Overheid en ICT – Bepaald geen liefdesbaby

(Dit is een aangepaste versie van een eerdere internetconsultatie)

Registratie in een speciale database kent een aantal bezwaren:

- Het is een ineffectief middel, en vergroot daarnaast onveiligheid voor hen die niet kunnen of willen geregistreerd staan.
- Het is immoreel om een gestigmatiseerde groep te registreren. De redenering dat er wel meer beroepen zijn met vergunningen gaat niet op voor sekswerk, zolang het werk niet is genormaliseerd.
- Een database volgt de regel dat als het kán lekken, dan zál het lekken, want elk computersysteem bevat zwakheden, vooral de menselijke.
- Daarnaast is de grondslag die men nu via de Wgts probeert te creëren een onjuiste (voor inhoudelijke juridische argumenten verwijs ik u graag door naar de brief van SekswerkExpertise en Vereniging voor Vrouw en Recht).

In de (oorspronkelijke) Memorie van Toelichting:

Indien prostituees onvoldoende vertrouwen hebben in de beveiliging van het systeem en bang zijn dat hun gegevens op straat komen te liggen, kan dit ertoe leiden dat ze juist de illegaliteit in gaan met alle risico's voor veiligheid en gezondheid van dien. Dit zou bijzonder onwenselijk zijn en een tegengesteld effect bereiken van wat beoogd wordt.

Nou, we hebben nieuws! Sekswerkers hebben inderdaad geen vertrouwen in de beveiliging van het systeem.

Eens even langs lopen hoe het staat met de ICT projecten van de Overheid:

"Wie naar de projecten van de afgelopen jaren kijkt, ziet variaties op steeds weer dezelfde thema's. Een aan moedwillige blindheid grenzend optimisme bij verantwoordelijke bestuurders, die in digitale verbouwingen een kans zien om snel politieke dromen te verwezenlijken, maar weinig willen begrijpen van de soms enorme inspanningen die dat vergt." (bron: artikelen NRC)

"De Overheid loopt hopeloos achter in kennis" schrijft Huib Modderkolk in zijn boek 'Het is oorlog en niemand die het ziet'. Als er één les te trekken valt uit dit boek is dat in ELK systeem binnen is te dringen.

Rop Gongrijp: "Het internet is een fundamenteel onveilige plaats. De overheid zou daarom eens moeten ophouden privacygevoelige gegevens in databases te stoppen".

Niks te verbergen?

Het argument rondom privacy dat je toch niks te verbergen heb (lees: fout gedaan) betekent in de eerste plaats dat je dus niet geregistreerd hoeft te worden. Want waarom zou je bij voorbaat verdacht moeten zijn? En hen die wel wat te verbergen hebben zullen de registratie vermijden dan wel het gesprek in gaan en weten wat ze moeten antwoorden om het te blijven verbergen.

Daarnaast is privacy versus veiligheid een valse tegenstelling, het gaat om rechtsbescherming, en zéker gemarginaliseerde groepen hebben die behoefte.

Globaal zijn er 5 categoriën van incidenten:

1. Falende ICT projecten
2. Een datalek (als blunder)
3. Een datalek (bewust veroorzaakt door een derde partij)
4. Een hack
5. Data ten onrechte voor andere/uitgebreidere doelen gebruikt

