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

RAPPORT NATIONAL TURC*

E. Eylem AKSOY RETORNAZ & Sinan ALTUNÇ*

(B) Les pratiques législatives et les concepts juridiques

(1) Comment les lois pénales relatives aux cyber-crimes sont-elles codifiées dans votre pays? Sont-elles contenues dans un titre unique ou un code unique ou sont-elles réparties dans les divers codes ou divers titres? (Veuillez fournir les textes utiles).

Les réglementations pénales relatives aux cyber-crimes se trouvent d'abord dans le Code pénal turc (CPT). Donc il n'y a pas de loi pénale spécifique relative aux cyber-crimes.

Mais dans certaines lois telles que la « Loi sur les œuvres intellectuelles et artistiques » et la « Loi sur la signature électronique », on peut trouver des dispositions sur les cyber-crimes.

Par exemple l'article 72 de la Loi sur les œuvres intellectuelles et artistiques, celui qui produit, offre à la vente, vend ou possède pour l'utilisation personnelle les programmes ou hardwares techniques afin de rendre ineffectif les programmes qui ont été produits pour éviter la multiplication illégalement d'un programme informatique, sera puni avec une peine d'emprisonnement de 6 mois à 2 ans.

(2) Quel est l'impact des décisions judiciaires sur la formulation des lois pénales relatives aux cyber-crimes?

Il est très rare que les décisions judiciaires aient l'effet sur la formulation des lois pénales en Turquie. Mais quand même il y a quelques décisions importantes qui ont influencé l'élaboration de la loi. Une de ces décisions est l'affaire Coşkun Ak. Coşkun Ak était l'administrateur de forum au Superonline [un fournisseur de service (internet service provider - ISP) turc]. Il a été tenu responsable pour un message anonyme publié au forum, en 2001. Il a été puni par les dispositions du CPT, parce qu'il n'y avait pas de normes spécifiques pour les crimes commis par l'intermédiaire de l'internet. Donc on a introduit un article dans la Loi sur la presse et essayé de résoudre les problèmes issus de l'utilisation de l'internet.

Ces dispositions n'ont pas été suffisantes et le besoin d'une loi spécifique s'est montré. Alors en 2007 la « Loi no. 5651 sur la régulation les publications faites dans le domaine d'internet et sur le combat avec les infractions commises par l'intermédiaire de ces publications » a été mise en vigueur.

---

* 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.

* Dr. iur. E. Eylem AKSOY RETORNAZ: Collaboratrice scientifique, Université de Galatasaray, Faculté de droit, Département de droit pénal et de procédure pénale.
Dr. Sinan ALTUNÇ: Maître de conférence, Université de Bahçeşehir, Faculté de droit, Département de droit pénal et de procédure pénale.

(3) Pour rattraper l'évolution des besoins et des circonstances ainsi que pour atteindre de nouveaux objectifs, certaines lois sont les sujets de fréquentes modifications. Normalement, ces modifications prennent la forme de nouvelles lois. Dans certains cas, ces nouvelles lois, au lieu de simplement modifier les parties de la loi qui doivent être modifiées, présentent les modifications nécessaires dans un texte consolidé avec tous les amendements passés. Cette technique est appelée "la refonte". Est-ce la façon dont les lois sur la cyber-criminalité sont mises à jour et adaptées aux changements de réalité dans votre pays? Veuillez fournir les références et les citations appropriées.

Comme on en a déjà parlé, jusqu'à la Loi no. 5651, les modifications ont été faites par les articles particuliers dans le lois. Mais la Loi no. 5651 est completement relative à l'internet. Quant aux changements effectués au sein du CPT afin de incriminer les actes commis par l'intermédiaire de l'internet, on a modifié les parties intéressées.

(C) Les infractions spécifiques à la cybercriminalité

(1) En ce qui concerne l'élément moral, les infractions relatives à la cybercriminalité doivent-elles être intentionnelles? Ont-elles besoin d'une intention spécifique?

Les infractions relatives à la cybercriminalité doivent être intentionnelles. Elles n'ont pas besoin d'une intention spécifique.

(2) Y a-t-il également des infractions par négligence dans ce domaine?

Ces infractions ne sont pas l'objet de la négligence. Mais dans l'article 243 alinéa 3 du CPT, il s'agit d'une circonstance aggravante quand les données se perdent ou se changent. Quand même ce résultat peut être réalisé par négligence.

(3) Si oui, veuillez fournir une liste de ces infractions.

-

(a) L'intégrité et la fonctionnalité du système informatique

1. Accès illégal et interception de la transmission

a. Objet : système ou données?

Votre droit pénal érige-t-il en infraction pénale l'entrave grave et non autorisée faite au fonctionnement d'un ordinateur et/ou d'un système électronique en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant ou supprimant des informations ou des données à partir d'un système informatique, logiciel ou programme?

