Aftrap juridische actie tegen risicoprofiling door Nederlandse overheid

Op vrijdagavond 19 januari 2018 organiseert het Platform Bescherming Burgerrechten in theater De Nieuwe Liefde in Amsterdam een avondvullende bijeenkomst over "profiling" door de overheid met behulp van het Systeem Risico Indicatie(SyRI). Die avond vindt de aftrap plaats van de rechtszaak tegen de Staat der Nederlanden vanwege het op grote schaal maken van risicoprofielen maken van haar burgers met SyRI. Het doel van dit systeem is in zichzelf al ongeëvenaard, omdat het niet beoogt om uitkerings-, belasting en arbeidsfraude vast te stellen, maar om de risico's hierop in kaart te brengen. Met andere woorden, dit systeem voorziet in de mogelijkheid om risicoprofielen van niet-verdachte burgers te maken. Weinigen hebben weet van de omvang van het maken van deze risicoprofielen. De rechtszaak gaat gevoerd worden door het Public Interest Litigation Project (PILP) en het Nederlands Juristen Comité voor de Mensenrechten(NCJM) in samenwerking met het Platform Bescherming Burgerrechten. Deikwijs Advocaten zal in de rechtszaal acteren. Het NCJM beoogt het strategisch procederen voor mensen- en burgerrechten in Nederland. De campagne van het Platform Bescherming Burgerrechten, die rond deze rechtszaak van start is gegaan, heeft de zeer toepasselijke titel: "Bij voorbaat verdacht" gekregen. Op dit moment staat een overleg met het ministerie van Sociale Zaken en Werkgelegenheid gepland waarin de aangesloten partijen hun eisen omtrent SyRI op tafel leggen. Mocht daar geen gewenst resultaat uit komen, dan wordt de rechtszaak in gang gezet. Formeel is vanwege de rechtsgang een dergelijke stap noodzakelijk.

Lanceringsbijeenkomst

Op de 19e januari 2018 zullen Tommy Wieringa en Maxim Februari, die zich als ambassadeur bij de campagne hebben aangesloten, een lezing houden. Daarnaast zullen hoogleraar theoretische sterrenkunde Vincent Icke en dr. Aline Klingenberg van de Rijksuniversiteit Groningen optreden als spreker. De bijeenkomst zal worden gemodereerd door journalist en auteur Bart de Koning. Aan het eind van de avond is er ruimte voor discussie en vragen vanuit het publiek.

Belang

Zoals in de inleiding betoogd is met de wet SyRI een heel andere principe van benadering van burgers tot stand gekomen. Niet het vaststellen van eventuele fraude bij individuele burgers is het doel, maar maken van risicoprofielen waarin gezien de methodologie ook niet-verdachte burgers in voor zullen komen. Men maakt daarbij gebruik van voor de burger niet inzichtelijke algoritmen. De bestanden met mensen die aan deze profielen voldoen blijven twee jaar bewaard. Uiteraard kan door een minimale wijziging in het zoekprotocol de bewaartijd weer met twee jaar verlengd worden. De uitvoering van dit alles vindt plaats door een private organisatie, opgericht door de centrale overheid en perifere overheden, de Stichting Inlichtingenbureau, gevestigd in het centrum van Utrecht. Deze constructie is nogal doortrapt, omdat daardoor deze uitvoeringsorganisatie niet onder de gebruikelijke verantwoordelijkheden van de overheid valt, zoals de openbaarheid van bestuur. Daardoor zullen WOB-verzoeken niet werken.

SyRI

Voor het kunnen uitvoeren van profiling zijn data nodig. Die zijn afkomstig van vele rijks- en gemeentelijke computersystemen die gekoppeld zijn in het SUWINET. Die koppeling is mogelijk gemaakt door de Wet structuur

uitvoeringsorganisatie werk en inkomen. Het maken van de risicoprofielen werd mogelijk door een ministerieel besluit van 1 september 2014 genaamd: Besluit tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI. Eén en ander is zonder debat door de toenmalige minister van Sociale Zaken en Werkgelegenheid Lodewijk Asscher, door de Tweede en eerste Kamer geloodst. Zowel de Raad van State als de Autoriteit Persoonsgegevens waren uitermate kritisch over dit besluit, maar de trein reed voort.

Omvang gegevens

Een idee van de omvang van de hoeveelheid te koppelen data krijgt men door het zien van het aantal te koppelen databases. Het gaat om arbeidsgegevens, gegevens inzake bestuursrechtelijke maatregelen en sancties, detentiegegevens, fiscale gegevens, gegevens over roerende en onroerende goederen, handelsgegevens, huisvestingsgegevens, identificerende gegevens, inburgeringsgegevens, nalevingsgegevens, onderwijsgegevens, pensioengegevens, re-integratiegegevens, schuldenlastgegevens, uitkerings-toeslagen- en subsidiegegevens, vergunningen en ontheffingen, en zorgverzekeringsgegevens.

