragen. De apotheek die in de voorlichting zelfs niet had aangegeven dat het om het LSP ging kwam weg met een nieuw 'toestemmingsformulier' waar dat wel op vermeld wordt. Andere apotheken die allemaal tot eind 2018 gemankeerde info gaven werden verder niet onderzocht of benaderd. Van een van de personen die nooit toestemming gaf blijft AP stug volhouden dat dat wel zo is… waarbij de rechtbank constateerde dat schriftelijk toestemming verlenen niet HOEFT van de wet en het dus per definitie een welles nietes kwestie blijft als een apotheker iemand tegen zijn zin in aanmeld en volhoudt dat deze persoon daar toestemming toe verleende. En, net als in de zaak van een van de leden van Vrijbit, Jongejan versus de IGJ, worden mensen die ontdekten dat ze in het systeem zijn terechtgekomen als niet belanghebbend beoordeeld zodra zij hun BSN uit het EPD-LSP hebben laten verwijderen.

Na intern beraad werd besloten om niet in hoger beroep te gaan. Dit omdat de politiek er inmiddels door de stuurgroep ‘gespecificeerde toestemming’ op was gewezen dat het inzetten op zo’n toestemmingssysteem wegens onuitvoerbaarheid een heilloze weg was. En er dus eindelijk geïnvesteerd diende te gaan worden in alternatieve systemen voor de uitwisseling van medische gegevens die wel privacyproof zijn en waarbij het medisch beroepsgeheim beschermd blijft(zoals reeds bestaande systemen als Whitebox).

Uit onderzoek van de stuurgroep was naar voren gekomen dat er toestemming gegeven zou moeten worden over 160 categorieën. De stuurgroep concludeert op basis daarvan dat "de huidige uitwerking”onvoldoende werkbaar en uitvoerbaar is voor burgers, patiënten en zorgaanbieders." De stuurgroep vroeg aan minister Bruins (VVD) hoe het nu verder moest. Daarmee leek het erop dat we alsnog voor niks jarenlang geïnvesteerd hadden in deze handhavingsverzoeken, tijdrovende bezwaarprocedures en beroepszaken, zoals we op de website lieten weten; https://www.vrijbit.nl/dossiers/dossier-epd/item/1099-uitspraak-in-rechtszaken-vrijbit-over-onrechtmatige-aanmeldingen-epd-teleurstellend-maar-niet-vergeefs.html.
De minister en de toezichthouder startten een overleg en Vrijbit werd zowaar door de AP uitgenodigd om haar inzichten te delen over de knelpunten en verkenning van alternatieven bij dataverwerking door de overheden verwerking van bijzondere persoonsgegevens in de zorg.

Dat was begin 2020. Hoe minister Bruins instortte tijdens een coronadebat is bekend.

Dat al in april het ministerie een gedoogregeling trof waardoor het EPD via het LSP werd opengesteld van 8 miljoen mensen die nooit toestemming gaven om in het LSP te worden opgenomen, konden we toen niet bevroeden. Door de paniek op de huisartsenpost(HAP) en spoedeisende/eerste hulp(SEH)om snel meer gegevens van patiënten te kunnen krijgen bij spoedopnames werden bij alle huisartsenposten de ‘toestemming’ voor aanmelding in EPD-LSP automatisch op ‘ja’ gezet van iedereen die niet uitdrukkelijk had aangegeven daar bezwaar tegen te maken. Dit zou tijdelijk gelden voor de duur van de coronaproblematiek. Dat daarmee alle zorgverleners inzage konden krijgen in een systeem wat apert onveilig is, o.a. omdat de informatie vaak gedateerd, onvolledig of gewoon onjuist is, werd gemakshalve even aan voorbij gegaan.

Bij het starten van de constructie van de corona-opt-in gaf het ministerie van VWS aan dat er een juridische basis voor zou komen, die is er een jaar later nog niet. Gelukkig heeft de AP, die oorspronkelijk akkoord ging op grond van een gemankeerde interpretatie van de wetgeving, inmiddels een kritischer houding aangenomen en is Bits of Freedom eind 2020 een onderzoek gestart. Het ministerie wil van de gelegenheid gebruik maken om de medische gegevens via huisartsen permanent open te stellen als patiënten daar niet uitdrukkelijk tegen protesteren.

Mitz

Mitz is de opzet van een toestemmingssysteem in de Zorg. Dit voorstel van de zorgverzekeringen beoogt om via een Online toestemmingsvoorziening (OTV) te kunnen overgaan op het invoeren van generieke toestemming voor het uitwisselen van medische persoonsgegevens.

In oktober stuurden we een felle inbreng aan het Open consultatie Informatie Beraadzorg en naar de minister van VSW, Eerste- en Tweede kamer en AP over het voorgenomen Mitz.