Dans le CPT, on a deux articles qui incriminent ces infractions. L'article 243, intitulé "entrer dans le système informatique" et l'article 244, intitulé "entraver, détériorer le système, effacer ou changer les données".

L'article 243 incrimine le fait d'entrer dans le système et y rester illégalement. L'article 244 incrimine l'entrave du fonctionnement d'un système informatique.

b. Exigence de la violation des mesures de sécurité?

Est-ce une exigence de votre droit pénal que le pirate effectue le piratage du système informatique en utilisant un ou plusieurs logiciels nécessaires pour vaincre les mesures de sécurité et gagner l'accès au niveau d'entrée ou à un niveau?

Non. Il suffit d'entrer dans le système informatique illégalement.

2. Les interférences de données et du système

a. Objet - la protection du système / matériel / données?

Votre droit pénal définit-il « l'ordinateur et / ou les données électroniques »? Est-ce que cette définition comprend des programmes, des logiciels ou de codage similaires?

Si vous avez une définition, veuillez la fournir accompagnée de la référence aux paragraphes des articles connexes ou de votre code.

"La Loi no. 5651 sur la régulation les publications faites dans le domaine d'internet et sur le combat avec les infractions commises par l'intermédiaire de ces publications" nous donne la définition de la donnée. D'après cette définition la donnée est la valeur sur laquelle il est possible de faire l'opération par l'ordinateur. Mais il n'y a pas de définition de l'ordinateur ou les données électroniques.

b. Acte - Destruction / modification / rendre inaccessible?

i. Votre droit pénal incrimine-t-il l'effacement non-autorisé, la modification, le fait de rendre inaccessible, d'acquérir des informations ou les données à partir d'un ordinateur, d'un système électronique ou un programme ? D'autres interférences similaires avec les informations ou les données à partir d'un ordinateur, d'un système électronique ou un programme sont-elles incriminées?

L'article 244 du CPT incrimine ces actes. L'alinéa 1 incrimine l'acte d'entraver ou de détériorer le fonctionnement du système informatique. L'alinéa 2 prévoit l'incrimination des faits de détériorer, d'effacer, de changer, de rendre inaccessible les données qui se trouvent dans le système. En plus on incrimine les faits d'installer des données dans le système ou d'envoyer les données existantes ailleurs.

ii. Votre droit pénal incrimine-t-il l'interception non autorisée de la transmission de quelque manière que ce soit de données informatiques ou électroniques et / ou d'informations?

D'une part l'article 124 du CPT sanctionne le fait d'entraver illégalement la communication qui se déroule entre les individus. La transmission des données informatiques ou électroniques peut s'entendre comme la communication. Donc « entraver la communication » résulte « entraver la transmission des données ».

D'autre part l'article 244 du CPT (susmentionné) peut aussi accepter en tant qu'une disposition qui incrimine l'interception non autorisée parce que l'article parle d'entraver le fonctionnement d'un système informatique.

3. Les fausses données

a. Objet - l'authenticité?

Votre droit pénal définit-il, comme une infraction pénale, la saisie non-autorisée, l'altération, l'effacement ou la suppression des données informatiques ou électroniques résultant de données inauthentiques, afin de protéger l'authenticité des données qui seront utilisées à des fins juridiques? Si vous disposez d'une définition, veuillez la fournir avec les références aux paragraphes pertinents ou articles de votre code et / ou lois spéciales.

La première disposition est l'article 136 du CPT. Cet article incrimine le fait de « donner, diffuser ou obtenir illégalement les données ». Parmi les articles qui régularisent les infractions informatiques il n'y a pas de disposition qui sanctionne clairement ce type de faits.

En plus dans la Loi sur la signature électronique, l'article 17 incrimine le fait de former un certificat électronique faux ou bien d'imiter ou d'abimer les certificats qui ont été créés légalement.

b. Acte - modification / suppression

Votre droit pénal incrimine-t-il la saisie non autorisée, le changement, l'effacement ou la suppression de données informatiques ou électroniques aboutissant à des données inauthentiques avec l'intention qu'elles soient considérées comme ou agissent sur des buts légaux, comme si elles étaient authentiques? Si oui, veuillez fournir la référence des paragraphes pertinents ou des articles de votre code.

La Loi sur la signature électronique, l'article 17 incrimine le fait de former un certificat électronique faux ou bien d'imiter ou d'abimer les certificats qui ont été crées légalement.

4. Les abus de dispositifs

a. Objet - type de dispositif?

