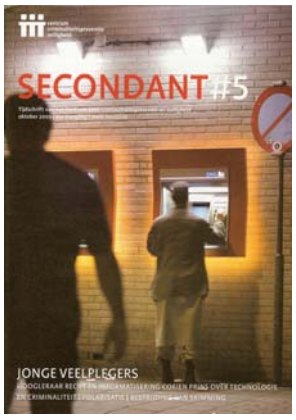
Interview Hoogleraar Recht en informatisering Corien Prins over risico's in de informatiesamenleving:

"Cybercrime is allesomvattend"

De overheid schiet tekort bij het voorkomen van internetfraude. Sterker nog de overheid werkt identiteitsfraude deels ook in de hand door geen paal en perk te stellen aan de informatiehonger van de overheid zelf en van het bedrijfsleven. Dat stelt professor Corien Prins in een interview met SECONDANT over de risico's van de digitalisering van de samenleving en de gevolgen voor de relatie tussen burgers en overheid. De hoogleraar Recht en informatisering aan de Universiteit van Tilburg pleit voor institutionele veranderingen om de aanpak van cybercrime effectiever te maken. "Cybercrime is allesomvattend en beïnvloedt de organisatie van de samenleving. De huidige instituties zijn niet berekend op bestrijding van hightech crime."

door Yvonne van der Heijden
De auteur is freelancejournalist.



Niet alleen maatschappelijke ontwikkelingen beïnvloeden de relatie tussen overheid en burger. Ook technologische ontwikkelingen zorgen voor veranderingen. "Je ziet bijvoorbeeld steeds vaker dat zowel de private als de publieke sector risico's naar de burger schuift", signaleert professor Corien Prins een trend in onze informatiesamenleving. "Als iemand fraude pleegt met jouw pinpas dan moet jij als burger bewijzen dat je je pincode goed hebt beschermd", noemt Prins als voorbeeld in een interview met SECONDANT op haar werkkamer op de Universiteit van Tilburg.

De hoogleraar Recht en informatisering reageert geprikkeld op de overheidscampagne *Veilig Internetten* waarvan minster Hirsch Ballin van Justitie deze zomer de aftrap heeft gegeven. Er ligt in haar ogen te veel de suggestie in besloten dat burgers veilig internetten volledig zelf in de hand hebben. Prins: "Het is goed dat de overheid op grote schaal informatie geeft over technologie en over de gevolgen van misbruik van technologie, want burgers zijn veel te naïef op dat vlak. Suggereren dat de oplossing bij de burger ligt, gaat echter veel te ver. De overheid heeft de plicht haar burgers te beschermen, ook tegen misbruik van nieuwe technologieën die het burgerschap aantasten. Bovendien heeft de overheid zelf ook een aandeel in de kwetsbaarheid en dus het terugdringen ervan."

“Wat betekent het als databestanden worden gekoppeld of door criminelen gekraakt?”

Professor Prins onderzoekt als lid van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) hoe het gebruik van technologie de relatie tussen overheid en burger beïnvloedt. “De inzet van technologie verandert de positie van de burger. Het elektronisch kinddossier, het patiëntendossier en de OV-chipkaart zijn enkele willekeurige voorbeelden waarbij de overheid digitaal persoonlijke gegevens opslaat. Welke gevolgen kan het hebben voor de burgers als de overheid op grote schaal informatie over ons allemaal verzamelt en bewaart? Wat betekent het als databestanden worden gekoppeld of door criminelen gekraakt? De kern van het probleem is dat we onvoldoende kritisch nadenken of we de berg informatie die wordt gecreëerd wel willen en hoe we informatie die daadwerkelijk nodig is, goed kunnen beveiligen tegen criminelen”, stelt Prins.