Citaat uit brief aan Tweede Kamer:

Onderwerp hernieuwde poging van Zorgverzekeraars Nederland om inbreuk te maken op de wettelijk verankerde toestemmingsvereisten inzake het uitwisselen van medische persoonsgegevens.

Opnieuw proberen de Zorgverzekeraars Nederland om korte metten te maken met de fundamentele beschermingsprincipes ten aanzien van het uitwisselen van medische gegevens. Deze keer met het plan om een Online toestemmingsvoorziening (OTV) te introduceren.

Dit plan, Mitz genaamd, bedoeld het huidige wettelijke kader te vervangen waarbij medische gegevens, buiten een medische behandelrelatie, enkel mogen worden uitgewisseld MITS de patiënt daarvoor welgeïnformeerd, voor een welomschreven doel en vooraf specifiek toestemming heeft gegeven.

Het plan omvat, naast deze onrechtmatige inbreuk op de privacy van patiënten en het medisch beroepsgeheim, tevens het voornemen om die toestemmingsvoorziening te koppelen aan het EPD-LSP systeem. Het Landelijk Schakel Punt waarvoor als randvoorwaarde ook geldt dat mensen te allen tijde het recht hebben om hun medische gegevens niet via dit systeem te laten uitwisselen. Het LSP waarvan in rechte is komen vast te staan dat de beheerder, VZVZ, iedere verantwoordelijkheid afwijst voor het feit dat er nog steeds mensen tegen hun uitdrukkelijke wil in het systeem worden aangemeld.

Omdat VWS het plan van ZN en VZVZ faciliteerde door het organiseren van een consultatie waarvan de uitkomsten - in tegenstelling tot wat bij open consultaties te doen gebruikelijk is- niet openbaar gemaakt worden, zal deze nieuwe aanval op de privacy van patiënten en het medische beroepsgeheim veel Kamerleden ongetwijfeld ontgaan zijn.

Vanwege het groot maatschappelijk belang dat, ook in tijden van de coronapandemie, het respecteren van de fundamentele burgerrechten en het behoud van het medisch beroepsgeheim niet het loodje leggen, vragen wij u bij deze om via deze weg de inbreng van onze organisatie op de raadpleging over het plan Mitz rechtstreeks bij de Kamerleden onder de aandacht te brengen.

Donorregistratie

In het kader van verzet tegen de nieuwe donorwet, die op 1 juli 2020 in werking trad, publiceerde Vrijbit een artikel met uitleg over de nieuwe wet en het bezwaar tegen de juridische constructie ervan. https://www.vrijbit.nl/dossiers/dossier-gezondheidszorg/item/1105-verzet-tegen-de-nieuwe-donorwet.html

Citaat:
Vrijbit wil niets afdoen aan het grote belang dat er voor patiënten in nood genoeg donoren nodig zijn om hen te kunnen helpen. Echter, de manier waarop de nieuwe wetgeving het aantal potentiële donoren wil vergroten, wijzen we af omdat het de Rijksoverheid volgens ons niet past om de registratie en verwerking van het lichaamseigen materiaal van mensen te kunnen toe-eigenen.

Dat geldt voor zowel deze donorwet, als voor het vastleggen van biometrische gegevens in het kader van de Paspoortwet, de geheime DNA databank als onderdeel van de wet op de inlichtingen en veiligheidsdiensten(Wiv2017) en de manier waarop via het wetsvoorstel 'zeggenschap eigen lichaamsmateriaal' de beschikking over hun lichaamseigen materiaal voor andere doeleinden dan medische behandeling ontfutselt wordt.

Donaties horen per definitie vrijwillige giften te betreffen, anders zijn het geen giften maar gedwongen afnamen.

We hebben ook bezwaar tegen de juridische constructie dat bij het donorregistratiesysteem totaal voorbij wordt gegaan aan het principe van noodzakelijk te verlenen specifieke toestemming, voor het mogen verwerven en verwerken van gevoelige persoonsgegevens, zoals vastgelegd in de wetgeving ter bescherming van persoonsgegevens. Het vastleggen van de naam, geboortedatum, adres, contactgegevens en het BSN van een potentiële donor zou ons inziens enkel na specifieke goed geïnformeerde toestemming vooraf, geoorloofd moeten zijn.

Een belangrijk punt van bezwaar is dat van de voorzienbaarheid. Met name waar de wet regelt dat de minister kan bepalen welke wetenschappelijke onderzoeken al dan niet geoorloofd zijn in het kader van de voor transplantatie afgenomen donaties, maakt dat mensen vooraf niet kunnen weten of hun lichaam nadat ze doodverklaard worden niet zal worden ingezet voor onderzoek waar men beslist niet mee akkoord zou willen gaan. Heel opmerkelijk is in dit verband ook dat in de donorwet en de voorlichting daarover op geen enkele wijze wordt vermeld dat met het afnemen van lichaamsmateriaal uiteraard ook het DNA van de persoon wordt afgegeven.

