3 - 1779/1

SÉNAT DE BELGIQUE

SESSION DE 2005-2006

28 JUIN 2006

Proposition de loi insérant un article 231*bis* dans le Code pénal, en vue de pénaliser la récolte illégitime d'identifiants personnels sur les réseaux électroniques de communication

(Déposée par M. Philippe Mahoux)

DÉVELOPPEMENTS

L'identité d'une personne est ce qui fonde l'existence de sa personnalité juridique. Dans le « monde réel », cette dernière est clairement circonscrite par les attributs de la personnalité constitutifs de l'état civil comme le nom patronymique. Ces attributs de la personnalité sont conférés et protégés en tant que telle par le droit positif.

Dans le « monde virtuel », les attributs de la personnalité ne sont attribués par aucune autorité publique, l'identité d'une personne est alors plus vaste et ses contours moins clairs. Certaines données numériques qui ont trait à l'identité d'un individu, comme un mot de passe d'un compte personnel sur l'Internet, par exemple, ne sont pas considérées comme des éléments constitutifs de l'identité juridique d'une personne. Or, ces dernières sont des lieux d'usurpations d'identités bien réelles.

Cette identité numérique est composée d'éléments qu'on peut appeler « identifiants ». Ces derniers (mot de passe, nom de compte informatique, pseudonyme virtuel, codes divers donnant accès à des données à caractère privé, etc ...) font de plus en plus l'objet d'actes malveillants.

Une des techniques apparue il y a environ deux ans et qui tend à se généraliser à grande vitesse, souvent avec des moyens sophistiqués, est le « phishing » ou « hameçonnage ». La technique est assez simple. Les

BELGISCHE SENAAT

ZITTING 2005-2006

28 JUNI 2006

Wetsvoorstel tot invoeging van een artikel 231*bis* in het Strafwetboek, teneinde het onwettige verzamelen van gegevens voor persoonsidentificatie op elektronische communicatienetwerken strafbaar te maken.

(Ingediend door de heer Philippe Mahoux)

TOELICHTING

Iemands identiteit vormt de basis van zijn rechtspersoon. In de « reële wereld » is die rechtspersoon duidelijk omschreven door de attributen die de burgerlijke staat vormen, zoals de familienaam. Deze attributen van de persoonlijkheid worden als dusdanig toegekend en beschermd door het positief recht.

In de « virtuele wereld » worden de attributen van de persoon door geen enkele overheid toegekend en is de identiteit van een persoon dus ruimer en minder afgelijnd. Een aantal digitale gegevens die met de identiteit van het individu te maken hebben, zoals het paswoord voor een persoonlijke account op het internet, worden niet beschouwd als elementen die deel uitmaken van de rechtspersoonlijkheid. Toch worden via de digitale gegevens reële identiteiten overgenomen en onrechtmatig gebruikt.

De digitale identiteit bestaat uit wat men « persoonsidentificerende elementen » kan noemen. Deze elementen (paswoord, naam van de internetaccount, virtueel pseudoniem, diverse codes die toegang geven tot privé-gegevens, enz ...) zijn steeds vaker het doelwit van kwaadwillige handelingen.

Een van de technieken die ongeveer twee jaar geleden is opgedoken en die snel veralgemeend lijkt te worden, vaak met gesofistikeerde middelen, is « phishing » of « het ontfutselen van gegevens ». De tech-

fraudeurs utilisent des courriels ou des sites internet fictifs ayant l'apparence de l'authenticité.

Le site ou les courriels annoncent qu'une banque, une compagnie d'assurance ou une institution publique a besoin de vérifier les données du destinataire ou que quelqu'un a essayé d'accéder à son compte et que celui-ci doit être contrôlé. Les fraudeurs tentent alors d'obtenir les éléments d'identification de celui-ci.

À partir des éléments d'identification récoltées; numéros de sécurité sociale, données confidentielles ou autres identifiants personnels, les fraudeurs peuvent ensuite ouvrir des comptes au nom de leurs victimes et demander des crédits, voire prélever directement des sommes. L'usurpation d'identité numérique vient alors aider à la constitution d'une infraction.

Cette activité associée à d'autres formes de fraude représente le plus grand risque pour les consommateurs dans les transactions en ligne, avec pour conséquence une perte de confiance dans les nouvelles technologies de l'information et de la communication, ainsi que des pertes financières pour les internautes abusés.

Selon la FTC (Commission fédérale du commerce aux États-Unis), 10 millions d'américains furent victimes d'usurpation d'identité numérique l'an passé, entraînant un coût pour les entreprises ou les particuliers estimé à 50 milliards de dollars.