Grote gevaren

Ook Wetenschappelijk Raad voor het Regeringsbeleid(WRR) maakt zich grote zorgen over dit soort big-data-toepassingen. Deze kunnen leiden tot een toename van sociale stratificatie. Makkelijk kan een cumulatief nadeel (discriminatie en oneerlijke behandeling) ontstaan voor bepaalde groepen uit de maatschappij. Meestal gaat het om de sociaal zwakkere groepen in de samenleving. Expliciet waarschuwt de WRR voor function-creep bij Big Data-analyse. Omdat het systeem er nu eenmaal is wil men meestal de mogelijkheden ondershands uitbreiden. Door dit soort surveillancetoepassingen, wat het profilen met Syri

de facto is, werkt de overheid in zeer sterke mate toe naar het vervreemden van de burger van diezelfde overheid. Met de mond beleidt de overheid echter het tegendeel.

Aandacht

Het profilen met de wet SyRI vindt al vanaf 2014 plaats. Het gaat niet om kleine hoeveelheden data en kleine hoeveelheden burgers. Het raakt ons allemaal. De rechtszaak hierover, gevoerd door het PILP en NCJM in samenwerking met het Platform Bescherming Burgerrechten verdient alle aandacht. Evenzo de campagne van laatstgenoemde organisatie onder de titel “Bij voorbaat verdacht”.

Ik kan u alleen maar aanraden om op 19 januari 2018 naar de aftrap te gaan in Theater De Nieuwe Liefde te Amsterdam.

Arjen Lubach maakt er een toch nog humoristische uitzending over op 8 mei 2016. Hij gaat over de sleepwet en SyRI(vanaf 6 min 55 sec.)

W.J. Jongejan

Autoriteit Persoonsgegevens ondergraaft stelselmatig eigen gezag

Het is opvallend hoe de Autoriteit Persoonsgegevens(AP), voorheen het College Bescherming Persoonsgegevens(CBP) al enige tijd opereert bij geconstateerde overtredingen. Ondanks het feit, dat die hebben plaatsgevonden is steevast het beleid om bij het beloven van beterschap geen sancties op te leggen. Volstaan wordt met de waarschuwing, dat het na beloofde verbeteringen niet weer mag gebeuren. Deze halfslachtige houding voedt de gedachte, dat de AP een toezichthouder is die de bij wet verkregen tanden(per 1 januari 2016 nog aangescherpt) niet wil laten zien door geen sancties op te leggen. Daardoor ontstaat het beeld, dat de AP een verlengstuk is van de wetgever en uitsluitend de implementatie van wetten met zachte hand corrigeert en helpt uitvoeren. Ze wordt het verlengstuk van de politiek en geen krachtige, onafhankelijke, toezichthouder. Het speelt eigenlijk bij alle zaken die de AP onderzoekt, maar twee onderzoeken die van groot belang zijn voor de privacy van de burger, licht ik er voor u uit.

Suwinet

Dit is een besloten systeem waarmee verschillende overheidsorganisaties maatschappelijk gevoelige persoonsgegevens uitwisselen in het kader van werk en inkomen. Een onderdeel van het UWV (Uitvoerings-instituut WerknemersVerzekeringen) ondersteunt, beheert en ontwikkelt het verder. Via diverse applicaties bestaat toegang tot (persoons)gegevens van burgers, waaronder financiële data. De bronhouders van de gegevens zijn onder andere de Gemeentelijke Sociale Diensten, het UWV en de Sociale VerzekeringsBank, maar ook de belastingdienst en de rijksdienst voor het wegverkeer.

Naast deze partijen hebben ook de Immigratie- en NaturalisatieDienst, de Inspectie SZW, gemeentelijke belastingdeurwaarders, gemeenten in het kader van de meld- en coördinatiepunten voortijdig schoolverlaters en de Stichting Netwerk Gerechtsdeurwaarders toegang tot het netwerk. Er zijn veel protocollen en richtlijnen voor de toegang gemaakt, maar daar bleek een meerderheid van de gemeenten zich niet aan te houden. Mensen die geen toegang zouden moeten hebben tot het systeem kregen dat wel, ook personeel van externe bureaus, die door gemeenten ingehuurd waren. Ook werd het Suwinet in enkele gevallen gebruikt voor een ambtelijk doel waarvoor het niet opgezet was, namelijk het parkeerbeheer. Veel overtredingen constateerde de AP bij onderzoek. Op 21 januari 2016 verscheen dat rapport over overtredingen bij 11 van de 13 onderzochte gemeenten. Wat gebeurt er? De AP maant de overtreders, volgt ze door een vervolgonderzoek te doen, maar legt geen enkele sanctie op aan de overtreders, die geacht werden te weten hoe het wel zou moeten.

