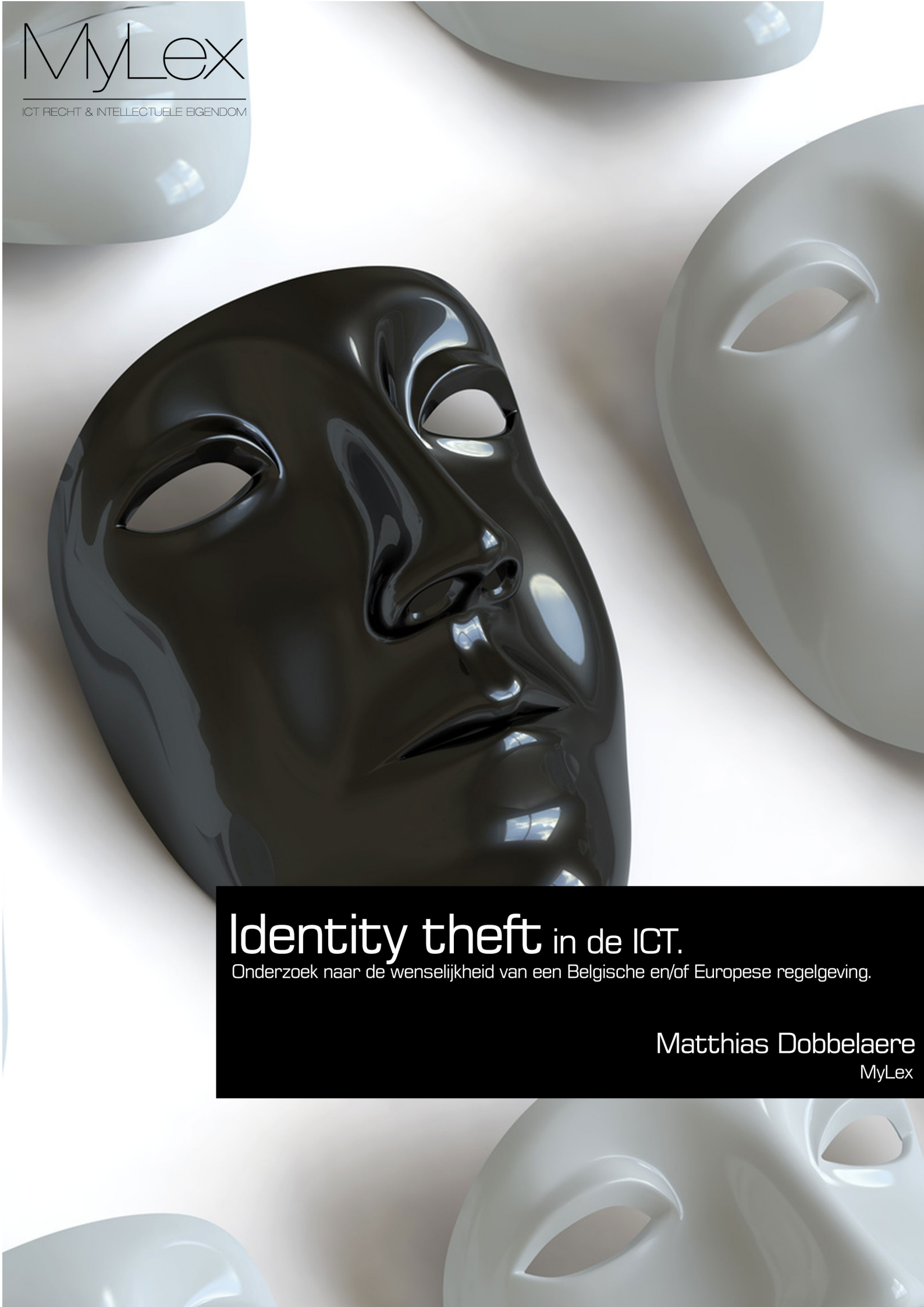
MyLex

ICT RECHT & INTELLECTUELE EIGENDOM



Identity theft in de ICT.

Onderzoek naar de wenselijkheid van een Belgische en/of Europese regelgeving.

Matthias Dobbelaere

MyLex

ONDERZOEK NAAR DE WENSELIJKHEID VAN EEN BELGISCHE EN/OF EUROPESE REGELGEVING OVER "IDENTITY THEFT".

MATTHIAS DOBBELAERE
Waarschoot
MyLex
2010.

145 pagina's.
NUR 824

Omslagontwerp: CYLIX Design Studio.

MyLex
Koudekeuken 2, 9950 Waarschoot, Tel. +32(9)329 51 19.

INHOUDSTAFEL

DEEL 1: INLEIDING EN BEGRIPSOMSCHRIJVING 10

HOOFDSTUK 1: INLEIDING 10

HOOFDSTUK 2: OPBOUW 11

HOOFDSTUK 3: DEFINITIE IDENTITY THEFT 12

HOOFDSTUK 4: IDENTITY THEFT SENSU LATO 14

AFDELING 1: Financiële identiteitsdiefstal 14

AFDELING 2: Identiteit klonen 15

AFDELING 3: Criminele identiteitsdiefstal 15

AFDELING 4: Medische identiteitsdiefstal 16

HOOFDSTUK 5: SENSU STRICTO: IDENTITEITSDIEFSTAL BEPERKT TOT DE ICT 17

DEEL 2: VORMEN EN TOEPASSINGSGEVALLEN 18

HOOFDSTUK 1: IDENTITEITSKAARTFRAUDE 18

AFDELING 1: Inleiding 18

AFDELING 2: Myths & Facts: kernfuncties van de eID. 19

§ 1. Authentificatie 19

A Authentificatie van documenten 19

B Authentificatie voor toelating website via certificaat. 20

C Authentificatie tot veilige chatruimtes 20

§ 2. Digitaal ondertekenen 21

§ 3. Lezen van data 22

§ 4. Encryptie en decryptie 23

§ 5. In de toekomst? 23

AFDELING 3: Internationale toepassing 23

AFDELING 4: Veiligheid en risico's 24

§ 1. Privacy. 24
§ 2. Softwarematige tekortkomingen 25
AFDELING 5: Identity Theft 26
HOOFDSTUK 2: FINANCIËLE ID-THEFT: SKIMMING 28
AFDELING 1: De techniek 28
AFDELING 2: Gevolgen 29
AFDELING 3: En wat met de identiteit? 31
AFDELING 4: Oplossingen 32
HOOFDSTUK 3: FINANCIËLE ID-THEFT: ONLINE BETAALSYSTEMEN 33
AFDELING 1: Beginstadium 34
AFDELING 2: Digipass 34
AFDELING 3: Toekomst? 35
AFDELING 4: Phishing 36
HOOFDSTUK 4: SOCIALE NETWERKSITES 37
AFDELING 1: Opkomst sociale netwerksites 38
AFDELING 2: Privacy & identiteitsdiefstal 40
AFDELING 3: Profielkaping: manieren 46
§ 1. Social engineering 46
A Persoonlijk contact 46
B E-mail 46
C Dumpster diving 47
§ 2. Automatische tools 47
AFDELING 4: Oplossingen 48
HOOFDSTUK 5: CHATPROGRAMMA'S 50
AFDELING 1: Pedofilie 50
AFDELING 2: Oplossing? 50

AFDELING 3: Chatboxen als instrument 51
HOOFDSTUK 6: WIFI-LIFTEN 51
AFDELING 1: Inleiding 51
AFDELING 2: Feitelijke omstandigheden WiFi-case 52
AFDELING 3: Strafbaarheid WiFi-Liften 54
AFDELING 4: Ontbreken van beveiliging: cijfers & gevaren 55
AFDELING 5: De uitspraak 56
AFDELING 6: Rechtsvergelijkend: het Datacenter-vonnis. 56
AFDELING 7: Besluit 57
HOOFDSTUK 7: LOCATION-BASED (SOCIAL NETWORKING) APPLICATIONS 58

DEEL 3: HUIDIGE EN TOEKOMSTIGE BEVEILIGINGSMECHANISMEN 62
HOOFDSTUK 1: PASWOORDEN 62
HOOFDSTUK 2: ENCRYPTIE 64
HOOFDSTUK 3: BIOMETRIE 65
HOOFDSTUK 4: ANTI ID-THEFT SOFTWARE 70
HOOFDSTUK 5: KWETSBAARHEID 72

DEEL 4: CIJFERS & KOSTEN VOOR DE OVERHEID, BEDRIJVEN EN PARTICULIEREN 74
HOOFDSTUK 1: RISICOGROEP IDENTITEITSDIEFSTAL 74
HOOFDSTUK 2: CIJFERS IN DE V.S. 75
HOOFDSTUK 3: CIJFERS IN HET V.K. 78
HOOFDSTUK 4: CIJFERS IN BELGIË. 79

DEEL 5: HET RECHT, EEN VERGELIJKING. 81
HOOFDSTUK 1: VERENIGDE STATEN 81

AFDELING 1: Federal Identity Theft and Assumption Deterrence Act 81
AFDELING 2: State vs. Leyda 82
AFDELING 3: Flores-Figueroa v. United States 83
AFDELING 4: FAIR AND ACCURATE CREDIT TRANSACTIONS ACT EN THE IDENTITY THEFT PENALTY ENHANCEMENT 85
AFDELING 5: USA v. Gonzalez 85
AFDELING 6: Federal Trade Commission 85
AFDELING 7: Wetgeving Staten 86
AFDELING 8: Identity Theft Data Clearinghouse 87
AFDELING 9: Social Security Number 88
AFDELING 10: Bewustwording 90
HOOFDSTUK 2: VERENIGD KONINKRIJK 92
AFDELING 1: Inleiding 92
AFDELING 2: Achtergrond Fraud Act 93
AFDELING 3: Achtergrond National Identity Card Act 99
AFDELING 4: Bewustwordingscampagnes 103

DEEL 6 : NOODZAAK VAN EEN BELGISCHE OF EUROPESE REGLEMENTERING INZAKE IDENTITY THEFT? 104

HOOFDSTUK 1: SITUATIE IN EUROPA 104
AFDELING 1: Cybercrime-verdrag 104
AFDELING 2: Europese Commissie 105
AFDELING 3: Wijziging richtlijn 2002/58/EG 107
AFDELING 4: Frankrijk 109
AFDELING 5: Duitsland 110
HOOFDSTUK 2: SITUATIE IN BELGIË 111

AFDELING 1: Valsheid in informatica (art. 210bis Sw.) 114

AFDELING 2: Informaticabedrog (art. 504quater Sw.) 118

AFDELING 3: Computerinbraak (art. 550bis Sw.) 121

AFDELING 4: Datamanipulatie (art. 550ter Sw.)..... 124

CONCLUSIE 127

BIBLIOGRAFIE 131

DEEL 1: INLEIDING EN BEGRIPSOMSCHRIJVING

HOOFDSTUK 1: INLEIDING

"Een van de rampen die het menselijk intellect heeft ontketend, is de bedreiging van het privé-leven, de persoonlijkheid en het denkvermogen zelf van het individu. Deze waarden die tot dusverre alles - zelfs de meest onmeedogende dictaturen - hebben overleefd, zijn de wezenlijke factoren van de vooruitgang en het leven van de beschavingen. Er bestaat immers geen vrije, dus vruchtbare, gedachte als zij niet kan ontluiken, groeien of zich verschuilen in de beslotenheid van het individu - al naar zijn soevereine keuze - bij zijn meest intieme emoties. Zonder de voortdurende mogelijkheid van beschermende geheimhouding en vergetelheid, bestaat er geen vrijheid, geen waardigheid en dus ook geen beschaving.

Maar als gevolg van de onstuitbare ontwikkeling van wetenschap en techniek, en vooral van de ordeloze, commerciële en totalitaire exploitatie ervan, zijn en zullen steeds meer middelen ontstaan waarmede steeds zwaardere inbreuken kunnen worden gepleegd op het privé-leven en de persoonlijkheid van het individu."

Met deze woorden begon in België schuchter het debat rond privacy en haar bescherming. Aanleiding hiervoor was het wetsvoorstel van 1971 betreffende "*de bescherming van het prive-leven en de persoonlijkheid."*[1] , waarbij de drie Senatoren Pierson, Hambye en Vanderpoorten een bezorgde vraag stelden omtrent privacybescherming. Hoewel zij uiteindelijk het onderspit zouden delven, waren de eerste woorden van het privacydebat gevallen.

Anno 2010 is privacybescherming geen marginaal verschijnsel meer, maar wel een grondrecht. Een grondrecht dat eenieder alsmaar hoger waardeert, dankzij onze hoogtechnologische en hyperindividualistische maatschappij die bereikbaarheid, beschikbaarheid en performantie als essentieel beschouwt. Het onvermijdelijke gevolg daarvan is de steeds krachtigere roep naar privacy, naar ongestoorde rust.

[1] De bescherming van het prive-leven en de persoonlijkheid., Hoofdstuk IV, Controle op de gegevens behandeld met elektronische of andere middelen, Senaat, Zitting 1971-1972, document 142.

Privacy heeft er sinds enkele jaren echter een te duchten vijand bij. Alsof de hoogtechnologische maatschappij nog niet genoeg druk legde op de gemiddelde privacy van de burger, dient nu ook rekening te worden gehouden met *identity theft* of *identiteitsdiefstal.* Er bestaat immers geen grotere privacyinbreuk dan een inbreuk op de identiteitsdata *an sich.* Met ongekende technologische mogelijkheden, een steeds grotere verruiming van de informatiemaatschappij en een aanmerkelijk grotere honger naar informatie, zowel vanuit overheidskanalen als uit de private sector, is het een kwestie van tijd vooraleer de identiteitsbom ontploft.

Identity theft is heden ten dage een bijzonder actueel punt, en staat hoog genoteerd op menig politieke agenda. Essentiële vraag is dan ook of we reeds in staat zijn de implicaties van ons online (en offline) gedrag in te schatten, en hoe we identiteitsdiefstal, in allebei haar fasen (zie *infra*), het meest efficiënt kunnen bestrijden.

Die actuele bezorgdheid[2] is overigens geen overbodige luxe. Met beangstigende cijfers en statistieken in de Verenigde Staten en het Verenigd Koninkrijk lijken de eerste maatregelen meer vijgen na Pasen. Of is het toch nog niet te laat?

HOOFDSTUK 2: OPBOUW

Dit onderzoek gaat dieper in op identity theft, met een focus op de ICT-sector. Omdat vaak zeer technische en nieuwe procedés aangewend worden om in de online wereld identiteiten te stelen, is het noodzakelijk de technologische factoren ruim te belichten, en dit ondanks de juridische oorsprong van deze verhandeling.

Ultiem doel van dit inleidend werk is dan ook om juristen kennis te laten maken met de techniek die achter identity theft schuilt en technici vertrouwd te maken met het toepasselijke recht bij identiteitsdiefstal.

Er wordt aan de hand van enkele definities een begripsomschrijving opgebouwd voor identity theft in de ICT (informatie en communicatietechnologie). Daarnaast kan men in het tweede deel een resem vormen en toepassingsgevallen van dergelijke identiteitsdiefstal terugvinden, van elektronische identiteitskaarten tot sociale netwerksites. Een derde deel

[2] J. DENLOF, A. BOUCAR, D. REYNDERS, "Fraude d'identité, le crime du future?", Brussel, Politeia, 2005, 116.

belicht de huidige en toekomstige beveiligingsmechanismen. Cijfermateriaal, onder meer betreffende de kosten kan men terugvinden in het vierde deel. Het vijfde deel beoogt dan weer een rechtsvergelijkende studie, met een grote aandacht voor de landen die reeds grondig werk maakten van regelgeving rond identity theft, zoals de V.S. en het Verenigd Koninkrijk. Belangrijk is na te gaan in hoeverre deze oplossingen toepasbaar zijn op het continentale stelsel. Als laatste wordt de noodzaak voor een Belgische, dan wel Europese, regelgeving onderzocht.

HOOFDSTUK 3: DEFINITIE IDENTITY THEFT

"But he that filches from me my good name/Robs me of that which not enriches him/And makes me poor indeed."

- W. Shakespeare, Othello, act iii. Sc. 3.

In België bestaat geen eenduidige of uniforme definitie van identity theft. Bovendien is er geen specifieke strafbaarstelling van identiteitsfraude. Een mogelijke oplossing is over de grenzen heen te kijken naar definities die in andere landen, die reeds verder staan in de aanpak van identity theft, worden gebruikt.

Zo wordt in de V.S. identity theft omschreven als "*knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal Law, or that constitutes a felony under any applicable State or local law".* [3]

In Canada wordt dat *"Par vol d'identité, on entend tous les types de crimes qui consistent à obtenir et à utiliser de façon frauduleuse l'identité d'une autre personne dans le but de commettre des fraudes ou d'autres activités criminelles, en visant en général des gains économiques".*[4]

Een Nederlandse studie, uitgevoerd door De Vries e.a.[5], onderzocht het begrip identiteitsfraude en trachtte via een internationale begripsvergelijking tot een eenvormige

[3] Identity theft and Assumption Deterrence Act .
[4] Section 403, Criminal Code of Canada.
[5] DE VRIES E.A., *Identiteitsfraude: een afbakening*, Den Haag, Boom Juridische uitgevers, 2007.

definitie te komen. Hun werkdefinitie werd uiteindelijk de volgende: "*Identiteitsfraude is het opzettelijk (en) (wederrechtelijk of zonder toestemming) verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging of: met de intentie om daarmee een wederrechtelijke gedraging te begaan".*

Het valt op dat deze werkdefinitie bijzonder ruim geformuleerd is. Dit is echter niet zonder reden. Zoals eerder vermeld, bestaat het misdrijf van identiteitsdiefstal immers uit twee fasen: enerzijds de onrechtmatige *inzameling* van de identiteitsgegevens, anderzijds het onrechtmatig *gebruik* ervan in het gewone handelsverkeer. Evenwel is het woord "intentie", gezien haar inherente subjectiviteit, m.i. vrij ongelukkig geformuleerd.[6]

Deze definities voldoen echter niet voor dit onderzoek, welke zich vanzelfsprekend toespitst op identity theft in de ICT.

Een eigen werkdefinitie, die wij hieronder verder zullen hanteren, is "*Identiteitsdiefstal in de ICT omvat enerzijds het opzettelijk en onrechtmatig inzamelen van identiteitsgegevens, geheel of gedeeltelijk bekomen door gebruik van een hardware- of softwarematig technisch procedé, en anderzijds het opzettelijk en onrechtmatig gebruik van deze gegevens, met inbegrip van, maar niet beperkt tot, elektronische middelen."*

Deze definitie stelt uitdrukkelijk twee gedragingen strafbaar, enerzijds de loutere *inzameling*, waarvan de strafbaarheid overigens door sommige minderheidsauteurs[7] wordt betwist, en anderzijds het *eigenlijke gebruik* ervan.

De aandachtige lezer merkt op dat indien de *inzameling* elektronisch (door middel van een hardware- of softwarematig procedé) gebeurde, het voor de definitie geen rol meer uitmaakt of de gegevens online dan wel offline worden gebruikt. Met andere woorden: een diefstal van identiteitsgegevens die elektronisch verkregen werden, maar *uitsluitend* 'offline' worden aangewend, valt onder bovenstaande definitie. Wanneer men een diefstal zou plegen in de reële wereld (bijvoorbeeld het stelen van een kredietkaart) en men gaat daarna deze gegevens online gaan misbruiken, valt men eveneens onder de werkdefinitie.

[6] N.S. VAN DER MEULEN, "Identiteitsfraude: de eerste stap, nu nog de rest", *Computerr.*, 2009, 38.
[7] A. SAVIRIMUTHU EN J. SAVIRIMUTHU, *Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective*, Scripted, 2007, (te consulteren op http://www.law.ed.ac.uk/ahrc/script-ed/vol4-4/savirimuthu.asp).

Anderzijds, wanneer men *uitsluitend* de identiteit steelt in de reële wereld en deze niet online plaatst of gebruikt, kan men niet onder deze definitie vallen. Dergelijke klassieke identiteitsdiefstal staat los van identity theft in de informatie- en communicatietechnologie. Bij wijze van volledigheid wordt hieronder kort ingegaan op de meest voorkomende categorieën van identiteitsdiefstal, onafhankelijk of zij nu wel dan niet in de ICT voorkomen.

HOOFDSTUK 4: IDENTITY THEFT SENSU LATO

AFDELING 1: FINANCIËLE IDENTITEITSDIEFSTAL

Financiële identiteitsdiefstal is veruit de meest voorkomende in het illustere rijtje. Een zeer courante praktijk is het kopiëren van bankkaarten (*skimming*). Skimmen kan op verschillende manieren gebeuren. Grofweg zijn er een viertal op te noemen: via een camera, meekijken over de schouder, een valse voorzetmond plaatsen en/of het gebruik van een *keypadlogger* die de pincode registreert.

Financiële identiteitsdiefstal is vanzelfsprekend niet gelimiteerd tot *skimming*. Ook de inbraak in computers met als doel kredietkaart- of betalingsgegevens te bemachtigen valt onder die noemer. Evengoed bestaan er virussen of *trojans*[8] die in alle stilte op zoek gaan naar financiële informatie.

Het doel van deze vorm van identiteitsdiefstal moge vrij duidelijk wezen. Eens voldoende gegevens bemachtigd (bijvoorbeeld in het geval van een kredietkaart; de naam, nummer en veiligheidscode) kan de dief ongestoord online aankopen verrichten, financiële transacties instellen naar eigen rekeningen (gewoonlijk via de zogenaamde 'middle-men'), et cetera.

Gezien het relatieve gemak waarmee criminele bendes dergelijke rekeningen kunnen plunderen, is ID-theft sinds enkele jaren uitgegroeid tot een bijzonder lucratieve business. Het mag dan ook niet verbazen dat in de Verenigde Staten, het land bij uitstek, het misdrijf identity theft, steevast naar de eerste plaats meedingt onder de meest voorkomende misdrijven.

[8] Een Trojan of ook nog Trojaans paard genoemd is een functie die verborgen zit in een programma dat door de gebruiker wordt geïnstalleerd. Via deze functie kunnen kwaadwillenden zich toegang verschaffen tot de geïnfecteerde computer en zo schade toebrengen aan de computergegevens of de privacy van de gebruiker. Men gebruikt de ook Engelse termen Trojan horse of trojan. De term refereert vanzelfsprekend naar het welbekende Griekse Paard van Troje.

AFDELING 2: IDENTITEIT KLONEN

Deze vorm spreekt ontegenzeggelijk tot de verbeelding. Waar bij financiële, criminele of medische ID-theft het misdrijf gewoonlijk relatief snel kan worden ontdekt, is dit voor identiteitsklonen absoluut niet het geval. Identiteitsklonen leven en werken onder iemands naam en identiteit, sommigen weten zelfs een volledig (en publiek) gezinsleven op te bouwen onder dergelijke valse identiteit. Een identiteit klonen gaat echter niet zomaar, daar deze gepaard gaat met aanmerkelijke voorafgaande investeringen. De identiteitskloon zal immers zo veel mogelijk informatie willen en moeten vergaren over het slachtoffer. Dat gaat van officiële informatie (zoals het rijksregisternummer, adresgegevens, maritale status, werkgegevens, et cetera) tot persoonlijke gegevens zoals vorige relaties, scholen, enzovoort.

Sociale netwerksites en zoekmachines herbergen een schat aan dergelijke gegevens, waarvan dankbaar gebruik kan worden gemaakt. Deze vorm van identiteitsdiefstal wordt vaak ontdekt als het slachtoffer onbekende afschriften toegestuurd krijgt, of dubbele adressen opmerkt.

Stellen dat dergelijke identiteitsdiefstal een enorme impact heeft op het slachtoffer is zoveel als een open deur intrappen. Men moet immers niet alleen rekening houden met de onmiddellijke gevolgen, maar evengoed met de lange termijn gevolgen. Het is immers niet ondenkbaar dat de identiteitskloon er een weelderige levensstijl er op nahoudt en dat op kap van de persoon wiens identiteit hij overnam. Het slachtoffer ziet zich dan geconfronteerd met schuldeisers maar vooral de moeilijke bewijsvoering van de identiteitsdiefstal. Bovendien worden identiteitsgegevens vaak doorverkocht in criminele circuits, zodat de kans op herhaling erg reëel is.

AFDELING 3: CRIMINELE IDENTITEITSDIEFSTAL

Dit betreft het bemachtigen van een identiteit, met als specifiek en vaak enig doel het plegen van een welbepaald misdrijf onder de identiteit van het slachtoffer. Een praktijk zo oud als de straat, welke dan ook voorkomt in de meest uiteenlopende gevallen.

Criminele identiteitsdiefstal komt vaak voor bij arrestatie en ondervraging. De dader zal zich uitgeven voor iemand anders, met behulp van persoonlijke gegevens zoals een rijbewijs, geboortedatum, rijksregisternummer en dies meer. Uiteraard dient rekening te worden

gehouden met fotografische bewijsmiddelen op dergelijke documenten, evenwel is de wijziging daarvan verre van een onmogelijke opdracht.

Net zoals bij vrijwel elke vorm van identiteitsdiefstal is het leveren van het bewijs van onschuld een bijzonder moeilijke opdracht.

AFDELING 4: MEDISCHE IDENTITEITSDIEFSTAL

Wanneer iemand de naam of zelfs de volledige identiteit van iemand anders misbruikt, met als doel medische diensten of goederen te bekomen, spreken we van medische identiteitsdiefstal. Dit kan vaak zeer vervelende fouten in medische dossiers teweegbrengen, tot – in het slechtste geval – ernstige fouten met betrekking tot de burgerlijke staat van iemands persoon (status van leven – sterfte, geboortes, etc.).

Deze vorm van identiteitsdiefstal is naar alle waarschijnlijkheid de minst bestudeerde en gedocumenteerde vorm. Dat valt allicht te verklaren door het medische beroepsgeheim dat hoog in het vaandel wordt gedragen. Een eerste vermeldenswaardig rapport, '*The World Privacy Forum medical identity theft report',* dateert al van 3 mei 2006, en werd uitgebracht door het World Privacy Forum.[9] Deze studie besloot onder andere "*It is crucial to see the problem of medical identity theft clearly. This will take research and serious studies by both the government and the private sector. Survey instruments need to be designed anew, and need to include questions that will call out and differentiate medical identity theft as a separate, unique crime so as to begin to better grasp its movements and characteristics.*

Consumer education programs for victims of financial identity theft are well-refined; medical identity theft victims are in need of this same kind of refined information that is focused on the problems unique to medical identity theft, such as problems with medical files and amending records at insurers."

Een tweede rapport, eveneens van de World Privacy Forum, wordt verwacht medio 2010.

[9] P. DIXON, "MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You", *World Privacy Forum Series,* 2006 (te consulteren op http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf).

HOOFDSTUK 5: SENSU STRICTO: IDENTITEITSDIEFSTAL BEPERKT TOT DE ICT

Deze verhandeling zal zich echter beperken tot de vormen van identiteitsdiefstal die zich rechtstreeks of onrechtstreeks in de ICT-sector voordoen. Aangezien deze vormen zich allang niet meer enkel tot de zuivere "*hackin*g" of "*online banking fraud*" toespitsen, maar ook zeer recente fenomenen impliceren zoals identity theft via sociale netwerksites, *wireless identity theft* (RFID), chatprogramma's, en de zeer actuele '*location-based services*', lijkt de scope van dit onderzoek op zich al ruim voldoende.

Het is onnodig te stellen dat deze vormen een zelfstandig onderzoek rechtvaardigen. Al te vaak wordt identity theft immers te algemeen behandeld, zonder de nodige distincties.

DEEL 2: VORMEN EN TOEPASSINGSGEVALLEN

HOOFDSTUK 1: IDENTITEITSKAARTFRAUDE

AFDELING 1: INLEIDING

De pure identiteitskaartfraude is zo oud als de straat, en vormt een belangrijk probleem in vrijwel alle staten. De bestrijding van dergelijke fraude kent vanzelfsprekend haar belang inzake terrorisme, illegaliteit en identiteitsdiefstal.

De eID of voluit de elektronische identiteitskaart werd in België ingevoerd door de wet van 25 maart 2003.[10] België bevond zich hier, ondersteund door ontwikkelaar Fedict, in een pionierspositie.[11] Met de eID creëerde België een geducht obstakel voor identiteitsdieven. De invoering en uitwerking van de eID verdient daarom nadere toelichting.

Art. 14, § 2 van de wet bepaalt dat de eID volgende gegevens moet bevatten:

- De identiteits- en handtekeningsleutels
- De identiteits- en handtekeningscertificaten
- De geaccrediteerde certificatiedienstverlener
- De informatie nodig voor de authentificatie van de kaart (…)
- De andere vermeldingen opgelegd door de wetten
- De hoofdverblijfplaats van de houder

Verder stipuleert de wettekst van 2003 dat bij het Rijksregister een centraal bestand wordt bijgehouden met de data van alle uitgereikte identiteitskaarten. De procedure van diefstal, verlies of vernieling wordt omschreven in art. 16.

Ter uitvoering van de wet werd op 25 maart 2003 eveneens een Koninklijk Besluit aangenomen.[12] Deze bevat de meer praktische en technische kenmerken van de eID. Het

[10] Wet van 25 maart 2003 tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, (te consulteren op http://www.juridat.be/cgi_loi/loi_N.pl?cn=2003032530).
[11] E. KINDT, "Algemene invoering van de elektronische identiteitskaart in België", *Computerr.*, 2005, 238.
[12] Koninklijk besluit van 25 maart 2003 houdende overgangsmaatregelen in verband met de elektronische identiteitskaart, (te consulteren op

K.B. bepaalt dat de Belgische eID qua formaat en qua chip de Europese normen nauwgezet opvolgt.

De eID impliceert tweeërlei voordelen. Het levert enerzijds een enorm administratief voordeel op, anderzijds vermindert het gevaar op identity theft gevoelig.[13] De essentiële gegevens worden opgeslagen op de chip. Het moet wel gezegd worden dat in de beginperiode met een verbijsterend gemak de kaarten gekopieerd of de gegevens erop gewijzigd konden worden. Vanzelfsprekend werd de beveiliging ondertussen sterk opgetrokken.

Uiteraard werd niet lichtzinnig overgegaan tot een invoering van de eID. Fedict lanceerde immers een eerste testfase[14] in elf gemeenten. Deze testfase werd afgesloten door het Koninklijk Besluit van 1 september 2004.[15] In het voorjaar van 2005 kregen alle gemeenten de opdracht elektronische identiteitskaarten uit te reiken. Dit kon ofwel op uitdrukkelijke vraag van de burger, ofwel werd automatisch de overschakeling naar een eID gemaakt wanneer de identiteitskaart moest worden hernieuwd. Tegen eind 2009 diende elke Belgische inwoner over een eID te beschikken.

AFDELING 2: MYTHS & FACTS: KERNFUNCTIES VAN DE EID.

§ 1. Authentificatie[16]

A Authentificatie van documenten

Men kan de eID aanwenden ter authentificatie van documenten. Men kan namelijk de *auteur* en de *integriteit van het document* (bijvoorbeeld: heeft het document sinds de aanmaak wijzigingen of updates ondergaan?) gaan controleren.

---

http://www.juridat.be/cgi_loi/loi_a.pl?language=nl&caller=list&cn=2003032532&la=n&fromtab=wet&sql=dt='koninklijk%20besluit'&tri=dd+as+rank&rech=1&numero=1).

[13] E. KINDT, "Country report for 'Belgium' in D12.7: Identity-related crime: Big problem or Big Hype?", *FIDIS,* 2008, 12-29 (te consulteren via http://www.fidis.net/fileadmin/fidis/deliverables/5th_workplan/fidis-wp12-del12.7_identity_crime_in_Europe.pdf).

[14] E. WEYTJENS, "eID", *Certipost,* 2003 (te consulteren op http://www.senate.be/event/05-06-03-ict/0603-01-nl/Weytjens-nl.ppt).

[15] Koninklijk besluit van 1 september 2004 tot wijziging van het Koninklijk besluit van 25 maart 2003 houdende overgangsmaatregelen in verband met de elektronische identiteitskaart, (te consulteren op http://eid.belgium.be/nl/binaries/WT7_tcm147-9988.pdf).

[16] J. DUMORTIER EN F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerr.,* 2009, 37.

Hier functioneert uiteraard het Europese gemeenschapsrecht[17] inzake de elektronische handtekening (zie *infra*).

B Authentificatie voor toelating website via certificaat.

Sommige websites kunnen vragen om identificatie via de eID of burgertoken. Het zijn voornamelijk door de overheid gestuurde websites die van deze opportuniteit volop gebruik maken. Voorbeelden zijn onder andere de website van Tax-on-web, van het Rijksregister[18] zelf, de website van het Agentschap Ondernemen[19] (waar men bv. een aanvraag tot subsidie van de KMO-portefeuille kan doen) en de website van de Sociale Zekerheid.[20]

C Authentificatie tot veilige chatruimtes

Kinderen hebben nood aan veilige chatruimtes. Reeds enkele jaren worden er grote inspanningen geleverd om kinderen op het net beter te beveiligen en in sommige gevallen zelfs te monitoren. Van levensgroot belang is hier de 'Kids-ID'[21], die zich niet beperkt tot een standaard identificatiemiddel, maar evengoed, dankzij de chip en pincode, kan gebruikt worden als beveiliging bij het chatten, bij aanvraag van een bibliotheekpas of zwembadabonnement en bij inschrijving op school. De Kids-ID wordt in vijftig landen aanvaard, al is België het enige land dat zo'n kaart heeft ingevoerd.

Opmerkelijk is tevens de "contact ouders"-code, die men ontvangt bij aanvraag van het Kids-ID. Hiermee kan men een lijst aanmaken met maximaal zeven telefoonnummers die dienst kunnen doen in geval van nood.

De Kids-ID is bedoeld voor kinderen jonger dan 12. Vanaf 12 jaar wordt er overgeschakeld naar de 'gewone' eID. Een jaar na de lancering van de Kids-ID hebben al zo'n 217.000

[17] Richtlijn 1999/93/EG van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen.
[18] http://www.ibz.rrn.fgov.be/index.php?id=141&L=1.
[19] http://www.vlao.be en http://ewbl-publicatie.vlaanderen.be/servlet/ContentServer?pagename=Ondernemen/Page/MVG_CMS4_Home&cid=1079086557099&c=Page
[20] http://www.socialsecurity.be.
[21] http://eid.belgium.be/nl/Welke_kaarten_/Kids-ID en http://eid.belgium.be/nl/binaries/FED14870-KidsIDFolderNL-HR_tcm147-60588.pdf .

kinderen zo'n kaart in hun bezit.[22] Dit overstijgt de verwachting, althans volgens ontslagnemend Minister van Binnenlandse Zaken Annemie Turtelboom. Ondanks het niet-verplicht karakter van de kaart, blijkt het desalniettemin een succes. Wellicht is het succes er gekomen dankzij de lage kostprijs (amper drie euro).

§ 2. Digitaal ondertekenen

Een digitale handtekening staat met stip op nummer één wat betreft de functionaliteit van een eID. Het is – mede dankzij de Europese Richtlijn – uitgegroeid tot een standaardbegrip. Die Europese richtlijn[23] schakelt sinds 1999 een digitale handtekening gelijk met een handtekening op papier. De elektronische identiteitskaart betekent een veilig middel voor de gekwalificeerde elektronische handtekening[24], die zowel door overheidsinstanties als door private spelers in tal van projecten kan worden geïntegreerd.

De Elektronische Identiteitskaarten bevatten twee soorten digitale certificaten waarmee de houders van de identiteitskaarten afhankelijk van hun leeftijd zichzelf kunnen identificeren en een elektronische handtekening kunnen gebruiken:

- Een identiteitscertificaat: de houder van de Elektronische Identiteitskaart kan dit certificaat gebruiken om zich te identificeren bij elektronische verrichtingen indien bij aanvraag van de Elektronische Identiteitskaart de leeftijd van 6 jaar werd bereikt. Het identiteitscertificaat bevat de identiteit van de houder en de openbare sleutel die overeenkomt met de privé-sleutel. Deze privé-sleutel mag enkel gebruikt worden voor een eID gebruikersidentificatie.

- Een Gekwalificeerd Certificaat voor Elektronische Handtekeningen (of handtekeningen): dit certificaat bevat de identiteit van de houder en de openbare sleutel die overeenkomt met de privé-sleutel, die enkel gebruikt mag worden om een elektronische handtekening te maken. Het Gekwalificeerd Certificaat voor

[22] X., "Kids-ID groter succes dan verwacht", *De Standaard,* 2010, http://www.deredactie.be/cm/vrtnieuws/binnenland/1.738398
[23] Richtlijn 99/93/EG.
[24] A.R., LODDER, J. DUMORTIER, EN S.H. BOL, "Het recht rond elektronische handtekeningen", *Informatica en recht,* 2005.

> Elektronische Handtekeningen voldoet aan de bepalingen van de Wet op Elektronische Handtekeningen en de Europese Richtlijn 1999/93 en kan op de identiteitskaart geactiveerd worden zodra de burger de leeftijd van 18 jaar heeft bereikt.[25]

Van essentieel belang is dat de 'handtekening' stoelt op het CITIZIN AC Certificaat.[26] Deze worden verleend door de CSP (Certification Service Provider) CERTIPOST. Het Rijksregister is als 'Registratieautoriteit (RA)' verantwoordelijk voor de uitgifte van de sleutels. De gemeentes treden op als LRA (lokale registratieautoriteiten).

De RA en de LRA zijn in hoofdzaak verantwoordelijk voor de identificatie van de burger, de registratie van gegevens die gecertificeerd moeten worden, machtiging tot uitgave van certificaten en het verschaffen van bepaalde waarborgen.

De beperktheid van deze bespreking laat niet toe de certificaten technisch volledig toe te lichten. De geïnteresseerde lezer wendt zich daarvoor best naar de website van eID Services – Certipost.[27]

§ 3. Lezen van data

De softwareapplicatie die de gegevens op de kaart afleest en weergeeft op het computerscherm van de particulier, onderneming of overheidsdienst is alom bekend. Benodigd hiervoor is uiteraard een kaartlezer, welke heden ten dage in sommige PC's en laptops standaard wordt meegeleverd (de zgn. "Smart Card Readers"). Anderen moeten een eID kaartlezer of DIGIPASS aanschaffen wil men van de leesmogelijkheid gebruik maken.

Ter illustratie: verschillende universiteiten en hogescholen maakten reeds gebruik van deze leesmogelijkheid om digitale studentenkaarten aan te maken.

---

[25] http://repository.eid.belgium.be/NL/downloads/Citizen/CPS_CitizenCA.pdf.
[26] http://repository.eid.belgium.be/NL/CitizenCA.htm.
[27] http://www.certipost.be/dpsolutions/nl/eid-overzicht.html

§ 4. Encryptie en decryptie

De eID maakt het mogelijk (e-mail-)berichten te encrypteren bij verzending. Encryptie is een beveiligingsmechanisme waardoor het tekstueel bericht 'onleesbaar' wordt gemaakt. Enkel diegene die over de decryptiecode beschikt kan het bericht wederom leesbaar maken.

Uiteraard kan de eID hier een gemakkelijke en goedkope oplossing bieden die tegelijk de ingewikkelde en vaak dure software (die door derden werd ontwikkeld) overbodig maakt.

§ 5. In de toekomst?

