Colloque Préparatoire
24-27 avril 2013, Moscou (Russie)
Section II – Société de l'information et le droit pénal

BELGIQUE*

(b) Vie privée

1. atteinte au secret des données privées

a. Objet – type de données privées ?

i. la loi de votre pays exige-t-elle que les collecteurs de données divulguent leur façon d'opérer avant de collecter les données privées du consommateur tels que, par exemple, quelle information est utilisée, comment elle est rassemblée et à quelles fins, si elle est partagée avec des tiers et si les consommateurs ont la maîtrise de ce qui est divulgué ?

En droit belge, le traitement de données à caractère personnel est régit par la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

En son article 9, la Loi du 8 décembre 1992 prévoit :

§ 1ier : Le responsable du traitement ou son représentant doit fournir à la personne concernée auprès de laquelle il obtient les données la concernant et au plus tard au moment où ces données sont obtenues, au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée:

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;

b) les finalités du traitement;

c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing;

d) d'autres informations supplémentaires, notamment:

- les destinataires ou les catégories de destinataires des données,

- le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,

- l'existence d'un droit d'accès et de rectification des données la concernant;

sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données;

e) d'autres informations déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la commission de la protection de la vie privée.

§ 2 : Lorsque les données n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données, fournir à la personne concernée au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée:

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant;

b) les finalités du traitement;

* Attention: Le texte publié constitue la dernière version originale du rapport national envoyé par l'auteur, sans révision éditoriale de la part de la Revue.

c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing; dans ce cas, la personne concernée doit être informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de direct marketing;

d) d'autres informations supplémentaires, notamment:

- les catégories de données concernées;
- les destinataires ou les catégories de destinataires;
- l'existence d'un droit d'accès et de rectification des données la concernant;

sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont traitées, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données;

e) d'autres informations déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la Commission de la protection de la vie privée.

Il y a, néanmoins, certains cas dans lesquels le responsable du traitement est dispensé de son devoir d'information :

a) lorsque, en particulier pour un traitement aux fins de statistiques ou de recherche historique ou scientifique ou pour le dépistage motivé par la protection et la promotion de la santé publique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés;

b) lorsque l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

La personne concernée a, comme le stipule l'article 10 de la Loi du 8 décembre 1992, le droit d'obtenir du responsable du traitement des données:

a) la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées;

b) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données;

c) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, dans le cas des décisions automatisées

ii. La loi de votre pays exige-t-elle que les sociétés et les entités faisant du commerce via internet informent le consommateur de l'identité du collecteur de données, si la procuration des données est volontaire ou requise, et quelles sont les mesures prises par le collecteur de données afin d'assurer la confidentialité, l'intégrité et la qualité des données ?

En ce qui concerne le commerce électronique, la Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information est d'application.

La « société de l'information » est définie comme : tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire du service.

Cette Loi dédie son chapitre III au devoir d'information et à la transparence qui doivent être pris en compte par quelconque société pratiquant le commerce via internet.

Ainsi, tout prestataire d'un service de la société de l'information assure un accès facile, direct et permanent, pour les destinataires du service et pour les autorités compétentes, au moins, aux informations suivantes:

1° son nom ou sa dénomination sociale;

2° l'adresse géographique où le prestataire est établi;

3° ses coordonnées, y compris son adresse de courrier électronique, permettant d'entrer en contact rapidement et de communiquer directement et efficacement avec lui;

4° le cas échéant, le registre de commerce dans lequel il est inscrit et son numéro d'immatriculation;

5° dans le cas où l'activité est soumise à un régime d'autorisation, les coordonnées de l'autorité de surveillance compétente;

6° en ce qui concerne les professions réglementées:

a) l'association professionnelle ou l'organisation professionnelle auprès de laquelle le prestataire est inscrit,

b) le titre professionnel et l'état dans lequel il a été octroyé,

c) une référence aux règles professionnelles applicables et aux moyens d'y avoir accès;

7° dans le cas où le prestataire exerce une activité assujettie à la taxe sur la valeur ajoutée, le numéro d'identification à la T.V.A.;

8° les codes de conduite auxquels il est éventuellement soumis ainsi que les informations relatives à la façon dont ces codes peuvent être consultés par voie électronique.

iii. La Loi de votre pays exige-t-elle des sites internet d'afficher une politique de confidentialité et d'expliquer comment les données personnelles seront traitées avant que le consommateur ne commence la vente en ligne ou quelconque autre transaction pour laquelle il doit procurer des données personnelles ?