Votre droit pénal incrimine-t-il le développement de la «boîte à outils » d'un hacker ou d'une partie de celle-ci (par exemple, les cartes d'acquisition de mots de passe et les enregistreurs de frappe, programmes blue-box, les war-dialers, les logiciels de cryptage, les programmes qui craquent les mots de passe, les scanners de vulnérabilité de la sécurité, des packet sniffers, etc) pour l'accès non autorisé à un ordinateur ou à des systèmes électroniques ou de transmissions?

Dans le domaine des cyber-crimes, on rencontre peu aux dispositions qui incriminent les actes préparatoires. Mais il y a deux cas où l'obtention ou la possession incriminent.

Selon l'article 72 de la Loi sur les œuvres intellectuelles et artistiques, celui qui produit, offre à la vente, vend ou **possède pour l'utilisation personnelle** les programmes ou hardwares techniques afin de rendre ineffectif les programmes qui ont été produits pour éviter la multiplication illégalement d'un programme informatique, sera puni avec une peine d'emprisonnement de 6 mois à 2 ans.

Selon l'article 245 alinéa 2 du CPT, celui qui produit, vend, transfert, achète ou accepte des faux cartes bancaires ou cartes de crédit seront punis avec la peine d'emprisonnement de 3 à 7 ans.

b. Acte - distribution publique / transfert à une autre personne?

i. Votre droit pénal incrimine-t-il l'utilisation non-autorisée de l'un des outils du hacker énumérés ci-dessus?

Pour incriminer l'utilisation non-autorisée de l'un des outils du hacker énumérés ci-dessus, cette utilisation doit être atteindre au niveau d'entrer non-autorisé au système informatique.

ii. Votre droit pénal incrimine-t-il la distribution publique et / ou le transfert à d'autres parties de l'information électronique piratée?

Dans l'article 244 alinéa 2, le fait de transférer les données qui se trouvent dans un système informatique à d'autres parties.

En outre, si l'information est en forme de la communication entre les individus, il s'agit de l'infraction de la divulgation illégale du contenu de la communication. Si cette infraction est commise par la voie de la presse ou la media, la peine sera augmentée.

Si ces informations sont en forme des voix ou des images relatives à la vie privée des individus, l'article 134 alinéa 2 du CPT sera applicable. L'article 134 alinéa 2 incrimine le fait de divulguer les voix ou les images relatifs a la vie privée des individus et prévoit une peine d'emprisonnement de 1 à 3 ans.

Enfin, selon l'article 136, le fait de donner, de diffuser ou d'obtenir illégalement les données personnelles est passible d'une peine d'emprisonnement de 1 à 4 ans.

c. Possession?

Votre droit pénal incrimine-t-il la possession de «boîte à outils » d'un hacker ou d'une partie de celle-ci (par exemple, les cartes d'acquisition de mots de passe et les enregistreurs de frappe, programmes blue-box, les war-dialers, les logiciels de cryptage, les programmes qui craquent les mots de passe, les scanners de vulnérabilité de la sécurité, des packet sniffers, etc) pour l'accès non autorisé à un ordinateur ou à des systèmes électroniques ou de transmissions?

Dans le domaine des cyber-crimes, on rencontre peu aux dispositions qui incriminent les actes préparatoires. Mais il y a deux cas où l'obtention ou la possession incriminent.

Selon l'article 72 de la Loi sur les œuvres intellectuelles et d'art, celui qui produit, offre à la vente, vend ou **possède pour l'utilisation personnelle** les programmes ou hardwares techniques afin de rendre ineffectif les programmes qui ont été produits pour éviter la multiplication illégalement d'un programme informatique, seront punis avec une peine d'emprisonnement de 6 mois à 2 ans.

Selon l'article 245 alinéa 2 du CPT, celui qui produit, vend, transfert, achète ou accepte des faux cartes bancaires ou cartes de crédit seront punis avec la peine d'emprisonnement de 3 à 7 ans.

(b) La vie privée

1. La violation du secret des données privées

a. Objet - type de données privées?

(Remarque: les données privées sont des données qui appartiennent à la vie privée des gens, mais n'identifient pas ou ne permettent pas d'identifier une personne, par exemple, l'état civil, l'orientation sexuelle, l'état de santé, les habitudes d'achat ou de préférences)

i. Les lois de votre pays exigent-elles que les collecteurs de données divulguent leurs pratiques d'information avant de recueillir des informations privées auprès des consommateurs comme, par exemple, la façon dont l'information est utilisée, la manière dont elle est recueillie et le but de cette collecte? Si elle est partagée avec d'autres et si les consommateurs ont un contrôle sur la divulgation de leurs données privées?