Informatiehonger

De overheid schiet voor Prins onder meer tekort bij het voorkomen van internetfraude. Sterker nog, de overheid werkt volgens haar identiteitsfraude deels in de hand door geen paal en perk te stellen aan de informatiehonger van de overheid zelf en van het bedrijfsleven. Prins: “Het is gewoon geworden om een kopie van een paspoort te maken, zoals in hotels. Het is in strijd met de wet, maar wordt oogluikend toegestaan. Daardoor komen naast naam en woonplaats, ook paspoortnummer, geboortedatum en burgerservicenummer in het computersysteem van het hotel. Misdadigers die op internet actief zijn vegen alle persoonlijke gegevens die ze links en rechts vinden bij elkaar en kunnen hun criminele gang gaan.”

“De oorspronkelijke betekenis van privacy is: ik wil met rust gelaten worden. Maar we worden al lang niet meer met rust gelaten.”

Prins deelt de kritiek van het College bescherming persoonsgegevens (CBP) dat gemeenten, provincies en andere overheden vaak te lichtzinnig omgaan met persoonsgegevens en vindt het goed dat het CBP richtlijnen heeft gepresenteerd voor de publicatie van persoonsgegevens door overheden op internet. “De oorspronkelijke betekenis van privacy is: ik wil met rust gelaten worden. Maar we worden al lang niet meer met rust gelaten. Onder beschermen van privacy waartoe ook de overheid gehouden is, valt in onze huidige samenleving ook het terugdringen van de kwetsbaarheid die voortvloeit uit het verzamelen van informatie. Privacy en identiteitsfraude hangen namelijk met elkaar samen.”

Slordig

Bij dit alles wil Prins wel de kanttekening maken dat burgers veel te slordig omspringen met hun persoonlijke gegevens en daardoor gemakkelijker slachtoffer worden van

identiteitsfraude. “Mensen hebben over het algemeen geen idee wat allemaal kan gebeuren met hun persoonlijke gegevens als criminelen er de hand op weten te leggen. Het niet zo moeilijk via internet aanvullende informatie te vinden over een persoon, zeker niet nu mensen zich massaal aansluiten bij netwerksites als Facebook en Hyves. Uiteindelijk is het vrij gemakkelijk om de identiteit van iemand anders aan te nemen. De campagne *Veilig Internetten* is in die zin wel degelijk zinvol om burgers bewuster te maken van de risico’s van identiteitsfraude. Want als je gegevens eenmaal op internet staan, komen ze er nooit meer af.”

Prins beaamt dat vóór de komst van computers en internet ook identiteitsfraude werd gepleegd met gestolen identiteitspapieren. “Maar de gevolgen daarvan waren veel minder verstrekkend. Het gaat nu niet meer zozeer om het stelen van persoonsgegevens op zich, maar veel meer om de technische mogelijkheden die er zijn om persoonlijke gegevens te combineren. Als je wordt gebeld door iemand die je voornamen weet en weet waar je woont en ook nog eens je paspoortnummer en BSN noemt, dan denk je toch op zijn minst dat je iemand van je bank aan de lijn hebt en niet dat je met iemand van doen hebt die nog meer persoonlijke gegevens van je wil lospraten, zoals de pincode van je bankpas.”

Doorlopend slachtofferschap

Ook de vorm van het slachtofferschap bij identiteitsfraude is door nieuwe technologieën ingrijpend veranderd. De digitalisering van allerlei systemen zoals in de zorg, op de arbeidsmarkt en bij de fiscus leidt er toe dat een geslaagde identiteitsfraude in een van de ketens zich bijvoorbeeld ongemerkt kan verspreiden naar andere ketens. Ook weet je als slachtoffer niet onmiddellijk dat bijvoorbeeld de gegevens van je bankpas of creditcard zijn gekopieerd. Prins: “Het is voor slachtoffers volstrekt onmogelijk geworden inzicht te krijgen in wat er is gebeurd. Als je creditcardgegevens zijn verkocht naar Oost-Europa zul je niet weten waar het ooit is begonnen en hoe je gegevens zich als een olievlek hebben verspreid. Er is sprake van doorlopend slachtofferschap.”