Le problème a été jugé sérieux outre-Atlantique. Le gouvernement des États-Unis d'Amérique a ainsi adopté le 16 juin 2005, *l'Identity Theft Penalty Enhancement Act*. Ce texte normatif vise à alourdir sensiblement la durée d'emprisonnement infligée à l'encontre des voleurs d'identité numérique qui avaient commis une infraction.

Dans un même ordre d'idée, le gouvernement anglais a annoncé fin mai 2005 la version finale de son nouveau « Fraud Bill ». Ce texte normatif vise à infliger jusqu'à 10 ans de prison contre ceux qui commettent ce type d'usurpation. Le texte doit passer très bientôt devant le Parlement britannique.

En France depuis quelques mois, parallèlement à l'amplification du phénomène, plusieurs campagnes publiques et privées ont été mises sur pied, afin de sensibiliser la population sur les dangers de l'usurpation d'identité numérique. Selon l'Observatoire de la cyberconsommation, la France est passé l'an dernier de la dixième à la cinquième place des pays les plus touchés, derrière les États-Unis, qui occupent le premier rang mondial.

Cette campagne publique considérée comme insuffisante, a donné lieu au dépôt par le sénateur Michel

niek is vrij simpel. De fraudeurs gebruiken mailberichten of fictieve internetsites die er authentiek uitzien.

De site of de mail verklaart dat een bank, een verzekeringsmaatschappij,of een overheidsinstelling de gegevens van de bestemmeling moet controleren of dat iemand heeft getracht binnen te breken in zijn rekening en dat die gecontroleerd moet worden. De fraudeurs proberen zo de identificatiegegevens van die persoon te krijgen.

Met de aldus verkregen identificatiegegevens (socialezekerheidsnummers, vertrouwelijke gegevens of andere persoonlijke identificatiegegevens) kunnen de fraudeurs dan rekeningen openen op naam van hun slachtoffers, leningen aanvragen of zelfs rechtstreeks sommen geld opnemen. De aanmatiging van een digitale identiteit is dus een hulpmiddel bij een misdrijf.

Deze activiteit vormt, samen met andere vormen van fraude, het grootste risico voor consumenten wanneer zij onlinetransacties doen. Het gevolg ervan is dat de consumenten hun vertrouwen verliezen in de nieuwe informatie- en communicatietechnologie en dat de bedrogen internetgebruikers er geld bij verliezen.

Volgens de FTC (Federale Handelsorganisatie van de VS), zijn vorig jaar 10 miljoen Amerikanen het slachtoffer geweest van identiteitsdieven. Men schat dat dit bedrijven en particulieren samen een bedrag van 50 miljard dollar heeft gekost.

In Amerika wordt dit als een ernstig probleem beschouwd. De Amerikaanse regering heeft dan ook op 16 juni 2005 *de Identity Theft Penalty Enhancement Act* aangenomen, waardoor de gevangenisstraf voor diefstal van een digitale identiteit waarmee een misdrijf is begaan, aanzienlijk wordt verhoogd.

Eind mei 2005 heeft de Britse regering in dezelfde lijn de nieuwste versie van haar « Fraud Bill » aangekondigd. Deze regelgevende tekst voorziet in een gevangenisstraf tot 10 jaar voor degene die dit soort diefstal begaat. De tekst wordt binnenkort aan het Engelse parlement voorgelegd.

In Frankrijk zijn, nadat het fenomeen is beginnen toenemen, al een paar maanden een aantal campagnes aan de gang die de bevolking bewust moeten maken van de gevaren van de aanmatiging van een digitale identiteit. Volgens het « Observatoire de la cyberconsommation » is Frankrijk vorig jaar van de tiende naar de vijfde plaats geschoven in de lijst van de meest getroffen landen, na de Verenigde Staten die op wereldvlak de eerste plaats innemen.

De overheidscampagne werd als onvoldoende beschouwd en senator Michel Dreyfus-Schmidt heeft

Dreyfus-Schmidt d'une proposition de loi tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques (Sénat de France, proposition n° 452).

L'usurpation numérique passe par différents supports et outre l'Internet, on assiste aussi au piratage de lignes téléphoniques (le « phreaking »), ou l'usurpation par téléphone. Cette dernière est très répandue au Japon notamment.

Dans le cadre juridique actuel, notre Code pénal sanctionne celui qui prend l'identité d'un tiers dans le but de le faire passer pour un délinquant. Les articles 227 à 232 du chapitre VI du Code pénal, qui traitent de l'usurpation de fonctions, de titres ou de noms, règlent cette question.