Selon l'article 20 alinéa 3 de la Constitution turque, « tout le monde a le droit de demander la protection de ses données personnelles. Ce droit inclut être informe de l'avoir accès à et de demander la correction et l'effacement de ses données personnelles et être informe si ces données sont utilisées les objectives envisagées. Les données personnelles ne peuvent être allé en procession que aux cas ou il est prévu dans la loi ou quand l'individu donne son consentement. Les principes et les procédures relatifs à la protection des données personnelles sont prévus pas la loi. » Il n'y a pas encore une telle loi en Turquie. Mais les travaux continuent sur le Projet de Loi sur la protection des données personnelles.

Dans les lois qui sont en vigueur, on rencontre des dispositions sur l'interdiction de collecte des données personnelles sans autorisation préalable ou sans consentement de l'individu. Par exemple on peut parler de la Loi sur la signature électronique. L'article 12 de cette loi règlemente la protection des informations. Selon cet article, quand on demande le certificat électronique d'un individu, les informations nécessaires ne peuvent être pris qu'avec son consentement et les informations obtenues ne peuvent pas être partagées avec les tierces personnes sans l'autorisation de celui-ci.

Dans l'article 73 de la Loi sur la banque, on parle de garder les informations apprises pendant les activités bancaires. La Loi sur les cartes bancaire et les cartes de crédit aussi prévoit une règle similaire dans l'article 23.

ii. Les lois de votre pays exigent-elles que les sociétés et les entités qui font des affaires sur internet, informent les consommateurs de l'identité de celui qui collecte des données, du fait du caractère volontaire ou obligatoire de la fourniture des données demandées ainsi que les mesures prises par le collecteur de données pour assurer la confidentialité, l'intégrité et la qualité des données?

Le Projet de Loi sur la régulation du commerce électronique est important. Ce projet de loi prévoit que, avant la signature du contrat, le fournisseur des services offre les informations sur la confidentialité aux consommateurs. Il doit expliquer s'il sera possible d'accéder au contrat suivant la signature et combien de temps cet accès sera possible. Le fournisseur des services sera responsable de la protection et de la sécurité des données personnelles.

iii. Les lois de votre pays exigent-elles des sites Web d'afficher leur politique de confidentialité et d'expliquer comment les renseignements personnels seront utilisés avant que les consommateurs entrent dans le processus d'achat ou de toute autre opération pour laquelle ils doivent fournir des informations sensibles?

Dans l'article 9/A de la Loi sur la protection du consommateur, on a fait une disposition sur les contrats à distance. La conclusion d'un contrat à distance peut se faire par tout moyen utile (par téléphone, courrier électronique, catalogue, etc.) sans qu'il y ait présence physique et simultanée des parties au contrat. Avant conclure un contrat à distance, quelques informations doivent être données aux consommateurs.

iv. Le droit pénal de votre pays incrimine-t-il l'omission de fournir les informations mentionnées ci-dessus (Cf : a.ii et a.iii)?

Le droit pénal turc accepte ce type d'omissions en tant que contravention et prévoit des sanctions administratives.

b. Acte - L'utilisation illégale et le transfert / distribution?

i. Le droit pénal de votre pays définit-il le transfert et la distribution illégale des données privées?

Le droit pénal turc définit les données. Dans l'article 2 de la Loi sur la réglementation des diffusions d'internet et contre les infractions commises par la voie d'internet, la donnée est définie comme toutes sortes de valeurs sur lesquelles on peut faire des opérations par ordinateur.

Le Projet de loi sur la protection des données personnelles définit la donnée personnelle en tant que toutes informations relatives aux personnes déterminées ou déterminables.

Mais le droit pénal turc n'a pas fait la définition le transfert et la distribution illégale des données privées.

ii. Le droit pénal de votre pays incrimine-t-il l'utilisation illégale, le transfert et /ou la distribution des données privées?

L'article 136 du CPT incrimine le transfert, la diffusion ou l'obtention illégale des données personnelles.

c. Justification?

i. Dans quelles conditions les lois de votre pays autorisent-elles la collecte, le traitement autorisé, le transfert et la distribution de données privées?

Premièrement, le droit turc autorise la collecte, le traitement autorisé, le transfert et la distribution de données privées/personnelles, quand il y a le consentement de l'intéressé. En fait, le consentement de l'intéressé est un fait justificatif général réglementé dans l'article 26 du CPT. Donc on peut appliquer cette justification dans ces cas-là.

Deuxièmement on parler de la légalité d'enregistrement des données personnelles. Un autre fait justificatif est l'ordre de la loi, réglemente dans l'article 24 du CPT. Donc si l'enregistrement est effectué à l'issue de l'ordre de la loi, il sera justifié. Par exemple, le Code de procédure pénale (CPP) nous montre les conditions qui autorisent la collecte ou la saisie.

ii. Quelle règle de nécessité est requise pour autoriser une collecte et /ou une distribution (convaincante, importante, raisonnable, pratique)?

Pour autoriser une collecte ou une distribution, la règle de nécessité doit être convaincante.