La Loi belge ne prévoit rien de ce genre en ce qui concerne spécifiquement les sites internet. Or, ceux-ci doivent bien évidemment prendre en compte les dispositions mentionnées au numéro ii.

iv. Les lois pénales de votre pays pénalisent-elles le manque de fournir les informations telles que mentionnées ci-dessus (a.i. ; a.ii. ; et a.iii.) ?

Les Lois du 8 décembre 1992 et du 11 mars 2003 prévoient en des sanctions pénales en cas de violation des devoirs d'information vis-à-vis du consommateur.

Ainsi, en cas de non-respect des obligations citées sous a.i, le responsable du traitement, son représentant en Belgique, son préposé ou mandataire qui n'a pas respecté les obligations s' expose à une amende allant de 100 à 100.000 euros.

Pour les obligations reprises sous a.ii, la Loi prévoit des amendes de 250 à 10.000 euros.

b. Acte – usage illégal et transfert/ diffusion

i. La Loi pénale de votre pays définie-t-elle le transfert et la diffusion de façon illégale de données privées ?

Les notions de transfert et de diffusion de manière illégale ne sont pas spécifiquement définies en loi belge.

Néanmoins, par "traitement", on entend toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel.

ii. Le Loi pénale de votre pays sanctionne-t-elle l'usage, le transfert et/ou la diffusion illégaux de données privées ?

ii.A. En matière de hacking

Le Code Pénal belge stipule en son 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 vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.
>
> Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans »
>
> § 2 : « Celui qui, avec une 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 vingt-six euros à vingt-cinq mille euro ou d' une de ces peines seulement. »
>
> § 3 : « Celui qui se trouve dans une des situations visées aux §§ 1er et 2 et qui:
>
> 1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique;
>
> 2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers;
>
> 3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système;
>
> est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six euros à cinquante mille euros ou d'une de ces peines seulement. »

ii.B. Concernant la transmission de données électroniques

L'article 314*bis* Code Pénal prévoit, en ce qui concerne *l'interception* d'un message transmit :

§ 1er Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, quiconque:

> 1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des

communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications;

2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque.

§ 2 Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, quiconque détient, révèle ou divulgue sciemment à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.

Sera puni des mêmes peines quiconque, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications ou de télécommunications privées.

§ 2bis Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, celui qui, indûment, possède, produit, vend obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au § 1er.

§ 3 La tentative de commettre une des infractions visées aux §§ 1er, 2 ou 2bis est punie comme l'infraction elle-même.

§ 4 Les peines prévues aux §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées à l'article 259bis, §§ 1er à 3

Les articles 124 et 125 de la Loi relative aux communications électroniques du 16 juin 2005 prévoient, en ce qui concerne *l'information déjà transmise* :

Art. 124 : S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut:

1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement;

2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu;

3° sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne;

4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non.

Art. 125 : § 1e Les dispositions de l'article 124 de la présente loi et les articles 259bis et 314bis du Code pénal ne sont pas applicables:

1° lorsque la loi permet ou impose l'accomplissement des actes visés;

2° lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques;

3° lorsque les actes sont accomplis en vue de permettre l'intervention des services de secours et d'urgence en réponse aux demandes d'aide qui leur sont adressées;

4° lorsque les actes sont accomplis par l'Institut sur ordre d'un juge d'instruction et/ou dans le cadre de sa mission générale de surveillance et de contrôle;

5° lorsque les actes sont accomplis par le service de médiation pour les télécommunications ou à la demande de celui-ci dans le cadre de ses missions légales de recherche [1][et ne concernent pas l'écoute de communications;

5°/1 lorsque les actes sont accomplis par les agents habilités par le ministre qui a l'économie dans ses attributions, dans le cadre de leurs missions légales de recherche et ne concernent pas l'écoute de communications;

5°/2 lorsque les actes sont accomplis par la Commission d'éthique pour les télécommunications ou son secrétariat ou à la demande de l'un d'eux dans le cadre de leurs missions légales de recherche et ne concernent pas l'écoute de communications;

6° lorsque les actes sont accomplis dans le seul but d'offrir des services à l'utilisateur final consistant à empêcher la réception de communications électroniques non souhaitées, à condition d'avoir reçu l'autorisation de l'utilisateur final à cet effet.

c. Justification

i. sous quelles conditions la Loi de votre pays autorise-t-elle la collecte, le traitement, le transfert et la diffusion de données privées ?