Fedict sloeg de handen in elkaar met Living Tomorrow en somde enkele toepassingen van de eID op die in de nabije toekomst hun intrede zullen maken[28]:

- Het digitale prikbord (eID functioneert als beveiliging, betalingsmiddelen en verificatie bij aflevering).
- Identificatie via eID bij *e-shopping* (vermijden van onbeschermde kredietkaartgegevens en bij afschermen van producten ten voordele van bepaalde doelgroepen bijvoorbeeld sigaretten, alcohol, etc. bij minderjarigen).
- Virtuele kaarten op Smartphone: bankkaarten, eID, SIS-kaart enzovoort.
- Inschrijven op opleidingen via de eID.
- Vervanging van bedrijfsbadges, accounts tot beveiligd extra- en intranet, tijdsregistraties, logins en paswoorden, …
- Andere toepassingen:
    - Medische gegevens op eID (strikt vertrouwelijke opslag van deze gegevens, teneinde een snelle diagnose en interventie mogelijk te maken)
    - Invoering treinabonnementen op de eID
    - …

AFDELING 3: INTERNATIONALE TOEPASSING

"National identification systems have been proliferating in recent years as part of a concerned drive to find common identifiers for populations around the World. Whether the driving force is immigration control, anti-terrorism, electronic government or rising states of

[28] http://welcome-to-e-belgium.be/nl/home.php?nav=1_eid_what.php.

identity theft, identity cards systems are being developed, proposed or debated in most countries". [29]

Europa wil nu vooral eenheid creëren voor de eID kaarten. De EU begon in juni met een proef daaromtrent. De geüniformiseerde eID zou het mogelijk maken om toegang te verkrijgen tot digitale overheidsdiensten in andere lidstaten met de eID uit eigen land. Dit wordt het STORK-project genoemd.

Het project STORK[30] ('Secure Identity Across Borders Linked') stelt het volgende:

"Thus in the future, you should be able to start a company, get your tax refund, or obtain your university papers without physical presence; all you will need to access these services is to enter your personal data using your national eID, and the STORK platform will obtain the required guarantee (authentication) from your government."

De deelnemende landen, waaronder België, verklaarden op 11 november 2009 dat zij hun raamwerk voor het uniforme eID model rond hebben. Dit raamwerk zal gebruikt worden in vier pilootprojecten in 2010.[31]

AFDELING 4: VEILIGHEID EN RISICO'S

§ 1. Privacy.

In het privacydebat is de eID nooit ver weg. En terecht. In bepaalde situaties loert, vaak door de onkunde of onwetendheid van de gebruiker, een datadiefstal of –verlies om de hoek.

De eID zal in de nabije toekomst steeds meer centrale functies overnemen. Waar nu de chip een beperkt aantal gegevens bevat - er staat amper meer op dan op de oude 'plastieken' identiteitskaart -, zal men steeds uitgebreider gaan archiveren en steeds meer functies gaan toekennen aan de eID.

Maar is dit een probleem? Men kan zich alleszins de vraag stellen[32] of het wenselijk is dat hetzelfde identificatienummer (het Rijksregisternummer) wordt gebruikt door allerlei privé-

[29] C.J., BENNET, D., LYON, "Playing the Identity Card, surveillance, security and identification in global perspective", 2008, 1.
[30] http://www.eid-stork.eu/.
[31] http://www.eid-stork.eu/index.php?option=com_content&task=view&id=201&Itemid=69.

en publieke instanties (denk maar aan een bibliotheekinschrijving, banken, verzekeraars, reisagentschappen, et cetera). De Verenigde Staten hebben met hun *Social Security Number* (zie *infra*) al ruimschoots bewezen dat dit geen bijzonder goed idee zou zijn.

Nochtans zijn er enkele veiligheidscriteria ingebouwd. Wanneer de overheid een e-Government project wil lanceren waarbij gebruik wordt gemaakt van het Rijksregisternummer dient zij hiervoor toelating aan te vragen bij de Commissie voor de bescherming van de persoonlijke levenssfeer[33] (en eventuele subcommissies).

Uiteraard zal ook een privé-instelling deze machtiging moeten verkrijgen wil zij gebruikmaken van het Rijksregisternummer.[34]

Onlangs werd door de Privacycommissie een campagne gelanceerd "Think Privacy"[35] met als motto "*Privacy is a human right: Treat it with care*" waar men uitdrukkelijk wijst op de gevaren van een eID.

Waar de bezorgdheid om privacy inbreuken nu nog eerder voorzichtig naar voren wordt geschoven[36], kan men rechtmatig vermoeden dat in de (nabije) toekomst de roep naar privacy en het doordacht gebruik van de eID steeds luider zal weerklinken.

§ 2. Softwarematige tekortkomingen

De eID haalde in de beginperiode meermaals het nieuws met kritieke beveiligingsproblemen in de software.

Het probleem werd aangekaart door BelSec.[37] Hackers (beter: crackers) die de gegevens van een identiteitskaart wilden bemachtigen hoefden zich hiervoor amper moeite te troosten. Normaliter is een eID kaart enkel leesbaar met de software ontwikkeld door Fedict ("eID

---

[32] J., DUMORTIER, "eID en de paradoks van het rijksregisternummer", *Business ICT,* 2006, (te consulteren via https://www.law.kuleuven.be/icri/publications/655Column_BusinessICT_06_eID.pdf).
[33] http://www.privacycommission.be.
[34] http://www.privacycommission.be/nl/sectoral_committees/national_register/competences/use-RR.html#N100BA.
[35] http://www.privacycommission.be/nl/new/topic/wedstrijd-Privacy-Day-2010.html.
[36] W. SCHREURS, "Ik ben user 712. Recht op toegang tot persoonsgegevens en op mededeling van de logica van geautomatiseerde verwerking", *Computerr.,* 2009-40, 68.
[37] http://belsec.skynetblogs.be/post/5868360/how-to-hack-intercept-the-information-on-an-b.

Viewer"). Het volstond echter om zelf een bepaalde code te schrijven en dat programma de naam van een browser (zoals bv. Internet Explorer of Firefox) mee te geven.

Deze bevindingen werden meegenomen door volksvertegenwoordiger Roel Deseyn in een parlementaire vraag[38] van 14/01/2009 waarbij werd gevraagd: *"(…) zeker als het gaat over de veiligheid van de elektronische identiteitskaart (…) is het belangrijk veiligheidslekken te dichten. U weet dat er een probleem gesignaleerd werd. Er zou door Fedict een veiligheidspatch ter beschikking worden gesteld (…) maar wanneer mag men de veiligheidspatch verwachten?"* en *""Wat het veiligheidslek betreft, ik ben het ermee eens dat de verschillende kaartlezers, de verschillende versies van middleware en de verschillende applicaties moeilijk te beheren zijn. De overheid moet daarin echter een regierol spelen. Heel belangrijk is echter de sensibilisering. Als het pc-systeem geïnfecteerd is dan mag men met de beste middleware en kaartlezers komen aanzetten, maar dan stelt er zich toch een probleem met het eventueel onrechtmatig verkrijgen van gegevens die van de kaart naar de computer zijn gegaan."*

Het antwoord van toenmalig Minister van Binnenlandse Zaken Guido De Padt beperkte zich tot het poneren van de stelling dat de eID kaarten *an sich* veilig zijn – aangezien zij voldoen aan de Europeesrechtelijke normen -, maar dat de software beter geëvalueerd moest worden, en er een grotere waakzaamheid moest gestimuleerd worden bij de burgers.

AFDELING 5: IDENTITY THEFT

Hoewel de eID hier zeer ruim werd besproken, mag de scope van onderhavig onderzoek vanzelfsprekend niet uit het oog worden verloren. Kernvraag van dit debat blijft dan ook of het risico op identity theft door de invoering van eID is afgenomen. Mijn inziens dient bevestigend op deze vraag geantwoord te worden. Hoewel men zich uiteraard dient te hoeden voor al te lichtzinnig gebruik, en het ontstaan van nieuwe vormen van misbruik, kan men niettemin veilig stellen dat de eID een stuk moeilijker te kopiëren of te frauderen valt, en het daarenboven in betrouwbare authentificatie kan voorzien.

Een betrouwbare elektronische identiteit (eID) is bovendien niet meer dan een noodzaak voor de overheidsinstanties die steeds meer uitsluitend vertrouwen op digitale registers en

[38] http://www.scribd.com/doc/10962917/Parlementaire-Vraag-EID.

data. Hoe meer afstand we nemen van papieren formulieren en face-to-face identiteitsmanagement, hoe prominenter de vraag naar betrouwbaar bewijs van diens identiteit naar voren treedt.[39] Eén enkel betrouwbare elektronische identiteit is immers een absolute vereiste voor alle e-government programma's.

Zoals hierboven aangehaald kan eID vanzelfsprekend ook in de private sector zijn nut bewijzen (bijvoorbeeld bij banken, werkgevers, vliegtuigmaatschappijen, online e-commerce toepassingen, et cetera). De eID infrastructuur moet wel zeer duidelijk aanduiden hoever deze private actoren toegang kunnen krijgen tot de zeer waardevolle identiteitsdata. Bovendien dient men bij het uitstippelen van de toegangsbevoegdheid voor dergelijke private actoren een grote transparantie naar de burger toe waarborgen.

In realiteit is een absolute '*proof of identity*' een onwerkbaar gegeven. Wat uiteraard niet wegneemt dat zowel de publieke instanties als eventuele private gebruikers en leveranciers alle mogelijke (lees: technisch beschikbare) en redelijke maatregelen dienen te nemen om de identiteit correct vast te stellen en maximaal te beschermen.

Een technische oplossing is bijvoorbeeld TPM (*Trusted Platform Module*). Uit een zeer specifiek en relevant onderzoek[40], namelijk "*Preventing Identity Theft with Electronic Identity Cards and the Trusted Platform Module"* aan de *Technische Universität München* bleek dat TPM bijzonder geschikt is om identity theft te voorkomen bij authentificatie. De TPM chip kan immers een bijkomende en platformeigen encryptie verzorgen van de sleutelinformatie op de eID, en zorgt er voor dat zowel aanvallen gericht op het wijzigen van sleutelinformatie als pogingen tot diefstal van identiteitsgegevens afgeblokt worden. Het basisidee van TPM is zich te beschermen tegen identity theft met TPM Authentificatie, eventueel in samenhang met een individuele pincode, waarmee de gebruiker toegang krijgt tot de sleutel. Gezien de hoge techniciteit van bovengenoemde TPM gaan wij hier niet verder op in.

Het is aangeraden op de hoede te zijn voor een al te grote dramatisering van de gevaren. Momenteel bevat de eID immers niets meer dan de essentiële basisinformatie die, hoewel

[39] J. FISHENDEN, "eID: Identity Management in an Online World", *Microsoft UK*, London (te consulteren via http://ntouk.com/papers/eID.doc).
[40] A. KLENK, C. EUNICKE, H. KINKELIN, G. CARLE, "Preventing Identity Theft with Electronic Identity Cards and the Trusted Platform Module", *EUROSEC,* 2009, (te consulteren via http://www.net.in.tum.de/fileadmin/bibtex/publications/papers/klenk_eurosec2009.pdf).

op zichzelf uiteraard waardevol, niets meer is dan de informatie die reeds op de papieren identiteitskaart stond. Men dient bovenstaande overwegingen dan ook voornamelijk mee te nemen voor toekomstige eID-projecten die een ongetwijfeld grotere impact zullen hebben op 's mens identiteit.

HOOFDSTUK 2: FINANCIËLE ID-THEFT: SKIMMING

Skimming[41] kan men definiëren als het op onrechtmatige wijze bemachtigen en kopiëren van bank- of kredietkaartgegevens. Dergelijke ruime definitie omvat echter een zeer breed scala aan incidenten. Zoals reeds eerder gesteld behandelen wij hier enkel gevallen die onder de werkdefinitie van identity theft in de ICT vallen. Incidenten die zich volledig offline voordoen (bijvoorbeeld: men leest de gegevens van een bankkaart aan de bankautomaat, maakt een kopie van de bankkaart en haalt geld af via een automaat) worden hier niet besproken.

Niettemin doet skimming zich bijna uitsluitend 'offline' voor. Toch is een uiteenzetting om twee redenen onontbeerlijk. Enerzijds is het vandaag veruit de belangrijkste en meest gebruikte vorm van identity theft, en anderzijds wordt er quasi steeds een online luik aan gekoppeld (de tweede fase), aangezien men vaak online transacties doet met de ingezamelde bank- of kredietkaartgegevens of deze gegevens via obscure en gespecialiseerde websites verder doorverkoopt.[42]

AFDELING 1: DE TECHNIEK

De techniek van skimming is ondertussen bij het brede publiek bekend, en dit zeker na de recente media-aandacht sinds het voorval in Hasselt, waarbij een honderdtal personen die geld afhaalden uit een bankautomaat aan de Grote Markt, het slachtoffer werden van skimming.[43] Skimming bestaat uit twee hoofdelementen, enerzijds het kopiëren van de magneetstrip op de bank- of kredietkaart en anderzijds het filmen van de pincode door middel van een (kleine, verborgen) camera. Met deze twee elementen hebben de skimmers

[41] R. BEECKMANS, "Politioneel en gerechtelijk onderzoek inzake skimming van bankkaarten: casusbespreking: opportuniteiten, noodzaak en risico van een multidisciplinair aanpak in functie van de bewijsgaring", *onuitg.*,Leuven, 2004.
[42] J.T. WELLS, *Principles of fraud examination*, Wiley, New Jersey, 2005.
[43] P. VAN LEEMPUTTEN, "Hasseltse bankkaarten gekopieerd", *ZDNet België,* 2009, (te consulteren via http://www.zdnet.be/news/102048/hasseltse-bankkaarten-gekopieerd/).

voldoende informatie om een fysieke kopie van de bankkaart te maken en/of online de rekening van het slachtoffer te plunderen.

Puur technisch[44] maakt men gebruik van een magnetische leeskop, een voorkantlampje, een batterij uit een mobiele telefoon, een kleine filmcamera (vaak op USB technologie) en de benodigde elektronica om een bank- of kredietkaart te lezen.

Men denkt in bovengenoemde situering onmiddellijk aan publieke, en vaak onbewaakte, bankautomaten. Evenwel komt skimming steeds meer voor in de betaalapparatuur van gewone handelszaken. Veel tijd hebben skimmers immers niet nodig om hun apparatuur te plaatsen, enkele momenten van onachtzaamheid blijken voldoende.

Een belangrijke vraag is wat criminelen nu precies met de informatie aanvangen. Er zijn enkele opties. Men kan aan de hand van de gekopieerde magneetstrip een fysieke kopie ontwerpen van de bank- of kredietkaart. Indien de camera de pincode heeft kunnen vastleggen kan de skimmer hiermee moeiteloos in handelszaken aankopen verrichten. Een andere (en vaak gecumuleerde) optie is het online plunderen van de rekening. Hoe streng of complex de e-banking beveiliging ook moge zijn, wanneer men de nodige informatie en pincode in handen heeft, kan men hiermee ongestoord toegang verkrijgen tot het online portaal.

In de praktijk blijkt deze operatie maximaal een aantal uren in beslag te nemen. Gespecialiseerde bendes plunderen massaal dergelijke gekraakte rekeningen, om daarna de informatie te versturen naar beruchte databases. Vooral Oost-Europa blijkt een geliefd toevluchtsoord voor dergelijke bendes.[45]

AFDELING 2: GEVOLGEN

Maar wat zijn nu de gevolgen voor het slachtoffer? Financieel lijkt een en ander wel mee te vallen, men kan immers slechts tot € 150 aansprakelijk worden gesteld, ongeacht hoeveel de skimmer kon versluizen naar andere rekeningen. Dit op voorwaarde dat er geen grove

[44] W. DE MOOR, "Details en foto's NS-skimapparaat gepubliceerd", *Tweakers.net,* 2008, (te consulteren via http://tweakers.net/nieuws/57329/details-en-fotos-ns-skimapparaat-gepubliceerd.html).
[45] D. REIJERMAN, "NS gaat kaartautomaten aanpassen om skimmen tegen te gaan", *Tweakers.net,* 2008, (te consulteren via http://tweakers.net/nieuws/57282/ns-gaat-kaartautomaten-aanpassen-om-skimmen-tegen-te-gaan.html).

nalatigheid of fraude ten laste kan worden gelegd. Hoewel banken een nogal bedenkelijk ruime definitie hanteren van 'grove nalatigheid', zal men zich in de praktijk vaak niet de moeite troosten om dergelijk bewijs te leveren. Dit gunstig regime is te danken aan de Wet betreffende elektronische betalingen[46], waarvan artikel 8, § 2 het volgende stipuleert:

"*Tot aan de kennisgeving zoals vermeld in § 1, tweede lid, is de houder aansprakelijk voor de gevolgen verbonden aan het verlies of de diefstal van het instrument voor de elektronische overmaking van geldmiddelen tot een bedrag van 150 euro, behoudens indien de houder met grove nalatigheid of frauduleus heeft gehandeld, in welk geval het bepaalde maximumbedrag niet van toepassing is.*

Worden onder andere beschouwd als grove nalatigheid: het feit, vanwege de houder, zijn persoonlijk identificatienummer of enige andere code in een gemakkelijk herkenbare vorm te noteren, en met name op het elektronisch instrument voor de overmaking van geldmiddelen, of op een voorwerp of een document dat de houder bij het instrument bewaart of met dat instrument bij zich draagt, alsook het feit van de uitgever niet onverwijld in kennis te hebben gesteld van het verlies of de diefstal.

Wat de beoordeling van de nalatigheid betreft, houdt de rechter rekening met het geheel van de feitelijke omstandigheden. Het produceren door de uitgever van de registraties bedoeld in artikel 6, 8°, en het gebruik van het betaalmiddel met de code die enkel door de houder is gekend, vormen geen voldoende vermoeden van nalatigheid vanwege de houder.

De bedingen en voorwaarden of de combinaties van bedingen en voorwaarden in de overeenkomst betreffende het ter beschikking stellen en het gebruik van het instrument voor de elektronische overmaking van geldmiddelen, die tot gevolg zouden hebben de bewijslast voor de verbuiker te verzwaren of de bewijslast voor de uitgever te verlichten, zijn verboden en nietig.

Na de kennisgeving is de houder niet meer aansprakelijk voor de gevolgen verbonden aan het verlies of de diefstal van het instrument voor de elektronische overmaking van geldmiddelen, behalve indien de uitgever het bewijs levert dat de houder frauduleus heeft gehandeld."

[46] Wet van 17 juli 2002 betreffende de transacties uitgevoerd met instrumenten voor de elektronische overmaking van geldmiddelen, *BS* 17 augustus 2002, inwerkingtreding 1 februari 2003, (te consulteren via http://www.juridat.be/cgi_loi/loi_N.pl?cn=2002071732)

Na de kennisgeving wordt het risicobedrag dus tot nul gereduceerd. Hoewel deze regeling bijzonder voordelig is voor de consumenten, kan men vraagtekens plaatsen bij de grote eindverantwoordelijkheid die hier bij de banken gelegd wordt. Niettemin dient men te constateren dat dergelijke 'incentive' een zeer efficiënt beleid in de hand werkt. Gebruikers worden immers – gewoonlijk – snel op de hoogte gebracht van een eventuele skimmingsactie, terwijl het blokkeren van de kaarten haast simultaan gebeurt (vaak zal men wanneer men een 'skimmingshaard' vaststelt, uit veiligheidsoverwegingen een zeer ruime perimeter nemen en een groot aantal bankkaarten blokkeren, ook al is het zeer goed mogelijk dat deze geen slachtoffer zijn). Het is dan ook in deze optiek dat het bovengenoemd wetsartikel werd gecreëerd, en uiteraard met de bedenking dat banken beter geplaatst zijn om een groot verlies of diefstal te dragen dan een gemiddelde consument. Het totale verlies veroorzaakt door aanvallen op het netwerk van bankautomaten in Europa bedroeg in 2006 maar liefst 306 miljoen euro.[47]

AFDELING 3: EN WAT MET DE IDENTITEIT?

Men moet zich anderzijds bewust zijn dat het verhaal niet stopt bij de financiële oplichting. De krediet- of bankkaartgegevens worden vaak uitgewisseld of doorverkocht aan schimmige Oost-Europese websites die voor een handvol euro's de kredietkaartgegevens doorsluizen naar het criminele milieu. Hoewel een belangrijk aandeel van de vergaarde nummers uiteraard geblokkeerd zullen zijn, zal men zonder enige moeite bij de aankoop van een dergelijke database nog werkende en actieve kredietkaartnummers terugvinden.

Als de skimmers aan de hand van bank- of kredietkaartgegevens ook relevante identiteitsgegevens wisten te vergaren (wat mits een kleine moeite kinderspel blijkt) dan neemt het verhaal een volledig nieuwe wending. Men heeft in dit geval niet alleen te maken met een louter financiële tegenslag, men dient daarnaast nog alle zeilen bij te stellen om zijn of haar identiteitsgegevens te beschermen. Gezien deze binnen de kortste tijd circuleren op duistere websites en andere onlineportalen, is dit een bijzonder moeilijke, zoniet onmogelijke opdracht.

[47] X., "ADT pakt het skimmen van passen aan ", *Beveiligingsnieuws*, 2007, (te consulteren via http://www.beveiligingnieuws.nl/beveiliging/6546/ADT_pakt_het_skimmen_van_passen_aan.html).

In een dergelijk geval kent skimming bijzonder zware administratieve en morele gevolgen, welke de (beperkte) financiële last volledig overschaduwt. Vaak wordt skimming veel te eenzijdig benaderd door politionele en juridische diensten en durft men geen koppeling te maken met identiteitsdiefstal. Een jammerlijke zaak, aangezien men hier een kans laat liggen om reeds in een vroeg stadium de gegevens op te sporen en te vernietigen. Doet men dit niet, dan loopt men het risico in een jarenlang durend administratief en juridisch gevecht te belanden, waar men tot in den treure toe zijn of haar ware identiteit dient te bewijzen.

AFDELING 4: OPLOSSINGEN

Er zijn vanzelfsprekend enkele oplossingen beschikbaar. De meest voor de hand liggende – maar tevens de meest vergeten – oplossing is het toetsenbord afschermen door middel van de hand of een ander object wanneer men de pincode moet intypen. De magneetstrip wordt in dergelijk geval wel gekopieerd maar men krijgt de pincode niet in handen. Hoewel men met enig technisch inzicht en via enkele omwegen financiële of identiteitsgegevens zou kunnen koppelen aan deze magneetstrip nemen skimmers hier vaak de moeite niet voor, begrijpelijk wanneer er 'gemakkelijkere' doelwitten bestaan die de voorzorg om hun pincode af te schermen niet nemen.

Uit het oogpunt van een bank of handelaar kan men eveneens opteren, zowel bij betaalterminals als bij private handelssystemen, voor een loutere fysieke afscherming door een metalen constructie te plaatsen boven het keyboard. Dergelijke – alweer – simpele ingreep blijkt efficiënt genoeg om meekijkende blikken, hetzij fysiek, hetzij technisch, te weren.

Naast deze bijna evidente oplossingen, bestaan er tal van technische maatregelen die banken kunnen implementeren. Een reeds genomen oplossing was het vervangen van de magneetstrip door de intelligente chip[48], die nu al terug te vinden in de meeste kredietkaarten en bankkaarten. Hoewel de loutere magneetstrip een goedkope manier vormde om informatie op te slaan en uit te lezen, was deze strip ontegenzeggelijk een passief instrument, dat daarenboven uiterst gemakkelijk door derden (lees: onbevoegden)

[48] M. TEN HOUTEN, "De pinpas is hopeloos verouderd", *SYNC.*nl, 2007, (te consulteren via http://sync.nl/de-pinpas-is-hopeloos-verouderd/2).

kon worden gelezen. De apparatuur om dat te doen is voor een handvol euro's vrij te koop op het internet.

Europa koos in 2005 dan ook resoluut voor de EMV betalingsstandaard.[49] In 2010 zullen alle bankpassen vervangen zijn, al hoeven winkeliers pas in 2013 over EMV betaalautomaten te beschikken. De technologie werd reeds geïmplementeerd in de meeste krediet- en betalingskaarten[50], waardoor de beveiliging gevoelig toenam. Maar zoals veelvuldige recente voorbeelden ons aantoonden, zijn we er nog lang niet.

De ultieme oplossing tegen skimming vormt het draadloos of contactloos betalen. De mogelijkheid bestaat om te werken met lezers, maar mits enige technische inspanningen kan men er evengoed voor opteren om kredietkaartgegevens te koppelen aan een smartphone die dan via WiFi, 3G of Bluetooth de betaling kan afhandelen. Gezien op dergelijke manier de controle volledig bij de gebruiker ligt (bij een lezer moet men nog steeds fysiek de betaalkaart laten lezen) zorgt dit, diefstal of misbruik van de smartphone niet te na gesproken, m.i. voor een ultieme beveiligingsgraad. De eID – al dan niet via smartphone – kan hier bovendien een uitstekend controlemechanisme bieden.

HOOFDSTUK 3: FINANCIËLE ID-THEFT: ONLINE BETAALSYSTEMEN

Online banking kent reeds een lange geschiedenis. Van registersleutels tot stemherkenning, de administratieve voorkeur van de banken voor de nieuwe technologieën ging hand in hand met een groter verlangen naar veiligheid op het internet. Banken investeren miljarden in nieuwe technologieën om hun klanten gerust te stellen. Maar is er, ondanks de vele onderzoeken, financiële input en tests, veel reden tot juichen?

Hierna volgt een bondige historiek van de verschillende betalings- en beschermingsystemen op het internet. Er wordt eveneens een blik op de toekomst geworpen.

[49] R. ARNFIELD, "Here comes EMV: the world is watching in the new year as Europe takes a major step on its road to a chip-based payment system. Will the U.S. be left behind?", *HighBeam,* 2005, (te consulteren via http://business.highbeam.com/137021/article-1G1-127432153/here-comes-emv-world-watching-new-year-europe-takes).
[50] http://www.bcc.be/index/nl_BE/5088994/5094013/Waarvoor-dient-de-chip.htm.

AFDELING 1: BEGINSTADIUM

Reeds in 2000 waren elektronische overschrijvingen (automaat, internet en telefoon) goed voor 47 procent van het totaal aantal overschrijvingen. Ook het pure internetbankieren won snel aan populariteit en nam bijgevolg een hoge vlucht. Voor de algemene verspreiding, effectiviteit en relatief hoge graad van beveiliging kreeg België dan ook een schouderklopje van de Europese werkgeverskoepel die in hun UNICE-rapport ons land toen vergeleken met de rest van Europa en de Verenigde Staten.

De eerste toepassingen van het online bankieren maakten gebruik van een eenvoudige gebruikersnaam en paswoord. Er was wel een bijkomende filter ingebouwd, gezien de bank eerst telefonisch verifieerde of de gebruiker wel de rechtmatige rekeninghouder was, waarop men de gebruiker vervolgens voorzag van een gepersonaliseerd wachtwoord. Dat deze methode niet bijzonder veilig kan genoemd worden, is een open deur intrappen. Al snel werd duidelijk dat er nood was aan een objectieve en bijkomende verificatiemethode.

Dit werd gevonden in de registersleutel, een bestandje dat werd geïnstalleerd in het register[51] van de computer, welke een database is (in het besturingssysteem van Microsoft Windows) waarin instellingen worden opgeslagen van zowel het besturingssysteem zelf, als van applicaties, gebruikers en apparaten. In het eerste stadium werd door lokale kantoren vaak hulp geboden om deze sleutel op de PC te installeren. Eens de sleutel geïnstalleerd was in het register, controleerde de bankwebsite bij het inloggen of 1) de gebruikersnaam, 2) paswoord en 3) de sleutel zelf correct waren.

AFDELING 2: DIGIPASS

Al snel kwamen banken tot de conclusie dat dergelijke sleutels met een bijzonder gemak gefraudeerd of nagemaakt konden worden. Men opteerde dan ook reeds in 2004 (de eerste was Fortis bank) om een Digipass of 'codeberekenaar' in te voeren.

Dexia volgde als tweede bank in 2006, weliswaar met een licht verschillend concept.[52] In tegenstelling tot Fortis, waar de Digipass louter diende om een code te berekenen, gebruikte men de Dexia Digipass daadwerkelijk als chipkaartlezer, wat natuurlijk een hogere graad van

[51] J. VANDERAERT, *Werken met het Windows-register,* Culemborg, Centraal Boekhuis, 2005.
[52] http://datanews.rnews.be/nl/90-101-11005/dexia-rust-e-banking-klanten-uit-met-vasco-digipass.html

beveiliging met zich meebracht. Bij Fortis genereerde de gebruiker immers een variabele identificatiesleutel via een driehoekssysteem: een gebruikersnummer, geheime code en de interne 'logica' van het apparaat zelf.

Vandaag maken alle Belgische banken gebruik van de door Vasco ontwikkelde Digipass. Noch Fortis, noch Dexia waren de eersten op de Belgische markt om e-banking op dergelijke manier te beveiligen. Die eer was weggelegd voor de Nederlandse internetbank Rabobank.[53]

Diezelfde bank toont zich blijkbaar een pionier op het gebied van online financiële beveiliging, gezien zij als eerste de mogelijkheid aanbood om via de eID een online rekening te openen.[54] Voor het online bankieren blijft de bank zweren bij de Digipass, hoewel er bijzonder goede argumenten zijn voor het inzetten van de eID.

AFDELING 3: TOEKOMST?

En wat brengt de toekomst? Verschillende mogelijkheden worden momenteel volop overwogen en onderzocht. Zo bestaat de mogelijkheid om de verificatie te laten gebeuren door een vingerafdruklezer, spraakherkenning, iris-scanning, et cetera.

Hoe ambitieus deze projecten ook mogen zijn, dient men zich niettemin te hoeden voor al te veel optimisme. De zwakste schakel in het gehele beveiligingsproces zit nog steeds tussen de stoel en de computer. Zolang deze schakel niet voldoende geïnformeerd is over bepaalde beveiligingsrisico's, getraind is om dergelijke risico's te herkennen en er correct mee om te gaan, zijn de ambitieuze projecten een maat voor niets.[55]

Goede hackers (of crackers) zijn namelijk in de eerste plaats uitstekende *social engineers* (denk maar aan Kevin Mitnick[56], ongetwijfeld één van de bekendste hackers die veelvuldig gebruikmaakte van *social engineering)*. Social engineering kan onder andere bereikt worden door nieuwsgierigheid, medeleven of angst bij het slachtoffer op te wekken, waardoor deze

[53] W. VISTERIN, "Rabobank.be is internetbank pur sang", *ZDNet België*, 2003, (te consulteren via http://www.zdnet.be/itprofessional/32222/rabobank-be-is-internetbank-pur-sang/).
[54] J. VAN OOST, "Rabobank gaat eID gebruiken", *ZDNet België,* 2009, (te consulteren via http://www.zdnet.be/news/97562/rabobank-gaat-eid-gebruiken/).
[55] J. GRIJPINK, "Identiteitsfraude als uitdaging voor de rechtstaat", *Privacy & Informatie*, 6e jaargang, 2003.
[56] K.D. MITNICK, *The art of deception: controlling the human element of security,* Indiana, Wiley, 2003.

laatste vertrouwelijke informatie prijsgeeft die bijna op geen enkel andere manier te verkrijgen is.

Dit is belangrijk op te merken, gezien het gros van de bevolking bij de term 'hacking' nog steeds refereert naar allerlei technische hoogstandjes, waardoor ze allerlei *security, anti-virus en anti-spyware software* aankopen. Niet dat deze geen enkel nut zouden hebben, doch lijkt een informatieve training van de gebruiker zelf veel nuttiger (de zogenaamde *security awareness)*. Technologie, en deze beveiligen, is één ding, kennis een ander.

Bovenstaand kader leent zich bijzonder goed om het begrip 'phishing' (of 'pharming') verder uit te werken.

AFDELING 4: PHISHING

Phishing is een vorm van internetfraude, die voornamelijk bij het online bankieren bijzonder vaak voorkomt. Het principe is vrij eenvoudig: men verstuurt een bericht (bijvoorbeeld in de vorm van een e-mail) dat men één of andere actie dient te ondernemen, zoniet wordt de rekening afgesloten, worden er extra kosten aangerekend, enzovoort. Deze e-mail lijkt in veel gevallen bijzonder goed op officiële berichten van de bankinstelling (inclusief logo, huisstijl, vermomde URL's). Nietsvermoedend klikt de ontvanger dan ook verder, maar in plaats van de officiële website te bezoeken, belandt de bezoeker op een valse (bank)website die qua opmaak een kopie is van de echte website. De bezoeker logt in met een kredietkaartnummer, gebruikersnaam en wachtwoord, waarop deze gegevens vervolgens in de handen van criminelen terechtkomen.

Hierbij wordt vaak gebruikgemaakt van URL-spoofing, wat het nabootsen van de URL (de link, www.***.be) inhoudt. Ook aan de hand van zogenaamde *keyloggers*, dit is software die alle toetsaanslagen bijhoudt, kan men relatief eenvoudig wachtwoorden en andere gevoelige gegevens achterhalen.

Prima facie lijkt het moeilijk te ontkomen aan phishing. De meest recente phishing e-mails beginnen er namelijk steeds 'authentieker' uit te zien en het aantal gevallen neemt

bovendien sterk toe.[57] Toch dient algemeen geweten te zijn dat banken weinig tot nooit e-mails direct aan klanten versturen (op persoonlijke e-mailadressen). Zij doen dit bij voorkeur via hun klantenportaal. En mocht de uitzondering voorvallen dat men toch een e-mail krijgt van een bankbediende zal deze nooit (mogen) vragen om financiële- of identiteitsgegevens door te geven, te wijzigen of anderzijds te beïnvloeden.

Phishing kan aldus vergeleken worden met de online variant van skimming.

Pharming wordt vaak aanzien als synoniem voor phishing. Helemaal correct is dit nochtans niet: bij pharming worden de DNS-servers[58] zelf aangevallen, en wordt het legitieme internetadres van een bepaalde domeinnaam gewijzigd. De bezoeker tikt bijvoorbeeld www.kbc.be maar komt terecht op een nagebootste website op een andere webserver. Deze vorm vereist beduidend meer technische kennis dan phishing.

Onderzoek wees uit dat meer dan de helft van alle slachtoffers van phishing, simultaan het slachtoffer werden van identiteitsdiefstal.[59]

HOOFDSTUK 4: SOCIALE NETWERKSITES

Sociale netwerksites worden door beveiligingsexperts met stip aangeduid als de sterkste groeier onder de risicoplatformen voor identity theft. En terecht.

Sociale netwerksites lenen zich om twee redenen bijzonder goed tot identiteitsdiefstal.

Allereerst lijken, de vele waarschuwingen ten spijt, mensen al te vaak niet te beseffen welke enorme risico's vasthangen aan de openbaarheid van informatie. Waar men enkele jaren terug nog moord en brand schreeuwde om diens privacy, gooit men nu lustig elk klein detail, elke gebeurtenis op Facebook, Netlog, Twitter, Hyves en in mindere mate LinkedIn. Dergelijke platformen bieden niet alleen een gedroomde kans voor de identiteitsdief, ze doen *a fortiori* het werk voor hem. Vele netwerksites, met Facebook op kop, sleutelen

[57] N.S. VAN DER MEULEN, *Achter de schermen: de ervaringen van slachtoffers van identiteitsroof,* Justitiële verkenningen, jrg. 32, nr. 7, 2006.

[58] Het Domain Name System (DNS) is het systeem en protocol dat op het Internet gebruikt wordt. Alle domeinnamen en IP-adressen staan in een database en een DNS-server matcht deze gegevens. Een DNS-server vertaalt niet, omdat er geen enkele logica zit tussen de domeinnamen en IP-adressen.

[59] A. LITAN, *Gartner Phishing Attack Victims Likely Targets for Identity Theft,* Gartner, 2004, 2.

steeds opnieuw aan hun privacyverklaringen zodat de bescherming steeds meer miniem wordt (onder het argument van *user-based* diensten, zoals *geo-locating*, waarover later meer), zodat de *persoonlijke* informatie die mensen op hun profiel plaatsen een alsmaar groter risico loopt publiek te worden.

Het is schrijnend vast te stellen dat de meeste internetgebruikers het gevaar niet lijken te beseffen.[60] Een klein – doch daarom niet minder verbijsterend – voorbeeld. Een gemiddeld Facebook lid heeft tussen de 300 en 400 'vrienden'. In de standaardinstellingen van Facebook krijgen niet alleen de eigen vrienden maar ook de 'vrienden van diens vrienden' een quasi volledige toegang tot het profiel. Een eenvoudige rekensom leert ons dat het profiel van X, die 350 vrienden heeft, die elk op hun beurt 350 vrienden hebben, toegankelijk is voor maar liefst **122.850 personen.**[61] Ons kent ons, poneert men dan.

Weinigen zouden door deze cijfers, al is het maar even, niet uit het lood geslagen zijn. En het gaat nog verder. *For the sake of argument* gaat Facebook (en andere sociale netwerksites in haar kielzog) haar privacyrechten nog verder afbouwen, zodanig zelfs dat zij haaks lijkt te staan op de Europese privacyrichtlijn. Een conflict tussen de Europese Commissie en Facebook hangt logischerwijze dan ook in de lucht.

Gezien de sociale netwerksites met stip op nummer één staan als misdrijfplatform van de toekomst, gaan wij hieronder bijzonder uitvoerig in op de risico's van identity theft.

AFDELING 1: OPKOMST SOCIALE NETWERKSITES

Vraag blijft of de sociale netwerksites dan echt zo'n nieuw fenomeen zijn. Als we kijken naar de oprichtingsdata van dergelijke *friend portals* dan dienen we te concluderen van niet. De oermoeder van alle sociale netwerksites, Facebook, bestaat sinds 4 februari 2004.[62] In eerste instantie konden alleen studenten van het Harvard College lid worden, met later

[60] E. KINDT EN S. VAN DER HOF, "Identiteitsgegevens en –beheer in een digitale omgeving: een juridische benadering", *Computerr,* 2009, 44.
[61] In deze berekening werden de zogenaamde 'gemeenschappelijke' vrienden niet meegerekend omdat dit een onvoorspelbare variabele is. Bij een hoge graad aan overeenstemming tussen 2 profielen (zeer gekende vrienden, collega's enzovoort) heeft men een ruw gemiddelde van 60 gemeenschappelijke vrienden. Dit betekent ongeveer een percentage van 14,07% (17.284 personen op 122850), wat het totaal zou doen neerkomen op 105.565,01.
[62] K.M. BALOUN, *Inside Facebook: Life, Work and Visions of Greatness*, onuitg., 2006.

uitbreidingen tot eerst volledig Harvard en dan enkele andere universiteiten. In 2006 opende Facebook zijn poorten voor het wijde publiek, waardoor iedereen kon registreren.

Bij onderzoek van de beschikbare statistieken (zijnde de officiële aangeboden door Facebook[63]), merken we de volgende evolutie op:

- 2004: 1 miljoen gebruikers
- 2005: 5,5 miljoen gebruikers
- 2006: 12 miljoen gebruikers
- 04/2007: 20 miljoen gebruikers
- 10/2007: 50 miljoen gebruikers
- 08/2008: 100 miljoen gebruikers
- 01/2009: 150 miljoen gebruikers
- 02/2009: 175 miljoen gebruikers
- 04/2009: 200 miljoen gebruikers
- 07/2009: 250 miljoen gebruikers
- 09/2009: 300 miljoen gebruikers
- 12/2009: 350 miljoen gebruikers
- 02/2009: 400 miljoen gebruikers

Het moge uit bovenstaande statistiek duidelijk wezen dat het aantal leden de laatste 2 jaar exponentieel is gestegen.