2. Violation du secret professionnel

a. Objet - type de données privées?

i. Les lois de votre pays exigent-elles des professionnels de divulguer :

- Les informations collectées et les pratiques de gestion avant la collecte d'informations personnelles de leurs patients ou clients;

- Leurs pratiques de divulgation;

- Leurs obligations éthiques professionnelles;

- Et si les patients ou les clients ont un contrôle sur la divulgation de leurs données personnelles?

Dans les lois turques, on prévoit que les personnes mentionnées ci-dessus, doivent garder les informations personnelles qu'ils sont informées au cours de leurs professions. Par exemple, les avocats ne peuvent pas divulguer

les informations que leurs clients leur ont données. En plus selon l'article 46 du CPP, les avocats ne peuvent pas faire témoignage sur ces informations sans qu'il y ait l'autorisation de leurs clients.

Selon l'article 258 du CPT, il est interdit pour les fonctionnaires de divulguer les informations dont ils sont informés au cours de leur fonction.

Quant aux médecins, l'article 134 du CPT peut être appliqué. Dans cet article, la divulgation des voix et des images relatifs à la vie privée des individus est incriminée. En plus, le décret sur la déontologie médicale parle de la même interdiction dans son article 4, alinéa 1. L'interdiction similaire pour le témoignage des médecins est réglementée le même article 46 du CPP.

ii. Quelles sont les données spécifiquement protégées, le cas échéant?

Les données dont ils sont informés au cours de leur profession sont protégées.

iii. La législation pénale de votre pays autorise-t-elle ou même exige-t-elle de la part des médecins, des avocats, des prêtres, etc… de violer la confidentialité dans certaines situations ou pour certaines raisons prévues par la loi? Dans quels cas serait-ce possible? (Exemples de cas : croire raisonnablement qu'il y a des abus voire un cas de maltraitance à l'égard d'un enfant, des femmes ou des personnes âgées)?

Dans l'article 278 on incrimine le fait de ne pas dénoncer l'infraction. A l'alinéa 4 de cet article, on parle des personnes qui ont le droit de ne pas témoigner. Ces personnes ne seront pas sanctionnées sauf si ils ont la charge d'éviter la commission d'une infraction.

En plus de cela, les articles 279 et 280 réglementent des infractions similaires. L'article 279 incrimine la non-dénonciation des fonctionnaires, et l'article 280 celle des membres de la profession de la santé. Donc ces gens là sont tenus de violer la confidentialité dans les situations susmentionnées.

En outre, la Loi de la protection de la santé générale prévoit de dénonciation des maladies vénériennes.

b. Sujets - Type d'auteurs?

Le droit pénal de votre pays identifie-t-il les catégories de professionnels qui sont liées par des règles spécifiques de confidentialité?

L'article 46 du CPP réglemente l'abstention du témoignage à cause de la profession. Dans cet article quelques professionnels sont mentionnés. Ce sont les avocats, les médecins, les pharmaciens, les dentistes, les accoucheuses, tous les autres membres de la professions de santé, les conseillers financiers et les notaires.

A part, l'article 239 du CPT le fait de donner ou de divulguer les informations à caractère secret commercial, bancaire ou de client.

En dernier, l'article 258 punit les fonctionnaires qui divulguent les informations qui doivent rester secrètes.

c. Acte - l'utilisation illégale et le transfert / distribution?

Quels sont les actes (par exemple la collecte illégale, l'utilisation, le transfert et la distribution) qui sont spécifiquement punis par le droit pénal de votre pays?

Dans le cas où la collecte des informations est considérée légale, la divulgation et le transfert illégaux des informations secrètes peuvent être punis. Ici celui qui collecte les informations le fait parce que c'est sa profession.

Par exemple, la police a le pouvoir de collecter des informations si elle a un ordre de l'autorité légitime. Mais si la collecte est illégale, alors cette fois-ci celui qui collecte sera responsable.

3. Traitement illégal de données personnelles et privées

a. Objet?

Votre droit pénal incrimine-t-il l'acquisition illégale et non autorisée, la transformation, le stockage, l'analyse, la manipulation, l'utilisation, la vente, le transfert etc, de données personnelles et privées?

L'article 135 du CPT punit l'enregistrement des données personnelles et l'article 136 du CPT punit la délivrance ou l'obtention illégale des données.

b. Sujet?

Votre droit pénal identifie-t-il particulièrement les catégories de personnes et les entités qui sont concernées par cette interdiction pénale et ses sanctions?