Daarnaast voorzien wij ook allerhande bezwaren ten aanzien van mensen die niet taalvaardig genoeg zijn om de impact van de hun toegestuurde aanmaning om een keuze te maken, te begrijpen. Hetgeen zeker ook geldt voor die personen die niet vanwege hun laaggeletterdheid maar wegens verstandelijke vermogens of geestelijke gesteldheid niet geacht mogen worden om adequaat op degelijke overheidspost te reageren. Wie kan garanderen dat de betrokkenen dergelijke post daadwerkelijk ontvingen (waarbij te denken valt aan studentenhuizen, verzorgingsinstellingen, verpleeginrichtingen en mensen die post op hun thuisadres krijgen terwijl ze elders verblijven omdat ze op wereldreis zijn of in het ziekenhuis liggen)?

De opslag van de data van personen die aangewezen worden om de keuze te maken, waar het geen naaste familie betreft is ook een punt van zorg. Hoe kan die persoon weten, laat staan toestemming geven om zijn persoonsgegevens in het register op te nemen? Hoe kan men verwachten dat iedereen die deze keuze maakt, ook als een situatie wijzigt zo alert is om dat aan het Donorregister door te geven.

Wat betreft de gevaren van grootschalige persoonsgegevens in een ICT database van de overheid, volstaat inmiddels, na alle ICT debacles, de opmerking dat het redelijk is om te twijfelen aan het veilig en correct functioneren van zo'n systeem. We hebben het dan over twijfels aan adequaat en up to date te houden beveiliging, correcte verwerking van data en wijzigingen daarin, het inregelen van een systeem waardoor alleen wie daar recht op heeft toegang kan krijgen (zowel in het geval van doorgeven van de keuzes als bijvoorbeeld bij het opvragen van gegevens door derden).

Aan het operationeel maken van het nieuwe donorregister kleven meerdere bezwaren. Waarvan voor Vrijbit vooral van belang is dat een dergelijk systeem per definitie geen opt-out systeem zou behoren te zijn.

Wij kregen nul reacties op onze oproep om bevindingen door te geven n.a.v. de mogelijkheden voor bezwaarden.

Een alternatieve route via Nederlandse Transplantatie Stichting bleek bij navraag onbegaanbaar.

Actie tegen toestemmingsvraag aanmeldzuilen Tergooi-ziekenhuis

Na een melding dat het Tergooi ziekenhuis bij de aanmeldzuilen, die vanaf 9 november 2020 in gebruik werden genomen, de identiteitsbewijzen zou scannen, ging Vrijbit op onderzoek uit. Het bleek niet te gaan om het opslaan van de data van de ID-bewijzen, wel om het uitlezen van de RFID-chip in de documenten. De gezichtsopname werd daarbij in elk geval ook niet automatisch opgeslagen maar werd van gevraagd of mensen daar toestemming voor gaven.
Wie die toestemming niet geeft zal -net als voorheen- geen pasje krijgen maar bij ieder nieuwe ziekenhuisbehandeling zich weer opnieuw moeten laten identificeren.

Wat we op deze manier echter ook ontdekten was dat er via de zuil generieke toestemming gevraagd werd om medische gegevens te mogen uitwisselen met andere zorgverleners. We namen contact op met het ziekenhuis en lieten weten dat ‘die vraag zo niet gesteld mag worden volgens de wet', dit omdat het geen invulling is van de wettelijke plicht om voor het uitwisselen van medische gegevens buiten de directe behandelpraktijk *(dus bij een specifieke bepaalde medische behandeling betrokken medezorgverleners)*, enkel data mogen worden uitgewisseld nadat een patiënt daar vooraf 1)op grond van goede en begrijpelijke info en 2) uitsluitend voor een exact, welomschreven doel toestemming gevraagd wordt.

In dit geval gaat het om een generieke toestemmingsvraag voor een niet omschreven doel. Hetgeen dus op zowel het punt van transparantie en 'well informed consent' als m.b.t. het vereiste specifieke doelbindingsprincipe tekortschiet. Daarmee is de vraag onrechtmatig en dient derhalve verwijderd, dan wel aangepast te worden.