Een andere bekende sociale netwerksite is Netlog, welke haar maatschappelijke zetel in Gent heeft. Zij haalde op 10 augustus 2009[64] de kaap van vijftig miljoen leden. Op 3 november 2009 won Netlog de *Deloitte Technology Fast 50 Award*, en werd zo de snelste groeier van de Benelux genoemd.

Over de bijdrage van deze sociale netwerksites, die overduidelijk floreren in de Web 2.0 gemeenschap, wordt duchtig gediscussieerd. Ze wegdenken kan echter niet meer, deze netwerksites zijn gemeengoed geworden en zullen blijven bestaan. Al is dat misschien niet in de huidige – nog steeds statische, wat passieve - vorm, maar het principe dat men online

[63] http://www.facebook.com/press/info.php?timeline
[64] P. VAN LEEMPUTTEN, "Netlog haalt 50 miljoen leden", *ZDNet België,* 2009, (te consulteren via http://www.zdnet.be/news/106217/netlog-haalt-50-miljoen-leden/).

terug kan grijpen naar het dorp van vroeger, zal niet snel meer verlaten worden. *Augmented reality*[65] rukt snel op, en er wordt dan ook verwacht dat de sociale netwerksites hier handig gebruik van zullen maken.

AFDELING 2: PRIVACY & IDENTITEITSDIEFSTAL

In de inleiding hierboven werd reeds gewezen op de enorme gevaren verbonden aan dergelijke sociale netwerksites, zeker wat privacy en identiteitsdiefstal betreft. Privacy is duidelijk een duaal recht. Enerzijds wordt – wanneer de nood hoog is – er te pas en te onpas naar gegrepen (en de veel te ruime privacywet leent zich daar bijzonder goed voor), maar anderzijds verliest het recht elke dag de strijd met de gemiddelde gebruiker, die veel, soms te veel, informatie wetens en willens 'blootlegt'. Het privacyrecht lijkt dan ook een bijzonder ambigue positie te hebben ingenomen. Facebookbaas Mark Zuckerberg verklaarde in een video-interview[66] met Techcrunch het volgende: "*Mensen zijn het gewend geraakt om niet alleen meer informatie in verschillende vormen te delen, maar ook openlijker en met meer mensen. Die sociale norm is iets wat is geëvolueerd met de tijd. We zien het als onze rol in het systeem om voortdurend te innoveren en te updaten, om zo de huidige sociale normen te weerspiegelen".*

Die relativering van privacy is een bijzonder gevaarlijke en kwalijke evolutie. Dit geldt des te meer voor mensen die – ironisch genoeg – zelf medeverantwoordelijk zijn voor die 'geëvolueerde sociale norm'. Kieron O'Hara, onderzoeker in elektronica- en computerwetenschappen aan de universiteit van Southampton, kwam in zijn onderzoek – gepresenteerd op de jaarlijkse conferentie van de Media Communication and Cultural Studies Association in Londen – tot de conclusie dat het online zetten van persoonlijke details de privacy van iedereen kan ondermijnen.

[65] Toegevoegde realiteit (TR) (eng: Augmented reality) is een vakgebied dat zich hoofdzakelijk bezighoudt met het zo realistisch mogelijk toevoegen van computergemaakte beelden aan rechtstreekse, reële beelden. In plaats van informatie af te beelden op klassieke en geïsoleerde beeldschermen, worden de data geprojecteerd in het gezichtsveld van de gebruiker, meestal door middel van een head-mounted display of head-up display. Het maakt het verschil tussen de reële wereld en de virtuele wereld steeds kleiner en zorgt tevens voor eenvoudigere en gebruikersvriendelijkere interfaces, ook voor complexere toepassingen.

[66] http://www.ustream.tv/recorded/3848950

Dergelijk gedrag zorgt er bovendien onrechtstreeks voor dat het recht op privacy langzaamaan vervaagt, ook voor wie niet op internet zit.[67]

"If you look at privacy in law, one important concept is a reasonable expectation of privacy. As more private lives are exported online, reasonable expectations are diminishing. When our reasonable expectations diminish, as they have, by necessity our legal protection diminishes".[68]

Als – door weliswaar iedereen gekend – voorbeeld gaf O'Hara het voorbeeld van de *'embarrassing photo'*. Inderdaad, waar tot voor enkele jaren zo'n foto het mikpunt van spot zou zijn van *enkele vrienden*, hoogstwaarschijnlijk beperkt tot de aanwezigen, zet men nu, door de talrijke 'tagging' methoden, diens reputatie op het spel voor vrienden, kennissen, collega's en (toekomstige?) werkgever(s). Wanneer het *taggen*[69] van een foto gebeurt zonder toestemming van de betrokkene (of zelfs het uploaden of publiek bekendmaken ervan) is dit uiteraard in strijd met het recht op afbeelding. Stellen dat dit recht praktisch vaak niet kan worden afgedwongen, hetzij uit vriendschappelijke redenen, hetzij uit schroom of onmacht, is niet meer dan een open deur intrappen.

Maar Facebook ligt, samen met andere sociale netwerksites, steeds meer onder vuur. EU-commissaris voor ICT Viviane Reding, ook bekend door haar inbreng in het *'three strikes and you're out'* debat, overwoog recentelijk[70] maatregelen te nemen tegen de gewijzigde privacystandaard op Facebook. Wie namelijk een profiel aanmaakt op de sociale netwerksite maakt deze volgens de standaardinstellingen toegankelijk *voor iedereen*, tenzij hij zelf die instellingen wijzigt.

---

[67] R.C.P. MARBUS, S. FENNEL-VAN ESCH EN A.P.C. ROOSENDAAL, "Identiteit en openbaarheid in sociale online-omgevingen", *Computerr.,* 2009-39, 64.

[68] Z. KLEINMAN, "How online life distorts privacy rights for all", *BBC* News, 2010, (te consulteren via http://news.bbc.co.uk/2/hi/technology/8446649.stm).

[69] Tagging is een optie gebruikt door sociale netwerksites waarbij de uploader van een bepaalde foto vrienden kan selecteren. Deze foto wordt dan niet alleen gepubliceerd op het profiel van diegene die werd aangeduid, hij komt ook nog eens terecht in de fotolijst van de betrokkene. Men kan zich vanzelfsprekend 'untaggen', maar hiermee wordt de foto zelf niet verwijderd. Men dient dus steeds aan de uploader zelf de verwijdering te vragen. Facebook biedt een policy aan voor het verwijderen van foto's, maar beperkt zich hierin tot ongepaste foto's, welke een schending van een wettelijke of reglementaire regel inhouden, dan wel een inbreuk op de goede zeden.

[70] S. VAN NIEWERBURGH, "EU pakt privacyinstellingen Facebook aan", *ZDNet België,* 2010, (te consulteren op http://www.zdnet.be/news/112632/eu-pakt-privacyinstellingen-facebook-aan/).

De Commissie is de mening toegedaan dat dit omgekeerd moet, zoals voor februari 2010 het geval was.

Dat een conflict tussen de EU en Facebook onvermijdelijk is, staat als een paal boven water. Zwitserland en Duitsland onderzoeken nu al of foto's, filmpjes en andere informatie op sociale netwerksites een inbreuk uitmaken op hun nationale privacywetgeving.[71]

Beide landen hebben Facebook om nadere uitleg gevraagd bij de praktijk waarbij gebruikers privémateriaal van vrienden en kennissen, die *geen* Facebooklid zijn, online plaatsen. Hoewel men uiteraard dient uit te gaan van de positieve bedoelingen van bovengenoemde landen, dient men hier toch een kanttekening te maken.

Immers het is en blijft, Facebook zal het graag horen, de verantwoordelijkheid van de eindgebruiker om de rechten te verwerven op het materiaal dat door hem online wordt geplaatst, of het nu om audiovisueel materiaal (auteursrecht en naburige rechten), bedrijfsinformatie (merkenrecht en mogelijk know-how) of persoonsgegevens (privacyrecht) gaat. Facebook kan hier als objectieve online tussenpersoon onmogelijk elke upload controleren, zoiets zou neerkomen op pure censuur. Het recente conflict tussen Google en China toonde ons voldoende aan dat censuur geen antwoord is, of zij dit nu gebruikt voor de bescherming van een Staat, dan wel om niet-gebruikers tegen gebruikers te beschermen.[72]

Het lijkt er dan ook op dat bovengenoemde landen op een dwaalspoor zitten. Facebook en andere sociale netwerksites aanpakken is één ding, men moet echter de geweren op de juiste actoren en de juiste zaken richten. De gewijzigde set standaardregels terugbrengen naar een hogere graad van privacy is daarentegen weldegelijk een goed *begin*.

Update: op 12 mei 2010 maakte de Artikel-29 werkgroep, waarin de Europese privacywaakhonden verenigd zijn, officieel bekend[73] dat de recente wijzigingen van de

---

[71] X., "Nationale privacywetten overtreden?", *De Standaard*, 2010 (te consulteren via http://www.zdnet.be/news/114294/conflict-tussen-europa-en-facebook-dreigt/).

[72] Google werd recentelijk aangevallen door hackers. Bij nader onderzoek bleek dat deze groep hackers in China werden gelokaliseerd. Een Chinese overheidsinmenging werd vermoed, maar kon niet worden bewezen. Als reactie op deze aanval, weigerde Google nog langer de zoekresultaten te filteren. China besloot daarop de zoekmachine officieel te blokkeren. Google.*cn* verwijst nu door naar Google.*com.hk* (Hong Kong).

[73] ARTICLE 29 DATA PROTECTION WORKING PARTY, *European data protection group faults Facebook for privacy setting,* Press Release, Brussel, 12 mei 2010,
(te consulteren via http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_12_05_10_en.pdf).

standaardinstellingen van Facebook als "onacceptabel" dienen te worden aangemerkt. Het adviesorgaan van Europese Commissie vindt dat de standaardinstellingen juist moeten waarborgen dat enkel geselecteerde contacten toegang hebben tot het gebruikersprofiel. Ook de automatische indexatie door zoekmachines wordt op de korrel genomen.

De vraag rijst natuurlijk waarom Facebook zo moeilijk doet over de privacy van haar leden . Men kan zich terecht de vraag stellen of het in haar belang is dat zij voldoende gehoor biedt aan haar gebruikers, in plaats van, zoals de huidige tendens, de grenzen van de privacy steeds meer af-, ja zelfs aan te tasten.

Aan de openbaarheid van gegevens zijn vanzelfsprekend voordelen verbonden voor de sociale netwerksite, hoe kan het ook anders. Voornaamste reden blijkt uiteraard marketing. *Targeted ads* oftewel gepersonaliseerde reclame op maat van diens interesses en activiteiten is *hot* in de huidige marketingwereld. Onder andere Google AdWords, Facebook ads, en Google's Gmail maken hier lustig gebruik van. Maar ook de eenvoudige klantenkaart in de supermarkt (de bekende punten) registreert elke aankoop en bouwt aan de hand van de identiteitsgegevens op de klantenkaart een volledig en gedetailleerd profiel op van een bepaalde gebruiker. Tot grote blijdschap van de één (geen reclames voor pampers aan 60-plussers), tot grote ergernis van de andere, die wel verlegen zit om privacy.

Online behavioral targeting[74] is niet meer uit de virtuele maatschappij weg te denken. Op basis van iemands browseractiviteiten selecteert Google de juiste advertenties. Een voorbeeld; een persoon zoekt op vakanties. Naast de gewone, gratis zoekresultaten (*organische resultaten)* zijn er aan de bovenkant en rechterkant ook betalende advertenties zichtbaar. Deze advertenties zullen algemeen inspelen op het sleutelwoord "vakantie". Wanneer die persoon daarna in Google ingeeft "vakantie Italië", enkele websites bezoekt, terug naar Google surft en terug "vakanties" intikt, zal dat tot een gans anders resultaat leiden dan bij de eerste zoekopdracht. Google heeft deze zoekopdrachten immers geëvalueerd, waardoor er nu gespecialiseerde advertenties zichtbaar zijn, gericht op vakanties in Italië, ook al geeft de persoon enkel "vakanties" in. Afhankelijk van de bewaartijd van dergelijke zoekopdrachten *en haar inhoud* kunnen deze evaluaties

[74] P. KOTLER, G. ARMSTRONG, *Principles of Marketing*, New Jersey, Pearson Education, 2009, 151.

weldegelijk een belangrijke schending van diens privacyrechten inhouden. Voor marketeers zijn deze nieuwe mogelijkheden uiteraard een zegen.

Maar ook sociale netwerksites halen een zeer belangrijk deel van hun inkomsten uit online advertenties. Hoewel onder marketeers – terecht – de perceptie leeft dat deze advertenties minder doeltreffend zijn dan de Google advertenties (gezien de sfeeromgeving totaal verschillend is, bij een gerichte zoektocht dan wel een 'ontspannend' facebookbezoek), haalt Facebook een belangrijk aandeel thuis. Het spreekt voor zich dat hoe meer informatie openbaar is, hoe meer informatie kan worden gelezen en geëvalueerd door algoritmen.

Zowel haar eigen marketingdienst, als externe partners en adverteerders maken hier dan ook dankbaar gebruik van.

Bekend voorbeeld zijn de talrijke advertenties voor online dating. Een belangrijk onderdeel van de gemiddelde Facebookervaring is het aanduiden van het bestaan van een relatie, en in welke staat zij zich bevindt (relatie, verloving, huwelijk). Opnieuw een belangrijk gegeven van informatie voor identiteitsdieven, maar dat terzijde. Wanneer men de relatiestatus op één van de drie bovengenoemde instelt zal men geen datingadvertenties te zien krijgen, met andere woorden enkel *singles* krijgen deze online advertenties te zien. Een bijzonder gemak voor adverteerders die op dergelijke manier onmiddellijk het juiste doelpubliek kan bereiken, maar opnieuw een klaarblijkelijke inbreuk op de privacyrechten.

Tot dusver behandelden wij bijna uitsluitend de relatie 'Facebook gebruiker <–> Facebook <–> externe/Facebook gebruiker'. Niettemin staat de relatie 'Gebruiker - Facebook' ook danig onder druk. Het privacyreglement van Facebook bepaalt immers letterlijk dat de sociale netwerksite een licentie verwerft op *alle* informatie die gedeeld wordt door personen op het Facebook netwerk (dit zijn statusupdates, teksten, audiovisueel materiaal, geo-locaties[75] enzovoort) en die mag gebruiken, niet alleen voor eigen reclamecampagnes, maar eveneens mag doorspelen aan externe partners en adverteerders. Dit uiteraard op voorwaarde dat de informatie publiek gedeeld staat (welke de standaardoptie is, men kan eveneens kiezen voor "Enkel tonen aan vrienden", in zo'n geval kunnen de gegevens – vooralsnog – niet

[75] Zie *infra.*

ingezameld worden). Een uitreksel [76] uit de 'Facebook Statement of Rights and Responsibilities' (de markantste fragmenten worden onderlijnd):

"Sharing Your Content and Information

You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

1. For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.

2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).

3. When you add an application and use Platform, your content and information is shared with the application. We require applications to respect your privacy settings, but your agreement with that application will control how the application can use the content and information you share. (To learn more about Platform, read our About Platform page.)

4. When you publish content or information using the "everyone" setting, it means that everyone, including people off of Facebook, will have access to that information and we may not have control over what they do with it.

5.We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them)."

Dat dergelijke IE-licentie bijzonder verregaand kan zijn hoeft geen verdere uitleg. De sociale netwerksite mag alle gegevens opslaan, analyseren en desgevallend gebruiken in manieren

[76] http://www.facebook.com/terms.php

die zij vooropstelt. Zij kan met andere woorden de foto van een willekeurig persoon plaatsen bij eender welke advertentie, ook al schendt deze de morele waarden van de betrokken persoon (datingadvertenties, geweldadige content, dierenleed, enzoverder).

AFDELING 3: PROFIELKAPING: MANIEREN

§ 1. Social engineering

Social engineering, zoals reeds hierboven kort aangehaald, is een methode waarbij gebruikgemaakt wordt van de nieuwsgierigheid, angst of medeleven van het slachtoffer. Een van de bekendste hackers, Kevin Mitnick, wordt beschouwd als autoriteit op het gebied van social engineering. In zijn boek, '*The Art of Deception*', worden de verschillende technieken bijzonder uitgebreid besproken. De drie meest voorkomende vormen worden hieronder kort beschreven.

A Persoonlijk contact

Voor diegenen met voldoende communicatieve vaardigheden is dit ongetwijfeld de meest effectieve vorm. De hacker doet zich voor als bankbediende, helpdeskmedewerker, politionele of justitiële medewerker, enzovoort. Actueel leveren zoekmachines en sociale netwerksites een schat van informatie om het slachtoffer correct te profileren (zo kan men eventueel ter staving van het verhaal bijkomende persoonlijke informatie meegeven).

Het is dan ook sinds de opkomst en technische verbetering van zoekmachines dat *personal social engineering* met een zorgwekkend gemak kan worden gepleegd. Daar waar vroeger nog effectief moeite moest worden gedaan om persoonlijke informatie te achterhalen, leveren internetdiensten als *pipl.com* meteen een fysiek adres, webpagina's, sociale netwerkprofielen, artikels en foto's op. Een gedroomde *tool* dus.

B E-mail

Bij deze vorm stuurt de hacker of cracker e-mails die een breed pallet aan boodschappen kunnen bevatten. Bekende varianten zijn e-mails die afkomstig lijken van banken of andere financiële instellingen (zie *supra*), gewonnen loterijen of vakanties, valse giften voor rampen, enzovoort. Men roept in de e-mail op tot actie: men dient bijvoorbeeld te surfen naar een (valse) website, zeer frequent zal men op dergelijke valse website identiteits- of andere

gevoelige gegevens (rekeningnummer, rijksregisternummer, pincodes, adresgegevens, et cetera) proberen te achterhalen. Uiteraard is de effectiviteit van bovenstaande procedure afhankelijk van de graad van detail bij de namaak van de website en de technische kennis van de hacker of cracker. De e-mail kan bovendien een besmette bijlage bevatten zoals een virus of trojan. Bij het openen van dergelijke bijlage (en bijhorende installatie ervan) stelt dit de verzender in staat om bijvoorbeeld de computer over te nemen (automatische algoritmen zoeken vervolgens naar persoonlijke informatie, kredietkaartgegevens, …) of de computer te plaatsen in een *botnet*.[77] Zeer recent nog werd het Mariposa botnet, één van de grootste in zijn soort, stilgelegd.[78] Het netwerk bestond uit maar liefst 12,7 miljoen computers. Het stal bank- en kredietkaartgegevens en infecteerde pc's bij verschillende grote bedrijven en meer dan veertig banken. Het netwerk werd voor de eerste keer opgemerkt in december 2008, daarna werd het één van de grootste in zijn soort.

C Dumpster diving

Hoewel de oudste techniek is dit meteen ook de minst interessante voor dit onderzoek. Deze zeer vaak gebruikte en bijzonder gevaarlijke vorm bestaat erin – zoals de titel laat vermoeden – dat identiteitsdieven snuisteren in het (papier)afval van ondernemingen en in mindere mate ook in dat van particulieren. Facturen, rekeningen, offertes, orders en bankuittreksels leveren vanzelfsprekend enorm veel informatie. Gezien deze vorm geen affiniteit vertoont met de ICT wordt deze hier dan ook niet verder besproken.

§ 2. Automatische tools

Er bestaan heden te dage enkele automatische tools voor het kraken van Facebook (e.a.) profielen. Een bekende tool is de Fbcontroller[79] welke een creatie is van de Indiase hacker Azim Poonowala. De Fbcontroller (v1 dateert van 6 mei 2009) is eigenlijk een *network sniffer*, gezien het de communicatie tussen Facebook en computers die interactie hebben

[77] T. O'BRIEN, "Information Security Consultant Pleads Guilty to Federal Wiretapping and Identity Theft Charges", *U.S. Departement of Justice*, 2008, (te consulteren via http://losangeles.fbi.gov/dojpressrel/pressrel08/la041608usa.htm).
[78] M. DOBBELAERE, "Spanje arresteert botnetbeheerders", *MyLex,* 2010, (te consulteren via http://www.ictrecht.be/blog/blog_ictrecht/spanje_arresteert_botnetbeheerders.html).
[79] E. MILLS, "FBController allows for hijacking of Facebook accounts", *CNET,* 2009, (te consulteren via http://news.cnet.com/8301-1009_3-10234720-83.html).

met de website registreert. De laatste versie (tot nu toe) van Fbcontroller werd uitgebracht op 28 december 2009.[80]

Hoewel Facebook en andere sociale netwerksites alles in het werk stellen om dergelijke beveiligings *exploits* te voorkomen, zullen er altijd hackers, zelfs met de 'beste bedoelingen' , aanwezig zijn om bugs of fouten in de code op te sporen en te gebruiken. Het is de verantwoordelijkheid van de sociale netwerksites om snel en reactief hiertegen op te treden.

AFDELING 4: OPLOSSINGEN

Men zou – zeker voor wat phishing betreft – een veel veiliger alternatief moeten bedenken voor de onbeveiligde en niet-geëncrypteerde e-mails waarbij leden van sociale netwerksites worden verwittigd van een vriendschapsverzoek (of ander notificatie in verband met zijn of haar profiel).

Deze e-mails bestaat immers uit gewone HTML of platte tekst, waardoor de inhoud ervan zeer gemakkelijk kan worden gekopieerd en ingebracht in een e-mailprogramma of HTML editor. Vanaf dan is het kinderspel om de vertrouwde opmaak te behouden maar de achterliggende URL's (links) te wijzigen naar de valse website van de fraudeur.

Dat de grote spelers zoals Facebook, Netlog, Twitter, Hyves of LinkedIn hier weinig tot geen aandacht aan schenken is volstrekt onbegrijpelijk. In de praktijk, wanneer men een profiel wil kapen, is dit immers de meest courante praktijk (gezien de technische vereisten minimaal zijn). Men stuurt valse meldingen naar leden (voornamelijk valse vriendschapsuitnodigingen gezien de nieuwsgierigheid die deze opwekken) om zo de inloggegevens te bekomen. Het slachtoffer merkt dit vaak niet eens doordat hij of zij na het invullen van gebruikersnaam en paswoord, wordt doorgestuurd naar de legitieme website.

Als alternatief voor deze uiterst gevaarlijke methode van e-mails zou men kunnen voorzien in geëncrypteerde of beveiligde boodschappen, waarbij men gebruik maakt een bepaalde unieke code voor elke gebruiker die daarmee de melding afkomstig van de sociale netwerksite als geldig kan definiëren. Op die manier kan reeds een groot deel van de profielkapingen worden vermeden.

---

[80] J. SCHEEPERS, "Gratis tool om Facebook-accounts te kapen", *ZDNet België,* 2009, (te consulteren via http://www.zdnet.be/news/102109/gratis-tool-om-facebook-accounts-te-kapen/).

De huidige voorwaarden van sociale netwerksites bieden echter weinig garanties. Een bekende netwerksite als Facebook claimt een algehele licentie op elk gegeven dat de gebruiker genereert binnenin het sociale portaal, geeft deze gegevens door aan advertentiepartners en zet – sinds kort – standaard de persoonlijke gegevens publiek voor iedereen.

Bovendien is een algehele verwijdering van het profiel uiterst moeilijk te bekomen. Indien men zijn of haar profiel wil opzeggen (met alle foto's, gegevens, et cetera) dient men de gegevens één per één te verwijderen, om zeker te zijn dat derden deze foto's, berichten en andere niet meer kunnen gebruiken. Evenwel kwam recentelijk de dienst 'Web 2.0 suicide machine'[81] op de markt die gebruikers de mogelijkheid biedt om 'definitief' uit te schrijven. Men kan daarbij kiezen tussen verschillende sociale netwerken zoals Facebook, Twitter, LinkedIn of MySpace.

Dit is een bijzonder nuttige dienst gezien deze op automatische manier alle gegevens tracht te verwijderen. Facebook, als enige sociale netwerksite, maakte echter juridisch bezwaar tegen de dienst en claimde dat dergelijk gebruik in strijd was met haar voorwaarden.[82] De dienst biedt tot op heden nog de verwijdering aan voor Facebook profielen. Niettemin dient te worden opgemerkt dat de Web suicide machine niet het verhoopte succes was.

Maar natuurlijk is de meest effectieve manier, zoals steeds, de creatie van een grotere bewustwording bij het publiek.

Inderdaad, de meerderheid der gebruikers heeft nog nooit gehoord van (online) identiteitsdiefstal, laat staan dat men zich zorgen maakt over hun verstrekkende online identiteit en de eventuele verregaande gevolgen ervan. Het is immers niet in het belang van deze sociale netwerksites om hun gebruikers te sensibiliseren gezien zowel het aantal gebruikers als de aangeboden informatie sterk zouden teruglopen.

Niettemin moet men via campagnes de gebruiker dringend wakker schudden. De explosieve groei en de grote onbekommerdheid bij het delen van gegevens maken van sociale

[81] M. DOBBELAERE, "Digitale 'zelfmoord'", *MyLex,* 2010, (te consulteren via http://www.ictrecht.be/blog/blog_ictrecht/digitale_zelfmoord_suicideorg_privacy_sociale_netwerksites.html).
[82] P. MCNAMARA, "Facebook blocks 'Web 2.0 Suicide Machine", *Networkworld,* 2010, (te consulteren via http://www.networkworld.com/community/node/49470).

netwerksites gedroomde tools bij het opzetten van grote identity theft acties. Het valt te verwachten dat de sociale netwerksites een terughoudende houding aannemen tegenover dergelijke intentie. Het vaststellen van een objectieve aansprakelijkheid in hoofde van bovengenoemde websites wanneer er een (globale) identity theft voorkomt, kan dienen als voldoende motivatie. Het is nu, meer dan ooit, van levensbelang de gebruiker correct en uitvoerig te informeren. Financiële of commerciële redenen mogen hieraan niet in de weg staan.

HOOFDSTUK 5: CHATPROGRAMMA'S

Nog zo'n een typische online valkuil voor identiteitsdiefstal zijn de alom tegenwoordige chatprogramma's en 'chatboxen'. Hoewel enigszins aan populariteit verloren door de talrijke sociale netwerksites (en hun geïntegreerde chatprogramma's) dragen deze programma's inherent nog steeds levensgrote gevaren met zich mee.

AFDELING 1: PEDOFILIE

Publieke chatboxen zijn bijvoorbeeld vaak onbeveiligd, niet gecontroleerd en een poel voor identiteitsdieven[83], criminelen en pedofielen. Vooral deze laatste nemen vaak – zoniet altijd - een identiteit aan die hen in staat stelt om in contact te komen met minderjarigen. De opkomst van het internet en onbeveiligde chatboxen heeft onvermijdelijk geleid tot een vergemakkelijking in contactopname met minderjarigen.

AFDELING 2: OPLOSSING?

België, als geen ander land geschokt door een reeks pedofilieschandalen, ondernam al snel actie tegen het onbeveiligd chatten door minderjarigen. Hoewel meerdere voorstellen op tafel lagen, werd de oplossing gevonden in de Kids-ID, een elektronische identiteitskaart voor kinderen van 0 tot 12 jaar. De ID vervangt het vroegere kartonnen identiteitsbewijs dat ouders moesten aanvragen wanneer zij met het kind naar het buitenland wilden reizen.

[83] X., "Chat Rooms Becoming Breeding Grounds for ID Theft", *Identity Theft 911*, 2010, (te consulteren via http://identitytheft911.org/alerts/alert.ext?sp=672).

Ook “hallo ouders”, een informatieve website[84] in samenwerking met Child Focus waarop de Kids-ID gepromoot wordt, helpt om de bewustwording bij de bevolking te vergroten.

AFDELING 3: CHATBOXEN ALS INSTRUMENT

Chatboxen hebben hun populariteit bij identiteitsdieven aan nog een reden te danken. Het zijn namelijk gewoon dankbare portalen voor identiteitsdieven zelf. Via beveiligde chatportalen sturen ze geëncrypteerde berichten uit, waar kredietkaartgegevens, identiteitsgegevens, e-mailadressen, logins et cetera te koop (of te ruil) worden aangeboden. Dergelijke verkoop gaat meestal gepaard met een *sample* of voorbeeld (bv. enkele werkende kredietkaartnummers), waarna hackers of crackers gigantische databanken aan gegevens aankopen voor enkele dollars. Het is bijna een volwaardige markt, zij het illegaal.

HOOFDSTUK 6: WIFI-LIFTEN

Identiteitsdiefstal via WiFi [85] -lifting groeit aan populariteit. Het beangstigd aantal onbeveiligde draadloze netwerken in België biedt ook aan identiteitsdieven tal van opportuniteiten.

Maar wat is WiFi-lifting en hoe dienen we dit nieuw fenomeen correct te analyseren?

AFDELING 1: INLEIDING

WiFi-liften is het illegaal meesurfen op andermans, meestal onbeveiligd, draadloos netwerk. Welnu, is dergelijk surfgedrag op andermans internet strafbaar? Deze vraag moest onlangs voor het eerst door de Belgische strafrechter beantwoord worden. Het onderzoek naar de strafbaarheid van WiFi-liften is allerminst eenvoudig daar de Belgische wetgeving inzake informaticacriminaliteit onvoldoende aangepast is aan de noden van vandaag. Hieronder worden niettemin enkele criteria uiteengezet die de rechter kunnen helpen bij de beoordeling van de strafbaarstelling.

[84] http://www.halloouders.be/.
[85] Wireless-Fidelity.

AFDELING 2: FEITELIJKE OMSTANDIGHEDEN WIFI-CASE

Is surfen op andermans internet strafbaar? De allereerste rechtszaak over dit brandend actueel thema werd onlangs in België behandeld.

De officiële aanklacht van het openbaar ministerie luidde "externe hacking". Belangrijk is het verschil tussen 'externe' en 'interne' hacking te kennen. Externe hacking[86] houdt in: *het ongeoorloofd toegang verwerven tot een informaticasysteem of zich daarin handhaven.*[87] Interne hacking komt voor wanneer *hij die met bedrieglijk opzet of met het oogmerk om te schaden zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt..".*[88] Cruciaal zijn de verschillen tussen beide figuren. Daar waar het materieel element bij 'externe hacking' ligt in het ongeoorloofd toegang verkrijgen, ligt het materieel element bij 'interne hacking' in het overschrijden van de bevoegdheid. Naast het materiële, is ook het moreel element van uitermate groot belang. Bij 'externe hacking' spreken we over een algemeen opzet, bij 'interne hacking' over het bedrieglijk en/of met opzet (oogmerk) om te schaden.

In casu ging het om surfen op andermans internet, door het gebruik van een laptop met een Wi-Fi ontvanger. De eigenaar van deze laptop, een 22-jarige Pool, tapte herhaaldelijk vanuit zijn wagen in een welbepaalde straat draadloos internet af van een onbeveiligd netwerk. De man palmde het internet van zijn slachtoffers zodanig in, dat zijzelf niet meer in staat waren om op het internet te surfen (en dit door de datalimieten die door de provider worden vooropgesteld te overschrijden). Een voorbijganger vond het verdacht dat de man steeds in dezelfde straat met zijn laptop op zijn schoot zat te surfen en alarmeerde de politie.[89]

De man werd door het parket van Dendermonde aangeklaagd voor *externe* hacking, en dit omdat de draadloze connectie weliswaar illegaal is, maar anderzijds geen werkelijke schade heeft toegebracht (bv. diefstal van gegevens, het onmogelijk maken van toegang tot het systeem, het onklaar maken van essentiële bestanden, enz.).

---

[86] M. VAN HOOGENBEMT, "Externe hacking: analyse van recente rechtspraak", *Vigiles*, 2009-3, 136.
[87] Art. 550bis, §1 Sw.
[88] Art. 550bis, §2 Sw.
[89] X., "Jongenman kraakt internet buur", *De Standaard,* 2008, (te consulteren via http://www.standaard.be/artikel/detail.aspx?artikelid=9G1QCRSV).

Bij een kritische geest rijst vrijwel onmiddellijk volgende bedenking. Is men als eigenaar niet verantwoordelijk voor het beveiligen van de draadloze internetverbinding? Anders gezegd, indien men er, al dan niet bewust, voor kiest zijn netwerk *niet* te beveiligen, stelt men dit netwerk dan niet open voor gedeeld gebruik? De wetgever heeft de beveiliging niet opgenomen als voorwaarde in de strafbaarstelling, maar kon zij acht jaar geleden reeds weten welke de implicaties zouden zijn van onbeveiligde draadloze netwerken?

De strafrechtelijke basis voor de hoger besproken 'externe hacking' ligt vervat in art. 550bis, §1 Sw., ingevoerd door art. 6 van de Wet inzake informaticacriminaliteit van 28 november 2000. Art. 550bis Sw. richt zich specifiek tot het wederrechtelijk toegang verkrijgen tot een systeem of een deel ervan waartoe men niet gerechtigd is.

Van uitermate belang voor de strafmaat is de vraag of er sprake is van bedrieglijk opzet, aangezien de maximumstraf zonder het bedrieglijk opzet een gevangenisstraf van maximum 1 jaar kan opleveren, terwijl de aanwezigheid ervan deze maximumstraf tot 2 jaar kan doen oplopen.[90] Het is m.i. belangrijk het begrip 'bedrieglijk opzet' juist te kaderen inzake het "WiFi-liften". Het zou immers tot foute conclusies leiden indien men in deze het begrip 'opzet' al te letterlijk neemt aangezien men (quasi) steeds bewust connectie maakt met een netwerk. Men moet eerder kijken naar het al dan niet optreden van economische schade. Het bedrieglijk opzet moet hier dan ook worden begrepen als het toebrengen van economische schade door bv. de diefstal van gegevens terwijl men gebruik maakt van de draadloze internetverbinding. Indien men zich beperkt tot het legaal surfen kan er geen sprake zijn van een bedrieglijk opzet, en is de maximumstraf dan ook beperkt tot 1 jaar.

Art. 550bis, §4 Sw. stelt de strafmaat van de poging gelijk aan die van het voltooide misdrijf. De wetgever wou hiermee aangeven dat de poging op zich ernstig wordt genomen en dat zij bovendien een onmiddellijk gevaar voor het systeem betekent. Bv. de dader plaatst een virus op het systeem van het slachtoffer. Dit virus is geprogrammeerd om a) wachtwoorden te stelen en b) de antivirus software uit te schakelen. Enkel b slaagt. Er is geen sprake van een voltooid misdrijf. Niettemin is het systeem door verlies van beveiliging ernstig in gevaar.

[90] Art. 550bis, §1 Sw.

AFDELING 3: STRAFBAARHEID WIFI-LIFTEN

Uitgaande van de veronderstelling dat elke onrechtmatige verbinding met andermans draadloos netwerk een strafbaar feit zou uitmaken leidt dit tot zeer verregaande gevolgen. Een hotelgast die zijn laptop openklapt en via (bijvoorbeeld) het Windows 'Netwerk Center' automatisch verbinding maakt met een onbeveiligd draadloos netwerk zou zich schuldig maken aan 'externe hacking', terwijl de hotelgast in de overtuiging kan zijn verbinding te hebben gemaakt met het netwerk van het hotel. Hetzelfde zou gelden voor de persoon die met de laptop eenmalig, en al dan niet bewust, verbinding maakt met een onbeveiligd netwerk om snel iets op te zoeken of e-mails te bekijken.

Maken alle gevallen van WiFi-liften een strafbaar feit uit? Of is er nood aan criteria waaraan de rechter de concrete zaak kan toetsen? Indien men de eerste hypothese zou volgen kan men ontelbare situaties voorzien waarin een onoplettend persoon zich schuldig zou maken aan externe hacking. Dat laatste kan niet de bedoeling van de wetgever zijn en zou enkel zorgen voor grote rechtsonzekerheid, zowel bij eindgebruikers als bij politionele en gerechtelijke diensten. Daarom lijkt het aangeraden om enkele criteria voorop te stellen waaraan de rechter de feiten kan toetsen. Hoe deze er uit zouden moeten zien, volgt hierna.

De criteria die men kan vooropstellen zijn de volgende. Allereerst kan men kijken naar de ***frequentie*** van de inbreuk. Het kan immers niet de bedoeling zijn een eenmalige inbreuk – die zich beperkt tot het louter (legaal) surfen – te sanctioneren. Een tweede criterium die men kan aanwenden is die van het ***bandbreedte-verbruik*** van de gemaakte verbinding. Het is namelijk niet uitgesloten dat een persoon slechts eenmalig verbinding maakt met een welbepaald onbeveiligd draadloos netwerk en tegelijkertijd binnen een aantal uren de bandbreedte van het slachtoffer grotendeels opslorpt (bv. door het downloaden van films). Een derde en laatste criterium die men vervolgens kan hanteren is die van de ***onrechtmatigheid*** van het surfgedrag. Terwijl bovenstaande criteria eerder eenvoudig en technisch vast te stellen zijn, gaat dit derde criterium in op de eigenlijke inhoud van de verbinding. Het hoeft geen nader betoog dat surfen naar een e-mailaccount wezenlijk verschilt van het surfgedrag van iemand die op zoek is naar identiteits- en/of kredietkaartgegevens, kinderporno, illegale wapens of terreurwebsites. Het spreekt voor zich dat ook wanneer iemand niet wordt gevat door bovenstaande criteria strafbaar blijft wanneer hij eerst een beveiliging moet doorbreken vooraleer hij in staat is om verbinding te

maken met het draadloos netwerk. Deze criteria hoeven bovendien niet cumulatief vervuld te worden, voldoen aan één van de criteria is voldoende om strafbaar te kunnen worden gesteld.

Bovenstaande criteria sluiten in elk geval de onoplettende computergebruiker uit, evenals de persoon die, al dan niet wetens en willens, verbinding maakt met een onbeveiligd draadloos netwerk, maar zich daarin beperkt tot een eenmalige en kortstondige connectie met legaal surfgedrag. Toegepast op de concrete casus betekent dit dat een veroordeling gewenst is. Immers, het eerste criterium (*frequentie)* is van toepassing (herhaalde connecties), evenals de opslorping van bandbreedte waardoor het slachtoffer *in casu* niet in staat was om nog normaal te surfen. Het derde criterium is in deze zaak niet van toepassing.

AFDELING 4: ONTBREKEN VAN BEVEILIGING: CIJFERS & GEVAREN

Volgens een onderzoek van BIPT (Belgisch Instituut voor postdiensten en telecommunicatie) beschikt ruim 30% van de Belgische computergebruikers over een draadloos netwerk. In maar liefst 48% van de gevallen laat men na de draadloze internetconnectie te beveiligen.[91] Onderzoek in Nederland door Dimension Data[92] bracht aan het licht dat slechts 54% van de draadloze privénetwerken goed (met WPA of WPA2) is beveiligd. 28% gebruikt de zwakkere (en eenvoudig te kraken) WEP-encryptie en iets minder dan een vijfde is zelfs helemaal niet beveiligd. Voornaamste oorzaak van de niet-beveiliging is de onwetendheid van de eigenaar. Ook de technische onkunde kan een grote rol spelen. Echter mag niet alleen met de vinger worden gewezen naar de eindconsument. Aanbieders van draadloze netwerk-routers zouden verplicht moeten worden om een gebruiksvriendelijke 'wizard' (een programma dat stap voor stap de instellingen overloopt) uit te werken en daarin de klemtoon te leggen op de noodzaak van beveiliging. Een andere mogelijkheid is dat de aanbieder standaard de beveiliging incorporeert in het eindproduct en de gebruiker dan eenvoudigweg de nodige uitleg krijgt hoe deze beveiliging toe te passen.