“Als het kabinet werkelijk misbruik van internet wil verminderen, dan zal het op een andere manier met de politieorganisatie moeten omgaan”

De daadwerkelijke aanpak van cybercrime laat volgens Prins veel te wensen over. Op de eerste plaats heeft de politie onvoldoende kennis en capaciteit om internetcriminelen op te sporen en te vervolgen. Bovendien staat deze capaciteit bij de politie niet in verhouding tot de enorme toename van het gebruik van technologie. De achterstand in cyberspace kan de politie zelf niet worden aangerekend, benadrukt Prins. “Het is een politiek vraagstuk. Het oplossen van internetcrime is een tijdrovend proces waarmee de politie niet snel kan scoren. Als het kabinet werkelijk misbruik van internet wil verminderen, dan zal het op een andere manier met de politieorganisatie moeten omgaan. Dan moet het kabinet afstappen van de bonnenschrijfcultuur waarbij financiering onder meer gekoppeld is aan quota voor het uitschrijven van bonnen. Dan moet geld worden gestoken in

uitbreiding van capaciteit bij de politie en in opleiding en training op het gebied van e-crime. Bovendien moet de samenwerking anders worden georganiseerd want internet houdt niet op bij de grens van een politieregio."

Wijdvertakt

In het WRR-rapport dat in het najaar van 2010 moet verschijnen zullen aanbevelingen staan over onder meer aanpassingen die noodzakelijk zijn binnen instituties om de kwetsbaarheid terug te dringen. De ideeën die professor Prins daarover heeft, zijn nog niet uitgekristalliseerd. Ze geeft voorzichtig aan wat allemaal meespeelt bij de gedachtebepaling over dit omvangrijke vraagstuk.

"Overal ligt een deeltje van de informatie, van de bevoegdheden en van de verantwoordelijkheden"

"Kenmerkend voor het gebruik van nieuwe technologieën is dat ze wijdvertakt zijn, zowel in de publieke, als in de private sector. Cybercrime is allesomvattend en beïnvloedt de organisatie van de samenleving. De huidige instituties zijn niet berekend op bestrijding van hightech crime. Overal ligt een deeltje van de informatie, van de bevoegdheden en van de verantwoordelijkheden. Daarom vereist de aanpak van internetfraude ook institutionele veranderingen."

Prins: "Verder moeten we van onderop duidelijk zien te krijgen waarom iemand slachtoffer wordt van cybercrime. We moeten een scherp beeld hebben van de realiteit van alle dag. Hoe wij als burgers en als overheid met informatie omgaan in de samenleving, speelt ook mee. Het is veel meer dan een juridische kwestie of een privacyaangelegenheid. De houding die wij aannemen tegenover informatie is cultureel bepaald en niet onbelangrijk als het gaat over de implicaties van de inzet van technologie in onze relatie met de overheid."

Meer dan ICT

Professor Prins, die zich in Tilburg bezighoudt met actuele juridische problemen rond nieuwe technologieën, beklemtoont dat de vraagstukken die zij onderzoekt veel breder liggen dan ICT. Ook humane biotechnologie, nanotechnologie en neurotechnologie gecombineerd met het vermogen van de mens kennis te vergaren, behoren tot haar onderzoeksveld. "Ook deze technologieën raken de relatie tussen overheid en burger. Als de overheid recidive wil terugbrengen, kan dat door een misdadiger therapie te laten ondergaan. Maar als er sprake is van een gekend probleem in de hersenen, kunnen medicijnen een oplossing bieden. De vraag is welke gevolgen die aanpak heeft op de lange termijn en wie daarvoor verantwoordelijk en aansprakelijk is. Hoe ver gaat de zorgplicht van de overheid voor de burgers?", geeft Prins een voorbeeld uit de neurotechnologie.