Si les infractions contre la vie privée et le domaine secret de la vie sont commises (1) par les fonctionnaires en abusant leurs pouvoirs ou (2) en profitant de la facilité fournie par une profession, la peine sera augmentée. En outre l'article 140 du CPT prévoit la punition des personnes morales en cas de commission ces infractions.

c. Acte?

i.Votre droit pénal sanctionne-t-il les actes spécifiques qui constituent tout ou partie du traitement illégal des données personnelles et privées? Répondre pour chaque catégorie ci-dessous en citant la législation pertinente et, le cas échéant, les dispositions :

1. La collecte illégale

L'article 136 du CPT : « Celui qui donne les données personnelles à l'autrui, les diffusent ou les obtient illégalement sera puni par l'emprisonnement de un à quatre ans. » On peut considérer l'obtention illégale des données comme la collecte illégale.

2. L'utilisation illégale

L'article 136 du CPT : « Celui qui donne les données personnelles à l'autrui, les diffuse ou les obtient illégalement sera puni par l'emprisonnement de un à quatre ans. » Donner ou diffuser les données personnelles exige les utiliser. Donc ces actes définis dans cet article signifient en même temps l'utilisation illégale.

3. La rétention illégale

L'article 138 du CPT : « Celui qui s'abstient de supprimer les données qui se trouvent dans le système après un délai déterminé par la loi, sera puni par l'emprisonnement de six mois à un an. »

4. Le transfert illégal

L'article 136 du CPT : « Celui qui donne les données personnelles à l'autrui, les diffusent ou les obtient illégalement sera puni par l'emprisonnement de un à quatre ans. »

ii. Existe-t-il une différence si ces données personnelles et privées sont utilisées, transférées etc, pour des enquêtes de police ou à des fins judiciaires?

Quand les données personnelles et privées sont utilisées, transférées, etc. pour des enquêtes de police ou à fins judiciaires, cette utilisation, ce transfert, etc. ne seront plus illégaux. Il y a des dispositions dans le CPP qui rendent

ces actes légaux. Par exemple l'article 135 du CPP réglemente le constat, l'interception, l'enregistrement de la télécommunication du suspect ou de l'inculpé afin d'obtenir la preuve. En plus, l'article 134 du CPP donne le pouvoir de faire la perquisition, la transcription et la saisie sur les ordinateurs. Ces interceptions peuvent être effectuées suivant la décision du juge ou l'ordre écrite du procureur. La police est tenue d'appliquer cette interception. Donc s'il y a une telle décision ou un tel ordre, le fait de la police sera légal.

d. Justification?

i. Dans quelles conditions la loi de votre pays permet-elle la collecte, le traitement autorisé, le transfert et la distribution de données personnelles et privées?

Premièrement, le droit turc autorise la collecte, le traitement autorisé, le transfert et la distribution de données privées/personnelles, quand il y a le consentement de l'intéressé. En fait, le consentement de l'intéressé est un fait justificatif général réglementé dans l'article 26 du CPT. Donc on peut appliquer cette justification dans ces cas-là.

Deuxièmement on parler de la légalité d'enregistrement des données personnelles. Un autre fait justificatif est l'ordre de la loi, réglemente dans l'article 24 du CPT. Donc si l'enregistrement est effectué a l'issue de l'ordre de la loi, il sera justifié. Par exemple, le CPP nous montre les conditions qui autorisent la collecte ou la saisie.

ii. Quel cas de nécessité est requis pour une collecte autorisée et/ou la distribution de données à caractère personnel et privé (Convaincante, importante, raisonnable, pratique)?

Pour autoriser une collecte ou une distribution, la règle de nécessité doit être convaincante.

4. Le vol d'identité

(Remarque: le vol d'identité se produit lorsque quelqu'un s'approprie les renseignements personnels d'autrui, sans que ce dernier en ait connaissance, pour commettre un vol ou une fraude. Le vol d'identité est un moyen pour perpétrer des fraudes. En règle générale, la victime est amenée à croire qu'elle doit divulguer des renseignements personnels à une entreprise ou une entité légitime, parfois comme une réponse à une sollicitation d'e-mail de mettre à jour la facturation ou les renseignements sur l'adhésion ou comme une application frauduleuse d'affichage sur internet pour un emploi ou pour un prêt.)

a. Objet

i. Votre droit pénal incrimine-t-il le vol d'identité? Veuillez citer le texte légal pertinent.

L'identité doit être considérée comme une donnée personnelle. Donc l'article 136 du CPT qui réglemente l'obtention illégale des données personnelles peut être appliqué pour le vol d'identité.