---

[91] X., "Een draadloos netwerk beveiligen", *BIPT,* (te consulteren via *http://www.bipt.be/nl/520/ShowContent/2885/Draadloze_netwerken/Een_draadloos_netwerk_beveiligen.aspx*).

[92] X., "Draadloze netwerken slecht beveiligd", *Dimension Data,* 2008, (te consulteren via *http://www.dimensiondata.com/NR/rdonlyres/0586CF39-2C12-4077-9CD6-4D59280F7FE4/9668/Draadloze_privenetwerken_slecht_beveiligd1.pdf).*

Een draadloze netwerkverbinding onbeveiligd laten kan nochtans zware gevolgen hebben voor de eigenaar ervan. Een persoon die verbinding maakt met een onbeveiligd draadloos netwerk en vervolgens op zoek gaat naar kinderporno, illegale wapens, terreurorganisaties, etc. doet dit met de identificatie (IP-adres) van de draadloze netwerkverbinding. Politionele diensten die dergelijk surfgedrag op het spoor komen verdenken bijgevolg de (onschuldige) eigenaar. In dergelijk geval is het bewijs van onschuld zeer moeilijk te leveren en de gevolgen voor de eigenaar niet te overzien. Hetzelfde geldt voor diegene die via peer-to-peer programma's of nieuwsgroepen grote hoeveelheden auteursrechtelijk beschermd werk binnenhaalt. Wederom zal de verdenking op de eigenaar rusten. En last but not least kan men zich via het draadloos netwerk met een bijzonder gemak toegang verschaffen tot de verbonden computers of netwerkapparaten. Gezien daar veelal persoonlijke informatie aanwezig is (identiteitsgegevens, rijksregisternummer, e-mailadressen, gebruikersnamen en paswoorden, kredietkaartgegevens, et cetera) kan de identiteitsdief op een korte termijn een schat aan informatie verzamelen. Er is ontegenzeggelijk nood aan meer ruchtbaarheid en sensibilisering dringt zich dan ook op.

AFDELING 5: DE UITSPRAAK

Op 14 november 2008 werd bekend gemaakt dat de jongeman schuldig is verklaard aan surfen op andermans netwerk.[93] De strafrechter verleende de beschuldigde echter de gunst van opschorting van straf. Het lijkt er dus op dat de Belgische strafrechter met dit precedent een belangrijk signaal wou uitdragen, evenwel blijft een gefundeerde motivering uit. Het is nochtans van uitermate groot belang voor de rechtszekerheid dat er duidelijke en gemotiveerde criteria gehanteerd worden, die eventueel later consistent kunnen worden toegepast en/of in een wettelijk kader kunnen worden gegoten.

AFDELING 6: RECHTSVERGELIJKEND: HET DATACENTER-VONNIS.

Recentelijk werd een soortgelijke zaak in Nederland behandeld door de Amsterdamse rechtbank.

Een groep verdachten had in een studentenflat een klein datacenter aangesloten op de aanwezige internetverbinding. Het datacenter werd verborgen gehouden door tijdelijk

[93] X., "Jongeman schuldig aan surfen op andermans netwerk", *De Standaard,* 2008, (te consulteren via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF14112008_028).

verwijderde plafondplaten. De eigenaar ontdekte dit ruim een half jaar na het plaatsen en de groep werd beticht van diefstal van dataverkeer, capaciteit van bandbreedte en uiteraard het aftappen van internet. De uitspraak is op zijn minst min of meer opvallend te noemen. De meervoudige strafkamer van de Amsterdamse rechtbank oordeelde dat "*door ongeoorloofd gebruik te maken van bandbreedte de rechthebbende immers niet noodzakelijk de feitelijke macht verliest"*.[94] De rechtbank wees er ook op dat bovenstaande genoemde zaken geen 'goederen' zijn zoals in het artikel 310 van het Wetboek van Strafrecht staat aangegeven, waardoor van diefstal geen sprake is.

De gevolgen van deze rechtspraak zijn niet te onderschatten. Men kan hier een vrijgeleide in zien om in Nederland naar goeddunken gebruik te maken van onbeveiligde netwerken. Bovendien mag men de datalimiet bij dit gebruik volledig onwerkbaar maken (door excessief veel te downloaden) zonder dat dit als 'diefstal' kan worden aanzien. Een positief gevolg is dat eigenaars van een onbeveiligde verbinding sneller geneigd zijn om toch te beveiligen. Gezien de heimelijke installatie van een datacenter (dat uiteraard met kwaad opzet werd geïnstalleerd) had een matiging of een correctie van dit vonnis niet misstaan. Indien men deze zaak ook op de reeds geformuleerde criteria (zie *supra)* toepast, dan merken we dat hier een veroordeling op zijn plaats zou geweest zijn (toepassing *frequentie* en *bandbreedte-verbruik* criteria).

AFDELING 7: BESLUIT

Hoewel in de voorgaande zaken niet specifiek werd verwezen naar het misdrijf van identiteitsdiefstal (hoogstwaarschijnlijk omdat de justitiële en politionele ambtenaren het belang van identity theft nog niet voldoende inzien) kan men gemakkelijk het specifieke misdrijf met de case verbinden.

Gezien de hoge stijging van identiteitsmisdrijven en het dito aantal (onbeveiligde) internetverbindingen, kan men verwachten dat identiteitsdiefstal via WiFi alleen maar zal toenemen. Het belang van de uitspraak mag echter niet overschat worden. Er werd weliswaar besloten tot een veroordeling maar een effectieve straf evenals een gedegen motivering bleven uit. Niettemin zal dit vonnis ongetwijfeld gevolgen hebben voor de

[94] Rechtbank Amsterdam (meervoudige strafkamer), 11 september 2008, *http://www.boek9.nl.*

politionele en juridische kijk op dit fenomeen. Afsluitend kan gewezen worden op het eerder aangehaald discussiepunt. Draagt de eigenaar een verantwoordelijkheid in het beveiligen van het netwerk? De wetgever heeft in de Wet inzake Informaticacriminaliteit niet in een dergelijke verantwoordelijkheid voorzien. Anderzijds kon men acht jaar geleden onmogelijk de problematiek van WiFi-liften voorspellen. De toekomst zal moeten verduidelijken of, hetzij door een wijziging in de wetgeving, hetzij door innoverende rechtspraak, er al dan niet rekening zal gehouden worden met de rol en de aansprakelijkheid van de eigenaar.

Update: op 12 mei 2010 werd een opmerkelijk vonnis[95] geveld door het Duitse gerechtshof in Karlsruhe. De Duitse rechter oordeelde dat gebruikers eigen wachtwoorden moeten instellen, en dus geen gebruik mogen van de standaardinstellingen, afkomstig van de fabrikant van de WiFi-apparatuur. Het Hof komt daarmee terug op een eerdere uitspraak in 2008 waarin dergelijke beveiligings*verplichting* werd afgewezen. Het bezigen van encryptie (WEP, WPA[2], …) is daarentegen volgens de rechter niet verplicht. Het wijzigen van het standaardwachtwoord is aldus voldoende. Dit is zonder meer een belangrijke uitspraak, gezien de verantwoordelijkheid hier (althans deels) bij het 'slachtoffer' wordt gelegd.

HOOFDSTUK 7: LOCATION-BASED (SOCIAL NETWORKING) APPLICATIONS

Dé laatste aanstormende internethype is meteen een voltreffer op het vlak van privacy. *Location-based social netwerking games* en applicaties winnen gestaag aan populariteit. De bekende applicaties zoals Gowalla[96] en Foursquare[97] maken gebruik van de GPS die aanwezig is in de meeste smartphones. Meedelen waar je bent, is de grote mobiele (marketing-) belofte van het moment.[98] Als gebruikers hun locatie willen meedelen aan vrienden op hun sociaal netwerk (of vrienden binnen de applicatie zelf) dienen zij *"in te checken"* op de bewuste plaats. Eens dat gedaan, deelt de betrokkene zijn locatie en tijdstip mee aan elkeen die het lezen wil. Hoewel het aantal gebruikers van deze diensten in België

[95] Bundesgerichtshof Karlsruhe, *Haftung für unzureichend gesicherten WLAN-Anschluss*, (te consulteren via http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2010&Sort=3&nr=51934&pos=0&anz=101).
[96] http://gowalla.com/
[97] http://foursquare.com/
[98] M. VAN DER MADE, "Waar je bent, is de nieuwste mobiele hype", *Z24,* 2010 (te consulteren via http://www.z24.nl/bedrijven/it_telecom/artikel_129640.z24/Waar_je_bent_is_de_nieuwste_mobiele_hype.html).

nog eerder beperkt kan genoemd worden, zal deze hype naar verwachting binnenkort doorbreken. Immers, Facebook (eind april 2010)[99], Twitter en andere bekende sociale netwerksites werken aan hun eigen location-based diensten, zodat de software van *third parties* overbodig wordt.

De applicaties van Facebook, Twitter, Google (GMail Buzz) en andere bekende namen zijn bijna standaard aanwezig op de gemiddelde smartphone (iPhone, BlackBerry, HTC, …). Het is dan ook een kwestie van tijd eer de functie *"share your location"* wordt opgenomen in een update. Gebruikers zullen massaal hun locatie delen, daarvan melding geven en zo – hoogstwaarschijnlijk zonder het te beseffen – een enorm risico creëren op identiteitsdiefstal (de gewone diefstal niet te na gesproken).

Privacygewijs geeft deze ontwikkeling ook weinig reden tot juichen. Hoewel terecht de opmerking wordt gemaakt dat de gebruiker zelf kiest welke locaties en op welk tijdstip hij deze wil delen (er is met andere woorden geen automatisme, wat anders ongetwijfeld tot gênante situaties zou leiden). Evenwel kan men – jammer genoeg – van de gemiddelde gebruiker niet verwachten dat hij voldoende notie zou hebben van de risico's die gepaard gaan met dergelijke location-based services.

Dit werd zeer recent nog aangetoond met een eerder confronterende website. '*Please Rob Me*'[100] gaf live geo-locating statussen en meldingen weer van gebruikers overal ter wereld (via Twitter, Foursquare, …). De website kreeg in de pers een ruime belangstelling. Achteraf gezien bleek het om een *awareness* actie te gaan op poten gezet door *Forthehack*[101]. De dienst werd intussen afgesloten (er worden geen live meldingen meer getoond), en zij bevat nu – onder andere – deze waarschuwing:

"The goal of this website is to raise some awareness on this issue and have people think about how they use services like Foursquare, Brightkite, Google Buzz etc. Because all this site is, is a dressed up Twitter search page. Everybody can get this information."

[99] S. VAN NIEUWERBURGH, "Facebook laat zien waar je vrienden zijn", *ZDNet België*, 2010, (te consulteren via http://www.zdnet.be/news/113665/facebook-laat-zien-waar-je-vrienden-zijn/).
[100] http://pleaserobme.com/
[101] http://www.forthehack.com/

Dat deze waarschuwing geen bangmakerij is, bewezen de reeds bestaande inbraken en misdrijven. Op 25 maart 2010 kreeg Keri McMullen, nadat ze via haar Facebook-pagina had laten weten dat ze om 20u een concert ging bijwonen, om 20u42 inbrekers over de vloer. Ironisch genoeg en Web 2.0-gewijs werden deze inbrekers op video (webcam) gezet, waarna het slachtoffer zich realiseerde dat één van de inbrekers een 'vriend' was op Facebook.[102]

Vraag blijft dan waarom gebruikers in godsnaam hun locatie (al dan niet quasi-continu) willen meedelen. De meest valabele reden is dat dergelijke applicaties vertrekken vanuit het *game* principe: Foursquare bijvoorbeeld levert de mogelijkheid om 'Mayor' te worden van een bepaalde plek van zodra er genoeg check-ins zijn. Handelszaken spelen hier reeds op in door 'Mayor' promoties uit te delen (bijvoorbeeld eerste drank gratis, korting, et cetera). Dit zorgt uiteraard voor de nodige motivatie om een bepaalde plaats tot *jouw* plek te maken.

Een andere reden is het '*I'm in the room*'. Met location-based applicaties kan je immers live kijken wie van je vrienden aanwezig is op een bepaalde plek (een concert, theatervoorstelling, park, universiteit, …), wat het afspreken of een korte babbel een stuk eenvoudiger maakt.

Wegen bovenstaande redenen dan op tegen het enorme privacygevaar die gebruikers met dergelijke applicaties nemen? Het antwoord hierop dient te worden gegeven door de gebruiker zelf, gezien de eindverantwoordelijkheid finaal bij hem/haar ligt.

Ondergetekende testte – bij wijze van sociaal experiment en in functie van dit schrijven – de applicatie Foursquare enige tijd uit. Het moet zonder meer gezegd worden dat de incentives om de locatie bijna continu te delen, bijzonder groot zijn. Hoewel de applicatie nu nog is weggelegd voor de *early adopters* ligt de weg naar de 'gewone' gebruiker wijd open. De verraderlijkheid ligt net in het onschuldige van het gehele gebeuren: de gebruiker wordt immers beloond voor veelvuldige updates door middel van badges die wijzen op de anciënniteit in het spel. Niettemin loopt men ondertussen een enorm risico dat identiteitsdieven de verschillende updates nauwgezet bijhouden om een profiel te ontwikkelen van een bepaalde persoon. Immers, wanneer zij gedurende enkele weken kunnen bijhouden welke activiteiten een bepaalde persoon verricht, levert dit een bijzonder

[102] X., "Facebook 'Friend' Suspected in Burglary", *CBS News*, 2010, (te consulteren via http://www.cbsnews.com/stories/2010/03/25/earlyshow/main6331796.shtml).

gedetailleerd profiel op. Men dient daarom niet alleen op de hoede te zijn voor de gewone diefstal en gerelateerde misdrijven, ook identiteitsdiefstal komt onverbiddelijk om de hoek kijken.

Het valt nog af te wachten wat de juiste implicaties zijn van bovengenoemde toepassing. Echter, men mag verwachten – gezien het succes van de gewone sociale netwerksites – dat het onvermijdelijk een nieuwe grote hype zal worden. En een geliefde bron van informatie, uiteraard.

DEEL 3: HUIDIGE EN TOEKOMSTIGE BEVEILIGINGSMECHANISMEN

Hierna worden de meest voorkomende online beveiligingsmechanismen behandeld. Vanzelfsprekend kan niet elke methode op elk mogelijk platform of situatie worden toegepast.

HOOFDSTUK 1: PASWOORDEN

Paswoorden en pincodes domineren reeds lang het online gebeuren en zelfs het dagelijkse leven. De graad van beveiliging die gewone paswoorden of pincodes bieden is daarentegen bedroevend laag.

Gewone paswoorden bestaan uit letters, cijfers en eventueel enkele tekens. In het slechtste geval bestaat het paswoord enkel uit letters. Deze zijn dan wel makkelijk te herinneren voor de gebruiker (eigennamen, persoonsnamen, figuren, etc.) maar leveren een *enorm* risico op diefstal of hacking op. Gezien het kraken van dergelijke wachtwoorden met *brute force*[103] kinderspel is, wordt het gebruik ervan dan ook sterk afgeraden.

De meeste websites en diensten vereisen bij het instellen van een paswoord zowel cijfers en letters. Ook wordt meestal een minimum lengte voorgeschreven, immers hoe langer het paswoord, hoe moeilijker het te kraken is met *brute force* methodes.[104] Een andere voor de hand liggende raad is dat het paswoord niet beschrijvend mag zijn. Vaak bevat een paswoord persoonlijke informatie zoals de naam van een partner, kinderen, huisdieren enzovoort. Er bestaat weinig gevaarlijker uiteraard. Aangeraden is dan ook een mix van letters, cijfers en speciale karakters, hoe willekeuriger, hoe moeilijker te kraken. Dikwijls veranderen is de laatste tip die vaak wordt meegegeven.

Ter illustratie: met een *brute force* aanval zal een paswoord van vijf karakters binnen enkele uren worden achterhaald. Een teken met zes karakters neemt snel enkele dagen in beslag (op voorwaarde dat het paswoord geen woord is dat voorkomt in een woordenboek, gezien het dan veel sneller opduikt).

---

[103] J. ERICKSON, *Hacking: the art of exploitation*, San Francisco, No Starch Press, 2003, 214.
[104] I. VANSTEENKISTE, "Tips voor veilige en sterke wachtwoorden", *MindWell* Megazine, 2010, (te consulteren via http://www.mindwell.be/management_workplace/tips-voor-veilige-en-sterke-wachtwoorden/).

Over het web worden paswoorden meestal vervormd opgeslagen, met behulp van een algoritme. Dat proces wordt *hashen*[105] genoemd. In plaats van het originele wachtwoord op te slaan of tussen processen of systemen door te geven, wordt de versleutelde hashwaarde van het wachtwoord doorgestuurd. Een frequent gebruikte hashfunctie is de MD5 (Message Digest Algorithm 5)[106]. Gezien een uitleg hiervan de beoogde techniciteit van deze uiteenzetting ver zou overschrijden, wordt hier niet verder op ingegaan. Belangrijk is wel te onthouden dat een persoon die eventueel toegang zou hebben tot het bestand (database) waar de wachtwoorden zijn opgeslagen én het algoritme kent, het wachtwoord (normaliter) *niet* kan achterhalen (decodering). Men kan immers uit het wachtwoord de gehashte vorm berekenen maar niet andersom.

Dat dit alles geen maat voor niks is bewijzen de veelvuldige hacks die gebruik maken van SQL injecties. Vaak kunnen hackers zich door een fout in de websoftware toegang verschaffen tot de database van websites (waar gebruikers en hun paswoorden zijn opgeslagen). Wanneer dit voorvalt, zoals recentelijk met de uiterst bekende Nederlandse websites FOK, GeenStijl en Tweakers[107], kan de hacker een hele reeks md5-hashes bemachtigen. Het kost echter bijzonder veel moeite, zoals hierboven reeds gesteld, om deze per algoritme terug te laten berekenen (dit kan via enkele websites, zoals http://tools.benramsey.com/md5/). Mochten deze paswoorden echter niet gehasht worden (platte data) zouden de paswoorden uiteraard vrijelijk consulteerbaar zijn voor de hacker.

Paswoorden zijn inherent onveilig. Niet alleen door de talrijke technische tekortkomingen, maar nog veel meer door de menselijke tekortkomingen. Niet alleen zijn de meeste mensen niet in staat meerdere wachtwoorden te onthouden, vaak gebruikt men een eigennaam, of een stukje persoonlijke informatie die voor bekenden of identiteitsdieven al snel te achterhalen valt. Het zou te eenvoudig zijn om de inherente onveiligheid enkel toe te schrijven aan de techniek. Laksheid en onwetendheid maken van paswoorden een ongeschikt beveiligingsmiddel, zodat dergelijke beveiliging op termijn onverbiddelijk dient te verdwijnen.

---

[105] T. CORMEN, C.E. LEISERSON, R. RIVEST, C. STEIN, *Introduction to Algorithms*, Massachusetts, MIT Press, 2001, 245.
[106] S. BUNTING, *EnCase Computer Forensics,* Indiana, Wiley, 2008, 360.
[107] P. MOLENAAR, "Website FOK gehackt en onder vuur van ddos-aanval", *Tweakers.*net, 2009, (te consulteren via http://tweakers.net/nieuws/62003/website-fok-gehackt-en-onder-vuur-van-ddos-aanval.html).

HOOFDSTUK 2: ENCRYPTIE

Encryptie wordt reeds – maar nog veel te weinig – toegepast bij het versleutelen van e-mails, documenten, persoonlijke bestanden, et cetera.

We onderscheiden twee soorten encrypties, namelijk symmetrische en asymmetrische encryptie.

De oudste en eenvoudigste vorm betreft de symmetrische encryptie. In dit geval krijgen zender en ontvanger dezelfde *sleutel*. Deze sleutel moet vanzelfsprekend van tevoren gekend zijn, anders kan het document niet gedecodeerd worden. Het nut van symmetrische encryptie is niet erg hoog, gezien in veel gevallen deze vorm uiterst makkelijk gekraakt kan worden.

De modernere methode is asymmetrische encryptie (of *public key encryption*[108]*).* Bij deze vorm hebben zender en ontvanger elk een eigen *set* van sleutels, waarvan één set publiek is en de andere niet. Berichten die vervolgens met de publieke sleutel worden versleuteld (bijvoorbeeld toepassing van de eID), kunnen alleen met de geheime sleutel worden ontcijferd. Onbevoegden kunnen met andere woorden het bericht niet achterhalen. Berichten kunnen dus gecodeerd en digitaal worden ondertekend, wat het risico op identiteits- en gegevensdiefstal drastisch naar beneden haalt. Bovendien kent assymetrische encryptie het voordeel dat de uitwisseling van de benodigde sleutels kan plaatsvinden via een onveilig kanaal zoals het internet. Uiteraard is dit enkel op voorwaarde dat zender en ontvanger elkaars identiteit en integriteit kunnen vaststellen langs een betrouwbaar medium.

Opmerkelijk is dat de Belgische wetgever bij het opmaken van de regelgeving omtrent encryptie, de mogelijkheid heeft voorbehouden om bij K.B. het particulier gebruik van encryptie te verbieden. De argumentatie is dat wanneer teveel particulieren encryptie gebruiken, dit voor de politionele diensten op het vlak van ICT bijzonder moeilijk werken is. Dergelijk verbod is tot op heden niet geïmplementeerd, maar kan te allen tijden worden ingesteld.

---

[108] http://www.webopedia.com/TERM/P/public_key_cryptography.html
http://www.rsa.com/rsalabs/node.asp?id=2165

HOOFDSTUK 3: BIOMETRIE

Sinds het einde van de 20ste eeuw verricht men onderzoek naar de verschillende mogelijkheden die vervat liggen in de biometrie[109], ofwel het identificeren van personen aan de hand van lichamelijke kenmerken.

Recent, door de toenemende veiligheidsdreigingen, werden er verschillende nieuwe manieren ontwikkeld om de bescherming van gebouwen, software, hardware en andere te garanderen. Enkele bekende vormen zijn de vingerafdruk, retinascan (achterin het oog), irisscan (structuur iris van het oog), gezichtsherkenning, handpalmherkenning, stemherkenning et cetera.

Hoewel de **vingerafdruklezer** zowel in de actualiteit als bij particulieren steeds nadrukkelijker op de voorgrond komt (bijvoorbeeld voor toegang op laptops, gebouwen, etc), is het idee verre van nieuw te noemen. Nochtans zijn de toepassingen de laatste jaren indrukwekkend toegenomen. Zo kan een laptop standaard meegeleverd worden met een vingerafdruklezer, bestaan er externe harde schijven die enkel toegankelijk zijn met de vingerafdruk, computermuizen die enkel reageren op de juiste vingerafdruk, enzoverder. Hoewel het een bijzonder doeltreffende (en kostenefficiënte) vervanging kan betekenen voor het kwetsbare paswoord, zijn er toch enkele bedenkingen. Ten eerste rijst – zoals steeds bij biometrie – de vraag naar bescherming van iemands privacy.[110] De vingerafdruk (of andere) dient namelijk in een database te worden opgeslagen, anders is vergelijking niet mogelijk. Vraag is natuurlijk hoe die database beveiligd wordt en welke informatie er aan de biometrische gegevens worden gelinkt. Voorts is de technische volmaaktheid (*a fortiori* bij particuliere toepassingen) nog niet bereikt, zodat men vaak voorziet in een *escape strategy* waarbij men alsnog kan gebruik maken van een paswoord. In zo'n geval is de vingerafdruklezer niet meer dan een gimmick. Dat het niettemin in de praktijk wordt aangewend bewijzen de volgende gevallen.

[109] http://www.zetes.be/nl/fiches/corporate/technologies-products/technologies-generic/biometrics.cfm
[110] E. KINDT EN J. DUMORTIER, "Biometrie als herkenning- of identificatiemiddel? Enkele juridische beschouwingen", *Computerr.,* 2008, 132.

De Nederlandse supermarkt Albert Heijn testte samen met het betaalbedrijf Equens betalingen met behulp van een vingerafdruklezer.[111] *Prima facie* is dit een uitstekende oplossing tegen het bovengenoemde skimming. Equens creëerde een speciale lezer die de unieke eigenschappen van een vinger kan onthouden. Als de klant enerzijds zijn identiteitsgegevens en anderzijds zijn bank- of kredietkaartgegevens liet registreren (wat op zich ook niet helemaal zonder gevaar is) kon de klant aan de kassa afrekenen zonder fysiek betaalmiddel. De test werd door verschillende juristen onder de loep genomen in verhouding tot de Nederlandse privacywetgeving.

Hoewel het voorgaande absoluut als vooruitgang kan worden beschouwd, diende te worden vastgesteld dat na amper twee weken het systeem reeds werd gekraakt.[112] De 'hacker', een oud Atos Origin-medewerker, misleidde Tip2pay aan de hand van een rubberen kopie van andermans vingerafdruk.[113] Dergelijke rubberen kopieën lijken op het eerste zicht moeilijk te maken, maar hackers hebben voldoende aan een vingerafdruk die wordt nagelaten op een wijnglas, boek, of andere. De kraak was trouwens geïnspireerd op de actie in 2004 van de Chaos Computer Club, die erin slaagde om de vingerafdruk te kopiëren van de toenmalige Duitse minister van Binnenlandse zaken Dr. Wolfgang Schäuble.

Vingerafdruklezers lijken dus technisch gezien nog met een en ander te kampen. Een mogelijkheid om het procédé wat veiliger te laten verlopen is de combinatie met een pincode. Immers, een bank- of kredietkaart valt eveneens relatief gemakkelijk te kopiëren, maar er bestaat een tweede buffer in de vorm van een pincode. De combinatie van een vingerafdruk met een individuele pincode zorgt alleszins voor een hogere beveiligingsgraad.

Ondanks de hierboven geschreven nuance, levert een vingerafdruk weldegelijk een veiliger alternatief dan het kwetsbare wachtwoord. Niettemin werken heden ten dage veiligheidsexperts nog maar weinig met de vingerafdruk.

---

[111] R. PRUYN, "Nederlandse supermarkt test betalen met vingerafdruk", *ZDNet België,* 2008, (te consulteren via http://www.zdnet.be/news/86928/nederlandse-supermarkt-test-betalen-met-vingerafdruk/).
[112] M. DE NEEVE, "Vingerafdrukbetaalsysteem AH gekraakt", *Tweakers.*net, 2008, (te consulteren via http://tweakers.net/nieuws/54263/vingerafdrukbetaalsysteem-ah-gekraakt.html).
[113] B. DE WINTER, "Onderzoeker kraakt vingerafdrukbetaling Albert Heijn", *Webwereld*, 2008, (te consulteren via http://webwereld.nl/articles/51680/onderzoeker-kraakt-vingerafdrukbetaling-albert-heijn.html).

Biometrie bevat immers meer dan de vingerafdruk alleen. Zo dacht de luchthaven van Schiphol eraan om alle passagiers via de **irisscan** te identificeren. De irisscan zit momenteel verwerkt in hun programma 'Privium'[114], waarbij opnamen gemaakt worden van beide ogen. Na deze scan worden de irisdetails op een chip van de Privium Card opgeslagen. Bij een grenspassage worden de gegevens van de scan in de chip vergeleken met die van het oog. Schiphol benadrukt dat de gegevens na de scan *onmiddellijk* uit de apparatuur verwijderd wordt.[115] Deze irisscan werd ontworpen door Amsterdam Airport Schiphol, volgens haar eigen specificaties, welke een wereldprimeur uitmaakte.

Men is reeds enige tijd van plan om de irisscan voor alle reizigers te gebruiken, Schiphol experimenteert overigens al een lange tijd met de irisscan. In 2005 nam het reeds deel aan een test waarbij Nederlanders die naar de V.S. reisden versneld langs de douane konden. Hiervoor moesten ze, naast een irisscan, een vingerafdruk afstaan en hun instemming betuigen met een antecedentenonderzoek[116]. Hiervoor werd een verdrag tussen beide landen gesloten.[117]

Dat het nog ingewikkelder kan bewijst de Universiteit van Bath (Engeland).[118] De wetenschappers experimenteren, na de vingerafdruk, de iris en de oren, nu ook met de **neus** om iemands identiteit te verifiëren. Ze werken aan een experimenteel systeem dat mensen kan identificeren aan de hand van de contouren van diens neus. Softwarematig maakt men gebruik van PhotoFace, een programma ontwikkeld binnen de U.K.

Het PhotoFace-systeem vormt een 3D-model van iemands gezicht met behulp van meerdere foto's die genomen zijn uit verschillende hoeken van het gezicht en de neus. De schaduw die de neus werpt bij de verschillende foto's speelt bovendien een belangrijke rol. Het systeem baseert zich immers niet op de gehele neus om iemands identiteit vast te stellen (een vergelijking hierop zou te lang duren) maar baseert zich op drie delen: het *brugprofiel*, *de punt van de neus* en het *gebied tussen de ogen.*

---

[114] http://www.schiphol.nl/Reizigers/OpSchiphol/Privium.htm
[115] https://www.schiphol.nl/OpSchiphol/PriviumIrisscan/SnelleGrenspassageMetDeIrisscan.htm
[116] J. SCHEEPERS, "Irisscan op Schiphol volgend jaar voor iedereen", *ZDNet België,* 2008, (te consulteren via http://www.zdnet.be/news/88510/-irisscan-op-schiphol-volgend-jaar-voor-iedereen/).
[117] X., "United States and The Netherlands Launch Air Travel Partnership to Streamline Border Processing", *Homeland Security*, 2009, (te consulteren via http://www.dhs.gov/ynews/releases/pr_1240501085368.shtm).
[118] A. EVANS, "Software sniffs out criminals by the shape of their nose", *University of Bath*, 2010, (te consulteren via http://www.bath.ac.uk/news/2010/03/02/nose-recognition/).

De wetenschappers verklaarden dat er in de biometrie tot voor kort weinig tot geen aandacht uitging naar de neus, in tegenstelling tot de ruime aandacht voor de oren en de ogen. Toch neemt de neus een prominente plaats in op het gelaat, en kan men via de neustechniek sneller filteren uit een database dan met bijvoorbeeld volledige gezichtsherkenning. Vanwege de kostprijs en betrouwbaarheid lijkt het niettemin onwaarschijnlijk dat deze techniek de irisscan snel zal vervangen. Gezien men pas op 2 maart 2010 begonnen is met het onderzoek zijn er vooralsnog geen concluderende resultaten beschikbaar.

Waar tot hiertoe enkel particuliere of universiteitsprojecten werden besproken, verdient het **Humabio-project**[119] van de Europese Unie eveneens vermelding. De slogan van het project, *"fingerprints and faces can be faked, but not brain patterns"* laat weinig aan de verbeelding over. De EU werkt aan scanners die iemands hersenactiviteit en hartslag meten. Dergelijke scanners zouden de volgende generatie biometrische detectoren moeten worden. Het opzet van het Humabio-project is om een biometrisch systeem te vinden dat kan gebruikt worden om toegang tot bepaalde gevoelige locaties (en toegang tot gevoelige gegevens, zoals identiteits- of financiële informatie) te beperken, op een manier die niet als te ingrijpend wordt ervaren.

Hoewel de bovenstaande methodes en vormen uiteraard nog volop in ontwikkeling zijn bieden zij vandaag – op voorwaarde dat ze effectief en correct worden aangewend – een valabel, praktisch en veilig alternatief voor het achterhaalde paswoord.

De Belgische privacycommissie sprak zich, zoals enigszins te verwachten, vrij negatief uit ten aanzien van toepassingen steunende op biometrie. In een advies[120], d.d. 9 april 2008, concludeerde zij (gedeeltelijke overname van de belangrijkste passages):

"Het biometrisch gegeven, of het nu een afbeelding betreft dan wel het gegevensuittreksel van die afbeelding (de template) is een fysiek kenmerk van een individu. Dit gegeven kan op

[119] http://www.humabio-eu.org/ en http://cordis.europa.eu/ictresults/pdf/factsheet/INF70100_ICT_%20Results_Fact_sheet_0902_February_HUMABIO.pdf

[120] COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies uit eigen beweging over het verwerken van biometrische gegevens in het raam van authenticatie van personen, 9 april 2008, (te consulteren via http://www.privacycommission.be/nl/docs/Commission/2008/advies_17_2008.pdf).

zich informatie onthullen over een natuurlijke persoon maar ook de omstandigheden van de inzameling kunnen bijkomende persoonlijke informatie opleveren (zo kan de verwerking van gegevens betreffende de plaats en het ogenblik van de inzameling toelaten de aanwezigheid van een persoon op een bepaald ogenblik op een bepaalde plaats te achterhalen).

Het biometrisch gegeven kan een gevoelig gegeven zijn, bepaalde biometrische gegevens kunnen informatie vrijgeven over de gezondheidstoestand of de raciale herkomst.

Er bestaan eveneens risico's die verbonden zijn aan het gebruik van de biometrie zoals de identiteitsdiefstal. *De identiteitsdiefstal vormt een des te groter risico omdat de doelstelling van de biometrie er net in bestaat een sterkere authenticatie op te leveren (met andere woorden, een sterkere band tussen de gebruiker en zijn identiteit). Bovendien worden de gevolgen van identiteitsdiefstal vaak onderschat en zijn zij moeilijk aan te tonen. Anderzijds kan het gebruik van de biometrie nieuwe fysieke risico's inhouden voor de gebruikers. Zo werd vastgesteld dat bij diefstallen van luxewagens de dieven niet geaarzeld hebben om fysiek geweld te gebruiken om de biometrische veiligheidsmaatregelen waarmee het voertuig was uitgerust te omzeilen.*

Meer in het algemeen wenst de Commissie de aandacht te vestigen op de maatschappelijke keuze die gepaard gaat met een veralgemening van het gebruik van de biometrie. De uitbreiding van biometrische systemen zou een groot risico op desensibilisering van het publiek kunnen meebrengen ten aanzien van het steeds toenemende gebruik van hun gegevens en de gevolgen die deze verwerkingen zouden kunnen hebben op hun dagelijks leven. De Groep 29 onderstreept bijvoorbeeld dat het gebruik van de biometrie in schoolbibliotheken het risico inhoudt dat de kinderen zich minder bewust zullen zijn van de risico's die verbonden zijn aan de gegevensbescherming en de gevolgen die dit kan hebben voor hun latere leven.

De commissie eindigt in haar advies met te stellen dat ze principieel de optie van een biometrische systeem proportioneel acht, op voorwaarde dat de verantwoordelijke voor de verwerking *i.* geconfronteerd wordt met een situatie waar de verwerking van persoonsgegevens *noodzakelijk of proportioneel* is, *ii.* er gebruik wordt gemaakt van een biometrisch systeem dat betrekking heeft op fysieke kenmerken die geen sporen nalaten (bijvoorbeeld het Privium systeem van Schiphol, waarbij eens de gegevens zijn ingelezen en

geverifieerd, de gevoelige biometrische gegevens zoals een irisscan onmiddellijk worden verwijderd van de apparatuur) en *iii.* een hele waslijst aan door de Commissie opgemaakte aanbevelingen naleeft. Het mag duidelijk wezen: de CBPL (Commissie voor de bescherming van de persoonlijke levenssfeer) heeft het niet onmiddellijk begrepen op biometrische herkenning. En misschien wel terecht.

Ook in de rechtsleer[121] komt men bezorgde kritieken tegen. Voornamelijk het gebruik van biometrie inzake nieuwe 'identificatietechnologie', met centrale opslag van deze biometrische gegevens, houdt een bijzonder risico in op het fundamenteel recht op het privéleven. Aanpassingen aan de Wet Verwerking Persoonsgegevens en een bijhorende expliciete wettelijke regeling van biometrie dringen zich dan ook op.

Nochtans wordt identiteitsdiefstal een stuk moeilijker, zeker online. Als gebruikers op hun bank gaan inloggen met hun vingerafdruk, de identiteit in chatrooms wordt vastgesteld aan de hand van een irisscan, sociale netwerken gebruik maken van biometrie om de gegevens te controleren en vriendschapsverzoeken te verifiëren ziet de wereld er op slag een stuk veiliger uit.

Alhoewel, er zal nog steeds een nood zijn aan databases om de ingevoerde gegevens te vergelijken. De vraag rest dan: wie zal deze databanken creëren, onderhouden en bewaken? En wat met iemands privacy? Hoever mag men gaan in het eisen van biometrisch materiaal ter verificatie? Mag een bank haar cliënten verplichten bij het openen van een rekening om een vingerafdruk of irisscan af te geven?

Het valt te verwachten dat het antwoord op bovenstaande vragen in grote mate de toekomst van (online) beveiliging en privacy zal beïnvloeden.

HOOFDSTUK 4: ANTI ID-THEFT SOFTWARE

Samen met de verhoogde angst voor identiteitsdiefstal groeit het softwareaanbod dat zich specialiseert in het blokkeren van identiteitsdiefstallen.

[121] E. KINDT EN J. DUMORTIER, "Biometrie als herkenning- of identificatiemiddel? Enkele juridische beschouwingen", Computerr., 2008, 198.

Zo hebben alle grote namen in de antivirus sector reeds voorzien in een *plugin* of apart stukje software dat zich specifiek toespitst op identiteitsdiefstal. McAfee bracht in 2007 een whitepaper [122] uit omtrent identity theft. Hoewel uiteraard mede geïnspireerd door commerciële doeleinden, concludeert de auteur:

We must first admit that every one of us — individuals and businesses — are threatened and potentially vulnerable to identity theft; this is not something that happens only to others. Despite the seriousness of current incidents and the increasing threat, some basic principles allow us to significantly reduce the risk. Awareness is the best defense. Through awareness, we develop our senses to spot identity theft and to protect personal and corporate information, while maintaining the benefits of information technology."

Het document bevat bovendien een groot aantal praktische tips, en is daarom voor elke internetgebruiker een aanrader. Op basis van deze whitepaper ontwikkelde McAfee in haar bestaande virussoftware een nieuw component "*identity protection".* [123]

Ook Norton (Symantec)[124] speelt uitdrukkelijk in op identiteitsbescherming. Haar software claimt gebruikers te beschermen tegen hackers en phishing aanvallen, verifieert websites op hun authenticiteit en biedt een 'Identity Safe' als opslagplaats voor de aanmeld- en persoonsgegevens van de gebruiker.

Uiteraard dient dergelijke software met de nodige omzichtigheid te worden benaderd. Enerzijds zal software nooit *elke* dreiging kunnen voorkomen, anderzijds zal het vooral nuttig blijken bij massale of onpersoonlijke aanvallen (bijvoorbeeld: een massa phishing e-mail, virussen die keyloggers bevatten, etc.). Voor de meer persoonlijke aanval, zoals bij identiteitsdiefstal van specifieke personen is het nut betwijfelbaar. Hier geldt nog altijd het eerste principe: *awareness* of bewustwording is de beste oplossing.