DIS

De afgelopen jaar heeft de AP zich ook beziggehouden met de rechtmatigheid van het doorleveren van gegevens uit het DBC-Informatie Systeem(DIS) door de Nederlandse Zorgautoriteit(NZa) aan derden. Nadat eerst de organisatie DBC-onderhoud de verantwoordelijkheid droeg voor het DIS werd op 1 mei 2015 die verantwoordelijkheid ondergebracht bij de NZa. Het ging om ge-pseudonimiseerde zorggegevens, die bij nadere beschouwing toch herleidbaar waren tot individuen. De AP was tot dat onderzoek min of meer gedwongen door publiciteit omtrent de herleidbaarheid. De AP was al eerder op de hoogte van deze materie o.a. door de uitzending van de tv-rubriek Zembla in 2014. Het komt uiteindelijk tot een uitspraak van de AP over dit onderwerp op 7 maart 2016. Daarin zegt de AP dat de gegevensverzameling van het DIS op zich wel rechtmatig is, maar dat doorlevering aan derden, zoals bijvoorbeeld de minister van VWS en het Centraal PlanBureau

niet rechtmatig is. Het conceptrapport legde de AP eerst aan de NZa voor en paste het na een reactie van de NZa alsnog aan. Hoor en wederhoor bij mogelijke overtredingen hoort er te zijn, maar dat hoort plaats te hebben voor enig rapport uitgebracht wordt. Het voorleggen van een concept-rapport aan een onderzochte instantie is in mijn ogen al een zwaktebod. En wat gebeurt er met de geconstateerde overtredingen. De NZa belooft het niet meer te doen. De AP heeft daar vervolgens vrede mee ZONDER sancties op te leggen vanwege de begane overtredingen.

Vergelijking

De handelswijze van de AP ten aanzien van geconstateerde overtredingen is heel vreemd. Het is hetzelfde als wanneer een dief betrapt is op een serie diefstallen, belooft het niet meer te doen en vervolgens geen straf krijgt opgelegd.. De handelswijze van de AP strookt absoluut niet met het rechtsgevoel, omdat organisaties waar de AP toezicht op houdt zo altijd wegkomen bij overtredingen zonder sancties. Het is bijvoorbeeld bij de Autoriteit Financiële Markten(AFM) niet voor te stellen, dat een overtreder met de belofte het nooit meer te doen geen sanctie opgelegd krijgt.

Uiteindelijk ondergraaft deze uiterst zwakke handelswijze van de AP het vertrouwen van de burgers in de overheid. Een sterke en ferm optredende toezichthouder is in het belang van burger en overheid.

Zachte heelmeesters maken nu eenmaal stinkende wonden.

W. J. Jongejan

Autoriteit Persoonsgegevens blaft weer en bijt opnieuw niet

In januari en maart dit jaar besteedde Omroep Max tot twee keer toe in het programma Meldpunt aandacht aan het voorbereiden van het scannen van patiëntendossiers uit ziekenhuizen door gevangenen in België. In het tweede programma meldde omroep Max dat zeven Nederlandse ziekenhuizen het zo uitbesteden van dit werk bevestigden, maar dat men informatie had dat het om totaal veertien ziekenhuizen ging. In de Tweede kamer werden mondelinge vragen hier over gesteld, waarop de minister van VWS schreef dat de Autoriteit Persoonsgegevens (AP) actie moest ondernemen. Dat is nu gebeurt. De actie valt nogal tegen, want er zijn drie ziekenhuizen nader aan de tand gevoeld. Uiteindelijk ontdekte de AP dat één van die drie ziekenhuizen geen bewerkingsovereenkomst had afgesloten en dat bij de twee anderen deze niet voldeed aan alle wettelijk eisen voortvloeiende uit de Wet bescherming persoonsgegevens. Geen maatregel in de vorm van een boete dus, wel het verzoek om binnen korte termijn de zaken op orde te hebben. De ziekenhuizen hoorden echter op voorhand te weten dat het uitbesteden van werk aan papieren patiëntendossiers moet voldoen aan strenge voorwaarden. Voorbeelden dat het mis kon gaan waren al voorhanden. De AP deed trouwens geen onderzoek naar alle ziekenhuizen waarvan bekend was dat die zo handelden.