Na enig tegensputteren dat het heus wel in orde zou zijn, omdat de fabrikant van de zuil de vraag er anders niet geprogrammeerd zou hebben, werden we in het gelijk gesteld en beloofde men de vraag te verwijderen. Een klein succesje dus, met name omdat het ziekenhuis zelf contact op zou nemen met de leverancier ChipSoftBV, om geen enkel ander ziekenhuis zuilen te leveren met deze vraag.
Wel moesten we na enkele weken ,toen we controleerden of de vraag inderdaad verdwenen was, het ziekenhuis ook nog sommeren om op de website de voorlichting aan te passen die nog steeds vermeldde dat deze vraag gesteld zou worden. We werden vriendelijk bedankt dat we zo attent waren geweest het te melden. https://www.zorgictzorgen.nl/toestemmingsvraag-via-aanmeld-zuil-om-medische-data-te-delen-is-verbazingwekkend/

Voor verder achtergrondinformatie en dossierstukken uit het dossier gezondheidszorg. verwijzen we bij deze naar de publicaties op onze website https://www.vrijbit.nl/dossiers/dossier-gezondheidszorg.html
en naar de informatie op de website van een van onze meest actieve leden;
https://www.zorgictzorgen.nl/

De actie Kies-Keurig

In 2019 schreven we de minister en de Tweede Kamerleden aan met het verzoek om de aanvullende ID-plicht uit Kieswet te schrappen. Nadat in november dat jaar de Kamervoorzitter ons bericht stuurde dat de behandeling ervan op 25 maart 2020 aan de orde zou komen in de vaste Kamercommissie is daar door de coronavoorschriften voor thuiswerken niks van terecht gekomen. Op ons aanvullende verzoek om te laten weten wanneer dat alsnog het geval zou zijn, is taal noch teken vernomen.
Vervolgens werd er wel geregeld dat voor de Tweede Kamerverkiezingen, op 17 maart 2021, om de gezondheidsrisico's bij het stemmen zo klein mogelijk te maken, personen van boven de 70 de gelegenheid te geven om schriftelijk te stemmen. Daarmee nam de rechtsongelijkheid m.b.t. de

identificatie weer verder toe omdat voor deze stemmogelijkheid het volstond om een toegezonden stembiljet en stempas voorzien van handtekening terug te sturen. Het blijft een onverkwikkelijke zaak dat mensen voor deelname aan verkiezingen moeten bewijzen dat ze zich niet voor een ander uitgeven en voor het uitbrengen van stemmen bij volmacht kopieën van identiteitsbewijzen geëist worden volgens ons. De Kiesraad heeft laten weten dat de enige manier om dit te veranderen is om het via de politiek te regelen, dus rest ons niets anders dan daar aan de bel te blijven trekken. Om duidelijk te maken dat het zowel om rechtsongelijkheid gaat als om wantrouwen van de overheid tegenover de burgers.

ACTIE Wijvertrouwenslimmemetersniet

Vrijbit is principieel gekant tegen het gebruik van energiemeters voor gas- en elektriciteit die op afstand door de netwerkbeheerder en energieleverancier kunnen worden uitgelezen. De zogenaamde ‘slimme’ meters. De reden daarvoor is dat daarmee iemands energieverbruik door derden wordt geregistreerd en voor andere doeleinden kan worden gebruikt dan voor berekening van de kosten en verbruik. Allereerst vormt dat een aantasting van de privacy, omdat wie ‘real-time’ toegang heeft tot die gegevens, tot op het kwartier, nauwkeurig het gedrag van mensen ‘achter de voordeur’ in kaart kan brengen en deze gegevens daarmee de grondstof vormen om gedragspatronen uit samen te stellen. Waarmee dit soort gegevens een potentiële goudmijn vormen voor toepassingen van derden. Zijnde voor commercieel gebruik, voor crimineel gebruik en voor het controle door overheid-en semioverheidsdiensten. Het systeem van de ‘slimme’ 'spionage'meters is zelfs geschikt om rechtstreeks in te grijpen in het leven van mensen. Zie voor nadere uitleg: https://www.vrijbit.nl/dossiers/dossier-slimme-energiemeter/item/803-hoe-staat-het-met-de-%E2%80%98slimme%E2%80%99-meter-voor-gas-en-elektriciteitsgebruik-anno-november-2010.html

Dit jaar kreeg Vrijbit opnieuw hulpvragen van weigeraars om informatie over hun recht om te weigeren, hulp bij het weigeren en uitleg over het verschil van een digitale meter en een ‘slimme zijnde' een op afstand uitleesbare meter. In twee zaken werden mensen met succes geholpen om ervoor te zorgen dat een tegen hun zin in geplaatste ‘slimme’ meter kosteloos werd vervangen voor een exemplaar die niet op afstand uitleesbaar is.