La Loi du 8 décembre 1992 énumère les conditions dans lesquelles le traitement de données est autorisée :

> « Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants:
>
> a) lorsque la personne concernée a indubitablement donné son consentement;
>
> b) lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
>
> c) lorsqu'il est nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance;
>
> d) lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée;
>
> e) lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées;
>
> f) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi. »
>
> « Le traitement de données à caractère personnel concernant la vie sexuelle, est autorisé lorsque le traitement est effectué par une association dotée de la personnalité juridique ou par un établissement d'utilité publique, qui a pour objet statutaire principal l'évaluation, la guidance et le traitement des personnes dont le comportement sexuel peut être qualifié d'infraction, et qui est agréé et subventionné par l'autorité compétente en vue de la réalisation de ce but; ces traitements, qui doivent être destinés à

> l'évaluation, la guidance et le traitement des personnes visées dans le présent paragraphe et qui ne peuvent porter que sur des données à caractère personnel qui, pour autant qu'elles sont relatives à la vie sexuelle, concernent les personnes visées dans le présent paragraphe, sont soumis à une autorisation spéciale individuelle accordée par le Roi, dans un arrêté royal délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée. »

ii. Ces conditions doivent-elles avoir un certain degré de nécessité (obligatoire, important, raisonnable, suffisant) ?

Ceci varie en fonction de la mesure visée, voir c.i.

2. Violation du secret professionnel.

a. Objet – type de données privées?

i. La Loi de votre pays oblige-t-elle que les professionnels divulguent:

- *Leur pratiques de collection et traitement avant de demander de collecter les données personnelles de leur patients ou leur clients;*
- *Leur façon de divulguer ces informations*
- *Leurs obligations à caractère professionnelle en matière d'étique*
- *Et si les patients ou clients ont la maitrise des données qui sont divulguées?*

Pour ce qui concerne les professionnels, ceux-ci sont entièrement soumis aux lois citées ci-dessus. Il n'y a donc pas de loi spécifique leur concernant.

ii. Quelles données sont spécifiquement protégées, s'il y en a?

De nouveau, vu que les professionnels sont soumis aux lois susmentionnées, il n'y a rien de prévu pour eux spécifiquement.

iii. La Loi de votre pays permet-elle, voir même oblige-t-elle que les médecins, avocats, prêtres, etc. violent leur secret professionnel dans certaines situations ou pour certaines raisons établies par la Loi? Sous quelles conditions est-ce possible? (p.e. s'il y a lieu à croire qu'un enfant, qu'une femme ou qu'une personne âgée a été malmené?)

L'article 458 du Code Pénal stipule:

> « Les médecins, chirurgiens, officiers de santé, pharmaciens, sages-femmes et toutes autres personnes dépositaires, par état ou par profession, des secrets qu'on leur confie, qui, hors le cas où ils sont appelés à rendre témoignage en justice ou devant une commission d'enquête parlementaire et celui où la loi les oblige à faire connaître ces secrets, les auront révélés, seront punis d'un emprisonnement de huit jours à six mois et d'une amende de cent euros à cinq cents euros. »

Il est donc possible de lever le secret professionnel en cas de témoignage en justice ou devant une commission d'enquête parlementaire, ainsi qu'au cas où la Loi l'autorise.

La jurisprudence belge accepte, en outre, que le secret professionnel n'est pas absolu, et qu'il doit céder lorsqu'une nécessité l'impose ou lorsqu'une valeur jugée supérieure entre en conflit avec elle.

b. Sujet – qui sont les auteurs ?

La Loi pénale de votre pays identifie-t-elle les catégories de professionnels qui sont assujetties à une obligation de confidentialité ?