Verlengstuk wetgever

Uit eerdere acties van de AP blijkt dat deze instantie liever een braaf adviserend verlengstuk van de wetgever wil zijn en niet een actieve waakhond die maatregelen neemt in de vorm van boetes. Men kiest keer op keer voor de weg van het waarschuwen van overtreders, ze nog een keer op de wettelijke regels wijzen, ze uitgebreid de kans geven om de overtredingen te corrigeren in plaats van het opleggen van maatregelen zoals boetes. Een zeer duidelijk voorbeeld was de reactie op de overtredingen bij het gemeentelijke gebruik van het Suwinet. Bij het onderzoek in 2014 naar het correct registreren van de opt-in-toestemmingen voor het opvragen van medische gegevens via het Landelijk SchakelPunt(LSP) gebeurde hetzelfde. Wat ook pijnlijk duidelijk wordt is dat bij veel onderzoeken die de AP doet sprake is van een zeer beperkte steekproef onder de (potentiele) zondaars. Men hoopt bij de AP dat van de uitspraken bij enkele overtreders een regulerend dan wel corrigerend uitgaat bij de andere overtreders.

Budgettaire beperking

De beperkte steekproeven zijn ongetwijfeld het gevolg van de zeer beperkte budgettaire ruimte die de AP heeft. De voorzitter vroeg aan de regering het vijfvoudige van het huidige budget, maar kreeg dat niet. Men kan daarom maar één ding constateren. Dat is dat de beperkte slagkracht van de AP een bewuste politiek keuze is. Op deze wijze kan de regering c.q. een betrokken bewindspersoon altijd zeggen dat de AP een bepaalde zaak in onderzoek heeft en maatregelen zal treffen, wetende dat de output van de AP niet echt een klap met een bokshandschoen zal zijn, maar eerder een aai.

Gezag

De handelswijze van de AP is beslist niet krachtig te noemen. Zulks in tegenstelling tot de andere toezichthouders die we in Nederland kennen. Al dan niet forse boetes en maatregelen

tegen bestuurders deelden die uit, waartegen dan ook weer geprocedeerd werd. Het kan zijn dat de AP bewust de huidige handelswijze prefereert omdat men gewoon geen capaciteit heeft om naast het “handhaven” ook nog gerechtelijke procedures te voeren. Het blijft ook nu dus weer bij blaffen zonder te bijten.

Gezag moet je verdienen en komt niet vanzelf.

W.J. Jongejan

Autoriteit Persoonsgegevens schetst te rooskleurig beeld veilig gebruik Suwinet

Op 21 januari 2016 publiceerde de Autoriteit Persoonsgegevens(AP), voorheen het College Bescherming Persoonsgegevens(CBP), een overzicht over hoe het gesteld is met de navolging door gemeenten van de richtlijnen voor het gebruik van Suwinet. De AP stelt bij monde van haar vice-voorzitter Wilbert Tomesen dat de situatie verbeterd is en dat een aantal gemeenten

voldoet aan de norm, maar ook dat er nog steeds gemeenten zijn die dat niveau niet bereikt hebben. Hij wijst wel op de gevaren van het niet goed op orde hebben van de zaken vanwege de mogelijke inbreuken op de privacy. Toch blijft bij lezing van de stukken de indruk hangen dat alles nog veel te rooskleurig wordt voorgesteld..

Suwinet

Suwinet is een besloten systeem waarmee verschillende overheidsorganisaties maatschappelijk gevoelige persoonsgegevens uitwisselen in het kader van werk en inkomen. Via Suwinet kan veel informatie over iemand worden verkregen. Dit kan bijvoorbeeld gaan om gegevens over arbeidsverleden, opleiding, alimentatie, uitkering of boetes. (Woorden AP). Door de koppeling van een aantal grote bron-gegevenshouders is het van eminent belang dat de toegang tot de gekoppelde systemen goed geregeld, uitgevoerd en gehandhaafd wordt. Op zich is Suwinet al door de schaalgrootte een discutabel systeem vanwege de implicaties voor de privacy. Als ook de toegang niet goed geregeld blijkt te zijn en de handhaving van de regels dan bestaat er een nog groter maatschappelijk probleem.

Omvang

Waar de AP spreekt over het onderzoek bij de gemeenten gaat het slechts om een steekproef van slechts 13, variërend van klein tot groot, van alle Nederlandse gemeenten. De AP, onderbemand als ze al tijden is, zou ook geen grotere steekproef aankunnen. Van deze 13 gemeenten waren er slechts twee die alle zaken administratief volledig op orde hadden. Het waren niet geheel toevallig beide grote gemeenten die ongetwijfeld een eigen IT-afdeling en eigen IT-management in huis hebben. Dat is iets wat bij de kleinere gemeenten vaak stiefmoederlijk bedeeld is.