---

[122] F. PAGET, *Identity Theft: White Paper,* Santa Clara, McAfee, 2006, (te consulteren via http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf).
[123] http://www.mcafee.com/us/security_wordbook/identity_theft.html
[124] http://www.symantec.com/nl/be/norton/products/charts/comparison.jsp?pcid=ts

HOOFDSTUK 5: KWETSBAARHEID

De voorgaande alinea brengt ons naadloos tot de conclusie van deel 3. Hoeveel inventieve oplossingen er ook moge gevonden worden, in de vorm van encryptie, biometrie, mobiele authentificatie enzovoort, de kwetsbaarheid van elk systeem zal uiteindelijk bij de persoon zelf liggen. Denken dat software of nieuwe technologie deze kwetsbaarheid volledig kan uitsluiten, is niet meer dan een illusie.

Zelfs indien men er in slaagt quasi onfeilbare technische beschermingsmaatregelen in te voeren, blijft de zwakste schakel in het gehele identiteitsproces nog steeds de argeloze gebruiker die, bij gebrek aan voldoende publieke sensibilisering, nog al te vaak onwetend op allerhande e-mails en verdachte boodschappen en aanbiedingen ingaat. Of zoals Bruce Schneier in de Wall Street Journal besluit:

"Finally, any good authentication system uses defense in depth. Since no authentication system is perfect, there need to be other security measures in place if authentication fails. That's why all of a corporation's assets and information isn't available to anyone who can bluff his way into the corporate offices. That is why credit card companies have expert systems analyzing suspicious spending patterns. And it's why identity theft won't be solved by making personal information harder to steal. We can reduce the risk of impersonation, but it will always be with us; technology cannot "solve" it in any absolute sense. Like any security, the trick is to balance the trade-offs."[125]

Dat België, en zelfs de meeste lidstaten van Europa, hierin nog een lange weg af te leggen maken de ontwikkelingen in het V.K. meer dan duidelijk.

Het Verenigd Koninkrijk, één van de toplanden (naast de U.S. en Australië) die geplaagd worden door identity theft, besloot met steun van onder andere CIFAS, Home Office en Financial Fraud UK een publieke campagne of poten te zetten die het bewustzijn rond identity theft moest vergroten. Er werd voorzien in flyers, omvangrijke folders, spots in de media, en een informatie website.[126] De website maakt een onderscheid tussen het '*public*'

[125] B. SCHNEIER, "Why Technology Won't Prevent Identity Theft", *Wall Street Journal,* 2009, (te consulteren via http://online.wsj.com/article/SB123125633551557469.html).
[126] http://www.identitytheft.org.uk/

gedeelte en het *'business'* gedeelte. Dat laatste is niet toegankelijk zonder registratie en is specifiek opgericht om bedrijven te helpen het risico van ID-theft te verminderen.

Dergelijke initiatieven in België blijven – voorlopig – uit. Nochtans kan dergelijke campagne bijzonder kostenefficiënt gebeuren, de financiële implicaties van een website of online brochures zijn immers verwaarloosbaar. De dreiging van identiteitsdiefstal wordt steeds drukkender, en de tijd voor sensibilisering is *nu*.

DEEL 4: CIJFERS & KOSTEN VOOR DE OVERHEID, BEDRIJVEN EN PARTICULIEREN

HOOFDSTUK 1: RISICOGROEP IDENTITEITSDIEFSTAL

Het is altijd interessant om te weten welke groep in de bevolking het kwetsbaarst is voor een bepaald misdrijf of crimineel fenomeen. Bij identity theft is dat niet anders. Zoals hierboven omstandig omschreven levert de opkomst van zoekmachines, sociale netwerksites en ander technologische *hypes* een schat van informatie op voor de identiteitsdief. Het mag dan ook niet verwonderen dat onderzoekers vaststelden dat de risicogroep vooral bestaat uit jongeren tussen de 18 en 24 jaar.

Dat maakte The Washington Post bekend op 17 maart 2010.[127] Dit resultaat blijkt uit een betrouwbare en recente publicatie[128], uitgebracht door 'Javelin Strategy & Research'[129], welk al 7 jaar op rij een diepgaand onderzoek voert in de V.S. omtrent identity theft. Dit onderzoek gebeurde in samenwerking met Fiserv Inc., Wells Fargo & Company en ITAC, de 'Identity Theft Assistance Center'.

"*Millenials* (18 tot 24 jarigen) *don't protect enough or detect enough*" concludeerde James Van Dyke, CEO van Javelin. *"The 18-to-24 group is unique. They're going to college. They're away from home for the first time. They're sharing more information. More of their information is exposed. The old stereotype is true that people are sharing information willy-nilly and are waiting until they become a victim to listen to sound advice."*

The Post besloot nog: *"It's an interesting balance they have to strike in deciding how much to share in order to initiate or maintain a relationship but not overshare with their network."*

Hoewel bovenstaande een bijna logisch gevolg is van de grote informatisering van onze maatschappij, kan men toch enigszins een kritisch geluid laten horen bij bovenstaande

[127] A. KLEIN, "18- to 24-year-olds most at risk for ID theft, survey finds", *The Washington Post*, 2010, (te consulteren via http://www.washingtonpost.com/wp-dyn/content/article/2010/03/16/AR2010031604209.html).
[128] X., "Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back", *Javelin Strategy & Research,* 2010, (te consulteren via https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail).
[129] https://www.javelinstrategy.com/

conclusie. Jongeren zullen zonder discussie geneigd zijn sneller te participeren in nieuwe online trends die hun privacy en gevoelige gegevens in een onmiddellijk gevaar kunnen brengen. Evenwel moet men zich de vraag stellen of identiteitsdieven (die in de grote meerderheid gericht zijn op financiële identity theft) wel hun slag kunnen thuishalen bij bovengenoemd 'doelpubliek'.

Het immers niet ondenkbaar dat jongeren vaak over onvoldoende interessante gegevens beschikken. Zo zullen ze bijvoorbeeld niet beschikken over kredietkaarten of gigantische bedragen op hun bankrekeningen. Voor de pure identiteitsdiefstal, gericht op het aannemen van andermans identiteit, levert deze evolutie uiteraard wel een voordeel op voor identiteitsdieven. Of het ook noemenswaardige financiële belangen vertegenwoordigt valt toch enigszins te betwijfelen.

HOOFDSTUK 2: CIJFERS IN DE V.S.

Hiervoor grijpen we eveneens terug naar de Javelin-studie.[130]

Volgens de 'Javelin Strategy & Research" waren er in 2009 alleen al naar schatting 11,1 miljoen slachtoffers van identity theft in de V.S., 12% meer dan het jaar daarvoor. De dieven stalen in totaal een goede 54 miljard dollar. Identiteitsdieven stelen ongeveer 4.811 dollar per slachtoffer, maar de eindkost voor elk slachtoffer bedraagt, dankzij de '*money back*' toegeving bij de Amerikaanse banken, 'slechts' 373 dollar. De slachtoffers spenderen ongeveer 21 uur aan het oplossen van hun zaak en om hun geld terug te krijgen.

De studie had een bijzondere aandacht voor sociale netwerksites zoals Facebook en MySpace en besloot dat hoewel jongeren bedenkelijk zwaarder gecompromitteerd werden door het beschikbare (identiteits-)materiaal, de websites slechts voor een klein percentage verantwoordelijk zijn. Hoewel: 55% geeft aan nooit te weten zijn gekomen hoe hun identiteit werd gestolen. Het bovenstaande cijfer in verband met sociale netwerksites moet m.i. dan ook genuanceerd worden.

[130] X., "Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back", *Javelin Strategy & Research,* 2010, (te consulteren via https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail).

Hoewel deze cijfers bijzonder alarmerend zijn is er ook een positieve noot te bespeuren. De '*awareness campaigns'* beginnen langzamerhand hun vruchten af te werpen, nu blijkt dat de dataprotectie en andere voorzorgen garant staan voor een daling van 30% in de tijd die men nodig heeft om een identiteitsdiefstal of –fraude op te lossen. De gemiddelde duur bedraagt, zoals hierboven reeds gesteld, nu 21 uur. Bovendien doet de helft van de slachtoffers nu aangifte bij de politie, wat resulteert in een verdubbeling van de arrestaties, een verdriedubbeling van het aantal vervolgingen, en een verdubbeling van het aantal veroordelingen in 2009.

Niettemin is er weinig reden tot juichen. De cijfers zijn immers de hoogste ooit genoteerd sinds 2003, het enige goede nieuws is dat consumenten en bedrijven agressiever worden in het monitoren, detecteren en het voorkomen van identiteitsdiefstal, en dit met hulp van nieuwe technologieën, overheidsinstanties en andere private diensten.

Enkele critici merken op dat de cijfers in de V.S. niet relevant zouden zijn voor Europa. Immers, in de V.S. wordt gebruik gemaakt van het uiterst onveilige '*social security number'* (zie *infra*). Het volledig uitsluiten of veranderen ervan is onmogelijk, gezien het nummer een brede verspreiding kent onder overheidsdiensten en private bedrijven. Men is zich anderzijds terdege bewust van het hoge risico dat dit nummer met zich meebrengt, en men tracht bijgevolg het effectieve gebruik ervan zo laag mogelijk te houden.

Zo maken bijvoorbeeld financiële instellingen ondertussen geen gewag meer van het nummer in de gebruikers- of klantenfiche, en monitoren ze daarenboven meer proactief op identiteitsfraude en –diefstal. Identiteitsdieven maken echter steeds beter en op een meer intelligente en efficiënte manier gebruik van de beschikbare technologieën, zo merkt Javelin op. Enkele van hun meest kenmerkende bevindingen:

- Er is een stijging in het zogenaamde '*new account fraud*', welk resulteert in het openen van bankrekeningen met behulp van gestolen identiteitsinformatie. Er werd een stijging genoteerd van 6% tegenover 2008, zodat deze vorm nu 39% uitmaakt van alle gerapporteerde gevallen van identity theft.
- Bij data-inbreuken is het stelen van de volledige naam goed voor 63%, de adresgegevens voor 37%, en, met een stijging van 4%, het stelen van gezondheids- en verzekeringsgegevens. Het percentage van gestolen 'social security numbers' nam

dan weer af van 38% naar 32% (welk een teken aan de wand is dat bovengenoemde nummers minder aantrekkelijk worden voor identiteitsdieven gezien hun verminderde effectieve waarde).

- 75% van alle kaartfraude kwam van kredietkaarten, een stijging van 12% sinds 2008.
- Proactieve consumenten vormen blijkbaar een gevaarlijke dreiging voor identiteitsdieven. De helft van de slachtoffers die een identiteitsdiefstal rapporteerden zagen een effectieve arrestatie of veroordeling van de dader tegemoet.
- 18 tot 24 jarigen, de zogenaamde *millennials*, zijn het traagst in het ontdekken van identiteitsdiefstal. Het neemt hen gemiddeld tot twee keer meer tijd in beslag om de fraude te ontdekken. Bij een eventuele aanvaring met identity theft, zijn *millennials* wel snel geneigd maatregelen te nemen (informatie opvragen, software te installeren, …) en dit in tegenstelling tot de andere groepen.
- Zaakvoerders van KMO's lopen een bijzonder hoog risico. Zo blijkt uit het onderzoek dat deze personen 1,5 keer meer kans maken het slachtoffer te worden van identiteitsdiefstal. Als verklaring werd gewezen op het feit dat zaakvoerders of ondernemers vaak ook persoonlijke accounts of rekeningen gebruiken bij zakelijke transacties en zij daarenboven meer financiële transacties verrichten dan niet-zelfstandigen.

Een woord van waarschuwing wordt ook gericht naar de nieuw opgekomen technologieën. Zo bieden banken aan om rekeningen automatisch te monitoren op verdachte en ongewone transacties, en is er een duidelijke opkomst in anti-malware en antivirus programma's om specifiek te letten op identity theft. Consumenten, met dank aan de veelvuldige en continue bewustwordingscampagnes, nemen '*best practices*' of richtlijnen over om hun persoonlijke informatie veilig te stellen, controleren regelmatig hun rekeningen, behandelen e-mails en andere elektronische berichten een stuk kritischer, en investeren zelfs in smartphones om hun data ten allen tijde te kunnen consulteren en controleren.

Millennials zijn koploper om de nieuwe technologieën te gaan implementeren, doch meestal pas na er zich een incident heeft voorgedaan. De meest genomen actie is het installeren van anti-malware of ant-virus software.

Deze evolutie kent ook een keerzijde. Dergelijke software creëert in bepaalde gevallen een vals gevoel van veiligheid. Zoals boven reeds gesteld levert dergelijke software uiteraard bepaalde voordelen op, en zeker in geval van massa-aanvallen of *mass-mailings* die phishing op het oog hebben.

Wanneer de aanval echter persoonlijk wordt, kent dergelijke software vaak haar limieten. Niet verwonderlijk, aangezien social engineering (*supra*) zich niet laat leiden door softwarematige beveiligingen. Integendeel, het zorgt voor een vals gevoel van veiligheid waardoor men minder oplettend wordt. Nochtans is deze continue alertheid juist de sleutel tot een effectieve identity theft bestrijding.

Enkele – voor de hand liggende – zaken die worden aangeraden in het onderzoek is het regelmatig veranderen van paswoorden, geen account- of paswoordinformatie doorgeven aan derden, vergrendelen van computers en gevoelige informatie, gebruikmaken van een papierversnipperaar, up-to-date houden van anti-virus programma's, en de nodige discretie behouden bij het delen van informatie op e-commerce websites of platformen.

HOOFDSTUK 3: CIJFERS IN HET V.K.

Een andere koploper wanneer het gaat over identity theft, is het Verenigd Koninkrijk.

Identity theft zou het V.K. jaarlijks een slordige 1,7 miljard pond kosten, zo berekende de Home Office Minister Andy Burnham[131] in 2006. De eerste cijfers rond identity theft in de V.K. werden gepubliceerd door het Cabinet Office in 'Identity Fraud: A Study' in 2002. Zij kwamen uit op 1,3 miljard pond.

De overheid maakte echter al snel duidelijk dat het cijfer van 1,7 miljard pond niet enorm betrouwbaar kon worden genoemd[132], aangezien het door middel van een gecontesteerde methode werd berekend. Cijfers voor de volgende jaren zouden dan ook officieel gecontroleerd worden door het nieuw opgerichte IFSC. De 'Identity Fraud Steering Committee (IFSC) werd opgericht in 2003 door het Home Office om zowel met publieke en

[131] X., "ID theft 'costs UK £1.7bn a year", *BBC* News, 2006, (te consulteren via http://news.bbc.co.uk/2/hi/uk_news/politics/4672622.stm).
[132] M. MCGUIRE, *Hypercrime – The New Geometry of Harm,* GlassHouse, Oxford, 2007, 163.

private partners de mogelijkheid af te wegen om kostefficiënte beveiligingsmechanismen te ontwikkelen tegen identity theft.

De nieuwe methode om de kost te meten gaat niet enkel meer uit van het loutere financiële verlies van een organisatie of particulier, maar rekent ook de kost van de reactie aan, namelijk de investeringen gedaan om systemen te ontwikkelen die gevallen van identity theft opsporen, herkennen en vervolgen.

Deze cijfers bewijzen vanzelfsprekend een stijging in het aantal gevallen, alsook in de kosten. Het is echter te danken aan de vele bewustwordingscampagnes (*supra*) dat deze cijfers nog niet veel hoger liggen. Hoewel de cijfers in andere Europese landen, door de verschillende identiteitsmethodes geen vergelijk kennen, kan men niettemin het een en ander leren van deze aanpak.

HOOFDSTUK 4: CIJFERS IN BELGIË.

Het mag duidelijk wezen dat het in België nog zo geen vaart loopt als in de V.S. en het V.K. Niettemin wijzen bepaalde cijfers overduidelijk op een groeiend aantal informaticagerelateerde misdrijven. De *Politiële Criminaliteitsstatistieken*[133] (3de kwartaal van 2009) tonen het volgende aan:

- Het totaal aantal (gerapporteerde) gevallen[134] van informaticacriminaliteit steeg van 4 gevallen in 2000 naar ruim 9.188 in 2008. Reeds in het derde kwartaal van 2009 werd een voorlopig totaal opgemaakt van 8.190 gevallen.
- *Hacking* steeg van 3 gevallen in 2001 naar 510 in 2008 (voorlopig totaal 2009: 453).
- *Valsheid in informatica* (zie ook *infra)* steeg van 1 geval in 2001 naar 423 in 2008 (voorlopig totaal 2009: 267)
- *Informaticabedrog* (zie ook *infra*) steeg van 3 gevallen in 2000 naar maar liefst 8.189 gevallen in 2008 (voorlopig totaal 2009: 7.415).
- Sabotage steeg dan weer van 1 geval in 2005 naar 49 in 2008 (voorlopig totaal 2009: 49).

[133] Federale Politie, *Politiële Criminaliteitsstatistieken,* 2000 – Kwartaal 3 2009, (te consulteren via http://www.polfed-fedpol.be/crim/crim_statistieken/2009_trim3/pdf/nationaal/rapport_2009_trim3_nat_Belgie_nl.pdf).
[134] Deze impliceren zowel voltrokken misdrijven als pogingen.

Meer specifiek zijn de cijfers van de FCCU (2008).[135] Zij verdelen de door hen onderzochte meldingen, die effectief hebben geleid tot de vaststelling van een misdrijf of tot relevante informatie over een misdrijf, in klassen. De meest relevante klassen zijn de volgende:

- *ICT crime:* in 2007 werden 348 gevallen genoteerd, in 2008 waren dat er al 616.
- *Oplichting – internetfraude*: in 2007 goed voor 4.706 gevallen, in 2008 werd een daling vastgesteld naar 2.593 gevallen.
- *Oplichting – Afrikaanse oplichting:* in 2007 goed voor maar liefst 8.780 gevallen Een significante daling in 2008: 3.635 gevallen.
- *Oplichting – phishing*: van 1.262 gevallen in 2007 naar 493.

Het totaal aantal effectieve meldingen daalde van 17.089 in 2007 naar 8.953 in 2008. Buiten *ICT crime* (welke voornamelijk het hacken van een webmailaccount betreft), zien we dus, althans voor de voor ons relevante klassen, een significante daling. Dit is zonder meer toe te schrijven aan het nieuwe eCops-systeem, dat haar nut reeds meer dan eens bewees. Stijgingen vallen dan weer te noteren bij aanzet tot ontucht bij minderjarigen, geweld of bedreigingen tegen personen en meldingen van racisme.

Enigszins vreemd is de contradictie tussen de stijgende cijfers van de politiële criminaliteitsstatistieken en de cijfers in dalende lijn afkomstig van het FFCU. Opgemerkt dient te worden dat de cijfers van politiële criminaliteitsstatistieken elke melding opnemen, ongeacht of het over een voltrokken misdrijf gaat dan wel een poging daartoe, zelfs als deze feiten niet nader onderzocht worden of leiden tot vaststelling van een misdrijf. De cijfers van de FCCU, zoals hierboven reeds uitdrukkelijk gesteld, hebben enkel betrekking op meldingen die geleid hebben tot de vaststelling van een misdrijf (ook tot belangrijke informatie).

[135] Federale Gerechtelijke Politie, Directie economische en financiële criminaliteit, *Jaarverslag 2008,* http://www.polfed-fedpol.be/pub/rapport_activites/pdf/2008_ecofin_nl.pdf.

DEEL 5: HET RECHT, EEN VERGELIJKING.

HOOFDSTUK 1: VERENIGDE STATEN

AFDELING 1: FEDERAL IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT

Het is niet geheel onlogisch eerst de wetgeving van het land te onderzoeken dat ongetwijfeld het meest geplaagd wordt door het fenomeen van identiteitsdiefstal.

Gezien de indrukwekkende cijfers mag het dan ook niet verwonderen dat de V.S. reeds in 1998 stappen ondernam, en identity theft uitdrukkelijk strafbaar stelde via de '*Federal Identity Theft and Assumption Deterrence Act'.*

Hierin wordt volgende definitie van identity theft gehanteerd: "*knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law"*.[136]

In de act zijn straffen opgenomen tot 15 jaar gevangenis en met een maximum geldboete van $250.000. Veel belangrijker is het feit dat de Act letterlijk en zeer uitdrukkelijk stelt dat diegene die zijn of haar identiteit is gestolen behandeld dient te worden als een *slachtoffer*.[137]

Daarvoor was die (bedenkelijke) eer enkel weggelegd voor diegenen die effectief financieel verlies leden.[138] Door deze wijziging konden de CIA, de FBI en andere diensten de misdaad effectief juridisch opsporen en vervolgen. Het creëerde bovendien het recht in hoofde van het slachtoffer om restitutie te bekomen ingeval van een veroordeling.

[136] 18. U.S.C. 1028, Pub. Law 105-138, 112 Stat. 3007
[137] R. BEST, W. MANZ, *Federal identity theft law: major enactments of the 108th Congress : a legislative history of the Fair and Accurate Credit Transactions Act and Identity Theft Penalty Enhancement Act, Volume 9*, Hein, U.S., 2005.
[138] http://www.ckfraud.org/title_18.html

AFDELING 2: STATE VS. LEYDA

Een interessante zaak op het niveau van de *Washington Supreme Court* betreft *State vs. Leyda*[139]*,* welke handelt over de terminologie in de strafbaarstelling.

Leyda en een vriend bemachtigden in 2002 een kredietkaart, toebehorend aan een zekere Cynthia Austin. Leyda gebruikte de kaart een eerste maal op 21 oktober 2002, om goederen aan te kopen in een *Bon Marce* winkel. Vijf dagen later gebruikte hij de kaart opnieuw voor *twee* nieuwe aankopen in dezelfde winkel. Uiteindelijk, op 2 november, wou Leyda opnieuw de kaart gebruiken, maar werd deze keer aan een ondervraging onderworpen door het personeel, dat een vermoeden koesterde dat de kaart gestolen was. In paniek vluchtte Leyda de winkel uit, maar kon nog net worden ingerekend door de politie.

Aan Leyda werd, vanzelfsprekend, identity theft ten laste gelegd, en dat, opmerkelijk genoeg, maar liefst *viermaal* (voor elk feit apart). Hij werd veroordeeld op alle gronden, ging vervolgens in beroep (Court of Appeals), welke de veroordeling bevestigde. Uiteindelijk was het de *Washington Supreme Court* in 2006 dat zich diende uit te spreken over de geldigheid van de veroordeling.

Leyda argumenteerde dat hij onmogelijk veroordeeld kon worden op grond van identiteitsdiefstal, gezien de *definiëring* van het misdrijf in de *Identity Theft Statute.* Het artikel stipuleert immers: "*no person may knowingly obtain, possess, use, or transfer a means of identification or financial information of another person, living or dead, with the intent to commit, or to aid or abet, any crime"*.

Leyda betwistte de toepassing van dit artikel op zijn concrete situatie, gezien volgens hem de strafbaarstelling diende te draaien rond het onrechtmatig in bezit krijgen van de kredietkaart (*obtain*), veeleer dan elke keer voor het gebruik ervan (hij werd immers vier keer het misdrijf van identity theft aangewreven, gebaseerd op zijn vier inbreuken). De aanklacht die viermaal identity theft omvatte, was volgens hem dan ook een schending van het *double jeopardy* (ne bis in idem) beginsel. De Staat argumenteerde dat het artikel weldegelijk het woord "use" in

[139] STATE V. LEYDA, STATE of Washington, Respondent, v. Steven Edward LEYDA, Petitioner, No. 75866-2, 2006. (te consulteren via http://caselaw.findlaw.com/wa-supreme-court/1220663.html).

zijn definiëring bevat, en dat de wetgeving voorzag dat *elke keer* een gestolen kredietkaart werd *gebruikt,* er een *apart strafbaar* en *vervolgbaar* feit uit voortvloeide.

De *Washington Supreme Court* volgde Leyda. In haar antwoord naar de Staat viel te lezen dat het woord "use" in de wetgeving één van de vormen is waarop een identiteit kan worden gestolen, maar eens éénmaal aan een bepaalde vorm voldaan, is het misdrijf gepleegd. Met andere woorden: of men nu eenmaal of viermaal onrechtmatig gebruik maakt van een kredietkaart of andere, het misdrijf *identity theft* kan maar eenmaal gevorderd worden. Het resultaat was dat Leyda, hoewel hij tot vier keer toe de kredietkaart heeft gebruikt, maar eenmaal aangeklaagd kon worden. Immers, hij had ze slechts eenmaal *gestolen*. Het Hof merkte terloops nog op dat mocht Leyda meerdere identiteitsstukken gestolen hebben van Austin (bijvoorbeeld naast een kredietkaart, ook haar identiteitskaart), hij wel apart aangeklaagd kon worden voor beide feiten afzonderlijk.

Er kwam niettemin een sterke *dissenting opinion*. De twee tegenstanders argumenteerden dat het woord "use" weldegelijk moest worden geïnterpreteerd volgens de redenering van de Staat[140], in tegenstelling tot wat de meerderheid besloot.

AFDELING 3: FLORES-FIGUEROA V. UNITED STATES

In een andere ophefmakende zaak[141], die recent werd beslecht door de *Supreme Court*, was de uitermate belangrijke vraag aan de orde of de aanklager bij identity theft moest bewijzen dat de beklaagde *wetens en willens* (en dus met volle kennis van zaken) op de hoogte was dat hij een valse identiteit bezat of gebruikte. Het betrof met andere woorden een vraag naar *interpretatie* van het wetsartikel dat identity theft strafbaar stelt.

Het antwoord op bovengenoemde vraag kent vanzelfsprekend verstrekkende gevolgen. De feiten gaan als volgt.

Ignacio Flores-Figueroa werd in eerste aanleg veroordeeld wegens identity theft, en bestraft met vijfenzeventig maanden gevangenisstraf. Hij fulmineerde - in graad van beroep - dat de

[140] J. GARDNER, T. M. ANDERSON, *Criminal Law*, U.S., 2006, 368.
[141] IGNACIO CARLOS FLORES-FIGUEROA, Petitioner v. UNITED STATES, No. 08-108, 2009, (te consulteren via http://www.lexisone.com/lx1/caselaw/freecaselaw?action=FCLRetrieveCaseDetail&caseID=1&format=FULL&resultHandle=0db4f3d00e65c7a64f23ea5ff7cba8c2&pageLimit=10&xmlgTotalCount=4&combinedSearchTerm=%22Identity+theft%22&juriName=U.%20S.%20Supreme%20Court&sourceFile=GENFED;USLED).

veroordeling onrechtmatig was. Immers, zo argumenteerde hij, de aanklager had niet bewezen dat hij *kennis had* van de valse identiteit of dat hij *bewust en wetens en willens* de valse identiteit had aangenomen en misbruikt.

De *United States Court of Appeals for the Eight Circuit* had hier echter weinig oren naar en bevestigde de veroordeling. Ze besliste dat de aanklager niet noodzakelijk moest bewijzen dat Flores-Figueroa *wist* dat de identiteit die hij gebruikte aan een ander toebehoorde.

Ignacio Flores-Figueroa wist echter van geen ophouden. Hij deed een aanvraag bij het *U.S. Supreme Court* om zijn zaak te behandelen. De aanvraag werd goedgekeurd.

Uiteindelijk, op 4 mei 2009, nam de U.S. Supreme Court haar omstreden beslissing. Zo werd geoordeeld dat de aanklager weldegelijk moest bewijzen dat de identiteit *wetens en willens* werd misbruikt door de beklaagde. Immers, zo valt in het bewuste artikel te lezen, "*no person may **knowingly** obtain, possess, use, or transfer a means of identification or financial information of another person, living or dead, with the intent to commit, or to aid or abet, any crime"*. De meerderheid bij de *Supreme Court* vond dat bij een normale tekstuele lezing van het artikel, men niet anders kan besluiten dan dat '*knowingly*' slaat op het *wetens en willens* en dat zij aldus als een *voorwaarde* moet worden aanzien wil men het artikel kunnen toepassen.

Het Hof besloot, onder andere, het volgende: *"There are strong textual reasons for rejecting the Government's position. As a matter of ordinary English grammar, it seems natural to read the statute's word "knowingly" as applying to all the subsequently listed elements of the crime. The Government cannot easily claim that the word "knowingly" applies only to the statutes first four words, or even its first seven. It makes little sense to read the provision's language as heavily penalizing a person who "transfers, possesses, or uses, without lawful authority" a something, but does not know, at the very least, that the "something" (perhaps inside a box) is a "means of identification." Would we apply a statute that makes it unlawful "knowingly to possess drugs" to a person who steals a passenger's bag without knowing that the bag has drugs inside?"*.

AFDELING 4: FAIR AND ACCURATE CREDIT TRANSACTIONS ACT EN THE IDENTITY THEFT PENALTY ENHANCEMENT

Wat wetgeving betrof, bleef het trouwens niet bij de Identity Theft Act van 1998.

In 2003 werd er een nieuwe wet gestemd, de *Fair and Accurate Credit Transactions Act*. Deze kende slachtoffers van Identity Theft bepaalde rechten toe in hun relatie met schuldeisers, om sneller en effectiever negatieve informatie van hun kredietrapporten te laten verwijderen.

In 2004 uiteindelijk, zag de *Identity Theft Penalty Enhancement* het licht, welke een aanmerkelijke verzwaring van de straffen inhield, althans in bepaalde situaties (bijvoorbeeld: wanneer men zich bevindt in een arbeidsrelatie, of bij terrorisme of immigratie).[142]

AFDELING 5: USA V. GONZALEZ

Eén van de grootste zaken, zoniet dé grootste, omtrent identity theft in de V.S. betreft *USA v. Gonzalez*.

De 28-jarige Albert Gonzalez, eerder werkzaam als *federal informant,* bekende in 2009 dat hij de leiding had over een internationaal netwerk dat maar liefst 40 *miljoen* krediet- en bankkaartgegevens kon bemachtigen, afkomstig van verschillende grote Amerikaanse bedrijven.[143] Het was het grootste fraudenetwerk ooit gerapporteerd in de Verenigde Staten, en de bekendmaking ervan zorgde dan ook voor de nodige beroering.

Albert Gonzalez pleitte schuldig in de *federal court* van Boston, en bekende dat hij gebruik had gemaakt van lekken in de beveiliging van de verschillende computer- en databanksystemen om zo toegang te verkrijgen tot de kaartnummers.

Gonzalez werd op 25 maart 2010 veroordeeld tot 20 jaar gevangenisstraf.

AFDELING 6: FEDERAL TRADE COMMISSION

De Federal Trade Commission werd aangesteld als centrale autoriteit en fungeert als een verzamelpunt voor klachten (deze dienen namelijk zowel aan de lokale autoriteiten als aan

[142] R.L. MILLER, G.A. JENTZ, *Fundamentals of Business Law – Summarized Cases*, U.S., 2010, 143.
[143] U.S. v. GONZALEZ, U.S. District Court, District of Massachusetts, No. 1:08-cr-10223.

de FTC[144] te worden doorgegeven). Maar de FTC doet meer.[145] Zij initieert immers ook rechtszaken omtrent identiteitsdiefstal, en zo ook tegen bedrijven die niet voldoende veiligheidsmaatregelen nemen of de data van hun klanten te beveiligen. Een van de meest bekende zaken in deze betreft de *ChoicePoint*-case.[146] In 2006 gaf een *consumer data broker*, ChoicePoint Inc. aan dat haar database, die gegevens van maar liefst 163.000 klanten bevatte, gecompromitteerd was. De FTC spande vervolgens een federale rechtszaak aan en argumenteerde dat ChoicePoint de *Fair Credit Reporting Act* overtrad door confidentiële informatie (krediethistoriek van klanten) vrij te geven aan instellingen die hiervoor geen legitiem doel aangaven. Daarenboven beging ChoicePoint een schending op de *FTC Act* door valse verklaringen af te leggen omtrent haar privacy policies. Het geschil eindigde uiteindelijk in een schikking van 15 miljoen dollar, mét de belofte om nieuwe procedures te implementeren omtrent de vrijgave van belangrijke informatie- en identiteitsgegevens.

AFDELING 7: WETGEVING STATEN

Naast de eerder genoemde wetgeving op federaal niveau, voorzagen zowat alle Staten eveneens in aparte wetgeving.[147] Sommige daarvan zijn bijzonder specifiek. Zo omschrijft, bij wijze van voorbeeld, de wet "*Financial Identity Theft law*" in Illinois[148] het misdrijf van (financiële) identiteitsdiefstal als volgt: "*a person commits the offense of financial identity theft when he or she knowingly uses any personal identifying information or personal identification document of another person to fraudulently obtain credit, money, goods, services or other property in the name of the other person".*

Het wetsartikel bepaalt bovendien dat wanneer de identiteitsdiefstal wordt gepleegd op personen ouder dan zestig jaar of een mindervalide persoon, er zwaardere straffen van toepassing worden.

Nevada[149] splitst het misdrijf van identity theft dan weer op in twee delen: enerzijds bestaan er regels voor het *bemachtigen* of *verkrijgen* van documenten die aan anderen toebehoren

[144] A. SCHWABACH, *The Law – Technology, Society and Compromises,* U.S., 2006, 140.
[145] ABA SECTION OF ANTITRUST LAW, *Antitrust Law Developments*, 6th edition, ABA Publishing, U.S., 2007.
[146] ChoicePoint, No. I-06-CV-0198 (N.D. Ga. Jan. 26, 2006).
[147] J. BEVERLEY, *Protect your digital privacy – Survival skills for the Information Age,* U.S., 2002, 377.
[148] 720 ILCS 5/16G
[149] Nev. Rev. State § 205.465

en anderzijds voor het *bezitten, doorgeven of doorverkopen* van documenten of informatie die iemands identiteitsgegevens bevat, welke kan gebruikt worden voor een financieel voordeel.

Florida[150] volgt nog een andere denkpiste. Zij beschouwt het frauduleus bezitten of de *poging daartoe* van identiteitsmateriaal als een *third degree felony* (min of meer vergelijkbaar in ons stelsel met een *misdaad*, daar waar de andere staten identiteitsdiefstal als een *misdemeanor* (wanbedrijf) beschouwen. Daarenboven voegt ze nog een andere strafbaarstelling toe, wanneer een persoon de identiteit van een ander gebruikt zonder zijn of haar toelating of misbruikt om deze laatste schade toe te brengen.

AFDELING 8: IDENTITY THEFT DATA CLEARINGHOUSE

Maar het bleef niet bij de loutere wetgeving. Het opbouwen van een nationaal klachtenbestand is een maatregel dat vrijwel simultaan met de nieuwe Act in de V.S. werd geïnitieerd.[151] Via het zogenaamde Identity Theft Data Clearinghouse wordt al sinds november 1999 informatie verzameld waarmee slachtoffers van identiteitsdiefstal een helpende hand wordt geboden in het zoveel mogelijk beperken van hun materiële en morele schade. Met deze voorziening kan bovendien een waardevol inzicht verkregen worden in de omvang van identiteitsfraude en –diefstal en de verschillende gedaantes en vormen waarin beide zich uiten. Dit Clearinghouse is zoals gezegd een direct gevolg van de expliciete wettelijke erkenning – een jaar daarvoor met de bovengenoemde *Federal Identity Theft and Assumption Act* – van identiteitsdiefstal als een strafrechtelijk delict.

De omvang van identiteitsdiefstal staat in een directe relatie met de kwetsbare kanten van het identificatiemiddel of haar infrastructuur. Preventie dient in de eerste plaats dan ook in te spelen op deze onveiligheden en, waar mogelijk, deze zo snel mogelijk uit de wereld te helpen.

[150] Fla. Stat. Ann. § 817.568
[151] J.E.J., PRINT EN N.S. VAN DER MEULEN, *Identiteitsdiefstal: lessen uit het buitenland*, Justitiële verkenningen, jrg 32, nr. 7, 2006, p. 13

AFDELING 9: SOCIAL SECURITY NUMBER

In de Verenigde Staten realiseerden beleidsmakers zich al snel dat vooral het SSN, het Social Security Number, een bijzonder zwakke schakel was in het gehele identificatieproces.[152] Het SSN kent zijn oorsprong in de *Social Security Act* van 1935. Een bijproduct van deze wet was het instellen van een *uniek nummer* voor elke burger die sociale zekerheidsbonussen genoot of sociale zekerheidstaksen betaalde. De bedoeling was om een nummer te gebruiken als primaire herkenningsbron voor de administratie voor de sociale zekerheid. Het *Social Security Number* zag het levenslicht.

Evenwel bleef het niet bij die enkele maatregel. In 1943, onder het bewind[153] van Roosevelt werd gekozen om de SSN te autoriseren als primaire herkenningsleutel voor overheidsdatabanken. Hoewel deze praktijk werd stopgezet in 1975 (teweeggebracht door de Privacy Act van 1974), was het hek reeds lang van de dam.

The Privacy Act voerde een hele reeks veranderingen in. Ten eerste stelde het bepaalde voorwaarden aan het opvragen en gebruik van het SSN door overheidsdiensten. Zo moesten deze diensten een '*Privacy Act Disclosure Notice'* richten aan de SSN-houders, waarin zij dienden uit te leggen (1) welke legitimatie zij konden voorleggen, (2) wat het beoogde doel was (3) welke eventuele secundair gebruik van de SSN's kon worden gemaakt en (4) wat de gevolgen waren wanneer men deze informatie niet wou onthullen.

Ten tweede werd – in tegenstelling tot de passage hierboven – in een versoepeling voorzien voor federale en lokale overheden. Zo hing de *Disclore Notice* af van het feit of de aanvraag van het SSN verplicht of vrijwillig was. Het is belangrijk om op te merken dat er geen specifieke verbodsbepalingen of straffen bestaan voor het (onrechtmatig) gebruik van de SSN's in het bedrijfsleven.

Ten laatste erkende de *Privacy Act* het rechtmatige gebruik van de SSN's als *primaire herkenningssleutel* voor alle federale instellingen, die dit nummer reeds gebruikten voor 1 januari 1975. Deze laatste passage zorgde er meteen voor dat de principiële stopzetting in 1975 vooral theorie bleef.

---

[152] H. BERGHEL, *Identity Theft, Social Security Numbers, and the Web,* Communications of the ACM, 02/2002 vol. 43 nr. 2

[153] Executive Order 9397

Samenvattend was het *Social Security Number* dus wijdverspreid in gebruik, zowel bij federale als lokale instellingen. Door deze algemene erkenning van het nummer raakten ook private bedrijven en instellingen helemaal in de ban van deze herkenningsleutel. Het had immers alles weg (na ruim veertig jaar) van een betrouwbaar middel om iemands identiteit vast te stellen. Ironisch genoeg was het SSN-nummer nooit bedoeld als algemeen identificatiemiddel, en al helemaal niet voor commerciële exploitatie. Nochtans is het net deze evolutie geweest die het grote probleem en opkomst van identity theft heeft gecreëerd.

De meningen lopen evenwel uiteen. Terwijl sommigen m.i. terecht argumenteren dat het wijdverspreide gebruik van het SSN ervoor zorgt dat een identiteitsdiefstal of privacyinbreuk al te gemakkelijk kan worden voltrokken, zijn er anderen die beweren dat er in de *constitution* of grondwet van de Verenigde Staten zelfs geen melding wordt gemaakt van het begrip *privacy*, en dat het commercieel gebruik van het SSN volledig legaal is zolang dit gebruik de relevante richtlijnen en wetgeving respecteert.

En toch, zelfs de grootste criticasters moeten toegeven dat het SSN aan de grondslag ligt van het identity theft probleem in de V.S. Van alle identiteitsdata die men kan verkrijgen, fungeert de SSN als de *heilige graal*. Immers, met dit primair herkenningsnummer kan men informatie opvragen in zowat alle overheids- en commerciële databanken. En dankzij het internet, is de verkrijging en bijhorend onrechtmatig gebruik van het SSN een fluitje van een cent.