1. Falende ICT projecten

- Vernieuwing van de ICT systemen bij de NVWA, na 65 miljoen bleek er maar weinig te werken.
- De problemen met een ICT-verbouwing bij het Centraal Bureau Rijvaardigheidsbewijzen (CBR) zorgen voor grote vertraging bij rijbewijskeuringen.
- De Belastingdienst probeert sinds 2005 een systeem te bouwen dat alle transacties van de fiscus zou verwerken, na negen jaar en 203 miljoen euro gaven ze het op.
- Defensie bouwt sinds 2002 aan 'Speer'. Na volgens eigen zeggen 433 miljoen euro te hebben uitgegeven – de Algemene Rekenkamer kwam op 900 miljoen euro uit – gaf het ministerie het in 2015 op.
- Het bevolkingsregister BRP. Daarvan werd de ontwikkeling in 2017 stopgezet, na tien jaar bouwen en 100 miljoen aan uitgaven.
- De digitalisering van de rechtspraak, die in april 2018 na zes jaar en ruim 200 miljoen euro (oorspronkelijk werden de kosten op 7 miljoen euro geschat) werd stopgezet.
- Werkzoekenden werden helemaal wanhopig van werk.nl van uitkeringsinstantie UWV.
- Het EPD, het Elektronische Patiëntendossier, is een echt hoofdpijndossier. Ging van start in 2008 onder Min van VWS, en functioneert nog niet.
- Het lukt tot nu toe niet om bij de KVK om de systemen van het Handelsregister te vereenvoudigen.

2. Datalek (als blunder)

Justitie (OM) blundert door gegevens van personeel Fruithandel in strafdossier te stoppen, medewerkers doodsbang omdat de verdachten van coke handel toegang hebben gekregen tot deze gegevens.

In 2018 zijn er 20.881 datalekken gemeld aan de **Autoriteit Persoonsgegevens (AP**). Vergeleken met voorgaande jaren is het aantal meldingen fors gestegen. Het meest voorkomende type datalek is het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger (63% van de meldingen). Het kwijtraken of de diefstal van een gegevensdrager zoals een laptop of usb-stick (14%) is daarna het meest voorkomende type datalek. **De meeste datalekken dus zijn het gevolg van menselijk falen**.

Een kleine greep uit de nieuwsberichten:

- USB stick gestolen bij Officier van Justitie in Rotterdam (maart 2016)
- De politie heeft afgelopen nacht bij een huiszoeking in Emmen een draaiboek en een usb-stick laten liggen (nov 2012)

- Een medewerker van het ministerie van Buitenlandse Zaken heeft de stick laten liggen in een huurauto in Polen. Eerder raakten medewerkers van het ministerie van Defensie usb-sticks kwijt. Een daarvan werd ook teruggevonden in een huurauto. (2007)
- Ziekenhuizen lekken dagelijks privacygevoelige informatie, grotendeels veroorzaakt door onbeveiligde verbindingen en door menselijke fouten. Bijvoorbeeld door niet-beveiligde USB-sticks te laten slingeren (2017).

3. Datalek (bewust veroorzaakt door een derde partij)

- RDW gegevens, de gegevens van 11.5 miljoen mensen in Nederland lopen het risico lopen om deel te worden van een online handel (via Telegram) van persoonsgegevens. De handelaren deze gegevens van contactpersonen bij de RDW zelf.
- Een antiprostitutiegroep uit Duitsland heeft sekswerkers bewust geout door persoonlijke details online te zetten via Google Maps, "Whore Hunt 2.0" (mei 2016) https://www.dazeddigital.com/artsandculture/article/31321/1/german-sex-workers-have-addresses-leaked-on-google-maps en https://www.vocativ.com/324131/sex-workers-dox/index.html

4. Hack

In 2021 zijn er bijna 25.000 datalekken gemeld, met als opvallend detail dat datalekken ten gevolge van een cyberhack bijna is verdubbeld (naar 9%). De jaarcijfers van 2022 zijn nog niet bekend op dit moment.

- Diginotar was een combinatie van een hack (door Iran) en van stupide gemakzucht (er was een kabeltje doorgetrokken om niet steeds de beveiligde kluis in te moeten waar het koud was).
- Hack bij UWV in mei 2019: 117.000 cv's gestolen va werkzoekenden.
- Website Hookers gehackt (oktober 2019). De accountgegevens van de 250.000 gebruikers van Hookers zijn uitgelekt door een lek in de populaire forumsoftware vBulletin. Een hacker heeft de emailadressen van de leden buitgemaakt en biedt ze te koop aan voor 300 dollar.
- De lijst hoe er gehackt kan worden is eindeloos. Door malware in de router, malware op een usb stick, een DDos aanval, malware via downloads, een emailbijlage, een nagebouwde website, dmv phishing (gegevens ontfutselen), kwetsbaarheden in niet geupdate software, een zero day exploit, door ransomeware, openbare wifi of andere manier van afluisteren, en door spullen te laten rondslingeren en kwijt te raken, maar uiteindelijk is meestal de mens de zwakste schakel.
- Ransomeware staat momenteel in de belangstelling, die heeft vooral een financieel doel.