La Loi indique quels catégories de professions sont visées par l'article 458 CP : ce sont les médecins, chirurgiens, officiers de santé, pharmaciens, sages-femmes et toutes autres personnes dépositaires. Il n'y a donc pas de liste précise de professions ayant un secret professionnel.

La jurisprudence accepte que les juges et magistrats, les notaires, les officiers de police et les traducteurs sont eux aussi soumis au secret professionnel.

c. Acte – usage illégal et transfert/ diffusion

Quels actes (p.e. collecte, usage, transfert et diffusion illégaux) sont spécifiquement sanctionnées par la Loi pénale de votre pays ?

La Loi sanctionne la révélation de secrets dont le professionnel prend connaissance lors de l'exercice de sa profession.

L'article 458 du Code pénal s'applique à tous ceux auxquels leur état ou leur profession impose l'obligation du secret confié, soit que les faits qu'ils apprennent ainsi sous le sceau du secret leur aient été confiés par des particuliers, soit que leur connaissance provienne de l'exercice d'une profession aux actes de laquelle la loi, dans un intérêt général et d'ordre public, imprime le caractère confidentiel et secret.

3. Traitement illégal de données personnelles et privées

a. Objet ?

La Loi criminelle de votre pays sanctionne-t-elle l'acquisition, le traitement, le stockage, l'analyse, la manipulation, l'usage, la vente, le transfert etc. illégal de données personnelles et privées ?

La Loi belge sanctionne en son article 550*bis* CP :

> « § 1er 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 vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.
>
> Si l'infraction visée à l'alinéa 1er, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.
>
> § 2
>
> Celui qui, avec une 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 vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement.
>
> § 3
>
> Celui qui se trouve dans une des situations visées aux §§ 1er et 2 et qui:
>
> 1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique;

2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers;

3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système;

est puni d'un emprisonnement de un à trois ans et d'une amende de vingt-six euros à cinquante mille euros ou d'une de ces peines seulement.

§ 4

La tentative de commettre une des infractions visées aux §§ 1er et 2 est punie des mêmes peines.

§ 5

Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 4, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement. »

b. Sujet ?

la Loi pénale de votre pays identifie-t-elle spécifiquement les catégories de personnes et entités incluses dans ces dispositions pénales ?

Il n'y a pas de catégories de personnes et entités qui sont visées spécifiquement.

c. Acte ?

i. La Loi pénale de votre pays sanctionne-t-elle certains comportements spécifiques qui constituent l'entièreté ou une part du traitement illégal de données personnelles et privées ? Répondez pour chaque catégorie citée ci-dessous en mentionnant les dispositions légales, s'il y en a.

1. Collecte illégale

L'article 550bis, § 3, 1° CP stipule :

« Soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique; »

2. Usage illégal / 3. Détention illégale / 4. Transfert illégal

Ces comportements-ci sont visées par la même disposition du Code Pénal.

L'article 550bis, § 5 CP stipule :

« Celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions prévues au §§ 1er à 4, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement. »

ii. Y a-t-il une différence si ces données privées et personnelles sont utilisées, transférées, etc. à de fins policières ou judiciaires ?

L'article 88*ter* de Code de l'Instruction Criminelle (CIC) prévoit :

> § 1er Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée:
>
> – si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et
> – si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.
>
> § 2 L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès.
>
> § 3 En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39bis s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées.
>
> Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique sans délai cette information au ministère de la Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.

L'article 39*bis* CIC, quant à lui, stipule :

> « § 1er Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28sexies, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique.
>
> § 2 Lorsque le procureur du Roi ou l'auditeur du travail découvre dans un système informatique des données stockées qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.
>
> § 3 Il utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.
>
> Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi ou l'auditeur du travail utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles.

> Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.
>
> § 4 Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.
>
> § 5 Le procureur du Roi ou l'auditeur du travail informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.
>
> § 6 Le procureur du Roi ou l'auditeur du travail utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.
>
> Des moyens techniques appropriés sont utilisés pour leur conservation au greffe.
>
> La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents. »

d. Justification

i. Sous quelles conditions la Loi de votre pays autorise-t-elle la collecte, le traitement, le transfert et la diffusion de manière légale de données privées et personnelles ?