De netbeheerder bleven fanatiek doorgaan met de verdere ‘ uitrol ’van het plaatsen van het huidige aanbod van ‘slimme’ meters. Hoewel 4 tot 5 miljoen van deze 'slimme' energiemeters op korte termijn vervangen zullen moeten gaan worden omdat ze niet in staat zijn om doorlopend gegevens over het energieverbruik te versturen omdat ze verouderde G3-netwerktechnologie gebruiken die na de komst van G5 gaan worden uitgeschakeld. Het systeem van de netbeheerders loopt óók gevaar, omdat hun vergunning voor gebruik van de radiofrequentie in 2024 opnieuw wordt geveild.

De netbeheerders vrezen een miljoenenverlies te leiden. Vrijbit denkt vooral aan de energieverspilling van de binnen de beoogde leeftijd af te schrijven meters. En aan de milieuschade van al die ‘slimme’ meters die niet alleen een veel kortere levensduur hebben dan analoge meters, maar ook in tegenstelling met de oude meters na gebruik als chemisch afval dienen te worden vernietigd.

Hoe dan ook, blijven de mensen die geen gebruik willen maken van het betaald kunnen terugleveren van door henzelf opgewekte energie de mogelijkheid houden om van de installatie van een 'slimme' energiemeter verschoond te blijven. Ook volgens de Rijksvoorlichting en de AP.

Betalingsverkeer

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.

Vrijbit startte daarom de brieven actie PSD2 niet zonder mijn toestemming waarbij particulieren van de bank eisen dat hun financiële persoonsgegevens niet aan derden worden verstrekt, onder de nieuwe wet voor betalingsverkeer PSD2. De actie bestond uit het versturen van brieven naar de Triodos Bank, ABN-AMRO, Rabobank, de Autoriteit Persoonsgegevens en diverse privacy deskundigen. Op de website publiceerden we een artikel met toelichting en een chronologisch verslag over de invoering van PSD2 voor wie zich nader in dit onderwerp wil verdiepen.
We werkten hierbij nauw samen met de actie 'PSD2me niet' die vanuit Privacy First werd gevoerd.

Acties tegen digi drang-en dwang

Ook dit jaar is Vrijbit weer regelmatig in actie gekomen tegen, met name overheden die op oneigenlijke wijze doen voorkomen alsof communicatie via digitale weg de enige mogelijkheid vormt.

Zo ook de juridische afdeling van de gemeente Utrecht die voor het op last van de rechter moeten terugbetalen van griffiegeld naam adres en bankgegevens via e-mail wenste te ontvangen. Ook ging er een vinnige brief uit naar het stadsbestuur over de drone surveillance boven de stad op 5 mei.

In mei leverde we via de internetconsultatie van het ministerie BZ kritiek op de voorstellen van digitale identificatiemiddelen en private authenticatiediensten. Middelen ter uitvoering van de Wet digitale overheid , die de Tweede kamer in februari 2020 had goedgekeurd, te kunnen inloggen bij organisaties in het publieke domein (overheid, pensioenfondsen en zorgverzekeraars).
https://www.internetconsultatie.nl/identificatiemiddelen/reactie/eae27fd1-d5e9-4ad2-9248-27cb77e4b405

De belangrijkste kritiekpunten:

Fundamenteel

Het uitgangspunt dat het openstellen van overheidsdienstverlening automatisch zou leiden tot een veiliger systeem van i/e-overheids functioneren, vanwege de diversiteit, doet geen recht aan de ervaringen ten aanzien van de doorgeschoten privatisering binnen de publieke sector. Niet aan de inmiddels bekende nadelen ten gevolge van de vermenging van privaat-publieke taken op gebied van rechtszekerheid, aansprakelijkheid, toepasselijkheid van wetgeving en mogelijkheden voor toezicht op publieke belangen. Nog los van het feit dat dit ook een rare manier vormt van het ministerie om zich bij voorbaat in te dekken voor toekomstige overheids ICT-debacles, kan men met een dergelijk taalkundige formulering geen rechtvaardiging leveren voor een beleid dat voortgaat op het doodlopende pad van een verdere uitbouw van de privatisering in het publieke terrein.

De hele conceptopzet met betrekking tot het openstellen van overheidsdienstverlening via private authenticatiediensten ademt een ongewenste onderdanigheid uit van de overheid ten opzicht van de belangen -en lobby- vanuit het bedrijfsleven. Belangen die men zwaarder laat wegen dan de taak tot optreden van de overheid als bewaker van de nationale en individuele veiligheid en soevereiniteit van alle Nederlanders.

