Dossiers

Criminalité informatique: analyse de l'avant-projet de loi belge

Auteur: Bernard Magrez (bernard.magrez@dewolf-law.be)

Table des matières

I. Contexte
II. Bref état des lieux en Belgique
III. Examen de l'avant-projet
  A. Commentaires généraux sur l'avant-projet
  B. Commentaires des articles
    1. Faux et usage de faux en informatique
    2. Fraude informatique
    3. Hacking
    4. Sabotage
    5. Amélioration des moyens d'investigations
IV. Notes

*

* *

"Chaque année, le coût de la malveillance informatique se chiffre en milliard de dollars. Les multinationales et les grandes entreprises sont plus naturellement la cible des hackers et des espions industriels. 72.000 tentatives d'accès illicites ont lieu sur Internet chaque jour. Les entreprises devront prendre en compte la circonstance que la majeure partie de la criminalité informatique est due aux faits des employés "

OLIVIER HANSE[1]

*

* *

I.CONTEXTE

Monsieur l'Avocat général près la Cour d'appel de Bruxelles Oscar VANDEMEULEBROEKE débutait sa contribution au Colloque *"Internet sous le regard du droit "* (2) par ces mots :*"Aristophane dit que faire marcher droit un crabe est impossible. On peut se demander si, à l'heure actuelle, un pénaliste est capable d'appréhender - fût- ce avec prudence - ce qu'on appelle la criminalité informatique et celle des télécommunications, soit la criminalité télématique ".*

Tenter de cerner la criminalité informatique pour la sanctionner en tant que telle reviendrait à demander à une cage de partir à la recherche d'un oiseau.

La difficulté de tracer les contours pénaux de l'informatique est certainement l'extrême mouvance de sa technologie associée à l'ingéniosité criminelle. Celle-ci n'a pour limite que l'imagination de ses auteurs, lesquels ont en outre de multiples facettes (3), ce qui ne facilite pas la désignation du ou des pénalement responsables.

Egalement par l'interconnexion des réseaux, la délinquance bénéficie de la mondialisation de ses relations alors que ses recherche et répression se heurtent encore aux frontières des états.

Enfin, hormis les infractions classiques "informatisées" (4), la délinquance a pris également pour cible l'informatique.

Ces "nouveaux intérêts qui méritent protection " (5) donnent naissance = à un droit inédit, soit principalement et à l'heure actuelle, celui de la protection des informations véhiculées par des outils télématiques.

Le malaise de la doctrine face à cette originalité n'est pas sans rappeler celle qui tourmenta les auteurs en droit social des années 1970.

" Ne perdez jamais patience.
C'est souvent la dernière clef qui ouvre la porte... "
A. St EXUPERY

II. BREF ETAT DES LIEUX EN BELGIQUE

La Belgique se caractérise en ce domaine par un vide juridique relatif, comblé çà et là par quelques dispositions spécifiques sans grande cohérence (6) et par l'œuvre d'une jurisprudence instable. De son côté, le Conseil de l'Europe (7) - qui en 1985 s'était déjà penché sur le problème - invitait les états à légiférer dans le cadre de sa Recommandation 89/9. Il avait établi une liste minimale d'actes délinquants visant l'informatique et ses donnés (8).

En l'absence de réglementations spécifiques, la jurisprudence dut faire œuvre d'imagination afin de réaliser la délicate jointure entre un code pénal désuet et une technologie en pleine expansion créant de nouvelles valeurs.

Non sans s'écarter des principes rappelés par la Cour de cassation en son arrêt du 11 septembre 1990 (9), l'interprétation de la loi pénale devint "évolutive " (10), "contemporaine " (11) pour ne pas dire "analogique" (12).

Le droit pénal tel qu'adapté par les cours et tribunaux n'était pas totalement impuissant face à cette nouvelle délinquance, toutefois, il était inapte ou insuffisant à réprimer les comportements délinquants en matière télématique.

L'indécision du praticien était, enfin, renforcée par le peu de décisions de justice (13).