A part cela, dans l'article 142 alinéa 2, la sanction du vol est augmentée si cet acte est commis par l'utilisation des systèmes informatiques. Aussi dans l'article 158 alinéa 1, la sanction de l'escroquerie est augmentée, si elle est commise par l'utilisation des systèmes informatiques.

ii. Votre droit pénal proscrit-il les formes spécifiques de vol d'identité, comme le phishing, par exemple? Le phishing est défini comme une forme de vol d'identité en ligne qui utilise des emails usurpés conçus pour attirer les destinataires vers des sites frauduleux qui tentent de les inciter à divulguer des données financières personnelles telles que les numéros de cartes de crédit, les noms d'utilisateur et les mots de passe pour accéder aux comptes, les numéros de sécurité sociale etc…

Il n'y a pas en droit turc une disposition qui incrimine clairement ce type d'actes. Mais la Cour de cassation turque, applique les règles relatives à l'escroquerie.[1]

b. Sujet

Votre droit pénal contient-il une responsabilité pénale liée à la personnalité numérique d'une personne, ou à son Avatar, ou à son personnage numérique dans un jeu de simulation basé sur internet (par exemple Cityville, Farmville, etc)? Veuillez citer la loi pertinente.

Le droit pénal turc ne contient pas une responsabilité pénale liée à la personnalité numérique d'une personne, ou à son avatar, ou à son personnage numérique dans un jeu de simulation basé sur internet. On accepte que le droit pénal doive être *ultima ratio.* Donc si on incrimine ces types de faits, alors on élargit énormément le domaine d'intervention du droit pénal.

(c) la protection contre les contenus illicites: les TIC connexes

1. Objet

a. La pornographie infantile - des images d'enfants réels ou virtuels?

i. Votre droit pénal incrimine-t-il l'utilisation d'internet dans le but de stocker, d'accéder et de diffuser de la pédopornographie? Si c'est le cas, veuillez citer les textes légaux pertinants.

Le droit turc n'adopte pas une définition de la pédopornographie. Néanmoins, l'article 226 al. 3 du Code pénal turc (CPT) intitulé « l'obscénité » incrimine le fait d'utiliser des enfants afin de fabriquer des images, des sons et des textes de caractère obscène. Cette infraction est passible d'une peine privative de liberté de cinq ans à dix ans d'emprisonnement et de cinq mille jours de jours-amendes. Au titre du même alinéa de l'art. 226 CPT, « Celui qui aura importé, mis en circulation, vendu, diffusé, transféré, possédé, pris en dépôt, ou mise à disposition d'un tiers sera puni d'une peine privative de liberté de deux à cinq ans et de cinq mille jours de jours-amendes. »

Il convient de noter qu'en droit turc, à défaut d'une définition claire de ce qu'est l'obscénité, toute image, son et texte, même de nature érotique, peut être considéré comme obscène Cela constitue, à nos yeux, une violation de la légalité des délits et des peines.

La diffusion par voie de presse ou médias est prévue comme une circonstance aggravante dans l'art. 226 al. 5 CPT.

ii. En particulier, votre droit pénal :

Crée-t-il une nouvelle infraction qui cible les criminels qui utilisent internet pour leurrer et exploiter les enfants à des fins sexuelles?

[1] Dans une de ces decisions, la Cour de cassation applique les regles relatives à l'escroquerie. Selon le fait, l'inculpé a obtenu le code de MSN de la plaignante et apres lui demande d'envoyer de l'argent par la voie de MSN. La Chambre criminelle numéro 11 de la Cour de cassation applique l'article 158 dans cette affaire. (C. Cass. 11. chambre crim., 18.03.2010, 2007/5408, 2010/3253).

Incrimine-t-il:

1. la transmission,

2. la mise à disposition,

3. l'exportation

4. et l'accès intentionnel à de la pédopornographie sur internet;

Le fait de diffuser, de servir d'intermédiaire pour la diffusion, de mettre à disposition d'un tiers par voie de presse ou de publications constitue une circonstance aggravante de l'infraction d'obscénité au terme de l'art 226 al. 5.

Les termes «par voie de la presse et des publications» signifie «la diffusion d'informations par l'intermédiaire de moyens d'information de masse écrits, audiovisuels et électroniques» selon l'article 6 CPT consacré aux «définitions».

Se pose la question de savoir si l'internet pourrait être considéré comme un moyen écrits, audiovisuels et électroniques au sens de l'art 6 CPT.

Conformément à l'article 2 du Code sur internet une plate-forme Web signifie « une plateforme publique installée sur internet en dehors des logiciels de communication ou des systèmes informatiques personnelles ou organisationnelles ». Ni la diffusion du contenu obscène par le biais des logiciels de communication ni des systèmes personnels ou organisationnels n'entrent donc dans le champ d'application de la loi. Pour invoquer la responsabilité pénale au sens de l'art 226 al. 3 et la responsabilité des acteurs d'internet au sens de la loi 5651 sur internet, le contenu obscène doit donc être diffusé sur des sites Web accessibles à tout le monde.

Dans le même sens, la Cour de cassation turque, dans un arrêt rendu en 2007, considère que « *vu les dispositions en vigueur le transfère d'information ou de document par le courrier électronique ne peut être considéré une diffusion par voie de presse et des médias* ».