In concreto:

A- Het feit dat er geen principiële keuze wordt gemaakt voor het uitsluiten van authenticatiesystemen die niet gebaseerd zijn op een centraal georganiseerd systeem. Een vorm van negeren van de principes van privacy-in- ontwerp-architectuur ten faveure van bedrijven die wel brood zien in een verdere uitbouw van hun systemen voor private dienstverlening en gebruik van biometrische identificatiesystemen. Een inzet kortom die niet kiest voor een aanpak waarbij het mogelijke misbruik van het e-ID-middel tot het gebruik daarvan beperkt blijft maar uitnodigt tot grootschalige vormen van (georganiseerde) criminaliteit via de dataopslag. De hele opzet met zogenaamde waarborgen via een papieren randvoorwaarde dat een gescheiden opslag van gebruikersgegevens en gebruiksgegevens geëist wordt is een gotspe. Immers wijst de praktijk uit dat ‘function creep’ (het inzetten van projecten voor andere doeleinden dan oorspronkelijk bedoeld) bij een schat aan data altijd op de loer ligt, nauwelijks- en dan nog altijd enkel achteraf- te bestrijden valt en domweg met een andere opzet voorkomen kan worden.

B- Het voornemen om geen systemen uit te sluiten die gebouwd worden op grond van bedrijfsgeheimen in plaats van principieel enkel op ‘open source’ principes gebaseerde systemen te accepteren. Waardoor de mogelijkheden tot bescherming van iemands digitale identiteit tot een wassen neus verworden, voor zowel de burger zelf, als de verantwoordelijke en betrokken overheidsdiensten.

De overweging om het gebruik van het Burgerservicenummer (BSN)open te stellen voor private partijen introduceert een ongekend veiligheidsrisico voor iedere burger op misbruik van iemands identiteit en/of data die aan dit unieke persoonsregistratienummer gekoppeld zijn.

Dat het wetsvoorstel digi overheid (34.972)hiervoor een grondslag beoogt te introduceren, kan niet door de beugel en zal als het goed is ook een struikelblok vormen voor het aannemen van de wet omdat het BSN uitsluitend bedoeld is voor het verkeer tussen de overheid en de burger.

Private partijen, waarvan bij voorbaat nota bene al bekend is dat ze met behulp van dit ‘core ID’ een business model voor zich zien *‘waarbij er ruimte komt voor alternatieve middelen die bij voorkeur ook*

buiten de publieke sector gebruikt kunnen worden', behoren geen toegang/ beschikking te krijgen tot de data van het Nederlandse Bevolkingsregister en het BSN. Waar het BSN als koppelnummer de toegang vormt voor alle gegevens over een burger waarover de overheid beschikt, is het onacceptabel dat een minister zelfs maar overweegt om het gebruik hiervan toe te staan aan anderen dan overheidsdiensten, instellingen in zorg en onderwijssector voor zover zij dat nodig hebben voor de uitoefening van hun publieke taak en de betrokken burger zelf.

Ook hier geldt dat het hele issue niet van toepassing is als men kiest voor een decentraal authenticatie systeem (waarbij specifieke persoonsgegevens- waaronder het BSN, naam of geboortedatum verstrekt worden door de overheid en afhankelijk van de context door de burger zelf onthuld kunnen worden).

Praktisch

Ook in geval van het ontwikkelen van authenticatiesystemen geldt het devies: 'beter voorzichtig zijn dan achteraf spijt krijgen'. Het heilige geloof in het onbezorgd inzetten op ruime holle kaderwetgeving ten behoeve van de mogelijke AMvB invulling *met het oog op de verwachtingen van toekomstige innovatieve van technologische ontwikkelingen*, is daarmee in strijd. Dat het stellen van degelijke, transparante en te handhaven voorwaarden aan architectuurkeuzes en systeemprincipes innovatieve technologie zou uitsluiten is natuurlijk onzin.

Daarbij willen we speciaal aandacht vragen voor de gemakzuchtigheid waarmee het concept schermt met de ISO27001 certificering alsof dit een daadwerkelijk garantie zou bieden voor de feitelijke beveiliging en controle van de authenticatiesystemen. Waarbij de overheid, gezien de ervaringen met DigiNotar, toch inmiddels ook wel het besef hoort te hebben dat certificeringen in feite rekenkundige modellen betreffen en geen garantiebewijzen.

Hoe men zich dat verder voorstelt om toezicht te kunnen houden op internationale bedrijven die vanuit andere lidstaten een authenticatiedienst gaan exploiteren waarbij de Nederlandse overheidsdiensten toegang gaat worden verplicht, is ons een raadsel. Waar we nu al te maken hebben met nationale organisaties, zoals de zorgverzekeraars, die toezicht op hun publieke taak via jarenlange juridische procedures over een correcte omgang met persoonsgegevens kunnen frustreren met beroep op bedrijfsvertrouwelijke processen, valt niet in te zien waarom de overheid zelfs maar een deur op de kier zet voor commerciële partijen die wensen te kunnen beschikken over zowel de opslag van authenticatiegegevens als over de gegevens over gebruik van het identificatiemiddel.