Donnant suite à la décision du Conseil des ministres du 30 mai 1997, concernant les mesures à prendre dans le cadre de la lutte contre la criminalité informatique sur les autoroutes de l'informations, la Belgique est, enfin, en passe de se doter d'une législation sur la criminalité informatique.

D'emblée, il faut constater qu'à l'exception de l'article 6 § 3, alinéa 3, le projet de loi ne tient pas compte du contexte transfrontalier de la criminalité informatique. On suppose dès lors que le Juge s'en tiendra à l'article 3 du Code pénal. D'ailleurs, la doctrine et la jurisprudence l'interprètent comme donnant compétence aux juridictions belges pour connaître d'un crime ou d'un délit, dès lors qu'un élément constitutif de ce crime ou de ce délit a été réalisé en Belgique, sans entrer dans les conditions restrictives des articles 6 à 14 du titre préliminaire du Code d'instruction Criminelle pour la poursuite d'infractions extraterritoriales.

III. EXAMEN DE L'AVANT-PROJET

A. Commentaires généraux sur l'avant projet

Selon le projet d'exposé des motifs, la Belgique adopte une approche pragmatique en proposant " à la lumière de la situation internationale un certain nombre de démarches concrètes afin de fournir aux acteurs de la justice les instruments juridiques adéquats pour lutter contre la criminalité sur les autoroutes de l'information " (14).

L'avant-projet ne tente pas une refonte partielle du droit pénal en modifiant les notions existantes et se propose d'éviter une criminalisation excessive lorsqu'il introduit de nouveaux délits.

D'autre part, l'avant- projet donne de nouveaux moyens d'investigations en étendant les pouvoirs de recherche à l'information et à l'instruction, mais également en affinant la Réglementation en matière de repérage et d'interception des télécommunications et en faisant peser sur les opérateurs de réseaux et fournisseurs de services de nouvelles obligations.

Peu traditionnellement, l'avant- projet se refuse de définir les termes utilisés estimant que la terminologie doit rester neutre pour être évolutive (15).

Toutefois, le projet d'exposé des motifs donne ensuite les définitions du système informatique (16) et des données (17).

Assurément, cette démarche est singulière. Notre législateur n'aurait-il pas omis l'enseignement de la Cour de cassation en son arrêt du 11 septembre 1990 ?

B. Commentaires des articles

1. FAUX ET USAGE DE FAUX EN INFORMATIQUE

1.1. Texte de l'avant projet

Article 210 bis

§1. Celui qui commet un faux, en introduisant dans un système informatique, modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 26 francs à 100.000 francs ou d'une de ces peines.

§2. Celui qui fait usage des données ainsi obtenues, tout en sachant que celles- ci sont fausses, est puni comme s'il était l'auteur du faux.

§3. La tentative de commettre l'infraction prévue § 1er est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs à 50 000 francs ou d'une de ces peines.

§4. Les peines portées par les §§ 1 à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent un jugement ou un arrêt de condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 259 bis, 314 bis, 504 quater ou au titre IX bis de ce code.

1.2. Commentaires

Cette nouvelle prévention n'aura pas le mérite de mettre fin aux hésitations de la jurisprudence (18) sur la qualification d'écrit à conférer aux données informatiques. En revanche, elle crée une nouvelle incrimination autonome et spécifique.

En effet, le Législateur belge n'a pas fait choix de modifier la notion d'écrit en assimilant les données = électroniques au scripturales comme en France où la notion de faux a fait l'objet du nouvel article 441-1 (19).

Ce nouveau délit ne requérant aucune intention particulière (20) ne vise que le fait (et sa tentative) " de dissimuler intentionnellement la vérité par le biais de manipulations informatiques de données pertinentes sur le plan Juridique " (21) ou de faire usage de ses donnés (22).

L'application du nouvel article 220 bis CP supposera donc " la réalisation effective d'un inconvénient spécifique" (23).