Publiek debat ontbreekt

Ondanks de gevaren die het gebruik van technologie met zich meebrengt voor de samenleving in haar geheel en de burgers in het bijzonder ontbreekt in Nederland een publiek debat over de digitalisering van de samenleving. Onzichtbaarheid van wat zich afspeelt en onkunde, geeft Prins aan als twee bepalende factoren voor de stilte die hangt rond de maatschappelijke invloed van technologische ontwikkelingen. “Met nieuwe technologieën creëren we een wereld die niet wordt gezien en de kwetsbaarheid ervan evenmin. Ook is er bij burgers en overheid een groot gebrek aan kennis over de gevolgen van de inzet van technologie op allerlei terreinen. En iedereen is met zijn eigen toko bezig. Er is niemand die de optelsom van de toko’s maakt. De toenemende kwetsbaarheid van de samenleving door gebruik van nieuwe technologieën blijft daardoor vanuit juist de optelsom onbesproken”, aldus Prins.

“Stel dat de databank wordt gekraakt, dan krijgen misdadigers de beschikking over unieke kenmerken van mensen”

Bovendien is ‘publiek belang’ een ongrijpbaar begrip. “In het bedrijfsleven is beschermen tegen kwetsbaarheid meer ingeregeld. Je wordt afgerekend op financieel verlies als de beveiliging van het netwerk niet op orde was. Iemand moet hangen. Maar wie kan worden afgerekend op de kwetsbaarheid van de maatschappij?”, stelt Prins een retorische vraag. Ze neemt als voorbeeld de nationale databank biometrie die in de maak is en waarin alle vingerafdrukken en gezichtscans worden opgeslagen. “De biometrische databank is in beginsel alleen toegankelijk voor misdaadbestrijders en inlichtingendiensten. Maar stel dat de databank wordt gekraakt, dan krijgen misdadigers de beschikking over unieke kenmerken van mensen. De vraag wie verantwoordelijk is voor de kwetsbaarheid door technologische ontwikkelingen staat hiermee direct in verband.”

Kwetsbaarheid

De stelling van Prins is dat we leven in een kwetsbare samenleving. Dat is alleen al af te leiden uit actuele problemen, zoals de financiële crisis en de Mexicaanse griep die dreigt. “De digitalisering van de samenleving vormt een onderdeel van die kwetsbaarheid. Je wilt niet weten wat er gebeurt als er iets mis gaat met de systemen in de petrochemische industrie in Pernis. Als overheid kun je technologie inzetten om kwetsbaarheid buiten de deur te houden, zoals bij terrorismebestrijding. Maar aan de andere kant neemt de kwetsbaarheid van de samenleving toe door gebruik van technologie. Als er bij wijze van spreken één gek de stekker eruit trekt, weten we niets meer in dit land. Mijn boodschap aan de overheid is: denk ook eens na over andersoortige kwetsbaarheden en schep de juiste randvoorwaarden.”

Tot slot betoogt Prins dat de rol van de burger niet alleen verandert omdat de overheid technologie inzet. Technologie geeft burgers zelf instrumenten in handen om de overheid te controleren en ter verantwoording te roepen. Bijvoorbeeld met interactieve

toepassingen op internet, aangeduid met de term Web 2.0, kunnen burgers informatie verzamelen en hun eigen kennisplatform oprichten. Prins: “Web 2.0 stelt burgers in staat zelf content te creëren. Daarmee kunnen burgers een eigen vorm van invloed scheppen om van overheid en bestuur transparantie te verlangen. Zo is er een site waarop het stemgedrag van gemeenteraadsleden wordt bijgehouden en zijn er sites waarop burgers kunnen invullen wat er mis is in hun stad. Er kan daar een kennisniveau ontstaan dat iemand in z’n eentje nooit zou kunnen bereiken en dat betekent in potentie een versterking van de positie van de burger.” <<