Gewoon niet aan beginnen is ons advies. Geen mogelijkheid voor scheppen bij wet en AMvB maatregelen voorkomt dat er überhaupt toezicht zou moeten worden uitgeoefend om te controleren of bedrijven die gegevens wel gescheiden bewaren En hoe dan? En wie heeft toegang tot de bestanden, hoe zijn personeelsleden daartoe geautoriseerd, hoe wordt toegang tot gebruiksgegevens gelogd? In hoeverre zijn er uitzonderingen op analyse van- en controle op gebruiksgegevens in het kader van fraudebestrijding? Deze opsomming is niet compleet, maar geeft wel een indicatie van onze ongerustheid t.a.v. zelfs maar de mogelijkheden van toezicht kúnnen houden. Nog los van de capaciteit en capabiliteit van de dienst die dit zou moeten gaan uitvoeren.

Ook onderschreven we het 'Manifest Bescherm onze gezondheid, maar bescherm ook onze rechten' waarin, onder leiding van Bits of Freedom en Waag, een gelegenheidscoalitie van deskundigen

stelden dat zo'n Corona-contact-app, uitsluitend zou mogen worden ingevoerd mits hij zou voldoen aan de volgende 10 randvoorwaarden:
1. Eén doel: het onder controle krijgen van het virus.
2. Gebaseerd op wetenschappelijk inzicht en bewezen effectief.
3. Bewezen betrouwbaar en vanuit expertise.
4. De inzet van de applicatie is per definitie tijdelijk.
5. Niet tot individuen herleidbaar.
6. Zo min mogelijk gegevens worden gebruikt.
7. Geen centraal opgeslagen persoonsgegevens.
8. Veilig en bestand tegen misbruik.
9. Gebruiksvriendelijk en toegankelijk.
10. Nooit onder dwang van overheid en derden.

Waarbij we aantekenen dat Vrijbit van meet af aan sceptisch stond tegenover het hele contactapp circus, omdat het de zoveelste uiting vormde van een ongefundeerd geloof in technologische oplossingen. Hetgeen bevestigd werd toen niet alleen een groot aantal mensen wat beschikte over een voor de app noodzakelijke iPhone de app niet installeerden, zich van meldingen niks aantrok en meldingen bij gebrek aan testmogelijkheden voor wie mogelijk in aanraking was geweest met een besmettelijk persoon, sowieso geen zin bleken te hebben.

Websites

Om onze doelstellingen te verwezenlijken onderhouden wij de volgende zeven 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.

Ledenbestand

Met 201 leden sloten we 2020 af. Waarmee we mogen stellen dat het ledenbestand met jaarlijks wat afvallers en nieuwe aanmeldingen vrij constant blijft. Al zouden we graag groter groeien.

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.

Financieel jaaroverzicht

Saldo 1-1-2020			
Triodos betaalrekening			€ 1.333,07
Triodos spaarrekening			€ 500,00
Fysieke kas			€ 8,15
Totaal			€ 1.841,22
Totaal inkomsten			
Triodos			9362,75
Fysieke kas			208,2
Totaal			€ 9.570,95
Saldo + inkomsten=			€ 11.412,17
Totale uitgaven			
Triodos			€ 6.453,58
Fysieke kas			€ 132,07
Totaal			€ 6.585,65
€ 11.412,17	minus uitgaven		€ 6.585,65
			€ 4.826,52
Saldo 31-12-2020			
Triodos betaalrekening			€ 4.352,74
Triodos spaarrekening			€ 490,00
Fysieke kas			€ 84,28
Totaal			€ 4.927,02
Kasverschil;		plus	€ 100,50

Specificatie inkomsten 2020

Contributies lidmaatschap	€ 985,00
Donaties	€ 4.941,35
Actiemateriaal	€ 74,20
Restitutie griffie+ schadevergoeding	
overschrijding redelijke termijn rechtszaken	€ 3.570,40
Totaal	€ 9.570,95

Specificatie Uitgaven 2020

Bureau artikelen	€ 165,70
Catering	€ 133,64
Telefoon/internet	€ 741,71
Vakliteratuur	€ 111,99
Kranten/tijdschriften	€ 1.058,40
Webkosten	€ 1.952,81
Reiskosten	€ 369,20
Frankeerkosten	€ 207,10
Productie actiemateriaal	€ 33,75
Kosten betaalverkeer	€ 210,45
Rechtsbijstand	€ 861,40
Huur locatie	€ 739,50
Totaal	€ 6.585,65

Beleidsvoornemens Burgerrechtenvereniging Vrijbit 2021- 2022

Acties

Indien de leden hier mee akkoord gaan heeft het bestuur voorgesteld om de lopende acties zoveel mogelijk door te zetten, met als speerpunten:

1. De strijd tegen de biometrische dataverzameling door de overheid via de Paspoortwetgeving en het gebruik van digitale gezichtsherkenningstechnologie in de publieke ruimte.
2. Acties tegen de aantasting van het recht op privacy van patiënten en doorbreking van het medische beroepsgeheim.
3. Actie tegen risicoprofileringssystemen van overheid en het bedrijfsleven. Computersystemen die ten doel hebben om het gedrag van mensen exact te registeren, te analyseren en om te zetten in risicoprofielen en te koppelen aan andere bestanden. Met het doel om op basis van deze data middels onbekende rekenkundige formules(algoritmen) beslissingen te nemen over het benaderen, beoordelen en monitoren van individuen of groepen.