Si cette dernière condition évite, suppose-t-on, une criminalisation excessive, son introduction sera, à tout le moins, sujette à interprétation.

Enfin, relevant la gravité (24) de tels actes, le Législateur prévoit un régime de récidive spécifique.
Toutefois, ces peines sont moins sévères que celles prévues pour le "faux civil "(25).

1.3 Fiche synoptique

- Pas d'intention frauduleuse - altération de la vérité par des manipulations sur des données informatiques pertinentes sur le plan juridique.
- Faux en informatique : emprisonnement de 6 mois à 5 ans et/ou amende de 26 à 100.000 bef
- Tentative de faux en informatique : emprisonnement de 6 mois à 3 ans et/ou amende de 26 à 50.000 bef
- Usage de faux en informatique : emprisonnement de 6 mois à 5 ans et/ou amende de 26 à 100.000 bef
- Tentative de faux en informatique : non prévu.
- Récidive spécifique: peines doublées.
- Faits spécialement visés
    - fabrication de cartes de crédit fausses ou falsifiées,
    - faux en matière de contrats numériques.

2. FRAUDE INFORMATIOUE

2.1. Texte de l'avant projet

Article 504 quater.

§1. Celui qui, en vue de se procurer pour soi-même ou pour autrui un avantage patrimonial frauduleux, introduit dans un système informatique, modifie ou efface des données qui sont stockées, traitées ou transmises par un système informatique, ou modifie par tout moyen technologique l'utilisation possible des données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs à 50.000 francs ou d'une de ces peines.

§2. Celui qui, par la commission de l'infraction visée au §1er, obtient pour soi-même ou pour autrui un avantage patrimonial frauduleux est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 26 francs à 100.000 francs ou d'une de ces peines.

§3. Les peines portées par les §§1 et 2 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent un jugement ou un arrêt de condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 210 bis, 259 bis, 314 bis ou au titre IX bis de ce code.

2.2. Commentaires

Cette nouvelle incrimination suppose que la manipulation de données ait été réalisée dans l'intention de se procurer un avantage patrimonial frauduleux. Les peines sont alourdies si l'intention est réalisée. La tentative n'est pas visée.

Ces actes échappaient généralement aux sanctions.

En effet, le vol étant exclu (26), les définitions d'escroquerie et d'abus de confiance s'y prêtait mal dans la mesure où généralement il n'y a pas remise du corpus delicti ou encore de confiance trompée.

Les peines de la fraude informatique suivie de l'effet escompté sont identiques de celles du faux informatiques, on aurait pu s'attendre qu'elles soient plus sévères eu égard à l'intention frauduleuse.

Une récidive spécifique est également prévue.

2.3 Fiche synoptique

- Altération de la vérité par des manipulations sur des données informatiques dans l'intention de se procurer un avantage patrimonial frauduleux.
- Fraude informatique : emprisonnement de 6 mois à 3 ans et/ou amende de 26 à 50.000 bef
- Fraude informatique suivie d'effets : emprisonnement de 6 mois à 5 ans et/ou amende de 26 à 100.000 bef
- Tentatives : non prévu.
- Récidive spécifique: peines doublées.
- Faits spécialement visés:
    - utilisation d'une carte de crédit volée pour retirer de l'argent à un guichet automatique,
    - dépassement illicite du crédit par le biais de sa propre carte de crédit,
    - introduction d'instructions informatiques pour modifier le résultats d'opérations en vue d'obtenir un avantage financier,
    - détournement de fichiers ou de programmes dans un but de lucre.

3. HACKING

3.1. Texte de l'avant projet

Article 550 bis.

§1. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de 26 francs à 25 000 francs ou d'une de ces peines.

Si l'infraction visée au premier alinéa, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

§2. Celui qui, avec intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de 26 francs à 25.000 francs ou d'une de ces peines.