5. Data ten onrechte voor andere/uitgebreidere doelen gebruikt

- De Sleepwet, de Wiv, de Wet op de inlichten en veiligheidsdiensten, bij de evaluatie van september 2019 bleek dat gegevens zo breed worden opgeslagen, dat er geen sprake van is dat de interceptie 'zo gericht mogelijk' is. De CTIVD constateerde in eerdere rapportages al dat de inlichtingendiensten de rechtsbescherming van burgers nog niet op orde hebben. Dat levert 'hoge risico's' op voor onrechtmatig handelen door de diensten.
- SyRi, Systeem Risico Indicatie, het fraudesysteem van de Overheid, koppelde teveel systemen aan elkaar, gebruikte datamining en patroonherkenning in een soort blackbox

(algoritmes), maakte daardoor burgers bij voorbaat verdacht, en leverde tenslotte ook nog weinig op aan fraudezaken. Gelukkig is SyRi door de rechter naar de prullenbak verwezen, maar helaas is er een nog erger systeem uit voort gekomen, een soort SuperSyRi.

- Politie loerde jarenlang onterecht in data van milieucamera's (oktober 2019). Er ontbrak een wettelijke basis om de milieuzonecamera's (Amsterdam) te delen met de politie. Bovendien maken de deskundigen zich zorgen over de beveiliging van de privacygevoelige gegevens. Daarover zijn tussen de gemeente en politie geen formele afspraken gemaakt.
- Sekswerkers zijn in het verleden al geconfronteerd dat info in het ene systeem toch in het andere systeem terecht kwam, meestal algemene politiesystemen of de Marechaussee. Ook is er via het OM informatie gelekt naar het buitenland, waardoor de familie van sekswerkers werden ingelicht.
- In de MvT staat dat er geen koppeling wordt ingebouwd met de Belastingdienst en de Kamer van Koophandel. Nee, nú niet, maar die garantie is tot de deur.

Sekswerkers hebben met name te vrezen van:

- **Hun omgeving**. Wordt die lieve klant of die fijne partner een naarling die je op je zwakke plek wil raken? Outing door een bekende komt regelmatig voor, maar ook doxing komt voor. Dat is het achterhalen van de echte identiteit van een internetgebruiker, en het openbaren van die informatie op het web. Recent is doxing strafbaar geworden, heel goed, maar het kwaad is dan al geschied, het is beter het te voorkomen.
- **Hackers.** Er zijn er die 'online kattenkwaad' willen uithalen, en er zijn er die kwade bedoelingen hebben, en gericht gevoelige gegevens willen bemachtigen, bijvoorbeeld voor afpersing. Juist omdat sekswerk een gevoelig persoonsgegeven is, zal de database de bijzondere interesse hebben bij hackers.
- **Een combinatie van die twee.** Het is zeer denkbaar dat een hacker de database kraakt, waarna iemand uit de omgeving (klant of ex) gericht verder gaat zoeken, en de individuele koppeling weet te maken tussen BSN en NAW gegevens.

Conclusie

Behalve dat registratie niet werkt, de onveiligheid vergroot, immoreel is vanwege het stigma, een IT oplossing per definitie tot lekken en hacken zal leiden, is het ook zo dat sekswerkers weerbaar zijn. Ja, ook digitaal weerbaar, ze zijn taai en vasthoudend, overal ter wereld. Sekswerkers zijn door de geschiedenis heen creatief geweest in het vinden van nieuwe wegen en zo zal het ook gaan met het zoeken naar wegen buiten de registratie om. De WRS creëert op deze manier een waterbedeffect. Is dat het optuigen van weer een waardeloze Overheids-ICToplossing waard?