Daarnaast zullen we doorgaan met:

1. De actie '*wijvertrouwenslimmemetersniet'* om te voorkomen dat netbeheerders en elektriciteitsbedrijven 'slimme' meters voor gas-en elektriciteitsverbruik blijven opdringen aan particulieren die hier- met recht- bezwaar tegen hebben.
2. Actie *'Kies Keurig'* met als doelstelling om de aanvullende identificatieplicht bij verkiezingen te doen afschaffen.
3. Actie tegen de voortgaande digitaliseringsdrang-en dwang van de overheid.

Indien er voldoende menskracht voor is hopen we eveneens een doorstart te kunnen geven aan de actie PSD2- niet zonder mijn toestemming.

Ook de voorstellen tot wetswijziging van de Wet inlichtingen-en Veiligheidsdiensten(Wiv2017) zullen we op de voet blijven volgen.

De prikacties ten behoud van het gebruik van cash geld blijven we steunen.

Waarbij opgemerkt dient te worden dat Vrijbit weliswaar vaak actie voert tegen privacy inperkende praktijken en wet- en regelgeving, maar altijd met inzet om een bijdrage te leveren aan het op constructieve wijze bijdragen aan alternatieve 'privacy-proof' maatregelen.

Informatie voorziening

Het bijhouden van 'privacynieuws' en actuele ontwikkelingen die betrekking hebben op het recht op een privéleven blijft een van de hoofdmoten van het Vrijbit werk. Dat betreft zowel de eigen studie en archivering van actuele ontwikkelingen als het doorzetten van deze informatie naar belanghebbenden.

Advisering en hulpverlening

Alle aanvragen blijven we beantwoorden. De individuele hulpverlening zal waar mogelijk worden gecontinueerd.

Samenwerking

We blijven ernaar streven om zoveel mogelijk samen te werken met andere privacy organisaties. Dat geldt zowel voor de organisaties en gelegenheidscoalities binnen Nederland als voor het internationale actienetwerk via FreedomNotFear, Access Now en Privacy International.

De verbeterde samenwerking met de toezichthouder Autoriteit Personen (AP) zullen we blijven onderhouden met als opzet dat deze zich niet langer onderdanig en vanuit een gebrekkig kennisniveau conformeren aan overheid en bedrijfsleven, maar ten principale als medestander gaat optreden ter bescherming van de privacy belangen van de burger.

Websites

Er wordt doorgegaan met het aankondigen op de agenda van de Vrijbitwebsite van de diverse bijeenkomsten, debatten, symposia en lezingen die georganiseerd worden op het gebied van privacybescherming.

Doorgegaan wordt met het beveiligen, hosten en van actuele informatie voorzien van de huidige websites:
https:// www.vrijbit.nl , https:// www.privacynieuws.nl , https:// www.id-nee.nl , https:// www.ikgeentoestemming.nl, https:// www.wijvertrouwenslimmemetersniet.nl, https:// www.louisetegendepaspoortwet

Intern

De maandelijkse ledenbijeenkomsten, op de eerste zondag van de maand, zullen alleen bij voldoende opkomst worden gecontinueerd.
Contacten met leden en geïnteresseerden zullen veelal via e-mail en papierpost blijven plaatsvinden.

Aanvragen van een bezoek op locatie of werkoverleg elders in het land of het geven van interviews, zullen doorgaans ook via e-mail blijven plaatsvinden.
Telefonisch contact blijven we, vanwege een te grote belasting op de geringe bezetting op locatie, tot het minimum beperken.
De gewoonte om eens per maand de ledenadministratie en de boekhouding bij te werken blijft in stand. Hetgeen eveneens geldt voor het regulier bijhouden van de maandelijkse werkverslagen.

Intern zal geprobeerd worden om door te gaan met het creëren van een stabiele financiële basis en uitbreiden van het ledenbestand.

Slotwoord

Ondanks de beperkte financiële middelen wordt er enorm veel werk verzet, dit 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. Daarnaast willen we hierbij alle leden en donateurs hartelijk danken voor hun onmisbare steun!

Namens het bestuur,

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

Jaarverslag 2020

VRIJBIT

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.