§3. Celui qui se trouve dans une des situations prévues par les §§ 1 et 2 et qui, à cette occasion:

1. *soit prend connaissance de données qui sont stockées, traitées ou transmises par un système informatique ou prend de telles données de quelque manière que ce soit,*

2. *soit fait tout usage d'un système informatique,*

3. *soit cause tout dommage, même non intentionnellement, à un système informatique ou à des données qui sont stockées, traitées ou transmises par un tel système,*

est puni d'un emprisonnement de un à trois ans et d'une amende de 26 francs à 50.000 francs ou d'une de ces peines.

§4 La tentative de commettre une des infractions prévues aux §§ 1 et 2 est punie des mêmes peines que l'infraction elle-même,

§5. Celui qui, avec une intention frauduleuse ou dans le but de nuire, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique et par lesquelles les infractions prévues par les §§ 1 à 4 peuvent être commises, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs à 100.000 francs ou d'une de ces peines.

§6. Celui qui ordonne la commission d'une des infractions prévues aux §§ 1 à 5 ou qui y incite est puni - d'un emprisonnement de six mois à cinq ans et d'une amende de 100 francs à 200.000 ou d'une de ces peines.

§7 Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions prévues aux §§ 1 à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs à 100.000 francs ou d'une de ces peines.

§8. Les peines portées par les §§ 1 à 7 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent un jugement ou un arrêt de condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 210 bis, 259 bis, 314 bis, 504 quater ou dans un des articles du présent titre.

3.2. Commentaires

Dans l'affaire BISTEL, l'accès illicite avait pu être sanctionné par l'application de l'article 17 des lois coordonnées du 13 octobre 1930 concernant la télégraphie et la téléphonie sans fil.

Depuis l'abrogation de cette disposition, les auteurs de la chronique de jurisprudence "informatique " (27) semblent estimer que cet accès pourrait toutefois être sanctionné par l'article 111 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (28).

Nous partageons toutefois l'avis de Monsieur l'Avocat VANDEMEULEBROEKE selon lequel l'accès non autorisé un système

informatique ne constitue pas une infraction en Belgique (29).

En effet, il s'agit d'une intrusion et non d'une interception.

Délibérément, le Législateur exclut la condition d'une éventuelle effraction du dispositif de sécurité ce qui évitera de dévoiler les stratégies des entreprises en matière de sécurité mais également de couper court à toute responsabilité partagée.
Le texte de l'avant projet est assez complet pour permettre d'endiguer ce fléau.
Il distingue le hacking venu de l'extérieur (§1er) de l'interne (§2).

Si le hacker externe ne devra pas être animé d'une intention particulière (30), une intention frauduleuse ou un but de nuire est nécessaire au hacker interne.

Le §3 du nouvel article incrimine trois comportements spécifiques :

- prendre connaissance ou s'emparer des données, (espionnage - vol de données),
- faire usage du système informatique (vol en terme de temps - notamment blanchiment de son adresse afin de se procurer l'anonymat ou utilisation de ressources),
- causer un dommage par imprudence (destruction par imprudence (31))

On regrettera que ces trois types de comportements ne sont punissables que s'ils sont accomplis dans le cadre d'un hacking (32).

En effet, la victime et le Ministère public devront au préalable établir qu'il y a eu hacking au sens des §§ 1 et 2 du nouvel article. D'autre part, la controverse, sur le vol de données ne sera, hors hacking, pas résolue (33).

Enfin, il est malheureux que les procédures de blanchissement (effacement) d'adresses ne puissent être visées hors hacking alors qu'elles favorisent par l'anonymat créé, la transmission de contenus illicites notamment vers les " news groups ".

La tentative de hacking extérieure et interne a été incriminée mais non celle des trois types de comportements du §3. Ceci est à déplorer.

Par contre, le Législateur sanctionne les comportements qui pourraient favoriser le hacking, soit la gestion frauduleuse des " hackertools " (§5), le commanditaire (§6) et le receleur (§7).

A l'instar des autres dispositions, les peines sont aggravées lors d'une récidive spécifique.