Veel mis

In het overzicht van de conclusies van het onderzoek bij de

dertiengemeenten blijkt vooral dat het gaat om het niet hebben van een goedgekeurd beveiligingsplan en het niet goed controleren van de toegangsrechten tot Suwinet, Daarbij is dan ook sprake van het ontbreken van een correcte autorisatie. Het zijn allemaal overtredingen van artikel 13 van de Wet bescherming persoonsgegevens(Wbp). In één gemeente, Nunspeet, was sprake van een medewerker die toegang had tot Suwinet ten behoeve van de naleving van de Algemenen Plaatselijke Verordening(APV), parkeerbeheer en het bevolkingsonderzoek. Er is volgens de AP totaal geen wettelijke grondslag voor raadpleging van persoonsgegevens voor het toezicht op die zaken. Daardoor is er sprake van het overtreden van artikel 8 van de Wbg. Wat hier duidelijk wordt hoe makkelijk er sprake is van illegale "function-creep". Vanwege de beschikbaarheid van een zoeksysteem wordt er gewoon gebruik van gemaakt, ook al is het doel van dit systeem anders. Het is schokkend te constateren dat lagere overheden in deze steekproef vrij massaal de wet overtreden.

Tucht

Bij dit alles moet men bedenken dat zonder de controles van de AP de onderhavige gegevens niet boven water zouden zijn gekomen. Na bekendmaking van de resultaten van het onderzoek aan de gemeenten en voor algemene publicatie mochten de gemeenten nog een zienswijze inleveren om te beargumenteren dat de AP mogelijk stukken niet goed begrepen had en extra materiaal aan te dragen. Daarnaast maakten meerdere gemeenten in de zienswijze kenbaar dat ze de boodschap van de AP begrepen hadden en hun procedures inmiddels aangepast hadden. Het onderzoek had duidelijk een corrigerend effect.

Triest

Gezien de omvang van de steekproef en het totale aantal gemeenten in Nederland(390 per 01-01-2016) is het dus duidelijk slecht gesteld met de navolging van het beschikbare normenkader voor het gebruik van Suwinet door de gemeenten. Gemeenten blijken in groten getale regelgeving betreffende

privacy-gevoelige informatie niet op te volgen of de gebruiksgrenzen op te rekken. In wezen is er bij het gebruik van Suwinet sprake van een privacy-gevoeligheid die in de buurt komt van de medische datacommunicatie. Daar is de autorisatie en authenticatie geregeld door UZI-passen, kaartlezers en pin-codes terwijl bij de gemeenten sprake is van een blijkbaar slecht gestructureerde toegang tot Suwinet.
Het verhaal dat de Autoriteit Persoonsgegevens thans brengt, laat de negatieve punten wel zien. Er is een duidelijke PR-saus over gegoten door de nadruk te leggen op het verbeteren van de situatie en het voldoen van enkele gemeenten aan de normen. Het wordt eigenlijk gebracht als een soort nul-meting die voor verbetering vatbaar is. Helaas gaat het dan wel om slechts twee van de onderzochte dertien gemeenten en is het Suwinet al enige tijd in gebruik.
Het vertrouwen in hen die over ons gesteld zijn neemt door dit alles niet toe, terwijl de lokale overheid wel het goede voorbeeld zou moeten geven bij het navolgen van de wetgeving van de centrale overheid.

W.J. Jongejan.

Oud-chef MIVD wil inzage in elektronische patiëntendossiers bij terrorismebestrijding

Op maandag 16 november was in het programma Pauw(VARA) de oud-directeur van de Militaire Inlichtingen en Veiligheidsdienst(MIVD) Pieter Cobelens te gast. Met een enkele andere gasten werden de tragische aanslagen in Parijs die 72 uur eerder plaatsvonden besproken. Het koppelen van elektronische patiëntendossiers aan andere databestanden vindt hij noodzakelijk in het kader van terrorismebestrijding. Zijn bijdrage aan de discussie duurt van 7 min.38 sec. tot 11 min. 16sec. in de uitzending. (Zie de link in de eerste regel). Het waren zorgwekkende uitingen van iemand uit de hoek van de veiligheidsdiensten die niet alleen maar afgedaan kunnen worden als stoere praat na een serie aanslagen. Zijn woorden hebben diepere betekenis en hebben grote consequenties. Een nadere analyse.