Inmiddels is het uitgangspunt gewijzigd naar (zie ook *supra)* een zo'n restrictief mogelijk gebruik van het SSN nummer bij overheidsorganen en andere private organisaties.

Het zou nochtans veel doeltreffender zijn om een volledige herziening van het SSN-systeem uit te tekenen. Dit bleek praktisch evenwel niet werkbaar, met als voornaamste argument de financiële kost en het feit dat het SSN inmiddels verweven zit in de diepste publieke en private registers.

En nochtans, het had allemaal heel anders kunnen lopen. Had de toenmalige administratie zich gehouden aan het basisidee van het *Social Security Number*, namelijk het louter linken van bepaalde burgers aan sociale voordelen of belastingen, dan was identity theft in de V.S.

naar alle waarschijnlijkheid van een heel andere – en misschien meer Europese – proportie geweest.

AFDELING 10: BEWUSTWORDING

Waar de V.S. ook sterk op inspeelt, net zoals het Verenigd Koninkrijk (*supra*), zijn bewustwordingscampagnes. Zo werd onder andere de *AvoID Theft: Deter, Detect, Defend*[154] campagne op poten gezet, waar een grote hoeveelheid voorlichtingsmateriaal op terecht kwam. Ook werd een 'Identity Theft Task Force' opgericht, nadat toenmalig President Bush hiervoor via nieuwe wetgeving[155] de basis had gelegd. Zo valt in deze Executive Order onder andere te lezen (*eigen onderlinie*):

(…)

Section 1. Policy. It is the policy of the United States to use Federal resources effectively to deter, prevent, detect, investigate, proceed against, and prosecute unlawful use by persons of the information of other persons, including through:

(a) increased aggressive law enforcement designed to prevent, investigate, and prosecute identity theft crimes, recover the proceeds of such crimes, and ensure just and effective punishment of those who perpetrate identity theft;

(b) improved public outreach by the Federal Government to better (i) educate the public about identity theft and protective measures against identity theft, and (ii) address how the private sector can take appropriate steps to protect personal data and educate the public about identity theft; and

(c) increased safeguards that Federal departments agencies, and instrumentalities can implement to better secure government-held personal data.

(…)

Sec. 3. Functions of the Task Force. The Task Force, in implementing the policy set forth in section 1 of this order, shall:

---

[154] http://consumer.gov/idtheft/
[155] Executive Order 13402 – Strengthening Federal Efforts to Protect Against Identity Theft, 2006.

(a) review the activities of executive branch departments, agencies, and instrumentalities relating to the policy set forth in section 1, and building upon these prior activities, prepare and submit in writing to the President within 180 days after the date of this order a coordinated strategic plan to further improve the effectiveness and efficiency of the Federal Government's activities in the areas of identity theft awareness, prevention, detection, and prosecution;

(b) coordinate, as appropriate and subject to section 5(a) of this order, Federal Government efforts related to implementation of the policy set forth in section 1 of this order;

(c) obtain information and advice relating to the policy set forth in section 1 from representatives of State, local, and tribal governments, private sector entities, and individuals, in a manner that seeks their individual advice and does not involve collective judgment or consensus advice and deliberation and without giving any such person a vote or a veto over the activities or advice of the Task Force;

(d) promote enhanced cooperation by Federal departments and agencies with State and local authorities responsible for the prevention, investigation, and prosecution of significant identity theft crimes, including through avoiding unnecessary duplication of effort and expenditure of resources; and

(e) provide advice on the establishment, execution, and efficiency of policies and activities to implement the policy set forth in section 1

(…)

Deze Executive Order, daterend van 15 mei 2006, luidt duidelijk een agressievere aanpak tegen identity theft. Ondanks de erin vervatte krachtige woorden dienen we niettemin vast te stellen dat het misdrijf elk jaar nieuwe recordcijfers haalt.

Zoals reeds eerder gesteld koos de V.S. er dus voor om via een afzonderlijke regeling identiteitsdiefstal op federaal niveau strafbaar te stellen. Men wou daarmee reeds toen het duidelijke signaal geven dat deze vorm van criminaliteit niet slechts een specifieke *variant* uitmaakt van reeds bestaande delicten zoals fraude of diefstal. Een andere belangrijke drijfveer van de wet was om opsporingsambtenaren en handhavingsautoriteiten te stimuleren om op een ernstiger manier werk te maken van de aanpak van identiteitsdiefstal.

Zes jaar na de eerste identity theft Bill (in 1998) werden de straffen uit de originele Act opgetrokken via de *Identity Theft Penalty Enhancement Act. "Like other forms of stealing, identity theft leaves the victim poorer and feeling terribly violated,"* zo verklaarde toenmalig President Bush bij de ondertekening van de wet op het Witte Huis. *"The criminal can quickly damage a person's lifelong effort to build a good credit rating."*

"The law will make it more likely that thieves are prosecuted", volgens Betsy Broder, adjunct directeur van de FTC (Federal Trade Commission), Division of Planning and Information, *"A prosecutor is less likely to bring a case if they're not going to get any serious jail time when the get a conviction*."

"There's a reality in how prosecutors do their business and that reality is that they're going to take the cases that are easiest to prove and carry the most weight. Identity theft was basically being ignored".[156]

Het mocht duidelijk wezen: een sterkere en effectievere handhaving moest zonder dralen worden geïmplementeerd.

Het is nog maar zeer de vraag of men hier vandaag de vruchten kan van plukken. De cijfers laten alleszins anders vermoeden.

HOOFDSTUK 2: VERENIGD KONINKRIJK

Ook in het Verenigd Koninkrijk prijkt identiteitsdiefstal al enkele jaren op de agenda van menig beleidsmaker, bedrijf en organisatie. De cijfers zagen we al, maar wat gebeurde er op legislatief gebied?

AFDELING 1: INLEIDING

Het Verenigd Koninkrijk kent sinds 2003 een expliciete wettelijke regeling voor identiteitsdiefstal, maar tot een afzonderlijke strafbaarstelling, zoals in de Verenigde Staten, is men vooralsnog niet gekomen. De Fraud Act[157] en Identity Cards Act[158], beiden daterend

[156] D. MCGUIRE, "Bush signs identity theft bill", *Washington Post Online*, 2004, (te consulteren via www.washingtonpost.com/wp-dyn/articles/A51595-2004Jul15.html).
[157] Fraud Act 2006, (te consulteren via http://www.opsi.gov.uk/acts/acts2006/ukpga_20060035_en_1).
[158] Identity Cards Act 2006 (te consulteren via www.opsi.gov.uk/ACTS/acts2006/20060015.htm).

van 2006, omvatten de huidige regeling in de V.K. rond identiteitsdiefstal. De Identity Cards Act bevat een scala aan maatregelen om vijf beleidsdoelen te halen (in dezelfde Act of wet werd immers ook de strijd tegen terrorisme en de aanpak van de georganiseerde misdaad opgenomen). Belangrijk om op te merken is dat het V.K., in tegenstelling tot de V.S., een hoge verwachting koestert in biometrie als oplossing voor identiteitsdiefstal en de introductie van een nationale identiteitskaart.

Met de National Identity Card Act kwam daarenboven de nodige juridische grondslag voor de oprichting van een Nationaal Register (*National Identity Register).* Dit register bevat meer dan vijftig mogelijke categorieën van informatie, inclusief geboortedatum, geboorteplaats, hoofdverblijfplaats, bijkomende verblijven of eigendommen in het buitenland, een frontale en zijdelingse foto, handtekening, vingerafdrukken en andere biometrische informatie (irisscan, en gelaatsscan).[159] Het laat de regering toe om bijkomende categorieën in te voeren, doch dit dient via een bijkomende stemming te gebeuren.

Interessant is ook de opname van de verwachte kost van financiële identiteitsfraude over een periode van 10 jaar. Deze verwachting moet elke zes maanden gerapporteerd worden aan het Parlement. Ook werd de verantwoordelijkheid voor de correctheid van de gegevens in het register bij de burger gelegd: eens opgenomen in het register, is deze zelf verantwoordelijkheid voor het up-to-date houden van de bovengenoemde categorieën. Bij een gebrek aan medewerking werd een civiele boete opgenomen die maximum £1.000 kan bedragen.

Gezien de verregaande implicaties, lijkt het niet oninteressant om de achtergrond van deze beide wetten te schetsen.

AFDELING 2: ACHTERGROND FRAUD ACT

De *Fraud Act* werd gestemd op 8 november 2006 en trad in werking op 15 januari 2007. De wet geeft een definitie van het misdrijf *fraude,* en deelt het misdrijf vervolgens op in drie categorieën, namelijk (1) *fraud by false representation,* (2) *fraud by failing to disclose information* en (3) *fraud by abuse of position*.

[159] X., "Identity Cards Act 2006: An act facilitating 'a secure and reliable record of registrable facts about individuals in the United Kingdom'", 2009, (te consulteren via http://www.guardian.co.uk/commentisfree/libertycentral/2009/jan/15/identity-cards-act).

Deze wet verving verschillende oudere wetten en stafbepalingen, waarvan de meeste waren opgenomen in de Theft Act van 1978. De reden voor de vervanging ligt enigszins voor de hand. De wet was onvoldoende specifiek om de vaak complexe en moeilijke casussen omtrent (identiteits)fraude op te lossen.

De wet kwam bovendien tegemoet aan een rapport van 2002, uitgebracht door de Law Commission in 2002, getiteld '*Fraud*'[160], waarin werd gesteld dat bij het ontbreken van degelijke gespecialiseerde wetgeving, aanzienlijke problemen konden ontstaan rond de effectieve vervolging van nieuwe fenomenen rond (online) fraude.

Ook de Home Office ijverde in haar '*Consultation Paper on Fraud Law Reform*' voor nieuwe regelgeving, gezien de bestaande strafbaarstellingen rond fraude elkaar overlapten en faalden om een constitutief begrip van fraude op te bouwen.

Naast deze academische en juridische argumentatie, waren er nog andere redenen die de keuze voor een nieuwe wetgeving legitimeerden. Zo lijdt het geen twijfel dat in de laatste jaren informaticamisdrijven een aanmerkelijke groei hebben genomen. De (door de overheid gesubsidieerde) studie *'Get Safe Online Report'* [161], gepubliceerd in oktober 2006, suggereerde dat maar liefst 3,5 miljoen mensen in de V.K. reeds slachtoffer werden van online fraude, met een gemiddelde kost van 875 pond per persoon.

Een gespecialiseerde wet kon dan ook niet langer uitblijven.

Zoals reeds hierboven gesteld, deelt de wet *fraude* op in drie categorieën:

'Fraud by false representation' wordt als volgt gedefinieerd in de artikel twee van de wet (eigen onderlinie):

"A person is in breach of this section if he—

(a) dishonestly makes a false representation, and

(b) intends, by making the representation—

[160] THE LAW COMMISSION FRAUD (Report No. 276), juli 2002, http://www.lawcom.gov.uk/lc_reports.htm#2002
[161] The Get Safe Online Report', oktober 2006, http://www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if—

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

(3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of—

(a) the person making the representation, or

(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device

designed to receive, convey or respond to communications (with or without human intervention). "

De andere twee categorieën, hier van minder belang, worden gedefinieerd in artikel drie en vier. In elk van de drie gevallen is vereist dat de persoon die onrechtmatig handelde dit enerzijds *wetens en willens* deed. Of, zoals verwoord in de voorbereidende werken:

"The first question is whether a defendant's behaviour would be regarded as dishonest by the ordinary standards of reasonable and honest people. If answered positively, the second question is whether the defendant was aware that his conduct was dishonest and would be regarded as dishonest by reasonable and honest people."

Anderzijds moet de handeling gesteld zijn met het oog op het behalen van gelijk welk *voordeel* voor zichzelf of iemand anders.

Dit voordeel of *'gain'* is beperkt tot financieel (i.e. geld of eigendom) verlies, welk tijdelijk of permanent kan voorkomen. In artikel zes en zeven van de wet werden bovendien twee

subsidiaire misdrijven opgenomen, namelijk het *bezitten* (‘*Possession etc. of articles for use in frauds’*) en het *maken of toeleveren* van frauduleuze artikelen (‘*Making or supplying articles for use in frauds’*).

Bij wijze van voorbeeld: met bovenstaande bepaling kan men personen strafbaar stellen die in het bezit zijn van *skimmingapparaten* (apparaten die onrechtmatig de kaartgegevens lezen bij bankautomaten, gewoonlijk door middel van valse opzet- of mondstukken, zie ook *supra*) of zulks aanmaken of toeleveren. In België daarentegen kan men het *louter bezitten* of *aanmaken* van dergelijke apparaten onder de huidige wetgeving bijzonder moeilijk vervolgen. Immers, geen van de vier bestaande strafbaarstellingen rond informaticacriminaliteit (zie *infra*) voldoen.

Stellen dat bovengenoemde wet zich bijzonder goed leent om (online) identiteitsdiefstal te bestraffen, is niet meer dan een open deur intrappen.

In de voorbereidende handelingen, onder artikel 2 (*fraud by false representation)* staat zelfs een uitdrukkelijke verwijzing naar *phishing*, één van de eerder besproken vormen van online identity theft:

“(…) This offence would also be committed by someone who engages in "phishing": i.e. where a person disseminates an email to large groups of people falsely representing that the email has been sent by a legitimate financial institution. The email prompts the reader to provide information such as credit card and bank account numbers so that the "phisher" can gain access to others' assets.”

Met de *Fraud Act* kwam met andere woorden een effectief juridisch verweermiddel tegen de aanzienlijke groei van online identiteitsdiefstal en -fraude. Afgezien van de onwaarschijnlijk goede intenties, was de rechtsleer niettemin voorzichtig kritisch. Zo publiceerde onder andere Savirimuthu & Savirimuthu in 2007 een uitvoerige studie getiteld *Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective.*[162]

In hun conclusie benadrukten beide auteurs dat het belang en relevantie van de nieuwe wet niet onderschat mag worden. Het betekent een aanzienlijke vereenvoudiging in de

[162] A. SAVIRIMUTHU EN J. SAVIRIMUTHU, *Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective*, Liverpool, Scripted., 2007, (te consulteren via http://www.law.ed.ac.uk/ahrc/script-ed/vol4-4/savirimuthu.asp).

vervolging van identity theft en is daarom een waardevolle bijdrage in het juridisch internetlandschap. Maar, althans volgens hen, oplettendheid is geboden opdat men zich niet verkijkt op legislatief optreden. Het idee dat het recht in staat is de online veiligheid te controleren, moet afgedaan worden als een pure mythe. Beiden leggen de nadruk op persoonlijke, sociale en culturele processen die, in samenspraak met de nodige voorlichting en bewustwording vanwege de overheid, een meer effectief antwoord kan bieden dan het louter juridisch pad. In hun eigen woorden:

"(…) phishing or identity theft is not a problem that law can solve – ultimately online criminal behaviour is a social not technologically driven problem. Notwithstanding the limits on the criminal law, Luhmann provides us with a framework that goes beyond the juridicalisation of identity theft. (…)

The central point here is that notwithstanding the limits faced by law in conceptualizing risks posed by identity theft or phishing attacks, we need to acknowledge the fact that other social systems and organisations can respond reflexively. Such a process enables society to transform itself, not in the sense of converting inputs into outputs, but through the autopoiesis of risk communications."

Anderen[163] wijzen er dan weer op dat de bewuste wet zelf enkele nadelen incorporeert. Zo onderscheiden Johnson & Rogers drie tekortkomingen.

Ten eerste wordt het concept van *'dishonesty'* op de korrel genomen. De wet vereist, zoals hoger gesteld, een bedrieglijk opzet, dus *wetens en willens*, in hoofde van de beklaagde. De auteurs wijzen erop dat er reeds een aanzienlijk aantal bezwaren gerezen zijn tegen dit subjectief begrip, welke de vervolging (en *a fortiori* de bewijsvoering) er niet makkelijker op maakt.

Een tweede punt van kritiek betreft het ontbreken van degelijke definiëringen van sleutelbegrippen, zoals *'fraude'*, *'false'* of '*abuse'*.

De laatste, en misschien wel meest belangrijke, opmerking draait rond de ingevoerde drieledige opdeling van het misdrijf fraude. De auteurs bekritiseren dat fraude geen

[163] M. JOHNSON, K.M. ROGERS, *The Fraud Act 2006: The E-Crime Prosecutor's champion or the creator of a new inchoate offence?*, 2007, 1.

zelfstandig en algemeen misdrijf meer is. Dit is m.i. terecht. Hoewel de opdeling toelaat om legislatief en politioneel vroeger in te grijpen, werkt een limitatieve opsomming steeds beperkend. De vrees dat men nieuwe vormen van fraude uitdenkt, die niet binnen deze *heilige drievuldigheid* vallen, is dan ook zeer reëel.

De auteurs gaan ook de bijzondere interessante vraag na of en in hoeverre de nieuwe wet effectief bruikbaar is voor aanklagers. Er wordt gewezen op de sterke nadruk op 'e-misdrijven', zoals *phishing,* klonen van kredietkaarten, misbruik van online posities, etc., wat vanzelfsprekend een positieve ontwikkeling is. Dat gezegd zijnde, hangt de effectiviteit van de wet in grote mate af van de verdere ontwikkeling van cybercriminaliteit. De auteurs hekelen in deze het gebrek aan effectieve kennis rond informaticacriminaliteit. Met de (m.i. zeer terechte) woorden van Moitra[164]:

"…even though cyberlaws have already been and continue to be developed, our actual knowledge of cybercrime is still extremely limited. Laws are being developed on the basis of presumed technical possibilities of various deviant, harmful or dangerous activities over the Internet. These laws also seem to be influenced by individual cases and the presumed nature of cybercrime.

Our current information is mostly based on individual cases and anecdotes, some survey data whose generalisability is doubtful, various compilations of unverified reports and media announcements."

Niettemin, bij wijze van conclusie, de optimistische woorden van Barty & Carnell[165]: *"With identity theft and credit card scams a growing concern, the new legislation is likely to be welcomed by the financial and banking sector and, once passed, should result in a considerable increase in the number of prosecutions of technology related crime."*

[164] S.D. MOITRA, *Developing Policies for Cybercrime,* European Journal of Crime, Criminal Law and Criminal Justice, 2005, 435-464.
[165] S. BARTY, EN P. CARNELL, *Fraud Bill offers new protection against technology abuse,* World Internet Law Report, 2005, 20-21.

AFDELING 3: ACHTERGROND NATIONAL IDENTITY CARD ACT

De directe aanleiding voor de National Identity Card Act was de terroristische aanslag van 11 september 2001. De toenmalige Home Secretary David Blunkett[166] werd een vurig voorstander van de verplichte identiteitskaart, hoewel de regering hem hier initieel niet in wou volgen. Blunkett bevestigde dat het idee met een hoogdringendheid werd onderzocht in het kader van een nieuw pakket antiterroristische maatregelen. Sommige toenmalige ministers verloren bovendien elke ratio met wetsvoorstellen die politie en geheime diensten bijna ongelimiteerde macht toekenden, en met voorstellen tot aanpassing van de daarvoor recent geïmplementeerde Human Rights Act.

Het publiek gaf te kennen dat er een brede consensus was voor het invoeren van een nationale identiteitskaart, toch kon het voorstel zoals verwacht op harde oppositie rekenen van mensenrechtenorganisaties.

In 2002 begon het Home Office aan een consultatieronde voor de introductie van "*entitlement cards*"[167] (een *light* versie van wat de uiteindelijke ID-card moest worden) en in november 2003 publiceerde de regering haar plannen voor een nationale, verplichte identiteitskaart.

De overheid argumenteerde dat het plan essentieel was voor de veiligheid van het Verenigd Koninkrijk en de bescherming tegen terrorisme, georganiseerde misdaad *en identity theft* diende te garanderen. Er was evenwel nog discussie[168] over het al dan niet verplicht karakter van de nieuwe nationale identiteitskaart. Deze discussie vertraagde de publicatie van de wetsvoorstel tot april 2004. De Identity Cards Bill[169] zelf werd gepubliceerd in november

---

[166] N. MORRIS, "Blunkett giving 'high priority' to compulsory ID cards ", *The Independent,* 2001 (te consulteren via http://www.independent.co.uk/news/uk/politics/blunkett-giving-high-priority-to-compulsory-id-cards-670573.html).

[167] X., "Blunkett backs ID card plan", *BBC News,* 2002, (te consulteren via http://news.bbc.co.uk/2/hi/uk_news/politics/2084860.stm).

[168] E. BARNES, "Cabinet split over plan to fast-track ID cards", *ScotlandonSunday,* 2004, (te consulteren via http://scotlandonsunday.scotsman.com/identitycards/Cabinet-split-over-plan-to.2513463.jp) en X., "Compulsory ID cards 'ruled out', *BBC News*, 2001, (te consulteren via http://news.bbc.co.uk/1/hi/uk_politics/1572026.stm) en A. TRAVIS, "Cabinet leak hits Blunkett's ID card plan", *Guardian*, 2003, (te consulteren via http://www.guardian.co.uk/politics/2003/oct/13/freedomofinformation.humanrights)

[169] Identity Cards Bill, Explanatory notes, (te consulteren via http://www.publications.parliament.uk/pa/cm200405/cmbills/008/2005008.pdf) en http://www.homeoffice.gov.uk/docs3/identitycardsconsult.pdf

2004.[170] Net voor de tweede lezing van de Identity Cards Bill zou plaatsvinden, nam David Blunkett ontslag, welke er toe leidde dat de nieuwe Home Secretary, Charles Clarke (een liberaal-democraat), opriep tot een *legislatieve pauze* om de wet en haar implicaties grondig te evalueren, met als argument dat het de meest fundamentele civiele rechten raakt.

De Bill had ondertussen de formele ondersteuning van de conservatieven, onder de leiding van Michael Howard, hoewel verschillende hooggeplaatste partijleden hun ongenoegen over het wetsvoorstel hadden laten horen. Door de drukke legislatieve kalender slaagde de regering er niet in om de Bill door het Parlement te loodsen. In een 'manifest'[171] van de Labour partij stond te lezen dat men identiteitskaarten met biometrische data zoals vingerafdrukken zou invoeren, en een Nationaal Register zou oprichten ter bewaring van de gegevens. Doch, toen er uiteindelijk een nieuw Parlement werd gevormd, kende de oppositie tegen de identiteitskaart haar hoogtepunt. De oppositie argumenteerde dat de overheid burgers niet mocht verplichten[172] een identiteitskaart bij zich te dragen, doch de kaart veeleer slechts op een vrijwillige basis moest worden ingevoerd. Men bedacht ook allerlei financiële doemscenario's waarbij enige overdrijving niet geschuwd werd: zo werd geclaimd dat de kostenanalyse van de overheid, die werd geschat op 6 miljard pond over de komende 10 jaar wel erg optimistisch was. In juni 2005, maakte de Londen School of Economics[173] een rapport openbaar waarin de verwachte kost geschat werd tussen 10,6 en 19,2 miljard pond, een cijfer die door Clarke werd afgedaan als pure nonsens.[174]

De Bill kreeg zijn uiteindelijke derde lezing in de House of Commons op 18 oktober 2005[175], en werd aangenomen met 309 voor en 284 tegen.[176] Echter, sinds maart 2006 loopt de uitgifte van de identiteitskaarten steeds vertraging op.

---

[170] http://press.homeoffice.gov.uk/press-releases/Strengthening_Security,_Protecti
[171] The Labour Party *manifesto* 2005, (te consulteren via http://newsimg.bbc.co.uk/1/shared/bsp/hi/pdfs/LAB_uk_manifesto.pdf).
[172] http://www.parliament.the-stationery-office.co.uk/pa/cm200506/cmhansrd/vo060213/debtext/60213-24.htm
[173] D.E. WHITLEY, "Identity cards - report by the Science and Technology Select Committee", August 2006, *Londen School of Economics and Political Science,* 2006, (te consulteren via "http://www2.lse.ac.uk/newsAndMedia/news/archives/2006/ID_Cards_4Aug.aspx).
[174] X., "Big Brother's here now", *EDP24,* 2005, (te consulteren via http://new.edp24.co.uk/content/news/story.aspx?brand=EDPOnline&category=News&tBrand=edponline&tCategory=news&itemid=NOED03%20Sep%202005%2010%3A09%3A19%3A520).
[175] A. TRAVIS, "Clarke pledges ID card data will be limited to information on passports", *Guardian*, 2005, (te consulteren via http://www.guardian.co.uk/politics/2005/oct/18/humanrights.idcards).

Zo maakte de 'Identity and Passport Service', een tak van de Home Office, in december 2007 plots bekend dat zij de irisscan niet zou implementeren.[177] Plannen om personen, die een paspoortaanvraag verrichten, verplicht te registreren in het National Identity Register werden bovendien uitgesteld tot 2012.

Uiteindelijk, in november 2008, begon het UK Border Agency met het uitdelen van de eerste identiteitskaarten – een soort visum welke opgenomen was als *deel* van het ID plan – aan enkele inwoners van buiten de Europese Economische Ruimte. Er werden nog enkele kleine uitgiftes gedaan maar een grote *roll-out* bleef echter uit.

Het plan kreeg gedurende de hele legislatieve procedure zoals gezegd heel wat kritiek te verwerken. Deze kritiek kreeg onder andere vorm in de "NO2ID", een campagne opgezet door oppositie en protesterende organisaties. Ook de Liberty (*Liberty Protecting Civil Liberties & Human Rights)* was sterk gekant tegen de regeling, met als hoofdargument dat het plan te verregaand was en zeer verstrekkende gevolgen had voor de relatie burger – overheid[178].

Een zorg die door velen werd gedeeld omvatte de beveiliging van de bewuste database. Privacy-waakhonden wezen erop dat dergelijke databank een enorm risico inhield, en een bijzondere aantrekkingskracht zou hebben voor hackers.[179] Het zou daarenboven een reëel risico vormen voor kwetsbare groepen zoals de beschermde getuigen, beroemdheden en slachtoffers van huiselijk geweld[180]. Immers, hun gegevens zouden verkocht kunnen worden aan de 'hoogste bieder' of zouden circuleren tussen 'geïnteresseerde partijen'[181]. Hoewel men zich vanzelfsprekend van enige dramatische toon bewust dient te zijn, is het niettemin een valabel punt om rekening mee te houden. Geen enkel beveiligingsmechanisme zal ooit volledig waterdicht zijn, de ketting is immers maar zo sterk als zijn zwakste schakel,

[176] T. BRANIGAN, "Last minute concessions ease passage of identity cards bill", *Guardian*, 2005, (te consulteren via http://www.guardian.co.uk/politics/2005/oct/19/idcards.immigrationpolicy).
[177] X., "Government drops iris scan plan", *The Register*, 2007, (te consulteren via http://www.theregister.co.uk/2007/01/09/government_drops_iris_scans_for_id_cards).
[178] G. CROSSMAN, "Liberty's response to the Home Office Consultation on the Draft Identity Cards Bill", *Liberty (Protecting Human Rights),* 2004, (te consulteren via http://www.liberty-human-rights.org.uk/pdfs/policy04/id-card-draft-bill-response.pdf).
[179] X., "Daily Telegraph letters", *Telegraph*, 2005, (te consulteren via http://www.telegraph.co.uk/comment/letters/3615768/Daily-Telegraph-letters.html).
[180] http://www.no2id.net/TakeJane/nothing2hide
[181] X. "Identity Cards Act 2006", *Guardian*, 2009, (te consulteren via http://www.guardian.co.uk/commentisfree/libertycentral/2009/jan/15/identity-cards-act).

waardoor persoonlijke gegevens onvermijdelijk gekaapt zullen worden. En waar gewone gegevens nog met enige moeite gewijzigd kunnen worden, is dit allerminst het geval voor biometrische data. Eens deze informatie in handen is van onbevoegde derden, kan de identiteit van de persoon niet meer gered worden, met alle catastrofale gevolgen van dien.

De 'Identity and Passport Service' gaf een lijst[182] vrij van instanties en organisaties welke de identiteitsmogelijkheden uit het plan zouden gebruiken. De verwachting is dat minstens 265 overheidsinstanties en 44.000 private organisaties verificaties willen doen aan de hand van het Nationaal Register. Vanuit de 'NO2ID' werd de waarschuwing gegeven dat elke keer dat iemand zich verifieert met behulp van zijn identiteitskaart, deze verificatie zal worden opgeslagen. Na enige tijd zal men, aan de hand van automatische softwaremechanismen, in staat zijn bijzonder gedetailleerde profielen op te maken van individuele personen.

In bovengenoemd debat bestaat geen juist of fout antwoord, geen zwart of witte oplossing. Het is een moeizaam zoeken naar een cruciaal evenwicht tussen privacy en de nood tot identificatie en veiligheid. Van het op papier ambitieuze Britse project is in de praktijk nog maar bitter weinig terechtgekomen. De toekomst zal moeten uitwijzen welk pad het Verenigd Koninkrijk zal bewandelen.

Update: op 12 mei 2010 maakte de *Identity & Passport Service* van de Home Office officieel bekend[183] dat, in het licht van de nieuwe coalitieovereenkomst tussen de Conservatieven en de Liberalen[184], werd besloten om zowel de identiteitskaarten als het Nationale Register volledig te annuleren. Het officiële bericht gaat als volgt:

"The Government has stated in the Coalition Agreement that it will cancel Identity Cards and the National Identity Register. We will announce in due course how this will be achieved. Applications can continue to be made for ID cards but we would advise anyone thinking of applying to wait for further announcements."

Met dit bericht komt dan ook een (voorlopig) einde aan de bijzonder verhitte discussie rond identiteitskaarten in het Verenigd Koninkrijk.

---

[182] http://www.ips.gov.uk/identity/how-organisations.asp
[183] http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/53.htm
[184] X., "UK has first coalition government since 1945", *NEWEUROPE,* 2010, (te consulteren via http://www.neurope.eu/articles/UK-has-first-coalition-government-since-1945/100818.php).

AFDELING 4: BEWUSTWORDINGSCAMPAGNES

Bij een aparte strafbaarstelling is het niet gebleven. De Britse regering tracht identiteitsdiefstal ook aan te pakken via aanvullende wettelijke maatregelen. Er werd daarenboven sterk ingezet op bewustwordingscampagnes. Gewezen kan worden op de Identity Fraud Steering Committee (IFSC) en de Identity Fraud Forum (IFF), die beiden in 2003 werden opgericht, welke publieksvoorlichting tot één van hun belangrijkste taken rekenen. Er werd bovendien reeds eerder een vermelding gemaakt van de speciale website die werd opgezet om het publiek beter vertrouwd te maken met het fenomeen identiteitsdiefstal (www.identity-theft.org.uk). [185]

Een blik op de situatie in de overige landen van de Europese Unie leert dat het Verenigd Koninkrijk een redelijke unieke stap heeft gezet met de specifieke aanpak van identiteitsdiefstal. Immers, slechts enkele landen, zoniet geen enkel ander land buiten het Verenigd Koninkrijk, kent momenteel specifieke wetgeving[186]. Er heerst echter verdeeldheid in de rechtsleer wanneer een strafbaarstelling specifiek genoeg is om opgenomen te worden in bovenstaande lijst.[187]

[185] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Online Identity Theft,* U.K., 2009, 52.
[186] J.E.J., PRINT EN N.S. VAN DER MEULEN, *Identiteitsdiefstal: lessen uit het buitenland*, Justitiële verkenningen, jrg 32, nr. 7, 2006, p. 17
[187] N.S. VAN DER MEULEN, *Achter de schermen: de ervaringen van slachtoffers van identiteitsroof*, Justitiële verkenningen, jrg. 32, nr. 7, 2006.

DEEL 6 : NOODZAAK VAN EEN BELGISCHE OF EUROPESE REGLEMENTERING INZAKE IDENTITY THEFT?

HOOFDSTUK 1: SITUATIE IN EUROPA

AFDELING 1: CYBERCRIME-VERDRAG

Een van de belangrijkste Europese verwezenlijkingen op vlak van informaticacriminaliteit is het Cybercrime verdrag[188] van 23 november 2001. Dit verdrag voorziet in een aantal doelstellingen.[189]

Allereerst beoogt het verdrag het invoeren van gelijkaardige wetgeving in alle Europese landen, die toelaat specifieke informaticamisdrijven of –inbreuken, zoals integriteit, vertrouwelijkheid, beschikbaarheid en vervalsing van gegevens, bedrog of oplichting met behulp van informaticasystemen, et cetera te bestraffen. Ook niet-specifieke informaticamisdrijven, zoals bijvoorbeeld kinderpornografie of inbreuken op intellectuele eigendom (auteursrecht, naburige rechten, merkenrecht, …) zouden worden beteugeld.

Een ander oogmerk is de aanpassing van de strafprocedure aan het gebruik van informatica in de Europese landen, zodat naast de gewone huiszoekingen ook *netwerkzoekingen*[190] (opsporingen in particuliere of bedrijfsnetwerken) of het kopiëren van digitaal bewijsmateriaal mogelijk worden.

Het laatste, en misschien wel belangrijkste, doel van het verdrag is het stimuleren van een internationale samenwerking inzake de aanpak en preventie van fenomenen omtrent informaticacriminaliteit. Ook de uitlevering, opsporing en vervolging zijn onderhavig aan een aantal vormen van wederzijdse samenwerking.

Enig kritisch geluid dringt zich niettemin op. Tot dusver ondertekenden 46 landen het verdrag, doch de ratificatieteller bleef vooralsnog steken op 29 landen.[191] Een ander punt

[188] http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm
[189] J. DUMORTIER, *ICT-Recht,* Leuven, Acco, 2009-2010, 181.
[190] M. SCHELLKENS, R. KASPERSEN, A. HOFMAN, J. VERBEEK, C. VAN DER NET, J. TEMPELMAN, *Strafbare feiten op de elektronische snelweg, vertrouwelijkheid van e-mail, netwerkzoeking in theorie en praktijk*, IT&R 13 Nationaal programma informatietechnologie en recht, eJure,
[191] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

van kritiek is dat de landen die de grootste verantwoordelijkheid dragen voor kwaadaardige code, zoals China, Rusland en verschillende Latijns-Amerikaanse Staten, geen partij zijn in de overeenkomst.

AFDELING 2: EUROPESE COMMISSIE

In 2007 drukte de Europese Commissie in een mededeling[192] haar bezorgdheid en blijvende aandacht uit voor het groeiende fenomeen van informaticacriminaliteit. Maar zoals zo vaak mocht blijken, is de effectieve slagkracht van de Commissie erg beperkt en kan zij weinig zelfstandige legislatieve acties ondernemen. De mededeling focust dan ook op het aansturen en ondersteunen van grensoverschrijdende samenwerking inzake training, preventie en dialoog tussen de verschillende belanghebbenden, zowel in de publieke als private sector, justitiële verbeteringen, enzovoort.

Zo stelt de mededeling bijvoorbeeld (eigen onderlinie):

*"In practice, the term cyber crime is applied to three categories of criminal activities. The first covers **traditional forms of crime** such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over electronic communication networks and information systems (hereafter: electronic networks). The second concerns the publication of **illegal content** over electronic media (i.a. child sexual abuse material or incitement to racial hatred). The third includes **crimes unique to electronic networks**, i.e. attacks against information systems, denial of service and hacking."*

(…)

The combination of constantly evolving criminal activities and a lack of reliable information makes it difficult to obtain an exact picture of the current situation. Nevertheless, some general trends can be discerned:

• The number of cyber crimes is growing and criminal activities are becoming increasingly sophisticated and internationalised

• Clear indications point to a growing involvement of organized crime groups in cyber crime

[192] COM/2007/267 final., http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf

The majority of this Communication's statements on current trends have been taken from the Study to assess the impact of a communication on cyber crime, ordered by the Commission in 2006 (Contract No JLS/2006/A1/003).

• However, the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase.

(…)

*Most crimes can be committed with the use of electronic networks, and different types of fraud and attempted fraud are particularly common and growing forms of crime on electronic networks. Instruments such as **identity theft**, phishing, spams and malicious codes may be used to commit large scale fraud. Illegal national and international Internet-based trade has also emerged as a growing problem. This includes trade in drugs, endangered species and arms.*

(…)

*Targeted legislation against cyber crime should however also be considered now. A particular issue which may require legislation relates to a situation where cyber crime is committed in conjunction with **identity theft**. Generally, "identity theft" is understood as the use of personal identifying information, e.g. a credit card number, as an instrument to commit other crimes. In most Member States, a criminal would most likely be prosecuted for the fraud, or another potential crime, rather than for the identity theft; the former being considered a more serious crime. Identity theft as such is not criminalised across all Member States. It is often easier to prove the crime of identity theft than that of fraud, so that EU law enforcement cooperation would be better served were identity theft criminalised in all Member States. The Commission will in 2007 commence consultations to assess if legislation is appropriate.*

Fight against traditional crime in electronic networks
Initiate an in-depth analysis with a view to preparing a proposal for specific EU legislation against identity theft

(…)

De Commissie legt dus zeer uitdrukkelijk de nadruk op het fenomeen van identity theft, en stelt vast dat de huidige wetgeving van de lidstaten vaak niet voorzien is op dit groeiend probleem, zodat deze hun heil moeten zoeken in artikelen die de *fraude* an sich bestraffen, maar daarom niet het specifieke misdrijf van *identiteits*diefstal.

AFDELING 3: WIJZIGING RICHTLIJN 2002/58/EG

Een andere belangrijke en recente evolutie betreft de wijziging van richtlijn 2002/58/EG, welke een meldingsplicht voor beveiligingsinbreuken invoert.[193] Hierbij moet meteen opgemerkt worden dat deze meldingsplicht enkel van toepassing is op *openbare* elektronische communicatienetwerken en niet op *private* (of besloten) bedrijfsnetwerken of gebruikersgroepen.

De richtlijn bevat een wijziging van artikel 3, waaraan wordt toegevoegd dat (eigen onderlinie):
(…) "In geval van een inbreuk in verband met persoonsgegevens stelt de aanbieder van openbare elektronische communicatiediensten de bevoegde nationale instantie zonder onnodige vertraging in kennis van de inbreuk in verband met persoonsgegevens.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk ongunstige gevolgen zal hebben voor de persoonsgegevens en persoonlijke levenssfeer van een abonnee of een individuele persoon stelt de aanbieder ook de abonnee of de individuele persoon in kwestie onverwijld van de inbreuk in kennis.

In kennis stelling van een betrokken abonnee of individuele persoon van een inbreuk op persoonsgegevens is niet vereist wanneer de aanbieder tot voldoening van de bevoegde instantie heeft aangetoond dat hij de gepaste technische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de data die bij de

[193] Richtlijn 2009/136/EG, (te consulteren via http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:NL:NOT).

beveiligingsinbreuk betrokken waren. Dergelijke technologische beschermingsmaatregelen maken de gegevens onbegrijpelijk voor eenieder die geen recht op toegang daartoe heeft."

Deze *gepaste technische beschermingsmaatregelen* kunnen bijvoorbeeld bereikt worden door het toepassen van encryptie en MD5-hashing (zie *infra*).

"In de kennisgeving aan de abonnee of de individuele persoon worden ten minste de aard van de inbreuk op persoonsgegevens, alsmede de contactpunten voor meer informatie vermeld, en worden er maatregelen aanbevolen om mogelijke negatieve gevolgen van de inbreuk in verband met persoonsgegevens te verlichten. De kennisgeving aan de bevoegde nationale instantie bevat bovendien een omschrijving van de gevolgen van de inbreuk en van de door de aanbieder voorgestelde of getroffen maatregelen om de inbreuk in verband met persoonsgegevens aan te pakken.