3.3. Fiche synoptique

Hacking et infractions commises lors ou au moyen d'un hacking:

§1. Hacking extérieur sans intention frauduleuse :
emprisonnement de 3 mois à 1 an et/ou amende de 26 à 25.000,- bef

§2. Hacking extérieur avec intention frauduleuse emprisonnement de 6 mois à 2 ans

§3. Hacking interne avec intention frauduleuse : emprisonnement de 6 mois à 2 ans et/ou amende de 26 à 25.000,- bef

§3. A l'occasion d'un hacking, soit prendre connaissance et/ou s'emparer de données, soit user du système informatique, soit causer involontairement un dommage : emprisonnement de l à 3 ans et/ou amende de 26 à 50.000,- bef

§4. Tentative d'hacking (§§1 et 2) : peines identiques

§5. Toute manipulation de " hackertools " dans une intention frauduleuse : emprisonnement de 6 mois à 3 ans et/ou amende de 26 à 100.000,- bef,

§6. Commanditaire d'infractions aux §§ 1 à 5 : emprisonnement de 6 mois à 5 ans et/ou amende de 100 à 100.000,- bef

§7. Receleur: emprisonnement de 6 mois à 3 ans et/ou amende de 26 à 100.000,- bef

§8. Récidive: peines doublées.

Faits spécialement visés :

- toutes les formes d'hacking en ce compris l'escroquerie en matière de code d'accès.

4. SABOTAGE

4.1. Texte de l'avant projet

§1. Celui qui, dans le but de nuire, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout autre moyen technologique l'utilisation possible de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs à 25.000 francs ou d'une de ces peines.

§2. Celui qui, suite à la commission d'une infraction prévue au §1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 26 francs à 75. 000 francs ou d'une de ces peines.

§3. Celui qui, suite à la commission d'une infraction prévue au §1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de 26 francs à 100.000 francs ou d'une de ces peines.

§4. Celui qui, avec une intention frauduleuse ou dans le but de nuire, conçoit, met à disposition, diffuse ou commercialise des

données stockées, traitées ou transmises par un système informatique, alors qu'i1 sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs à 100.000 francs ou d'une de ces peines.

§5. Les peines portées par les §§ 1 à 4 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent un jugement ou un arrêt de condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 210-bis, 259 bis, 314 bis, 504 quater ou dans un des articles du présent titre.

4.2. Commentaires

Le droit pénal "classique" s'appliquait difficilement en la matière dans la mesure où, pour ce faire, les données devaient être considérées comme des écrits susceptibles d'être la base d'un droit ou d'engendrer une obligation. Si la notion d'écrit visé à l'article 527 CP est plus étendue que celle de l'article 241 CP, cette question gisant en fait, la réponse était quelque peu hasardeuse.

L'article 559 CP rencontre parfaitement le sabotage, toutefois la sanction d'une contravention de 3ème classe rend dérisoire son application.

Le Législateur comble cette lacune par l'introduction de ce nouvel article qui incrimine de manière graduelle le sabotage des données (§1), qui cause en outre un dommage à un quelconque système informatique (§2) ainsi que le sabotage du système informatique (§3).

Comme en matière de hacking, les actes préparatoires ont été visés, on regrettera que tel n'est pas le cas du commanditaire.
Ces infractions requièrent une intention frauduleuse ou le but de nuire.
La même attention a été apportée en matière de récidive.

4.3. Fiche synoptique

Sabotage de données et sabotage de systèmes informatiques:

§1. Sabotage de données : emprisonnement de 3 mois à 3 ans et/ou amende de 26 à 25.000,- bef,

§2. Sabotage de données causant un dommage : emprisonnement de 6 mois à 5 ans et/ou amende de 26 à 75.000,- bef,

§3. Sabotage d'un système informatique : emprisonnement de 1 à 3 ans et/ou amende de 26 à 100.000,- bef,

§§4 et 5. Toute manipulation dans une intention frauduleuse permettant d'élaborer un sabotage emprisonnement de 6 mois à 3 ans et/ou amende de 26 à 100.000,- bef,

§6. Récidive: peines doublées.