Oorlog

In de uitzending vraagt Jeroen Pauw aan Cobelens: "Hoe lang is het al oorlog". Deze begint met de opmerking dat het al speelde in Afghanistan met de bedoeling de oorlog daar te houden en dat Nederland terrorisme daarna ook in Mali volgde en bestrijdt. Zonder nadere vraag van Pauw gaat Cobelens verder: "We moeten alles doen met de spullen en middelen die we hebben….We moeten onze analytische capaciteit benutten en databases die we hebben aan elkaar koppelen. ..Data die we in grote stofzuigerzakken opbergen moeten we encrypten(versleutelen) en de sleutel bij de minister leggen…..Data die we in Nederland ter beschikking hebben moeten we aan elkaar koppelen. Als het nodig is moet je gegevens van de Sociale VerzekeringsBank(SVB), elektronische

patiëntendossiers, creditcard- en reisgegevens gebruiken “. Tenslotte zegt hij nogal bout en manipulatief: “Onze gezamenlijke veiligheid is van groter belang dan mijn privacy. Als ik dood ben heb ik niets aan mijn privacy”. Hierop kom ik later apart terug.

EPD/LSP

Als Cobelens hier spreekt over elektronische patiëntendossiers dan zal hij waarschijnlijk niet alleen doelen op het opvragen van medische data door veiligheidsdiensten bij individuele zorgaanbieders of ziekenhuizen. Het zou een dermate tijdverslindende operatie zijn in geval van acute dreiging en dan niet echt werkbaar. Waarop hij vooral doelt is in mijn ogen het gebruik door veiligheidsdiensten van de faciliteiten die het Landelijk SchakelPunt(LSP) biedt. Het maakt immers bij raadpleging van dossiers via het LSP niet uit waar een dossier zich bevindt om het te kunnen raadplegen. Waar hij in feite om vraagt is tweeledig: het overrulen van het beroepsgeheim en het hebben van een achterdeur(backdoor) in een landelijk werkend systeem. De facto zou het dan gaan om een Nederlandse variant van de Patriot Act. Het patiëntendossier, of het nu op papier of elektronisch wordt bijgehouden, heeft slechts één doel, namelijk het vastleggen van de ziektegeschiedenis en behandeling van iemand teneinde bij verder medisch handelen daar op terug te kunnen vallen. Het wordt niet bijgehouden voor overheden dan wel veiligheidsdiensten.

SVB

Met de SVB-gegevens doelt Cobelens op de gegevens die via het SUWINET te raadplegen zijn. Het gaat om een heel scala van (overheids)diensten die hun databases koppelden in het kader van fraudebestrijding. Dat hij deze instantie hier noemt is opvallend. Formeel hebben de veiligheidsdiensten hier geen inzagerecht. In de praktijk blijkt het SUWINET echter zo lek als een mandje en hebben veel meer personen en bedrijven inzage in de met het SUWINET verbonden diensten dan wenselijk

en ooit afgesproken is. Praktisch gesproken zou een dienst als de MIVD er zonder veel inspanning bij kunnen komen, hoe onwenselijk dat ook mag zijn in het kader van de privacy.

Conflict van plichten

Indien een arts op enige wijze door zijn beroepsuitoefening op de hoogte zou zijn van zeer ernstige bedreiging van individuen of de samenleving dan staat het die arts vrij eigenstandig en niet door dwang van veiligheidsdiensten contact op te nemen met bevoegde instanties om een dergelijke feit te melden. De arts kan zich dan beroepen op een conflict van plichten. De wetenschap dat veiligheidsdiensten inzage zouden willen en zouden kunnen hebben in medische dossiers gaat vroeg of laat ten koste van de zorg van patiënten omdat zorgverleners anders gaan aanzien tegen het registreren van gegevens in hun systemen. Het feit dat er decentraal elektronische patiëntdossiers bestaan en er ook een landelijk systeem functioneert om dossiers in te zien ongeacht de plaats van de bron, rechtvaardigt in genen mate het willen en kunnen inzien van medische dossiers.

Twee keuzes

Cobelens zet de rechtvaardiging voor het opgeven van privacy extra scherp aan door te stellen dat hij niets aan zijn privacy heeft als hij dood is. In wezen stelt hij zijn gehoor voor twee keuzes: òf privacy opgeven òf dood. Dit is een uiterst manipulatieve wijze van argumenteren. Keuzen betreffen over het algemeen niet een dichotomie maar kennen over het algemeen meer mogelijkheden dan de steller biedt. Het kiezen van deze twee keuzen is bewust gedaan om het debat in de samenleving te sturen richting het openstellen van databases, ook de medische. Wat via de gewone politieke weg niet lukt wordt nu gepoogd salonfähig te maken via een discussieprogramma.