Dans les conditions reprises sous 1.

ii. Ces conditions doivent-elles avoir un certain degré de nécessité (obligatoire, important, raisonnable, suffisant) ?

Ceci est à voir au cas par cas.

4. L'usurpation d'identité

a. Objet

i. La Loi pénale de votre pays sanctionne-t-elle l'usurpation d'identité ? Citez la loi applicable.

L'article 231 de Code Pénal prévoit :

> « 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 euros à trois cents euros, ou d'une de ces peines seulement. »

ii. La Loi pénale de votre pays interdit-elle certaines formes d'usurpation d'identité, tel que le phishing par exemple ?

Les articles 210*bis* et 504*quater* du Code Pénal sont formulés de manière générale :

> « Art. 210*bis* : § 1er Celui qui commet un faux, en introduisant dans un système informatique, en 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 vingt-six euros à cent mille euros ou d'une de ces peines seulement.

§ 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 visée au § 1er et est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cinquante mille euros ou d'une de ces peines seulement. »

«Art. 504*quater* : § 1er Celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six euros à cent mille euros ou d'une de ces peines seulement.

§ 2 La tentative de commettre l'infraction visée au § 1er et est punie d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six euros à cinquante mille euros ou d'une de ces peines seulement.

Le jurisprudence accepte que toutes formes de fraude en informatique, tel que le *phishing* ou le *skimming*, sont visées par ces dispositions.

b. Sujet.

La Loi pénale de votre pays prévoit-elle quelconque responsabilité civile en lien avec l'identité digitale d'une personne, ou son avatar, ou son rôle digital dans un jeu en réseau (p.e. Cityville, Farmville, etc.) ?

L'identité digitale d'une personne est protégée par les articles 210bis et 231 de Code Pénal. Ainsi, le tribunal de Termonde a jugé que l'ouverture d'un compte e-mail au nom de quelqu'un d'autre et l'envoi d'un e-mail via cette adresse e-mail à une tierce personne doivent être considérés comme une manipulation de données informatiques juridiquement pertinentes.

Le tribunal de Gand a jugé que le faux en informatique vise la falsification de données électroniques juridiquement pertinentes via la manipulation de données. La création d'un faux profil sur le site du réseau social Facebook et la diffusion de faux messages sur ce profil constituent une manipulation de ce type.

(d) Violation de propriété informatique, y compris la propriété intellectuelle.

La Loi pénale de votre pays proscrit-elle et sanctionne-t-elle les comportements suivants utilisant un système informatique ? Citez la loi d'application.

1. Fraude

La fraude informatique est visée à travers l'article 504*quater* CP précité, qui se situe dans le Titre IX : Crimes et délits contre les propriétés, Chapitre II : des fraudes.

2. Infraction de la propriété intellectuelle en matière informatique.

Il n'y a pas de dispositions spécifiques relatives à l' Infraction de la propriété intellectuelle en matière informatique. Il est accepté que les lois concernant la propriété intellectuelle en général sont d'application.

3. Espionnage industriel.

Il n'y a pas de disposition spécifique en matière d'informatique, or l'article 309 CP prévoit de manière générale :

> « Celui qui aura méchamment ou frauduleusement communiqué des secrets de la fabrique dans laquelle il a été ou est encore employé, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de cinquante euros à deux mille euros. »

(f) Délits de non-coopération.

La Loi pénale de votre pays sanctionne-t-elle la non-coopération avec les forces judiciaires en matière de criminalité informatique ?

La Loi belge ne sanctionne pas spécifiquement la non-coopération en matière informatique, néanmoins, le juge d'instruction peut obliger certaines personnes à collaborer (art. 88*quater* CIC) :

> « § 1er Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible. Le juge d'instruction mentionne les circonstances propres à l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi ou à l'auditeur du travail.
>
> § 2 Le juge d'instruction ou un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui, peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.
>
> L'ordonnance vises à l'alinéa 1er, ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156.
>
> § 3 Celui qui refuse de fournir la collaboration ordonnée aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six euros à vingt mille euros ou d'une de ces peines seulement.
>
> § 4 Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. »

Les sanctions applicables sont des sanctions pénales, et non des sanctions administratives.