5. AMELIORATION DES MOYENS D'INVESTIGATIONS

Les moyens d'investigation ont été renforcés pour faire face à la spécificité de la technologie de l'information.

Les articles 39 et 85 CIC ne permettant pas, à proprement parler, la saisie de données en raison du caractère immatériel de ces dernières, l'avant- projet remédie à cette lacune.

Il met également en place, et dans une certaine limite, la perquisition dans un système informatique et sur les systèmes liés - sorte de perquisition "virtuelle " -, crée de nouvelles obligations de collaboration et affine les modalités de dépistage et d'interception des télécommunications.

Enfin, les auteurs de l'avant- projet n'ont pas abordé la cryptographie estimant qu'elle dépasse le cadre de la lutte contre la criminologie informatique (34).

Une analyse plus détaillée paraît actuellement inutile dans le cadre de cette contribution dans la mesure où ces moyens sont, pour la plupart, ceux mis au service des Parquets et juges d'instruction.

IV. NOTES

1. Business & droit d'Internet, p. 179.

2. VANDEMEULEBROEKE, O., Le droit pénal et la procédure pénale confrontés à Internet, in Internet sous le regard du droit, CJBB, 1997, p. 151.

3. VANDEMEULEBROEKE, O., op. cit., p. 156 : "le fournisseur d'une infrastructure,le fournisseur d'accès, lequel possède une connexion permanente avec Internat et revend l'accès à un utilisateur,le fournisseur de services ou serveur. Il reçoit le message de son abonné et le transmet vers le destinataire final ou encore il est celui qui héberge des informations produites par un tiers et qu'il livre à son client,- l'utilisateur lequel peut être " domestique " ou " étranger ".

4. Celles où l'informatique n'est qu'un instrument ou un support dans l'accomplissement de l'acte répréhensible

5. Avant-projet des motifs, p. 1.

6. Notamment :
   - Loi du 15 janvier 1990 sur la banque carrefour (61)
   - Loi du 8 décembre 1992 relative à la protection de la vie privée
   - Loi du 8 août 1983 organisant le registre national des personnes physiques (11)
   - Loi relative au crédit à la consommation (101 par 12)
   - Loi du 30 juin 1994 relative au droit d'auteur (22-26)
   - Loi du 14 juillet 1991 sur les pratiques de commerce
   - Loi du 30 juin 1994 sur les écoutes téléphoniques
   - Loi du 30 juin 1995 relative à la protection juridique des programmes d'ordinateurs.

7. Conseil de l'Europe, Rec. No R 89/9 et son rapport : " La criminalité

informatique ". Annexe 1, p. 87.

8. Notamment :
la fraude informatique,
   - le faux en informatique,
   - les dommages affectant les données ou programmes informatiques, le sabotage informatique,
   - l'accès non autorisé,
   - l'interception non autorisée

9. *" Même si l'on admet que le juge pénal est autorisé à appliquer la toi pénale à des faits que le législateur était dans l'impossibilité absolue de prévoir à 1 'époque de la promulgation de la toi, cela n'est possible qu'à la double condition que la volonté du législateur d'ériger des faits de cette nature en infraction soit certaine et que ces faits puissent être compris dans la définition légale de la disposition pénale "* , Pas., 1991,1, 37.

10. VANDEMEULEBROEKE, O., op. cit., p. 239.

11. J.T., 1996, 230.

12. FRYDMAN, 0 ., les formes de l'analogie, Rev. de recherches juridiques, Droit prospectif, 1995, 4, cité par VANDEMEULEBROEKE, O., op. cit., p. 239.

13. La rareté de telles décisions s'explique aisément par les difficultés rencontrées dans le dépistage des fraudes et l'établissement de ses preuves suffisantes ainsi que par le silence circonstancié des victimes qui préfèrent ne pas faire échos de leurs mésaventures, ce d'autant plus lorsqu'il s'agit de fraudes internes.