(…)

Aanbieders houden een zodanige inventaris bij van inbreuken op persoonsgegevens, o.m. de feiten in verband met deze inbreuken, de gevolgen ervan en de herstelmaatregelen die zijn genomen, dat de bevoegde nationale instanties kunnen nagaan of de bepalingen van lid 3 worden nageleefd. De inventaris bevat uitsluitend de voor dit doel noodzakelijke gegevens. "

Men verduidelijkt het begrip "*inbreuk in verband van persoonsgegevens"* met volgende definiëring (ingelast in artikel 2): "*een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Gemeenschap"*.

Een inbreuk wordt als schadelijk voor de persoonsgegevens of privéleven van een abonnee of persoon beschouwd, wanneer er, bij wijze van voorbeeld, sprake is van identiteitsdiefstal of –fraude, aantasting van de reputatie, ernstige vernedering et cetera.[194]

[194] J. DUMORTIER, "Recente ontwikkelingen in het privacyrecht 2008-2009", *Recht in beweging 17de VRG-Alumni dag,* 2010, 161.

AFDELING 4: FRANKRIJK

In Frankrijk ligt de focus rond identiteitsdiefstal voornamelijk rond het financiële aspect. In 2006, volgens een rapport van de *Observatoire de la sécurité des cartes de paiements*, bedroeg de totale kost van frauduleuze kredietkaartverrichtingen maar liefst 252,6 miljoen euro. Een andere zorg is de hoge graad aan namaak van identiteitspapieren, zoals paspoorten en rijbewijzen.

Frankrijk kent daarenboven een uniek registratienummer per inwoner (*NIR: numéro national d'inscription au répertoire des personnes physiques*) welk – zoals de Verenigde Staten reeds ruimschoots aantoonden – niet zonder gevaar is.

Identiteitsdiefstal zal vooreerst – indien aan alle voorwaarden voldaan – bestraft kunnen worden via art. 434-23 Code pénal:

"Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Nonobstant les dispositions des articles 132-2 à 132-5 , les peines prononcées pour ce délit se cumulent, sans possibilité de confusion, avec celles qui auront été prononcées pour l'infraction à l'occasion de laquelle l'usurpation a été commise.

Est punie des peines prévues par le premier alinéa la fausse déclaration relative à l'état civil d'une personne, qui a déterminé ou aurait pu déterminer des poursuites pénales contre un tiers."

Vereist is dus de uitdrukkelijke aanname van de "naam van een andere persoon". Er werd vooralsnog geen rechtspraak genoteerd die het begrip *naam* verder invult. Het is dan ook nog onduidelijk of bijvoorbeeld ook een IP-adres (welk steeds meer als persoonsgegeven wordt aangeduid) of pseudoniem onder het begrip kan vallen.[195] Het blijkt dat bovenstaand artikel echter zelden gebruikt wordt door aanklagers.

[195] O. ITEANU, "Usurpation d'identité: la loi ou la technique pour se protéger?", *Journal de Net*, 2004.

Immers, er zijn ook andere mogelijke gronden beschikbaar, zoals daar zijn art. 313-1 Code pénal (fraude) en art. 441-1 (namaak). Ook art. 323-1 Code pénal (ongeoorloofde toegang tot informaticasystemen) werd reeds ingeroepen.

Vermeldenswaardig in deze context is ook een wetsvoorstel uit 2005. Dit wetsvoorstel voorzag de uitdrukkelijke strafbaarstelling van online identiteitsdiefstal. Het voorstel werd echter afgewezen, met als argumentatie dat het misdrijf reeds voldoende kan bestraft worden via de bestaande artikelen.

Nochtans werd in 2009 een nieuw wetsvoorstel (*loi LOPPSI*) gepresenteerd dat uitdrukkelijk online identiteitsdiefstal kwalificeerde. Deze wet zou art. 222-16 Code pénal amenderen en gaat als volgt:

"Le fait d'utiliser, de manière réitérée, sur un réseau de communication électronique l'identité d'un tiers ou des données qui lui sont personnelles, en vue de troubler la tranquillité de cette personne ou d'autrui.

Le fait d'utiliser, sur un réseau de communication électronique, l'identité d'un tiers ou des données qui lui sont personnelles, en vue de porter atteinte à son honneur ou à sa considération. "

Het *Forum des droits sur l'internet* is niet per se gekant tegen de invoering van bovengenoemd artikel, doch wijst wel op de vaagheid van de gebruikte termen.[196] Op 5 mei 2010 besliste de Senaat, vermoedelijk onder druk van de publieke opinie, om het bovengenoemd voorstel voor onbepaalde tijd uit te stellen.[197]

AFDELING 5: DUITSLAND

Ook in Duitsland bestaat geen uitdrukkelijke strafbaarstelling van identiteitsdiefstal. In het Duitse *Strafgesetzbuch* komt het woord *identität* (identiteit) niet voor. Ook rechtszaken die expliciet verwijzen naar identiteitsdiefstal blijken schaars, en komen enkel voor bij

[196] FORUM DES DROITS SUR INTERNET, http://www.foruminternet.org/specialistes/veille-juridique/actualites/projet-de-loi-d-orientation-et-de-programmation-pour-la-performance-de-la-securite-interieure-2909.html
[197] G. CHAMPEAU, "La loi Loppsi reportée sine die par le Sénat (MAJ)", *Numerama*, 2010, (te consulteren via http://www.numerama.com/magazine/15670-la-loi-loppsi-reportee-sine-dine-par-le-senat.html).

burgerrechtelijke geschillen. Er werd wel reeds in 2007 een uitvoerige studie[198] rond '*Identitätsdiebstahl'* (en nog meer specifiek rond phishing) verricht.

De auteur komt tot de conclusie dat volgende artikelen kunnen worden ingeroepen bij een eventuele identiteitsdiefstal: §263a StGB[199] (*Computerbetrug*, ICT-gerelateerde fraude), §269 StGB[200] (*Fälschung beweiserheblicher Daten,* ICT-gerelateerde namaak), §202c StGB[201] (*Vorbereiten des Ausspähens und Abfangens von Daten*, misbruik), §202a StGB[202] (*Ausspähen von Daten*, ongeoorloofde toegang tot informaticasysteem) en §303a StGB[203] (*Datenveränderung*, datamanipulatie).

Overigens zijn § 202a en §303a beiden omzettingen ingevolge het Cybercrime-verdrag.[204]

HOOFDSTUK 2: SITUATIE IN BELGIË

In België bestaat geen aparte strafbaarstelling voor identiteitsdiefstal. Wanneer men zich voordoet als een officier of houder van een officieel mandaat, komt men wel in aanvaring met art. 227bis Sw.[205], welk stipuleert: "*Met geldboete van tweehonderd frank tot duizend frank wordt gestraft hij die wederrechtelijk in het openbaar de titel of de graad aanneemt, als titularis of opvolger, van personen die deelnemen aan de uitoefening van openbare macht dan wel een burgerlijk of een militair openbaar ambt uitoefenen.)*

§ 2. Met geldboete van honderd frank tot vijfhonderd frank worden gestraft de reserveofficieren, gepensioneerde officieren, officieren en reserveofficieren titularissen van een eregraad, die de titel van officier of die van hun graad in het openbaar voeren, zonder die, al naar het geval, te doen voorafgaan door de vermelding " reserve- ", " gepensioneerd ", " ere- ", " erereserve "."

---

[198] D. SCHNEIDER, *Phishing, Pharming und Identitätsdiebstahl – von Postbank bis Paypal. Informationstechnische Grundlagen und strafrechtliche Beurteilung der Internetkriminalität,* onuitg., Waldkirch, 2007
[199] http://www.gesetze-im-internet.de/stgb/__263a.html
[200] http://www.gesetze-im-internet.de/stgb/__269.html
[201] http://www.gesetze-im-internet.de/stgb/__202c.html
[202] http://www.gesetze-im-internet.de/stgb/__202a.html
[203] http://www.gesetze-im-internet.de/stgb/__303a.html
[204] Cybercrime-Verdrag van 23 november 2001, (te consulteren via http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).
[205] Art. 206 Strafwetboek.

Dit artikel is uiteraard enkel van toepassing indien er gebruik wordt gemaakt van de identiteit van een personen die een *burgerlijk* dan wel *militair* openbaar ambt uitoefenen. Het valt dus niet algemeen in te zetten tegen identiteitsdiefstal.

Een andere bepaling betreft de onrechtmatige aanname van de titel van advocaat, geregeld in art. 227ter Sw.: *"Hij die in het openbaar de titel van advocaat aanneemt, zonder ingeschreven te zijn op het tableau van de Orde of op een lijst van stagiairs, of de titel van ereadvocaat zonder in het bezit te zijn van de in artikel 436 van het Gerechtelijk Wetboek bedoelde machtiging, wordt gestraft met geldboete van tweehonderd frank tot duizend frank."*

Interessanter is art. 231 Sw.: *"Hij die in het openbaar een naam aanneemt, die hem niet toekomt, wordt gestraft met gevangenisstraf van acht dagen tot drie maanden en met geldboete van vijfentwintig frank tot driehonderd frank, of met een van die straffen alleen."*

Artikel 231 Strafwetboek beoogt een veel ruimere strafbaarstelling, en zou met enige zin voor interpretatie ingezet kunnen worden voor verschillende vormen van identiteitsdiefstal.[206]

Er schuilt in bovenstaande redenering[207] echter een reëel gevaar. Het legaliteitsbeginsel *'nullum crimen, nulla poena sine praevia lege poenali'*[208], wordt tot op heden nog steeds beschouwd als één van de hoekstenen, zoniet dè hoeksteen, van het Belgische strafrecht. [209] In het strafrecht geldt de wet als ultieme bron van het recht. De contouren van het strafrecht zijn dermate sterk afgelijnd, dat vervolgende overheden slechts mogen optreden wanneer dat gemachtigd is door een wettelijk, en precies uitgedrukte norm.

Men dient in het strafrecht gebruik te maken van het *lex certa*-beginsel, of de *substantiële dimensie van het* legaliteitsbeginsel. De formulering van de strafbare feiten moet duidelijk

[206] E. KINDT, "Country report for 'Belgium' in D12.7: Identity-related crime: Big problem or Big Hype?", *FIDIS,* 2008, 12-29 (te consulteren via http://www.fidis.net/fileadmin/fidis/deliverables/5th_workplan/fidis-wp12-del12.7_identity_crime_in_Europe.pdf).
[207] E. KINDT EN E. SZAFRAN, "Informaticacriminaliteit: Nullum crimen, nulla poena sine lege? Een beknopt overzicht van de evolutie in rechtspraak en wetgeving", noot onder Corr. Gent 11 december 200, inz. ReDaTack, *Computerr.*, 2001.
[208] F. TULKENS, M. VAN DE KERCHOVE, *Introduction au droit pénal. Aspects juridiques et criminoliques,* Diegem, 1997, 184.
[209] E. CLAEYS, *Legaliteit en rechtsvinding in het Strafrecht. Een grondslagentheoretische benadering*, Leuven, 2003, 15.

en ondubbelzinnig zijn, zodat omwille van de rechtszekerheid daaruit een heldere afgrenzing van de strafbaarheid valt te lezen.[210] Het legaliteitsbeginsel draagt ook de rechterlijke plicht om de strafwet op een strikte en enge wijze te interpreteren (*beginsel van strikte interpretatie)* met zich mee, en dit om de voorspelbaarheid van een eventueel overheidsoptreden voor de rechtsonderhorige te garanderen.

In navolging van het bovenstaande kan men niet anders dan besluiten dat art. 231 Strafwetboek, hoe interessant ook, in veel gevallen niet zal kunnen worden ingeroepen. Immers, een strikte lezing van bovengenoemd artikel leert ons dat enkel diegene die:

1) in het openbaar
2) een naam aanneemt,
3) die hem niet toekomt,

bestraft wordt.

De vereiste van openbaarheid zal een eerste bron van discussie zijn. Wanneer is de identiteitsdiefstal (of tenminste de veruitwendiging ervan) publiek of openbaar? De meest voor de hand liggende toepasselijke voorbeelden zijn het stelen of misbruiken van een identiteitskaart in het openbaar of in de publieke sfeer, door zich op valselijke wijze te legitimeren, en het stelen of misbruiken van een sociaal netwerkprofiel. Men kan veel moeilijker argumenteren dat bijvoorbeeld *skimming,* of *online betalingsfraude* onder deze voorwaarde zou vallen, laat staan dat beide vormen iets te maken zouden hebben met de tweede voorwaarde.

Deze tweede voorwaarde vereist immers een misbruik van de naam van een persoon. Wederom, het stelen van een naam is gebruikelijk bij identiteitskaartdiefstal en –misbruik, misbruik van sociale netwerkprofielen (bijvoorbeeld de kaping van iemands Facebook, Netlog of LinkedIn profiel en bij chatprogramma's (op voorwaarde dat hier geen gebruik gemaakt wordt van een gebruikersnaam, wat eerder onwaarschijnlijk is).

Het spreekt voor zich dat financiële identiteitsdiefstal hier niet van toepassing kan zijn. Hoewel het allesbehalve uitgesloten is dat criminelen bijhorende identiteitsgegevens

[210] N.D. JÖRG, C. KELK, *Strafrecht met mate*, Amsterdam, 2001, 33.

bemachtigen tijdens de *skimming*, online betalingsfraude of andere, is dit in de overgrote meerderheid van de gevallen niet het opzet. Het doel is hier vaak niet het stelen van de naam, maar wel het stelen van kredietkaart- of bankgegevens, pincodes, et cetera. Hoewel men deze gegevens vaak kan herleiden naar een specifieke persoon, en aldus persoonsgegevens vormen, is hier geen sprake van een loutere naamsdiefstal. Financiële identiteitsdiefstal (welke, nogmaals benadrukt, veruit de meest voorkomende vorm is) valt bijgevolg niet onder het toepassingsgebied van art. 231 Strafwetboek.

De derde voorwaarde, "*die hem niet toekomt",* is een vanzelfsprekendheid, daar men maar moeilijk zijn eigen identiteit kan stelen.

Concluderend biedt art. 231 dus een eerste preliminaire uitweg voor het ontbreken van een aparte strafbaarstelling voor identiteitsdiefstal. Niettemin blijkt duidelijk dat artikel 231 Sw. voorbehouden is voor de klassieke, niet digitale, vormen. Het misbruiken van een paspoort, het opgeven van de volledige naam bij een politiecontrole, enzovoort. Het artikel kan geenszins haar nut bewijzen in de meer recente vormen, *a fortiori* die dewelke zich afspelen in de ICT-sfeer.

De vraag rest ons of er dan helemaal geen artikel kan worden ingeroepen tegen een digitale identiteitsroof in België? Een antwoord hierop kan wellicht gevonden worden in de vier aparte strafbaarstellingen, ingevoerd door de wet van 28 november 2000 inzake informaticacriminaliteit [211] , namelijk *valsheid in informatica* (art. 210bis Sw.), *informaticabedrog* (art. 504quater Sw.), *ongeoorloofde toegang tot informaticasysteem* (art. 550bis Sw.) en *data- en informatica-sabotage* (art. 550ter Sw.).

AFDELING 1: VALSHEID IN INFORMATICA (ART. 210BIS SW.)

§ 1. Hij die valsheid pleegt, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in te voeren in een informaticasysteem, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, waardoor de juridische draagwijdte van dergelijke gegevens verandert, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en

[211] J. DUMORTIER, B. VAN OUDENHOVE EN P. VAN EECKE, "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles*, 2001-2, 44.

met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 2. Hij die, terwijl hij weet dat aldus verkregen gegevens vals zijn, hiervan gebruik maakt, wordt gestraft alsof hij de dader van de valsheid was.

§ 3. Poging tot het plegen van het misdrijf, bedoeld in § 1, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank of met een van die straffen alleen.

§ 4. De straffen bepaald in de §§ 1 tot 3 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 259bis, 314bis, 504quater of in titel IXbis. ".

Art. 210bis Sw. beoogt de opzettelijke vervalsing via datamanipulatie met betrekking tot juridisch relevante gegevens, te bestraffen.[212] Deze gegevens worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem. Datamanipulatie houdt het *wissen, invoeren en wijzigen* van gegevens *in een informaticasysteem* in.

Essentiële voorwaarde is dat de *juridische draagwijdte* van de gegevens veranderd wordt, bijvoorbeeld: een opgave van een vals kredietkaartnummer bij een e-commerce website of toepassing, het vervalsen van een digitale handtekening of officiële documenten, et cetera. Opmerkelijk is dat bovengenoemd artikel voorziet in een bijkomende of aparte strafbaarstelling die het *gebruik* van de vervalste gegevens omvat (art. 210*bis*, §2).

Kan *valsheid in informatica* ingeroepen worden bij identiteitsdiefstal? De constitutieve bestandsdelen van deze eerste strafbaarstelling zijn:

1) Juridisch relevante gegevens:

   Wanneer spreekt men over *juridisch relevante gegevens?* Men heeft bij de formulering van het artikel voornamelijk verwezen naar interpretaties die wij vroeger al hadden bij het *offline* valsheid in geschrifte, namelijk contracten, diploma's, attesten, enz.

[212] G. VERMEULEN, *Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen,* Antwerpen, 2007, 434.

Geschriften die men aldus in een bepaalde situatie gebruikt om een bepaald recht te doen gelden.

De vraag stelt zich dan ook of dit ook het geval is bij diefstal of misbruik van identiteitskaarten (vervalsing) en kredietkaarten (skimming – online diefstal). In het eerste geval bestaat er weinig discussie, een identiteitskaart valt immers perfect onder de noemer die de wetgever in gedachte had bij het opstellen van het artikel. In zekere mate kan men hetzelfde zeggen van een krediet- of bankkaart, hoewel dit laatste allesbehalve duidelijk is. Een kredietkaart verleent immers geen direct *recht*, en het is dan ook bediscussieerbaar of zij kan vallen onder *juridisch relevante gegevens.* Niettemin is de vraag of de data in kwestie een juridische daagwijdte heeft een feitenkwestie, die door de rechter ten gronde dient beantwoord te worden.[213]

2) Waarheidsvermomming:

   Waarheidsvermomming komt voor wanneer de weergegeven informatie, door de onrechtmatige wijziging, onwaar is geworden.

   Het artikel geeft zelf twee voorbeelden, namelijk enerzijds "*hij die valsheid pleegt, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in te voeren in een informaticasysteem, te wijzigen, te wissen"* en anderzijds "*of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, waardoor de juridische draagwijdte van dergelijke gegevens verandert".*

   Een geval als skimming (het namaken van bankkaarten, financiële identiteitsdiefstal) leunt bijvoorbeeld het dichtst aan bij het tweede criterium.

3) Verandering van de juridische draagwijdte van juridisch relevante gegevens:

   Dit is een uiteraard geen gemakkelijk gegeven. Men dient dus effectief een *verandering* in de juridische draagwijdte te hebben bewerkstelligd. Dit betekent dat een zuivere identiteitsroof uit de boot valt. Immers, men kan verkiezen om identiteiten (volledige naam, adresgegevens, et cetera) te stelen met het oog op, bijvoorbeeld, wederverkoop. Hier heeft de identiteitsdief zelf geen *verandering* toegebracht aan de juridische draagwijdte van de relevante gegevens, waardoor art. 210*bis* niet van toepassing kan worden verklaard. Hetzelfde geldt voor een persoon die, in de hypothese van een

[213] J. DUMORTIER, *ICT-Recht,* Leuven, Acco, 2009-2010, 185.

huiszoeking, wordt gearresteerd voor *bezit* van skimmingapparaten (apparaten of technische hulpmiddelen die dienen om de bank- of kredietkaart te lezen, te kopiëren, valse kaarten te maken, enzovoort. Uitgaande van de veronderstelling dat de persoon de apparaten niet zelf gemaakt heeft, maar eerder heeft aangekocht voor gebruik of wederverkoop, lijkt een toepassing van art. 210*bis* eveneens zeer moeilijk, gezien hij niet zelf *een verandering* heeft doorgevoerd.

4) Bijzonder opzet (bedrieglijk opzet en/of oogmerk te schaden)
   Bijzonder opzet is, in tegenstelling tot het gewone misdrijf van valsheid in geschrifte, zoals geregeld in art. 193 Sw, niet vereist. Gewoon opzet volstaat, hoewel er discussie bestaat over de interpretatie (zie *infra).*

Door de strafbaarstelling *valsheid in informatica* kunnen alleszins handelingen als het vervalsen of namaken van kredietkaarten (skimming), e-contracten, het binnenbreken op online accounts, et cetera op eenduidige wijze gekwalificeerd worden, en op effectieve wijze bestraft.

Maar leent het zich ook tot de pure en enge interpretatie van *identiteits*diefstal? Interessant hierbij is een vonnis[214] dat zich uitsprak over de vraag hoe men het aanmaken van een e-mailaccount op *naam* van iemand anders en het vervolgens verzenden van een e-mail via dit e-mailadres naar een derde, diende te kwalificeren. De rechter kwam tot de conclusie dat de aanmaak van dit e-mailadres moest worden beschouwd als een *manipulatie van juridisch relevante gegevens*. Men dient wel enigszins een kanttekening te maken bij de bron van deze rechtspraak, de rechter in kwestie motiveert zijn beslissing bijvoorbeeld op basis van een 'bijzonder opzet', terwijl dit helemaal niet wordt vereist, in tegenstelling tot het 'gewone' misdrijf van valsheid in geschrifte.

Nochtans, de meerderheid van rechtsleer en rechtspraak gaat uit van de presumptie dat men beide artikels (art. 210*bis* en art. 193 Sw.) samen moet lezen, zodat het vereiste van bijzonder opzet ook van toepassing zou zijn op valsheid in informatica.[215] Dergelijke *interpretatie naar analogie* moet van de hand worden gewezen, daar het beginsel van strikte

[214] Corr. Dendermonde 28 november 2005, *N.J.W*,. 2006, afl. 138, 229-23, noot J. DUMORTIER.
[215] Corr. Dendermonde 14 mei 2007, *T. Strafr.*, 2007, afl. 6, noot E. BAYENS.

interpretatie, zoals inherent aanwezig in het legaliteitsbeginsel, immers onverkort geldt. Dit betekent dat voor art. 210*bis* een gewoon opzet voldoende is.

Sommige auteurs wijzen erop dat de opstellers van de artikels sterk geïnspireerd werden door een aantal toen vigerende ideeën, fenomenen of gebeurtenissen in de ICT-sector, en dat bij een strikte lezing van de artikels huidige fenomenen zeer moeilijk bestreden kunnen worden. Dit dient te worden bijgetreden. Deze vaststelling legitimeert niettemin in geen enkel opzicht een eventuele extensieve interpretatie van strafrechtsartikelen. Het is aan de wetgever om nieuwe fenomenen correct en snel strafrechtelijk te definiëren.[216]

AFDELING 2: INFORMATICABEDROG (ART. 504QUATER SW.)

Art. 504quater. § 1. Hij die, voor zichzelf of voor een ander, een bedrieglijk vermogensvoordeel verwerft, door gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of met enig ander technologisch middel de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.

§ 2. Poging tot het plegen van het misdrijf bedoeld in § 1 wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank, of met een van die straffen alleen.

§ 3. De straffen bepaald in de §§ 1 en 2 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen vijf jaar na de uitspraak houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210bis, 259bis, 314bis of in titel IXbis. ".

Oorspronkelijk heette de strafbaarstelling in art. 504quater Sw. datamanipulatie, en werd het oogmerk omschreven als het voor zichzelf of voor een ander een *bedrieglijk*

[216] C. VAN DEN WYNGAERT, S. VANDROMME, *Strafrecht, strafprocesrecht en internationaal strafrecht in hoofdlijnen*, Maklu, Antwerpen, 2006, 89.

vermogensvoordeel te verwerven strafbaar. Het was bovendien een toepassing[217] van art. 8 van het Cybercrime-verdrag (*Computer-related fraud*): *"(…) with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another*"[218].

Door de wet van 15 mei 2006 werd artikel 504quater Sw. echter gewijzigd en volstaat nu een "*onrechtmatig economisch voordeel"* om tot strafbaarheid te kunnen besluiten.[219]

In tegenstelling tot het voorgaande misdrijf is bijzonder opzet, met name bedrog, hier weldegelijk een vereiste.

Wanneer men elektronische gegevens manipuleert doet men dit zeer vaak met het doel een onrechtmatig voordeel te bekomen. Echter, essentieel verschillend van diefstal is dat men bij deze handeling geen zaken ontvreemdt, maar wel informatie of gegevens op vrijwillige wijze laat overhandigen, en dit door gebruik te maken van bedrieglijke of listige handelingen zoals het inbrengen van fictieve namen in een bestand of het veranderen van bepaalde gegevens.

Men kan zich de vraag stellen in hoeverre deze gedragingen eveneens gelding vinden in art. 496 Sw., dat namelijk de zuivere oplichting bestraft. Wanneer men de constitutieve bestandsdelen onderzoekt van oplichting komt men tot een drieledig resultaat: *primo* moet bij oplichting het doel zijn zich een *zaak* toe te eigenen die aan een ander behoort, *secundo* de afgifte van gelden, verbintenissen of roerende zaken, en *tertio* moet deze afgifte veroorzaakt zijn door het gebruik van bedrieglijke middelen.[220]

De rechtsleer gaf geen eenduidig antwoord op de vraag of art. 496 Sw. ook kon worden ingezet bij computercriminaliteit die zich toespitst op het verwerven van een vermogensvoordeel. Nochtans lijkt aan alle voorwaarden voldaan: de manipulatie van een informaticasysteem heeft immers tot doel het zich doen afgeven van geld of andere waardemiddelen, de afgifte van een *zaak* vormt eveneens geen probleem, daar de loutere inschrijving van een som geld op de creditzijde van een rekening gelijkgesteld wordt met het

[217] P. VAN EECKE EN J. DUMORTIER, "De implementatie van het Europese verdrag cybercriminaliteit in de Belgische Wetgeving", *Computerr.*, 2003-2, 123-133.
[218] S. POLAKIEWIEZ, *De wet van 28 november 2000 inzake informaticacriminaliteit: aspecten van materieel strafrecht,* onuitg., Antwerpen,
[219] B. VAN ROY, *"*Wijzigingen aan de Belgische bepalingen inzake informaticacriminaliteit", *Computerr.*, 2006-6, 314; Art. 14 Wet 15 mei 2006 tot wijziging van de artikelen 259bis, 314bis, 504quater, 550bis en 550ter van het Strafwetboek, *B.S.*, 12 september 2006, 46332-46333.
[220] J. DUMORTIER, *ICT-Recht,* Leuven, 2009-2010, 185.

verkrijgen van een roerend goed.[221] Oplichting als dusdanig vereist dus geen materiële overhandiging. De loutere *wijziging* of *vervalsing* van gegevens binnen een informaticasysteem kunnen dan ook als een *listige kunstgreep* gedefinieerd worden.

Het dient opgemerkt dat het uiteindelijk de rechter zal zijn die zich over dergelijke interpretaties dient uit te spreken. Er kan wel reeds gewezen worden op de Franse en Nederlandse rechtspraak die het misdrijf van *oplichting* van toepassing verklaren op frauduleuze girale overschrijvingen.[222] Anderen menen dan weer dat art. 496 Sw. te veel onzekerheid laat om oplichting met behulp van informatica als dusdanig te vervolgen.[223]

Met de introductie in 2006 wou de wetgever dan ook duidelijkheid creëren omtrent de correcte kwalificatie van dergelijke handelingen. Het nieuwe art. 504quater Sw. bestraft zij die met een bedrieglijk opzet een onrechtmatig economisch voordeel voor zichzelf of voor een ander tracht te verwerven door middel van elektronische gegevens in te voeren, te wijzigen, te wissen of op enige technologische wijze de normale aanwending van gegevens in een informaticasysteem wil veranderen. Of zoals het in de memorie van toelichting wordt uitgelegd: artikel 496 Sw. viseert de bedrieglijke manoeuvres die het vertrouwen van *personen* schenden, terwijl art. 504quater Sw. ongeoorloofde manipulaties van data ten aanzien van een *machine* betreft.

Voorbeelden van informaticabedrog kunnen gevonden worden in het gebruik van een gestolen kredietkaart om geld af te halen, het invoeren van programma-instructies met het oog op een onrechtmatig financieel voordeel, op een onrechtmatige manier het krediet van een kredietkaart overschrijden, programma's in andermans systeem installeren of wijzigen om via die programma's regelmatig betalingen te ontvangen[224], enzovoort.

Artikel 504quater Sw. biedt aldus een antwoord op financiële identiteitsdiefstal, als het gevolg van skimming (geld afhalen met gestolen kredietkaart), phishing (zie *supra)*, et cetera.

---

[221] Cass. 16 mei 1979, Pas., 1979, I, 1081.
[222] Cass. fr. Crim., 17 oktober 1967, *Bull.,* n.252; Hoge Raad, 11 mei 1982
[223] B. SPRUYT, *Computers op de strafbank. Analyse van het fenomeen informaticacriminaliteit*: *nationale en internationale strafrechtelijke perspectieven*, Antwerpen, Kluwer, 1988, 330.
[224] Portaal Belgium.be, Informatie en diensten van de overheid, *Informaticabedrog,* http://www.belgium.be/nl/justitie/veiligheid/criminaliteit/computercriminaliteit/informaticabedrog/

De zuivere identiteitsdiefstal zal daarentegen weer veel moeilijker toepassing kunnen vinden.

De correctionele rechtbank van Dendermonde[225] en Aarlen[226] bevestigden bovenstaande visie. Zij kwalificeerden immers het misbruik van andermans bankkaart als informaticabedrog. Ook het Hof van Cassatie[227] bevestigde deze visie, zo wordt het met een gestolen bankkaart geld afhalen uit een automatische biljettenverdeler niet meer gekwalificeerd als diefstal met een valse sleutel, maar als informaticabedrog.[228]

AFDELING 3: COMPUTERINBRAAK (ART. 550BIS SW.)

§ 1. Hij die, terwijl hij weet dat hij daar toe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, wordt gestraft met gevangenisstraf van drie maanden tot een jaar en met geldboete van zesentwintig frank tot vijfentwintig duizend frank of met een van die straffen alleen.

Wanneer het misdrijf, bedoeld in het eerste lid, gepleegd wordt met bedrieglijk opzet, bedraagt de gevangenisstraf zes maanden tot twee jaar.

§ 2. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt, wordt gestraft met gevangenisstraf van zes maanden tot twee jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen.

§ 3. Hij die zich in een van de gevallen bedoeld in de §§ 1 en 2 bevindt en :

1° hetzij de gegevens die worden opgeslagen, verwerkt of overgedragen door middel van het informaticasysteem op enige manier overneemt;

2° hetzij enig gebruik maakt van een informaticasysteem van een derde of zich bedient van het informaticasysteem om toegang te verkrijgen tot een informaticasysteem van een derde;

---

[225] Corr. Dendermonde, 14 mei 2007, T. Strafr. 2007, afl. 6, noot E. BAYENS.
[226] Corr. Aarlen 09 mei 2005, onuitg, Studiedag "IT als voorwerp van … én hulpmiddel bij juridische geschillen", S&D seminarie, uiteenzetting Mr. S. DE MEULENAER.s
[227] Cass. 6 mei 2003, *R.A.B.G.,* 2004, 367, noot Y. VAN DEN BERGE, "Informaticabedrog".
[228] C. VAN DEN WYNGAERT, S. VANDROMME, *Strafrecht, strafprocesrecht en internationaal strafrecht in hoofdlijnen*, Maklu, Antwerpen, 2006, 88.

3° hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan het informaticasysteem of aan de gegevens die door middel van het informaticasysteem worden opgeslagen, verwerkt of overgedragen of aan een informaticasysteem van een derde of aan de gegevens die door middel van het laatstgenoemde informaticasysteem worden opgeslagen, verwerkt of overgedragen;

wordt gestraft met gevangenisstraf van een jaar tot drie jaar en met geldboete van zesentwintig frank tot vijftigduizend frank of met een van die straffen alleen.

§ 4. Poging tot het plegen van een van de misdrijven, bedoeld in §§ 1 en 2, wordt gestraft met dezelfde straffen.

§ 5. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem en waarmee de misdrijven, bedoeld in §§ 1 tot 4, gepleegd kunnen worden, opspoort, verzamelt, ter beschikking stelt, verspreidt of verhandelt, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen. (…)"

Art. 550bis, §1 Sw. handelt over *externe* hacking, terwijl §2 *interne* hacking beteugelt. Binnen het misdrijf '*hacking*' wordt aldus een onderscheid gemaakt naargelang of de persoon die zich toegang verschaft tot een informaticasysteem hier al dan niet toegangsbevoegdheid voor heeft. Heeft de persoon *geen* toegangsbevoegdheid, dan is slechts algemeen opzet vereist, en dient niet te worden aangetoond dat hij met bedrieglijk opzet handelde.[229] Personen die daarentegen wel toegangsbevoegdheid hebben en deze bijgevolg overschrijden, zijn enkel strafbaar voor zover er sprake is van een bedrieglijk opzet.

Dit heeft zijn implicaties voor het zogenaamde *white hat hacking*.[230] Dit zijn hackers die uitsluitend tot doel hebben gaten in de beveiliging op te sporen en deze bekend te maken aan het bedrijf of beveiligingsinstantie. De *kick* of de eer voldoet, in tegenstelling tot bij *crackers,* die er weldegelijk op uit zijn schade toe te brengen aan systemen of personen.

[229] C. VAN DEN WYNGAERT, *Strafrecht, strafprocesrecht en internationaal strafrecht in Hoofdlijnen,* Antwerpen, 2009, 323.
[230] S.D. NELSON, K. ISOM, J. SIMEK, *Information security for lawyers and law firms. Section of Science & Technology Law,* American Bar Association, 2006, 124 (total 424 P;)

Door een doorgedreven verkeerdelijke mediatisering worden *crackers* steevast met de term hackers bekleedt.

Nochtans mag het duidelijk zijn dat het *excuus* van de *white hat* op geen genade zal kunnen rekenen. Het argument dat de hacker geen kwade bedoelingen heeft en slechts de gebreken in de beveiliging van het informaticasysteem wilde aantonen, leidt dan ook niet tot straffeloosheid, gezien algemeen opzet volstaat bij *externe* hacking (de hacker beschikt immers niet over een toegangsbevoegdheid).[231] Een bijzonder opzet of een *dolus specialis* dient dus enkel te worden aangetoond bij *interne* hacking (met andere woorden, bij personen die wel over een toegangsbevoegdheid beschikken).

Een doorbraak van een softwarematige of hardwarematige beveiliging is niet vereist, en dit in tegenstelling tot andere landen waaronder Nederland, Duitsland en Denemarken die uitdrukkelijk kozen voor het doorbreken van een beveiliging als voorwaarden van strafbaarstelling.

Ook strafbaar zijn een aantal voorbereidingshandelingen, zoals het bezitten of produceren van enige instrumenten (bijvoorbeeld *hacking tools*, waar beginnende hackers, ook wel *scriptkiddies* genoemd, vaak gebruik van maken) om te kunnen inbreken in computersystemen. Er weze opgemerkt dat deze handelingen pas strafbaar zijn wanneer zij plaatsvinden *met* een bijzonder opzet (bedrog of oogmerk om te schaden).

De twee meest geciteerde zaken[232] in dit verband zijn ongetwijfeld de zaak *Bistel*[233] en *ReDaTtack*. Bij de Bistel zaak werd voor de eerste keer in België iemand veroordeeld voor een inbraak in een computersysteem. De bedenkelijke eer was weggelegd voor een voormalig medewerker van de toenmalige Eerste Minister die, samen met nog een andere persoon, binnengedrongen was in het Bistelsysteem via de toegangscode van de premier. Ze hadden er gegevens geraadpleegd, evenwel zonder deze te kopiëren, te wijzigen of te wissen. Er bestond toen geen aparte strafbaarstelling, waardoor de rechter zich moest baseren op de bestaande wetgeving. Dit leverde een uiterst hilarisch resultaat op, in de zin

[231] Corr. Eupen, 13 december 2003, *Computerrecht* 2004, 129 en Corr. Hasselt, 21 januari 2004, *Computerrecht* 2004, 130, noot H. GRAUX
[232] G. VERMEULEN, *Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen,* Antwerpen, Maklu, 2007, 436.
[233] Corr. Brussel, 8 november 1990, (te consulteren via http://cwisdb.kuleuven.be/pisa/nl/juridisch/crack.htm).

dat ze, naast nog twee andere gronden, veroordeeld werden voor *diefstal van computerenergie*. Meer ernstige gronden waren valsheid in geschrifte (zij gebruikten immers een paswoord of toegangscode die hen niet toebehoorde, met de verzwarende omstandigheid van braak, inklimming en valse sleutels tot gevolg) en verduistering van een aan de regie toevertrouwde mededeling. Weinig verwonderlijk dat de uitspraak door het Hof van Beroep te Brussel[234] werd hervormd.

Ten eerste werd de argumentatie rond *valsheid in geschrifte* door het Hof van Beroep niet gevolgd. Zij waren immers van oordeel dat *"het introduceren, zelfs op ongeoorloofde wijze, van een paswoord in het Bistelsysteem dergelijke vervalsing niet uitmaakt en dat het door de beklaagden gebezigde paswoord in de vorm van een elektronische code geen geschrift, meer bepaald geen grafisch tekensysteem uitmaakt in de zin van art. 193 e.v. Sw.".*

En wat met de inzetbaarheid van artikel 550bis Sw.? *Prima facie* lijkt het artikel weinig geschikt om identiteitsdiefstal aan te pakken. Nochtans biedt het een geschikte (secundaire) uitvalsbasis. Immers, van zodra men zich (onrechtmatig) toegang verschaft tot een informaticasysteem, valt men onder toepassing van het artikel. Vele vormen van identiteitsdiefstal in de ICT zullen indirect onder haar toepassing vallen, zoals bijvoorbeeld een inbraak op een informaticasysteem waarbij men software installeert die krediet- of bankkaart informatie logt, of gebruikersnamen en paswoorden (sociale media en e-mailtoepassingen) rooft met behulp van zogenaamde keyloggers. Het spreekt voor zich dat vele vormen van ICT-identiteitsdiefstal niet kunnen plaatsvinden zonder, minstens indirect, de toelaatbare grenzen te overschrijden. Deze hacking dient dan wel eerder als *middel* om de identiteitsgegevens te bemachtigen, niet als *doel* op zichzelf.

Veel zal afhangen van een extensieve dan wel restrictieve interpretatie van interne en externe hacking. Sowieso is het ten stelligste af te raden dit artikel als primaire grond aan te wenden bij identiteitsroof, doch eerder als bijkomende of subsidiaire strafbaarstelling.

AFDELING 4: DATAMANIPULATIE (ART. 550TER SW.)

1. Hij die, met het oogmerk om te schaden, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist, of met enig ander technologisch middel de

[234] Brussel, 24 juni 1991.

mogelijke aanwending van gegevens in een informaticasysteem verandert, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen.