Opstelling

De wijze waarop de heer Cobelens opereerde in Pauw kan gezien worden als een opzetje om het vasthouden aan privacy en in het bijzonder het medisch beroepsgeheim steeds meer ter discussie te stellen in de samenleving. Een operationeel diensthoofd van de AIVD of MIVD is niet te verwachten in een dergelijk programma. Een oud-directeur kan echter makkelijk zaken ventileren ten faveure van deze diensten. Het liefst wil “men” ons doen geloven dat privacy dood is en nu ook de medische privacy. Niets is minder waar. Een samenleving waarin iedereen met een sleepnet via een scala van databases opeens tot verdachte kan worden gebombardeerd is geen vrije samenleving.

Privacy is wat Folkert Jensma, juridisch redacteur van het NRC-Handelsblad, ooit noemde: het recht de gordijnen te mogen sluiten.

W.J. Jongejan

Privacy-overtredingen bij Suwinet waarschuwing voor medisch pull-dataverkeer

Het afgelopen half jaar is het niet correcte gebruik van het Suwinet herhaaldelijk in het nieuws geweest. Het programma Argos berichtte er uitgebreid over, in veel kranten(o.a. NRC-

Handelsblad) werd er aandacht aan besteed. Eerder had het College Bescherming Persoonsgegevens(CBP) eind 2014 gerapporteerd, dat de gemeente 's-Hertogenbosch de zaken t.a.v. het Suwinet-gebruik totaal niet op orde had. In juni 2015 kondigde het CBP aan een lopend onderzoek naar het Suwinet-gebruik uit te breiden met acht gemeenten, nadat de Inspectie Sociale Zaken en Werkgelegenheid gemeld had dat het met het hanteren van de veiligheidsnormen slecht gesteld was. In de loop van anderhalf jaar was het aantal gemeenten dat aan de normen voldeed slechts gestegen van 4 naar 17%, een onbegrijpelijk laag percentage.

Suwinet

De grondvesten voor dit netwerk zijn gelegd in 2002 met als doel (persoons)gegevens van burgers tussen diverse overheidsorganisaties uit te wisselen in het domein Werk en Inkomen op basis van de Wet structuur uitvoeringsorganisatie werk en inkomen(SUWI). Het is een besloten netwerk dat ondersteund, beheerd en verder ontwikkeld wordt door een onderdeel van het UWV (Uitvoerings-instituut WerknemersVerzekeringen). Via diverse applicaties bestaat toegang tot (persoons)gegevens van burgers, waaronder financiële data. De bronhouders van de gegevens zijn onder andere de Gemeentelijke Sociale Diensten, het UWV en de Sociale VerzekeringsBank, maar ook de belastingdienst en de rijksdienst voor het wegverkeer. Naast deze partijen hebben ook de Immigratie- en NaturalisatieDienst, de Inspectie SZW, gemeentelijke belastingdeurwaarders, gemeenten in het kader van de meld- en coördinatiepunten voortijdig schoolverlaters en de Stichting Netwerk Gerechtsdeurwaarders toegang tot het netwerk. Er zijn veel protocollen en richtlijnen voor de toegang gemaakt, maar daar blijkt een meerderheid van de gemeenten zich niet aan te houden.

Inhoud

Welke soorten gegevens zijn zo al in te zien? Dat blijkt ontstellend veel te zijn: verblijfsplaats, gezagsverhouding op werk, arbeidsinformatie, inkomsten-verhoudingen, uitkeringsaanvragen, resultaat van opleidingen, loon, voertuigregistratie(bron: Rijksdienst voor het wegverkeer), gegevens belastingdienst, studiefinanciering, rechtstreeks betaalde alimentatie, onbelaste reiskosten, aanvragen re-integratie-trajecten, vorderingen, arbeidsgeschiktheid, medebewoners op het huidige adres, huwelijk/partnerschap en relaties.(bron: NRC dd 13-08-2015).

Kortom het hele sociale en financiële doopceel van iedere Nederlander. Het is als het ware de pendant van de medische domein met medische data van burgers die bij zorgaanbieders opgeslagen zijn. Men zou veronderstellen dat de partijen die toegang hebben tot Suwinet dan ook zorgvuldig omgaan met die data in het kader van de privacy, maar niets blijkt minder waar te zijn. Ondanks alle mooie woorden in protocollen en voorschriften wordt er in de praktijk de hand mee gelicht. Het is een netwerk geworden van brondossierhouders met zeer veel personen/instanties die toegang hebben tot die brondossiers, ook al zeggen de protocollen het tegenovergestelde.

Wat gaat er mis?