14. Exposé, p. l.

15. *" afin d'éviter que les concepts soient trop rapidement dépassés "*, Exposé, p. 7.

16. *" tout système permettant le stockage, le traitement ou la transmission de données "*, Exposé, p. 7

17. *" les représentations de l'information pouvant être stockées, traitées, et transmises par le biais d'un système informatique (..) La forme matérielle que revêtent ces données n'a pas d'importance pour l'avant-projet de loi "* Exposé, p. 7.

18. L'affaire BISTEL en fût la plus célèbre illustration belge : Le tribunal correctionnel de Bruxelles décida que l'introduction frauduleuse du mot de passe constituait un écrit et partant un faux (Corr. Bruxelles, 8 novembre 1990, J.T., 1990, 11), La Cour d'appel réforma le jugement et tranchant dans le sens opposé... (Bruxelles, 24 juin 1991, RDPC, 1992, 340).

    Sans qu'elle soit pour autant fermement établie, la solution qui prévaudra jusqu'à l'adoption de la nouvelle loi est selon l'opinion de la Cour d'appel de Liège que:

" pour être punissable, le faux en écritures doit se produire dans un écrit quel que soit le procédé mis en œuvre pour sa réalisation; (..) les données informatiques appelées par l'opérateur sur l'écran de son ordinateur ne sont que des impulsions magnétiques ne constituant pas des écrits au sens de la loi mais peuvent être l'instrument de leur réalisation, (..) la modification frauduleuse desdites données ne produira un écrit faux qu'à cette condition quelles soient inscrites sur un support matériel quel qu'il soit (papier, disquette, disque dur, ... "

(Liège, 26 février 1992, JLMB, 1992, p. 1346).

19. *" Article 441-1: Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques. Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 300 000 F d'amende. "*,http://www.rabenou.org.

20. L'intention d'enrichissement donnera lieu à application du nouvel article 504 quater CP (fraude informatique), celle de nuire au nouvel article 550 ter CP (sabotage).

21. Exposé, p. 8 .

22. On notera que la tentative d'usage de faux n'est pas visée par l'avant-projet.

23. Exposé, p. 8.

24. *"les risques importants occasionnés par ces délits qui peuvent être commis assez facilement mais dépistés plus difficilement ",* Exposé, p. 8 .

25. Réclusion de 5 à 10 ans.

26. L'auteur ne veut pas s'approprier les données.

27. J.T, 1996, 230.

28. *" prendre frauduleusement connaissance de l'existence ou du contenu de signes, de signaux, d'écrits,d'images, de sons ou de données de toute nature transmis par voie de télécommunications. en provenance d'autres personnes et destinées à celles-ci... "*

29. VANDEMEULEBROEKE, O., op. cit., p. 198 citant : VAN ECKE, P., Les défis de la société de l'informatique et les missions de la justice, p. 35 ; T.C. Bruxelles, 8 novembre 1990, computerrecht, 1991/1, 31.

30. Par contre, si tel est le cas les peines sont aggravées.

31. Le sabotage " intentionnel " comme précise l'avant- projet est plus sévèrement réprimé par le nouvel article 550 ter CP. On regrettera l'imprécision des termes dans la mesure où le sabotage est un acte qui a pour but de détériorer ou de détruire intentionnellement du matériel, des installations...

32. *" Dans le contexte du présent avant- projet de loi, ces trois comportements sont considérés comme punissables uniquement parce quels sont adoptés en même temps que ou après le " hacking " "* , Exposé, P. 10.

33. Pour conclure au vol, la jurisprudence et la doctrine ont dû assimiler une donnée à une chose tangible et en outre considérer que la soustraction frauduleuse était un acte modifiant le régime patrimonial dans le sens de la perte d'exclusivité de la possession d'un bien. La dérive est importante.

34. Exposé, p. 5.

ASBL "Droit et Nouvelles Technologies"
Rue de la Brasserie, 29 - 1050 Bruxelles - Belgique
Tél: +32 2 649 01 15 - Email: info@droit-technologie.org