À titre d'exemple, l'article 227 du Code pénal prévoit que *« quiconque se sera immiscé dans des fonctions publiques, civiles ou militaires, sera puni d'un emprisonnement d'un mois à deux ans »*. L'article 231 du Code pénal prévoit également que *« quiconque aura publiquement pris un nom qui ne lui appartient pas sera puni d'un emprisonnement de huit jours à trois mois, et d'une amende de vingt-cinq francs à trois cents francs, ou d'une de ces peines seulement »*.

En revanche, le « phisheur » ou « hameçonneur » qui s'empare d'un « identifiant personnel » sur internet pour commettre un acte malveillant dont l'usurpé sera la victime est difficile à appréhender au regard du droit positif actuel. Hormis la poursuite de l'infraction « terminale » que l'usurpation d'identité numérique contribue à constituer, il est très difficile — sur le plan pénal — dans l'état actuel de la législation de sanctionner les actes préparatoires comme la récolte de données.

Dans ce genre de situation, les tribunaux invoquent le plus souvent le délit d'accès frauduleux à un système de données informatiques pour poursuivre le délinquant, mais l'usurpation d'identité en tant que telle n'est pas sanctionnée : l'internaute-usager n'est pas protégé; on peut parler de vide juridique.

En conclusion, devant l'usurpation d'identité numérique, les victimes font face à une situation juridique incertaine et à des réponses techniques aujourd'hui insuffisantes comme le développement de procédés d'authentification permettant de détecter si le courriel provient véritablement de l'émetteur indiqué. C'est pourquoi il convient d'insérer dans le Code pénal une nouvelle infraction : la récolte illégitime d'identifiants personnels.

La présente proposition de loi a pour objet la modification du Code pénal par l'insertion d'un

een wetsvoorstel ingediend tot bestraffing van de aanmatiging van een digitale identiteit op informaticanetwerken (Franse Senaat, voorstel nr. 452).

De aanmatiging van een digitale identiteit kan op verschillende manieren gebeuren en naast het internet is er ook piraterij op de telefoonlijnen (« phreaking » genaamd), of de aanmatiging van een identiteit per telefoon. Deze techniek is in Japan zeer verspreid.

In het huidige juridische kader wordt bij ons door de Strafwet bestraft, hij die een naam aanneemt die hem niet toekomt met het doel de derde persoon voor een misdadiger te doen doorgaan. De artikelen 227 tot 232 van Hoofdstuk VI van het Strafwetboek behandelen de aanmatiging van functies, titels of namen en regelen deze kwestie.

Artikel 227 van het Strafwetboek bijvoorbeeld, bepaalt : « Hij die zich inmengt in openbare ambten, hetzij burgerlijke of militaire, wordt gestraft met gevangenisstraf van een maand tot twee jaar. » In artikel 231 van het Strafwetboek staat bovendien : « 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 euro tot driehonderd euro, of met een van die straffen alleen. »

De « phisher » of persoon die een persoonlijk identificatiegegeven van het internet haalt om een misdrijf te begaan waarvan de bestolene het slachtoffer wordt, is volgens het huidige positieve recht moeilijk te bestraffen. Buiten het vervolgen van het uiteindelijke misdrijf, gevormd door het onrechtvaardige gebruik van de digitale identiteit, is het strafrechtelijk beschouwd erg moeilijk om de voorbereidende handelingen — zoals het verzamelen van gegevens — te bestraffen.

In dit soort situaties beschouwen rechtbanken vaak dat het gaat om een misdrijf van frauduleuze toegang tot een systeem van informatica-gegevens om de misdadiger te vervolgen, maar het onrechtmatig aannemen van een identiteit wordt niet als dusdanig bestraft : de internetgebruiker is niet beschermd. Hier is dus sprake van een juridische leemte.

Wat het onrechtmatig gebruik van een digitale identiteit betreft, staan de slachtoffers dus voor een onzekere juridische situatie en oplossingen die vandaag technisch ontoereikend zijn, zoals de ontwikkeling van authentificatie-mechanismen waardoor men zou kunnen nagaan of het e-mailbericht echt van de veronderstelde afzender komt. Het is dus nodig om in het Strafwetboek een nieuw misdrijf in te voegen : het onwettige verzamelen van gegevens voor persoonsidentificatie.

Het voorliggende wetsvoorstel heeft tot doel het Strafwetboek te wijzigen door een artikel 231*bis* in te

article 231*bis* au chapitre VI du Code pénal traitant de l'usurpation de fonctions, de titres ou de noms.