§ 2. Hij die, ten gevolge van het plegen van een misdrijf bedoeld in § 1, schade berokkent aan gegevens in dit of enig ander informaticasysteem, wordt gestraft met gevangenisstraf van zes maanden tot vijf jaar en met geldboete van zesentwintig frank tot vijfenzeventigduizend frank of met een van die straffen alleen.
§ 3. Hij die, ten gevolge van het plegen van een van de misdrijven bedoeld in § 1, de correcte werking van dit of enig ander informaticasysteem geheel of gedeeltelijk belemmert, wordt gestraft met gevangenisstraf van een jaar tot vijf jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen.
§ 4. Hij die, met bedrieglijk opzet of met het oogmerk om te schaden, gegevens die worden opgeslagen, verwerkt of overgedragen door middel van een informaticasysteem, ontwerpt, ter beschikking stelt, verspreidt of verhandelt, terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren, wordt gestraft met gevangenisstraf van zes maanden tot drie jaar en met geldboete van zesentwintig frank tot honderdduizend frank of met een van die straffen alleen. (…)

Het opzettelijk beschadigen of vernielen van andermans goed wordt, vanzelfsprekend, onder vrijwel elke nationale wetgeving bestraft. Toch rijst er een probleem wanneer het gaat om vernietiging of beschadiging van *computergegevens*.[235] Gezien de traditionele wetsartikelen eerder betrekking hebben op tastbare voorwerpen, is een analoge toepassing naar immateriële zaken zoals elektronische gegevens moeilijk te verdedigen. Een veel gebruikt voorbeeld zijn virussen of *Trojaanse paarden* die in een informaticasysteem worden ingebracht.Om dit euvel te overkomen laste de wetgever in art. 550ter Sw. een nieuwe strafbaarstelling in, namelijk "*misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens die door middelen daarvan worden opgeslagen, verwerkt of opgeslagen"* ofwel kort "datamanipulatie".

[235] J. DUMORTIER, *ICT-Recht,* Leuven, Acco, 2009-2010, 185.

Het is een bijna vanzelfsprekendheid dat dit artikel, in veel gevallen omtrent identiteitsdiefstal in de ICT, zal kunnen worden ingeroepen. Gezien het gebruik van virussen, Trojaanse paarden, keyloggers, et cetera bijzonder populair is onder identiteitsdieven maken zij zich immers – subsidiair – schuldig aan datamanipulatie.

CONCLUSIE

We zagen in deze verhandeling allereerst de belangrijkheid van een correcte definitie, gezien het begrip identiteitsdiefstal een zeer grote lading dekt, en in sommige landen dan ook als een soort vangnet dient (denk maar aan de Verenigde Staten). Omdat er geen eensgezindheid bestaat rond het begrip in de rechtsleer werd gekozen voor een eigen definiëring, die doorheen het verdere onderzoek werd toegepast.

Vervolgens werd stilgestaan bij de vormen en toepassingsgevallen van identiteitsdiefstal. Van elektronische identiteitskaarten, skimming en banksystemen tot identity theft op sociale netwerksites en chatprogramma's. Ook de zeer recente vormen zoals draadloze identiteitsdiefstal (RFID en WiFi-liften) en *location-based applications* zijn niet onbehandeld gebleven.

Aandacht was er ook voor de huidige en toekomstige beveiligingsmechanismen. Waar nu eenvoudige paswoorden en in mindere mate encryptie gebruikt wordt, verwacht men in de toekomst een stijgend gebruik van biometrische gegevens. Deze evolutie kent veel kritiek in de rechtsleer, en voornamelijk het argument, dat eens deze biometrische gegevens gestolen worden er geen weg terug is, kan op veel bijval rekenen. Er is niettemin geen weg terug. Teveel overheden en private organisaties onderzoeken het nut van biometrische herkenningssystemen en een algemene, publieke implementatie daarvan kent haar voorzichtige intrede. Nochtans mag uit het eerdere relaas duidelijk blijken dat technologie en daarvan afgeleide beveiligingsmechanismen nooit helemaal onfeilbaar (zullen) zijn. Social engineering, om maar iets te zeggen, is nog steeds de meest succesvol toegepaste methode om iemands identiteit te ontvreemden. De nieuwsgierigheid, blijdschap of treurnis die dergelijke criminelen met valse boodschappen kunnen uitlokken, staat bijna garant voor een vrijwillige overgave van alle relevante identiteitsgegevens. Men dient zich terdege te realiseren dat eenieder, hoe goed beveiligd ook, hiervoor waakzaam dient te zijn. De Verenigde Staten en het Verenigd Koninkrijk, waar het probleem uiteraard een andere dimensie kent, trekken alvast zeer kenbaar de kaart van publieke bewustwording. Of het nu de slagkracht of de onwil betreft, feit is dat Europa tot dusver geen vergelijkbare campagnes ontwikkeld heeft. De nood is nochtans hoog.

In een vierde deel werd gewezen op de hoge kosten die het misdrijf van identiteitsdiefstal met zich meebrengen. Overvloedig cijfermateriaal was beschikbaar in de Verenigde Staten, waar identiteitsdiefstal ondertussen onverbiddelijk naar de top der misdrijven schiet. In een recent onderzoek werd bovendien de risicogroep kenbaar, de zogenaamde *millenials* of *Generatie Y*, de jongeren tussen 18 en 24 jaar. Verwonderlijk? Allesbehalve. Jongeren zijn verzot op nieuwe technologieën of functies (denk ook aan het nieuw opgekomen fenomeen van *location-sharing*) en zijn er bovendien mee opgegroeid, waardor de vertrouwdheid er mee niet gering te noemen is. Deze drang of aangeboren nieuwsgierigheid naar de mogelijkheden van nieuwe technologieën kent vanzelfsprekend de donkere keerzijde van het verlies van privacy. Hoe meer het wereldwijde web evolueert naar een *ruimte* waarin *delen en samenwerken* centraal staat, hoe meer informatiehonger we ontmoeten bij nieuwe toepassingen, (sociale netwerk-)sites, en andere platformen. De kennis en de bewustwording rond de gevaren – die al te vaak onderbelicht blijven – is een essentiële stap in een volwassen ICT-gebruik.

In het vijfde deel werd een rechtsvergelijkende studie ondernomen, die zich focuste – gezien de omvang van het probleem in die landen – op de Verenigde Staten en het Verenigd Koninkrijk. We merkten op dat in de V.S. een aparte strafbaarstelling, gecreëerd door de *Identity theft Act*, bestaat. In het Verenigd Koninkrijk bestaat eveneens een expliciete wettelijke regeling, maar tot een aparte strafbaarstelling is het vooralsnog niet gekomen. Vervolgens werd gepoogd een evaluatie te maken van de bestaande Belgische strafwetartikelen rond informaticacriminaliteit, en hun eventuele inzetbaarheid op het vlak van identiteitsdiefstal. De resultaten waren her en der bemoedigend, zo kunnen de meeste vormen van financiële identiteitsdiefstallen aangepakt worden via het misdrijf van *informaticabedrog*. Ook *valsheid in informatica* kan geldig worden ingeroepen bij het misbruiken of vervalsen van iemands eID, belangrijke (e-)documenten of zelfs bij skimming.

Dan rest ons enkel nog het behandelen van de kernvraag van dit onderzoek: bestaat er *hic et nunc* een noodzaak aan een nieuwe Europese of Belgische regelgeving?

Zoals enigszins te verwachten valt hierop geen eenduidig antwoord te geven. In het laatste deel is duidelijk geworden dat in België verschillende artikelen rond informaticacriminaliteit bestaan die bij een eventuele identiteitsdiefstal (afhankelijk van de precieze

omstandigheden) kunnen worden ingeroepen. De nood aan een aparte regelgeving lijkt op deze manier minder aanwezig. Doch de complexiteit van het gecombineerd aanwenden van wetsartikels, zou een aparte strafbaarstelling kunnen rechtvaardigen. Daarvoor zouden de criteria die in dit werk werden vooropgesteld eventueel een optie kunnen bieden.

Ook op Europees vlak gaf men reeds een aantal keer een sterk signaal naar het groeiende fenomeen van informaticacriminaliteit en in het bijzonder de stijgende vrees voor identiteitsdiefstal, niet in het minst gebaseerd op de huidige toestand in de V.S. en het V.K. Echte specifieke regelgeving of juridische maatregelen zijn er, ondanks de geuite vrees, evenwel niet gekomen.

Men kan bovendien moeilijk voor elk nieuw ICT fenomeen een aparte strafbaarstelling voorzien. Niet dat dit op zich per se een slecht idee zou zijn, maar het immobilisme van de wetgever verhindert dergelijke redenering. Men is dus noodgedwongen aangewezen op een (toegelaten) teleologische interpretatie van de strafwet. Deze interpretatie is een noodzaak, gezien men veilig mag aannemen dat de wetgever bij de creatie van de vier informaticamisdrijven niet echt op de hoogte was van het fenomeen (online) identiteitsdiefstal. Nochtans, zoals eerder veelvoudig gesteld, dient men principieel op te letten met dergelijke uitbreiding van de strafwet door middel van interpretatie. Niet alleen is een te ruime interpretatie (bijvoorbeeld naar analogie) gewoonweg verboden, ook teleologische interpretatie levert onmiskenbaar nadelen en gevaren op.

Bovenstaande argumentatie, en het feit dat in de toekomst steeds meer complexere vormen van identiteitsdiefstal zullen ontstaan (zoals heden bijvoorbeeld blijkt bij sociale netwerken, RFID, location-based services, …), in gedachte houdend, lijkt een aparte strafbaarstelling opeens minder onnuttig. Dergelijke aparte strafbaarstelling komt alleszins de rechtszekerheid en een effectief vervolgingsbeleid ten goede. Tegenstanders zullen geneigd zijn op te merken dat men niet *zomaar* voor elk nieuw fenomeen een nieuw artikel kan creëren (wat vanzelfsprekend correct is), evenwel is identiteitsdiefstal ondertussen al voldoende volwassen geworden, zodat zij het stadium van louter *fenomeen* al ver gepasseerd is. Bovendien kan maar moeilijk geargumenteerd worden dat een nieuw artikel, handelend over identiteitsdiefstal in de ICT, als te eng zal worden beschouwd. Een correcte definiëring van het wetsartikel kan immers tientallen vormen omvatten. Dergelijk

wetgevend initiatief wordt uiteraard het best gecoördineerd op Europees niveau, met de mogelijkheid tot invulling voor de eigen specifieke nationale kenmerken en problemen.

Maar misschien veel belangrijker nog dan een aparte strafbaarstelling, is de algemene bewustwording van de bevolking, zowel op nationaal als op Europees vlak.

Zowel overheden, bedrijven als particulieren zijn zich onvoldoende bewust van de dreiging die uitgaat van deze nieuwe vormen van identiteitsdiefstal, en de enorme impact die dergelijk misdrijf op een persoon zelf, en *a fortiori* op de economie en het staatsbeleid kan hebben. Het is tijd voor een ernstige sensibilisering bij particulieren en bedrijven, en een geïnformeerd vervolgingsbeleid bij de parketten.

Er wordt vanuit Europa met een mengeling van vrees en afschuw gekeken naar de cijfers die de Verenigde Staten en het Verenigd Koninkrijk neerleggen op vlak van identiteitsdiefstal. Willen we, ongeacht de verschillende stelsels, vermijden dat dergelijke cijfers bewaarheid worden op het Europese vasteland, dan kan een reactie niet langer uitblijven. De tijd, is nu.

- Matthias Dobbelaere.

BIBLIOGRAFIE

1. REGELGEVING

a. INTERNATIONALE REGELGEVING

- Cybercrime-Verdrag van 23 november 2001, (te consulteren via http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).
- Richtlijn 1999/93/EG van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen.
- Richtlijn 2009/136/EG, (te consulteren via http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0136:NL:NOT).
- Mededeling van de Europese Commissie van 22 mei 2007, "Communication from the Commission to the European Parliament, the council and the committee of the regions. Towards a general policy on the fight against cyber crime.", COM/2007/267 (te consulteren via http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf).
- Identity theft and Assumption Deterrence Act, 18. U.S.C. 1028, Pub. Law 105-138, 112 Stat. 3007.
- Executive Order 9397, "Numbering system for federal accounts relating to individual persons", 26 CFR, Cum. Supp., 402.502.
- Executive Order 13402 – Strengthening Federal Efforts to Protect Against Identity Theft, 2006.
- Nev. Rev. State § 205.465
- Fla. Stat. Ann. § 817.568
- Fraud Act 2006, (te consulteren via http://www.opsi.gov.uk/acts/acts2006/ukpga_20060035_en_1).
- Identity Cards Act 2006 (te consulteren via www.opsi.gov.uk/ACTS/acts2006/20060015.htm).
- Identity Cards Bill, Explanatory notes, (te consulteren via http://www.publications.parliament.uk/pa/cm200405/cmbills/008/2005008.pdf) en http://www.homeoffice.gov.uk/docs3/identitycardsconsult.pdf

b. BELGISCH RECHT

- Wet Informaticacriminaliteit, Wet 28 november 2000 inzake informaticacriminaliteit, *B.S.*, 3 februari 2001.
- Wet van 17 juli 2002 betreffende de transacties uitgevoerd met instrumenten voor de elektronische overmaking van geldmiddelen, BS 17 augustus 2002, inwerkingtreding 1 februari 2003, (te consulteren via http://www.juridat.be/cgi_loi/loi_N.pl?cn=2002071732).
- Wet van 25 maart 2003 tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, (te consulteren op http://www.juridat.be/cgi_loi/loi_N.pl?cn=2003032530).
- Koninklijk besluit van 25 maart 2003 houdende overgangsmaatregelen in verband met de elektronische identiteitskaart, (te consulteren op http://www.juridat.be/cgi_loi/loi_a.pl?language=nl&caller=list&cn=2003032532&la=n&fromtab=wet&sql=dt='koninklijk%20besluit'&tri=dd+as+rank&rech=1&numero=1).
- De bescherming van het privé-leven en de persoonlijkheid., Hoofdstuk IV, Controle op de gegevens behandeld met elektronische of andere middelen, Senaat, Zitting 1971-1972, document 142.
- COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, advies uit eigen beweging over het verwerken van biometrische gegevens in het raam van authenticatie van personen, 9 april 2008, (te consulteren via http://www.privacycommission.be/nl/docs/Commission/2008/advies_17_2008.pdf).

2. RECHTSPRAAK

a. INTERNATIONALE RECHTSPRAAK

- IGNACIO CARLOS FLORES-FIGUEROA, Petitioner v. UNITED STATES, No. 08-108, U.S. Supreme Court, 2009, (te consulteren via http://www.lexisone.com/lx1/caselaw/freecaselaw?action=FCLRetrieveCaseDetail&caseID=1&format=FULL&resultHandle=0db4f3d00e65c7a64f23ea5ff7cba8c2&pageLimit=10&xmlgTotalCount=4&combinedSearchTerm=%22Identity+theft%22&juriName=U.%20S.%20Supreme%20Court&sourceFile=GENFED;USLED).
- STATE V. LEYDA, STATE of Washington, Respondent, v. Steven Edward LEYDA, Petitioner, No. 75866-2, 2006., Washington Supreme Court (te consulteren via http://caselaw.findlaw.com/wa-supreme-court/1220663.html).
- U.S. v. GONZALEZ, No. 1:08-cr-10223, U.S. District Court, District of Massachusetts (Boston).
- Cass. fr. Crim., 17 oktober 1967, *Bull.,* n.252; Hoge Raad, 11 mei 1982
- Rechtbank Amsterdam (meervoudige strafkamer), 11 september 2008, http://www.boek9.nl.
- Bundesgerichtshof Karlsruhe, Haftung für unzureichend gesicherten WLAN-Anschluss, (te consulteren via http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2010&Sort=3&nr=51934&pos=0&anz=101).

b. BELGISCHE RECHTSPRAAK

- Cass. 16 mei 1979, Pas., 1979, I, 1081.
- Cass. 6 mei 2003, *R.A.B.G.,* 2004, 367, noot Y. VAN DEN BERGE, "Informaticabedrog".
- Brussel, 24 juni 1991.
- Corr. Brussel, 8 november 1990, (te consulteren via http://cwisdb.kuleuven.be/pisa/nl/juridisch/crack.htm).

- Corr. Eupen, 13 december 2003, *Computerrecht* 2004, 129 en Corr. Hasselt, 21 januari 2004, *Computerrecht* 2004, 130, noot H. GRAUX
- Corr. Aarlen 09 mei 2005, onuitg, Studiedag "IT als voorwerp van … én hulpmiddel bij juridische geschillen", S&D seminarie, uiteenzetting Mr. S. DE MEULENAER.
- Corr. Dendermonde 28 november 2005, *N.J.W*,. 2006, afl. 138, 229-23, noot J. DUMORTIER.
- Corr. Dendermonde, 14 mei 2007, *T. Strafr.*, 2007, afl. 6, noot E. BAYENS

3. RECHTSLEER

- ABA SECTION OF ANTITRUST LAW, *Antitrust Law Developments*, 6th edition, ABA Publishing, U.S., 2007.
- ARTICLE 29 DATA PROTECTION WORKING PARTY, "European data protection group faults Facebook for privacy setting", *Press Release*, Brussel, 12 mei 2010, (te consulteren via http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_12_05_10_en.pdf).
- BARTY, S. EN CARNELL, P., *Fraud Bill offers new protection against technology abuse*, World Internet Law Report, 2005, 20-21.
- BALOUN, K.M., *Inside Facebook: Life, Work and Visions of Greatness*, onuitg., 2006.
- BEECKMANS, R., "Politioneel en gerechtelijk onderzoek inzake skimming van bankkaarten: casusbespreking: opportuniteiten, noodzaak en risico van een multidisciplinair aanpak in functie van de bewijsgaring", *onuitg.*,Leuven, 2004.
- BENNET, C.J., LYON, D., "Playing the Identity Card, surveillance, security and identification in global perspective", 2008, 1.
- BERGHEL, H., *Identity Theft, Social Security Numbers, and the Web,* Communications of the ACM, 02/2002 vol. 43 nr. 2.
- BEST, R., MANZ, W., *Federal identity theft law: major enactments of the 108th Congress : a legislative history of the Fair and Accurate Credit Transactions Act and Identity Theft Penalty Enhancement Act, Volume 9*, Hein, U.S., 2005.

- BEVERLEY, J., *Protect your digital privacy – Survival skills for the Information Age*, U.S., 2002, 377 (totaal: 652) 720 ILCS 5/16G.
- BUNTING, S. , *EnCase Computer Forensics,* Indiana, Wiley, 2008, 360.
- CLAEYS, E., *Legaliteit en rechtsvinding in het Strafrecht. Een grondslagentheoretische benadering*, Leuven, 2003, 15.
- CORMEN, T., LEISERSON C.E., RIVEST, R. , STEIN, C., *Introduction to Algorithms*, Massachusetts, MIT Press, 2001, 245.
- DE VRIES E.A., *Identiteitsfraude: een afbakening*, Den Haag, Boom Juridische uitgevers, 2007.
- DENLOF, J., BOUCAR, A., REYNDERS, D., Fraude d'identité, le crime du future?", Brussel, *Politeia*, 2005, 116.
- DIXON, P. ,"MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You", *World Privacy Forum Series,* 2006 (te consulteren op http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf).
- DUMORTIER, J. , VAN OUDENHOVE B., EN VAN EECKE, P., "De nieuwe Belgische wetgeving inzake informaticacriminaliteit", *Vigiles*, 2001-2, 44.
- DUMORTIER, J., "eID en de paradoks van het rijksregisternummer", *Business ICT,* 2006, (te consulteren via https://www.law.kuleuven.be/icri/publications/655Column_BusinessICT_06_eID.pdf).
- DUMORTIER, J., EN ROBBEN, F., "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België", *Computerr.,* 2009-37, 52.
- DUMORTIER, J., "Recente ontwikkelingen in het privacyrecht 2008-2009", *Recht in beweging 17de VRG-Alumni dag,* 2010, 161.
- DUMORTIER, J., ICT-Recht, Leuven, Acco, 2009-2010, 185.
- ERICKSON, J. , *Hacking: the art of exploitation*, San Francisco, No Starch Press, 2003, 214.
- EVANS, A., "Software sniffs out criminals by the shape of their nose", *University of Bath*, 2010, (te consulteren via http://www.bath.ac.uk/news/2010/03/02/nose-recognition/).

- FISHENDEN, J., "eID: Identity Management in an Online World", *Microsoft UK*, London (te consulteren via http://ntouk.com/papers/eID.doc).
- ITEANU, O., "Usurpation d'identité: la loi ou la technique pour se protéger?", *Journal de Net*, 2004.
- JÖRG, N.D., KELK, C., *Strafrecht met mate*, Amsterdam, 2001, 33.
- GARDNER, J., ANDERSON,T. M., *Criminal Law*, U.S., 2006, 368.
- GRIJPINK, J., "Identiteitsfraude als uitdaging voor de rechtstaat", *Privacy & Informatie*, 6e jaargang, 2003.
- JOHNSON, M., ROGERS, K.M., *The Fraud Act 2006: The E-Crime Prosecutor's champion or the creator of a new inchoate offence?*, 2007, 1.
- KINDT, E. EN SZAFRAN, E., "Informaticacriminaliteit: Nullum crimen, nulla poena sine lege? Een beknopt overzicht van de evolutie in rechtspraak en wetgeving", noot onder Corr. Gent 11 december 2000, inz. ReDaTack, *Computerr.*, 2001.
- KINDT, E., "Algemene invoering van de elektronische identiteitskaart in België", *Computerr.,* 2005, 238.
- KINDT, E. EN DUMORTIER, J., "Biometrie als herkenning- of identificatiemiddel? Enkele juridische beschouwingen", *Computerr.,* 2008-132, 185.
- KINDT, E., "Country report for 'Belgium' in D12.7: Identity-related crime: Big problem or Big Hype?", *FIDIS,* 2008, 12-29 (te consulteren via http://www.fidis.net/fileadmin/fidis/deliverables/5th_workplan/fidis-wp12-del12.7_identity_crime_in_Europe.pdf).
- KINDT, E. EN VAN DER HOF, S., "Identiteitsgegevens en –beheer in een digitale omgeving: een juridische benadering", *Computerr,* 2009-36, 44.
- KLENK, A., EUNICKE, C. , KINKELIN, H. , CARLE, G. "Preventing Identity Theft with Electronic Identity Cards and the Trusted Platform Module", *EUROSEC*, 2009.
- LODDER, A.R., DUMORTIER, J. EN BOL, S.H., "Het recht rond elektronische handtekeningen", *Informatica en recht,* 2005.
- KOTLER, P., ARMSTRONG, G. , *Principles of Marketing*, New Jersey, Pearson Education, 2009, 151.
- LITAN, A. ,*Gartner Phishing Attack Victims Likely Targets for Identity Theft*, Gartner, 2004, 2.

- MCGUIRE, M., *Hypercrime – The New Geometry of Harm,* GlassHouse, Oxford, 2007, 375.
- MILLER, R.L., jentz, g.a., *Fundamentals of Business Law – Summarized Cases*, U.S., 2010, 143.
- MITNICK, K.D. , *The art of deception: controlling the human element of security,* Indiana, Wiley, 2003.
- MOITRA, S.D., *Developing Policies for Cybercrime, European Journal of Crime, Criminal Law and Criminal Justice*, 2005, 435-464.
- NELSON, S.D., ISOM, K., SIMEK J., *Information security for lawyers and law firms*, Section of Science & Technology Law, American Bar Association, 2006, 124.
- O'BRIEN, "Information Security Consultant Pleads Guilty to Federal Wiretapping and Identity Theft Charges", *U.S. Departement of Justice*, 2008, (te consulteren via http://losangeles.fbi.gov/dojpressrel/pressrel08/la041608usa.htm).
- ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Online Identity Theft,* U.K., 2009, 52.
- POLAKIEWIEZ, S., *De wet van 28 november 2000 inzake informaticacriminaliteit: aspecten van materieel strafrecht*, onuitg., Antwerpen.
- PAGET, F., *Identity Theft: White Paper*, Santa Clara, McAfee, 2006, (te consulteren via http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf).
- PRINT, J.E.J., EN VAN DER MEULEN, N.S., *Identiteitsdiefstal: lessen uit het buitenland*, Justitiële verkenningen, jrg 32, nr. 7, 2006, 13.
- R.C.P. MARBUS, S. FENNEL-VAN ESCH EN A.P.C. ROOSENDAAL, "Identiteit en openbaarheid in sociale online-omgevingen", *Computerr.,* 2009-39, 64.
- SAVIRIMUTHU A. EN SAVIRIMUTHU J., *Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective*, Scripted, 2007, (te consulteren op http://www.law.ed.ac.uk/ahrc/script-ed/vol4-4/savirimuthu.asp).
- SCHELLKENS, M. , KASPERSEN, R., HOFMAN, A., VERBEEK, J., VAN DER NET, C., TEMPELMAN, J., *Strafbare feiten op de elektronische snelweg, vertrouwelijkheid*

van e-mail, netwerkzoeking in theorie en praktijk, IT&R 13 Nationaal programma informatietechnologie en recht, eJure.

- D. SCHNEIDER, *Phishing, Pharming und Identitätsdiebstahl – von Postbank bis Paypal. Informationstechnische Grundlagen und strafrechtliche Beurteilung der Internetkriminalität,* onuitg., Waldkirch, 2007
- SCHWABACH, A. , *The Law – Technology, Society and Compromises*, U.S., 2006, 140.
- SPRUYT, B., *Computers op de strafbank. Analyse van het fenomeen informaticacriminaliteit*: *nationale en internationale strafrechtelijke perspectieven*, Antwerpen, Kluwer, 1988, 330.
- THE LAW COMMISSION FRAUD (Report No. 276), juli 2002, (te consulteren via http://www.lawcom.gov.uk/lc_reports.htm#2002).
- TULKENS, F., VAN DE KERCHOVE, M., *Introduction au droit pénal. Aspects juridiques et criminoliques,* Diegem, 1997, 184.
- VAN DEN WYNGAERT, C., VANDROMME, S., *Strafrecht, strafprocesrecht en internationaal strafrecht in hoofdlijnen*, Maklu, Antwerpen, 2006, 89.
- VAN DER MEULEN, N.S., *Achter de schermen: de ervaringen van slachtoffers van identiteitsroof,* Justitiële verkenningen, jrg. 32, nr. 7, 2006.
- VAN DER MEULEN, N.S., "Identiteitsfraude: de eerste stap, nu nog de rest", *Computerr.*, 2009, 38.
- VAN EECKE P. EN DUMORTIER, J., "De implementatie van het Europese verdrag cybercriminaliteit in de Belgische Wetgeving", *Computerr.*, 2003-2, 123-133.
- VAN HOOGENBEMT, M., "Externe hacking: analyse van recente rechtspraak", *Vigiles*, 2009-3, 136.
- VAN ROY, B. "Wijzigingen aan de Belgische bepalingen inzake informaticacriminaliteit", *Computerr.*, 2006-6, 314; Art. 14 Wet 15 mei 2006 tot wijziging van de artikelen 259bis, 314bis, 504quater, 550bis en 550ter van het Strafwetboek, *B.S.*, 12 september 2006, 46332-46333.VERMEULEN, G., *Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen*, Antwerpen, 2007, 434.
- WELLS, J.T., *Principles of fraud examination*, Wiley, New Jersey, 2005.

- WHITLEY, D.E., "Identity cards - report by the Science and Technology Select Committee", August 2006, *Londen School of Economics and Political Science,* 2006, (te consulteren via http://www2.lse.ac.uk/newsAndMedia/news/archives/2006/ID_Cards_4Aug.aspx).
- X., "Chat Rooms Becoming Breeding Grounds for ID Theft", *Identity Theft 911*, 2010, (te consulteren via http://identitytheft911.org/alerts/alert.ext?sp=672).
- X., "United States and The Netherlands Launch Air Travel Partnership to Streamline Border Processing", *Homeland Security, 2009*, (te consulteren via http://www.dhs.gov/ynews/releases/pr_1240501085368.shtm).
- X., "Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back", *Javelin Strategy & Research*, 2010, (te consulteren via https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail).

4. ANDERE BRONNEN

- ARNFIELD, R., "Here comes EMV: the world is watching in the new year as Europe takes a major step on its road to a chip-based payment system. Will the U.S. be left behind?", *HighBeam*, 2005, (te consulteren via http://www.bcc.be/index/nl_BE/5088994/5094013/Waarvoor-dient-de-chip.htm).
- BARNES, E., "Cabinet split over plan to fast-track ID cards", *ScotlandonSunday,* 2004, (te consulteren via http://scotlandonsunday.scotsman.com/identitycards/Cabinet-split-over-plan-to.2513463.jp)
- BRANIGAN, T., "Last minute concessions ease passage of identity cards bill", *Guardian*, 2005, (te consulteren via http://www.guardian.co.uk/politics/2005/oct/19/idcards.immigrationpolicy).
-

- CHAMPEAU, G., "La loi Loppsi reportée sine die par le Sénat (MAJ)", *Numerama*, 2010, (te consulteren via http://www.numerama.com/magazine/15670-la-loi-loppsi-reportee-sine-dine-par-le-senat.html).
- CROSSMAN, G., "Liberty's response to the Home Office Consultation on the Draft Identity Cards Bill", *Liberty (Protecting Human Rights),* 2004, (te consulteren via http://www.liberty-human-rights.org.uk/pdfs/policy04/id-card-draft-bill-response.pdf).
- DE MOOR, W., "Details en foto's NS-skimapparaat gepubliceerd", *Tweakers.net,* 2008, (te consulteren via http://tweakers.net/nieuws/57329/details-en-fotos-ns-skimapparaat-gepubliceerd.html).
- DE NEEVE, M., "Vingerafdrukbetaalsysteem AH gekraakt", *Tweakers.*net, 2008, (te consulteren via http://tweakers.net/nieuws/54263/vingerafdrukbetaalsysteem-ah-gekraakt.html).
- DE WINTER, B., "Onderzoeker kraakt vingerafdrukbetaling Albert Heijn", *Webwereld*, 2008, (te consulteren via http://webwereld.nl/articles/51680/onderzoeker-kraakt-vingerafdrukbetaling-albert-heijn.html).
- FEDERALE GERECHTELIJKE POLITIE, Directie economische en financiële criminaliteit, *Jaarverslag 2008,* (te consulteren via http://www.polfed-fedpol.be/pub/rapport_activites/pdf/2008_ecofin_nl.pdf).
- FEDERALE POLITIE, Politiële Criminaliteitsstatistieken, 2000 – Kwartaal 3 2009, (te consulteren via http://www.polfed-fedpol.be/crim/crim_statistieken/2009_trim3/pdf/nationaal/rapport_2009_trim3_nat_Belgie_nl.pdf).
- ITEANU, O.,"Usurpation d'identité: la loi ou la technique pour se protéger?", *Journal de Net*, 2004.
- KLEIN, A., "18- to 24-year-olds most at risk for ID theft, survey finds", *The Washington Post*, 2010, (te consulteren via http://www.washingtonpost.com/wp-dyn/content/article/2010/03/16/AR2010031604209.html).

- KLEINMAN, Z., "How online life distorts privacy rights for all", *BBC* News, 2010, (te consulteren via http://news.bbc.co.uk/2/hi/technology/8446649.stm).
- MCGUIRE, D., "Bush signs identity theft bill", *Washington Post Online*, 2004, (te consulteren via www.washingtonpost.com/wp-dyn/articles/A51595-2004Jul15.html).
- MCNAMARA, P., "Facebook blocks 'Web 2.0 Suicide Machine", *Networkworld,* 2010, (te consulteren via http://www.networkworld.com/community/node/49470).
- MILLS, E., "FBController allows for hijacking of Facebook accounts", *CNET,* 2009, (te consulteren via http://news.cnet.com/8301-1009_3-10234720-83.html).
- MOLENAAR, P., "Website FOK gehackt en onder vuur van ddos-aanval", *Tweakers.*net, 2009, (te consulteren via http://tweakers.net/nieuws/62003/website-fok-gehackt-en-onder-vuur-van-ddos-aanval.html).
- MORRIS, N., "Blunkett giving 'high priority' to compulsory ID cards ", *The Independent,* 2001 (te consulteren via http://www.independent.co.uk/news/uk/politics/blunkett-giving-high-priority-to-compulsory-id-cards-670573.html).
- PRUYN, R., "Nederlandse supermarkt test betalen met vingerafdruk", *ZDNet België,* 2008, (te consulteren via http://www.zdnet.be/news/86928/nederlandse-supermarkt-test-betalen-met-vingerafdruk/).
- REIJERMAN, D.,"NS gaat kaartautomaten aanpassen om skimmen tegen te gaan", *Tweakers.net,* 2008, (te consulteren via http://tweakers.net/nieuws/57282/ns-gaat-kaartautomaten-aanpassen-om-skimmen-tegen-te-gaan.html).
- SCHEEPERS, J., "Irisscan op Schiphol volgend jaar voor iedereen", *ZDNet België,* 2008, (te consulteren via http://www.zdnet.be/news/88510/-irisscan-op-schiphol-volgend-jaar-voor-iedereen/).

- SCHEEPERS, J., "Gratis tool om Facebook-accounts te kapen", *ZDNet België,* 2009, (te consulteren via http://www.zdnet.be/news/102109/gratis-tool-om-facebook-accounts-te-kapen/).
- SCHREURS, W., "Ik ben user 712. Recht op toegang tot persoonsgegevens en op mededeling van de logica van geautomatiseerde verwerking", *Computerr.,* 2009-40, 68.
- SCHNEIER, B.,"Why Technology Won't Prevent Identity Theft", *Wall Street Journal*, 2009, (te consulteren via http://online.wsj.com/article/SB123125633551557469.html).
- TEN HOUTEN, M., "De pinpas is hopeloos verouderd", *SYNC.*nl, 2007, (te consulteren via http://sync.nl/de-pinpas-is-hopeloos-verouderd/2).
- TRAVIS, A., "Clarke pledges ID card data will be limited to information on passports", *Guardian*, 2005, (te consulteren via http://www.guardian.co.uk/politics/2005/oct/18/humanrights.idcards).
- TRAVIS, A.,"Cabinet leak hits Blunkett's ID card plan", *Guardian*, 2003, (te consulteren via http://www.guardian.co.uk/politics/2003/oct/13/freedomofinformation.humanrights).
- VAN DER MADE, M., "Waar je bent, is de nieuwste mobiele hype", *Z24,* 2010 (te consulteren via http://www.z24.nl/bedrijven/it_telecom/artikel_129640.z24/Waar_je_bent_is_de_nieuwste_mobiele_hype.html).
- VAN LEEMPUTTEN, P., "Netlog haalt 50 miljoen leden", *ZDNet België,* 2009, (te consulteren via http://www.zdnet.be/news/106217/netlog-haalt-50-miljoen-leden/).
- VAN LEEMPUTTEN, P., "Hasseltse bankkaarten gekopieerd", *ZDNet België,* 2009, (te consulteren via http://www.zdnet.be/news/102048/hasseltse-bankkaarten-gekopieerd/).
- VAN NIEUWERBURGH, S., "Facebook laat zien waar je vrienden zijn", *ZDNet België*, 2010, (te consulteren via http://www.zdnet.be/news/113665/facebook-laat-zien-waar-je-vrienden-zijn/).

- VAN OOST, J., "Rabobank gaat eID gebruiken", *ZDNet België,* 2009, (te consulteren via http://www.zdnet.be/news/97562/rabobank-gaat-eid-gebruiken/).
- VAN NIEWERBURGH, S., "EU pakt privacyinstellingen Facebook aan", *ZDNet België,* 2010, (te consulteren op http://www.zdnet.be/news/112632/eu-pakt-privacyinstellingen-facebook-aan/).
- VANDERAERT, J., Werken met het Windows-register, Culemborg, Centraal Boekhuis, 2005.
- VANSTEENKISTE, I., "Tips voor veilige en sterke wachtwoorden", *MindWell* Megazine, 2010, (te consulteren via http://www.mindwell.be/management_workplace/tips-voor-veilige-en-sterke-wachtwoorden/).
- VISTERIN, W., "Rabobank.be is internetbank pur sang", *ZDNet België*, 2003, (te consulteren via http://www.zdnet.be/itprofessional/32222/rabobank-be-is-internetbank-pur-sang/X., "Kids-ID groter succes dan verwacht", *De Standaard,* 2010, http://www.deredactie.be/cm/vrtnieuws/binnenland/1.738398).
- WEYTJENS, E., "eID", *Certipost,* 2003 (te consulteren op http://www.senate.be/event/05-06-03-ict/0603-01-nl/Weytjens-nl.ppt).
- X., "Een draadloos netwerk beveiligen", *BIPT*, (te consulteren via http://www.bipt.be/nl/520/ShowContent/2885/Draadloze_netwerken/Een_draadloos_netwerk_beveiligen.aspx).
- X., "Compulsory ID cards 'ruled out', *BBC News*, 2001, (te consulteren via http://news.bbc.co.uk/1/hi/uk_politics/1572026.stm)
- X., "Blunkett backs ID card plan", *BBC News,* 2002, (te consulteren via http://news.bbc.co.uk/2/hi/uk_news/politics/2084860.stm).
- X., "Daily Telegraph letters", *Telegraph*, 2005, (te consulteren via http://www.telegraph.co.uk/comment/letters/3615768/Daily-Telegraph-letters.html).
- X., "Big Brother's here now", *EDP24,* 2005, (te consulteren via http://new.edp24.co.uk/content/news/story.aspx?brand=EDPOnline&categor

y=News&tBrand=edponline&tCategory=news&itemid=NOED03%20Sep%202005%2010%3A09%3A19%3A520).

- X., "The Get Safe Online Report", 2006, (te consulteren via http://www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf).
- X., "ID theft 'costs UK £1.7bn a year", *BBC* News, 2006, (te consulteren via http://news.bbc.co.uk/2/hi/uk_news/politics/4672622.stm).
- X., "Government drops iris scan plan", *The Register*, 2007, (te consulteren via http://www.theregister.co.uk/2007/01/09/government_drops_iris_scans_for_id_cards).
- X., "ADT pakt het skimmen van passen aan ", *Beveiligingsnieuws*, 2007, (te consulteren via http://www.beveiligingnieuws.nl/beveiliging/6546/ADT_pakt_het_skimmen_van_passen_aan.html).
- X., "Jongenman kraakt internet buur", *De Standaard,* 2008, (te consulteren via http://www.standaard.be/artikel/detail.aspx?artikelid=9G1QCRSV).
- X., "Draadloze netwerken slecht beveiligd", *Dimension Data,* 2008, (te consulteren via *http://www.dimensiondata.com/NR/rdonlyres/0586CF39-2C12-4077-9CD6-4D59280F7FE4/9668/Draadloze_privenetwerken_slecht_beveiligd1.pdf).*
- X., "Jongeman schuldig aan surfen op andermans netwerk", *De Standaard*, 2008, (te consulteren via http://www.standaard.be/artikel/detail.aspx?artikelid=DMF14112008_028).
-
- X. "Identity Cards Act 2006", *Guardian*, 2009, (te consulteren via http://www.guardian.co.uk/commentisfree/libertycentral/2009/jan/15/identity-cards-act).
- X., "Facebook 'Friend' Suspected in Burglary", *CBS News*, 2010, (te consulteren via http://www.cbsnews.com/stories/2010/03/25/earlyshow/main6331796.shtml).

- X., “UK has first coalition government since 1945”, *NEWEUROPE*, 2010, (te consulteren via http://www.neurope.eu/articles/UK-has-first-coalition-government-since-1945/100818.php).
- X., “Nationale privacywetten overtreden?”, *De Standaard*, 2010 (te consulteren via http://www.zdnet.be/news/114294/conflict-tussen-europa-en-facebook-dreigt/).