Gemeentelijke diensten blijken niet alleen gegevens op te kunnen vragen van onder hun aandachtsgebied vallende burgers, maar van alle burgers. Niet-gemeentelijke instanties die door de gemeente ingehuurd zijn, zoals private incassobureaus blijken niet correct geautoriseerd, toch toegang te hebben tot het netwerk. Inzage van gegevens beperkt zich niet tot debiteuren die aangemaand moeten worden, maar kan zonder beperking ook de data van alle burgers omvatten. De republiek Ierland bleek niet alleen toegang te hebben tot data van Ieren die woonachtig waren in ’s-Hertogenbosch, maar tot die van alle mensen die woonachtig zijn in Nederland. Bovendien bleek de aanvankelijke permissie niet op tijd verlengd te zijn. Het onderzoeksprogramma Argos, van Vara, VPRO en Human, stelt heel

terecht dat uitbesteden en toegang tot Suwinet niet samengaan.

Tegenhanger

Bij vergelijking met het medisch dataverkeer, waarvoor het Landelijk SchakelPunt(LSP) als allesbeheersend systeem gepusht wordt, valt op dat er daar ook sprake is van een fors aantal brondossierhouders met een zeer groot aantal personen die deze gegevens kunnen opvragen. Het gaat net als bij het Suwinet om pull-dataverkeer. De toegang is wel beveiligd met de UZI-pas met pincode, maar dat is geen garantie voor inzage door onbevoegden/on-geautoriseerden op de werkplek. In 2011 werd een onderzoek gepubliceerd bij apothekers, waaruit bleek dat zeer slordig omgegaan werd met de UZI-pas(niet uitloggen bij verlaten werkplek, elkaars inlog-gebruiken etc.). Onbevoegd toegang krijgen tot het systeem is in het medische data-netwerk van het LSP evengoed mogelijk als bij het Suwinet. Doordat zowel het Suwinet als het LSP een bijzonder groot aantal personen met een toegangsautorisatie kennen, is misbruik bij beide netwerken zeer wel mogelijk. In ziekenhuizen wordt de beveiligde toegang tot computerwerkplekken vaak door werknemers als lastig ervaren. Inlog op elkaars toegangspas, noteren van wachtwoorden op of bij het beeldscherm komt helaas vaak voor. Onbevoegde toegang tot het LSP-systeem is daardoor mogelijk.

Misbruik

Bij Suwinet is meermalen gerapporteerd dat ambtenaren zich meermalen toegang verschaften tot gegevens van Bekende Nederlanders(BN-ers) zonder ambtelijke noodzaak. Hoewel duidelijke protocollen over bestaan over wat wel of niet mag, blijken ambtenaren ongewenste menselijke zwakheden te bezitten. Van een ambtenaar in Leiden werd dit via de logging van de inzagen opgespoord. Welke straf deze ambtenaar kreeg bleef geheim. Bij misbruik van de toegang tot het LSP zijn hoge geldboetes vastgelegd. Controle op onterechte inzage is evenals bij het LSP-gebruik pas achteraf mogelijk. Evenals bij

het LSP-gebruik kan de burger bij het Suwinet opvragen of er gegevens over het netwerk zijn verzonden en wie met wie communiceerde.

Toegang

Hoewel er nog geen berichten zijn gepubliceerd over onterechte toegang tot patiëntgegeven via het LSP is het gewoon een kwestie van wachten tot zulks plaats vindt. In wezen vindt er op huisartsenposten al onterechte toegang plaats, omdat bij iedere patiënt die op de post komt en die in de LSP-index voorkomt de gegevens bij de brondossiers opgevraagd worden nog voor de huisarts de patiënt ziet. Louter het feit dat de post bezocht wordt is reden om de data op te vragen, niet de vraag van de dienstdoende huisarts om de gegevens te mogen inzien. Als reden wordt opgegeven dat zo het consult op de post niet vertraagd wordt door LSP-bevraging, maar het klopt niet dat in een aantal gevallen onnodig gegevens opgevraagd worden.

Het grote probleem met zowel Suwinet als LSP is de massale toegangsmogelijkheid van de brondossiers, waarbij gemakzucht en menselijke zwakheden maken dat gegevens onterecht kunnen worden ingezien. Hoewel er veel ruchtbaarheid gegeven is aan de Suwinet-problemen is het onbegrijpelijk dat er niet veel meer burgerprotest is tegen een overheid die de privacy van de eigen burgers ernstig schendt in weerwil van fraai papierwerk.

De hier gemaakte fouten moeten ons extra alert maken ten aanzien van problemen bij het medische pull-dataverkeer.

W.J. Jongejan

Voor reacties: zie sidebar op de volgende pagina