L'article 231*bis* vient après l'article 231 du Code pénal qui sanctionne la personne qui aura publiquement pris un nom qui ne lui appartient pas. La rédaction actuelle de l'article 231 du Code pénal ne permet pas de saisir la pleine réalité de l'usurpation électronique d'identité, dans la mesure où elle fait l'impasse sur la séquence préparatoire qui consiste à récolter de manière indue des éléments qui permettent tout de même de circonscrire la personnalité virtuelle de cette dernière.

De plus, l'article 231 du Code pénal aborde la question de l'usurpation uniquement à travers un des éléments de l'identité : le nom. Or, le nom est aujourd'hui insuffisant à définir un individu dans ses relations virtuelles avec autrui. Toute une série d'éléments de l'identité d'une personne peuvent venir circonscrire cette dernière dans le monde virtuel, bien qu'ils ne soient pas considérés comme des éléments constitutifs de l'identité juridique d'une personne.

Il est dès lors préférable d'ériger en nouvelle infraction le fait de récolter illégitimement sur tout réseau électronique de communication les identifiants personnels d'un particulier, d'une personne morale ou d'une autorité publique.

La récolte illégitime d'identifiants personnels sera punie d'une peine d'emprisonnement allant de trois mois à un an et d'une amende variant entre 250 et 15 000 euros.

Philippe MAHOUX.

*
* *

voegen in Hoofdstuk VI, betreffende de aanmatiging van ambten, van titels of van een naam.

Artikel 231*bis* komt na artikel 231 van het Strafwetboek, dat de persoon bestraft die in het openbaar een naam aanneemt die hem niet toekomt. De huidige formulering van artikel 231 omvat niet de volle realiteit van de elektronische aanmatiging van een identiteit, omdat er geen rekening wordt gehouden met de voorbereidende fase waarbij op onrechtmatige wijze gegevens worden verzameld die het mogelijk maken de virtuele identiteit van het slachtoffer te omschrijven.

Bovendien heeft artikel 231 van het Strafwetboek het alleen over de aanmatiging van de identiteit door middel van één van de elementen hiervan : de naam. De naam alleen is tegenwoordig echter onvoldoende om een individu te identificeren in zijn virtuele relatie tot anderen. Er zijn een hele reeks persoonsidentificerende gegevens die de persoon in de virtuele wereld omschrijven. Deze gegevens worden niet altijd beschouwd als elementen die de juridische identiteit van een persoon vormen.

Het is dus beter om het onwettige verzamelen van persoonlijke identificatiegegevens van een particulier, een rechtspersoon of een overheidsinstantie op een elektronisch communicatienetwerk, als een nieuw misdrijf te beschouwen.

Het onwettige verzamelen van persoonlijke identificatiegegevens zal worden gestraft met gevangenisstraf van drie maanden tot een jaar en met geldboete van 250 euro tot 15 000 euro.

*
* *

PROPOSITION DE LOI

Article 1er

La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2

Il est inséré un article 231*bis* du Code pénal, rédigé comme suit :

« Art. 231*bis*. — Sera puni d'un emprisonnement de trois mois à un an et d'une amende de 250 à 15 000 euros, quiconque aura illégitimement récolté sur tout réseau électronique de communication les identifiants personnels d'un particulier, d'une personne morale ou d'une autorité publique.

Par « identifiant personnel » on entend tout élément qui permet à un particulier, une personne morale ou une autorité publique d'être identifié distinctement.

Les peines prononcées se cumulent, sans possibilité de confusion, avec celles qui auront été prononcées pour l'infraction résultant de cette usurpation. ».

Art. 3

La présente loi entre en vigueur le jour qui suit celui de sa publication au *Moniteur belge*.

31 mars 2006.

Philippe MAHOUX.

WETSVOORSTEL

Artikel 1

Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

Art. 2

In het Strafwetboek wordt een artikel 231*bis* ingevoegd, luidende :

« Art. 231*bis*. — Met gevangenisstraf van drie maanden tot een jaar en met geldboete van 250 tot 15 000 euro wordt gestraft hij die onwettig op een elektronisch communicatienetwerk de persoonlijke identificatiegegevens heeft verzameld van een particulier, een rechtspersoon of een overheidsinstantie.

Onder « persoonlijke identificatiegegevens » worden verstaan alle elementen die het mogelijk maken om een particulier, een rechtspersoon of een overheidsinstantie duidelijk te identificeren.

De uitgesproken straffen zijn cumuleerbaar, zonder mogelijkheid tot strafvermenging, met de straffen die zijn uitgesproken voor het misdrijf dat het resultaat van de aanmatiging is.

Art. 3

Deze wet treedt in werking de dag na die waarop ze in het *Belgisch Staatsblad* is bekendgemaakt.

31 maart 2006.

66381 - I.P.M.