Permet-il aux juges d'ordonner la suppression de la pédopornographie affichée sur des systèmes informatiques dans votre pays;

La législation turque ne permet pas au juge d'ordonner la pédopornographie affichée sur des systèmes informatiques.

Cependant l'art. 8 de la loi 5651 permet au juge d'interdire l'accès à un site Web si des raisons suffisantes permettent de soupçonner que certaines infractions sont commises par l'intermédiaire d'un site Web. Ces infractions sont les suivantes : (i) l'incitation au suicide, (ii) les violences sexuelles faites aux enfants, (iii) le fait de faciliter la toxicomanie, (iv) la fourniture de produits dangereux pour la santé, (v) l'obscénité, (vi) la prostitution, (vii) les jeux d'argent, ainsi que (viii) les infractions régies par le Code turc 5816, qui incrimine les actes portant atteinte à la mémoire d'Atatürk.

Lorsqu'il est saisi d'une plainte ou par suite de ses propres constatations, le parquet peut demander à un juge d'ordonner l'interdiction d'accès au site Web concerné dans un délai de vingt-quatre heures. Le parquet peut, en cas d'urgence ordonner lui-même cette interdiction, qui doit ensuite être approuvée par un magistrat dans un délai de vingt-quatre heures (la décision du juge doit par conséquent suivre dans ce délai de vingt-quatre heures). L'interdiction donnée doit être appliquée dès que possible et exécutée par le fournisseur d'accès Internet dans un

délai de vingt-quatre heures à compter de l'ordonnance judiciaire. En cas de rejet de l'interdiction par le juge, le parquet est tenu de rétablir intégralement l'accès au site Web en question.

Lorsque le parquet conclut à l'absence de contenu incriminé sur le site Web concerné ou si le tribunal estime que ce contenu n'est pas constitutif d'une infraction, l'interdiction est levée et l'accès au site Web est rétabli.

Si le fournisseur d'accès Internet ou le fournisseur d'hébergement ne bloque pas intégralement l'accès au site Web en question, le personnel responsable est passible d'une peine de deux à six mois d'emprisonnement.

De plus, la Présidence des télécommunications et des transmissions, instituée par ladite loi et placée sous la tutelle du Conseil turc des télécommunications, est habilitée à interdire un site Web sans l'approbation d'un juge lorsque celui-ci est constitutif de l'infraction d'obscénité et que son contenu et son fournisseur d'hébergement réside hors du territoire turc ou lorsqu'un site Web comporte un contenu constitutif de violences sexuelles faites aux enfants ou obscène et que son contenu et le fournisseur d'hébergement réside en Turquie. Cette interdiction doit ensuite être appliquée par le fournisseur d'accès Internet. Chaque fois que l'auteur de l'infraction et son lieu de résidence sont identifiés, la présidence est tenue d'en informer le parquet, afin que ce dernier engage des poursuites.

Le particulier qui estime qu'un site Web porte atteinte à ses droits subjectifs (l'enfant victime, les parents qui ont l'autorité parentale ou son tuteur dans le cas d'obscenité) peut demander au fournisseur d'accès Internet ou au fournisseur d'hébergement la suppression de ce contenu et la publication d'un droit de réponse pendant une période de sept jours et sur un espace aussi étendu que le contenu initialement présenté, à l'endroit même de sa présentation. Les fournisseurs d'accès Internet ou le fournisseur d'hébergement sont tenus de répondre favorablement à cette demande dans un délai de deux jours. Passé ce délai, la demande est présumée rejetée. Dans ce cas, le juge de paix local peut en être saisi dans un délai de quinze jours. Il lui incombe alors de statuer dans un délai de trois jours sans procès. Sa décision est susceptible d'appel devant les juridictions supérieures.

Lorsque le juge de paix fait droit à la demande, le fournisseur d'accès Internet ou le fournisseur d'hébergement à l'obligation de supprimer le contenu en question et de publier un droit de réponse du plaignant dans un délai de deux jours. En cas de refus d'exécuter la décision du juge de paix, le personnel responsable du fournisseur d'accès Internet ou du fournisseur d'hébergement est passible d'une peine de six mois à deux ans d'emprisonnement.

Permet-il à un juge d'ordonner la confiscation de tout matériel ou équipement utilisé dans la perpétration d'une infraction de pédopornographie;

En droit turc, le juge peut prononcer la confiscation des objets qui ont servi ou devaient servir à commettre une infraction ou qui sont le produit d'une infraction à condition que ces objets n'appartiennent pas à des tiers en vertu de l'art. 54 al. 1 CPT. Les objets dont la production, le stockage, l'utilisation, le transport, l'achat ou la vente constitue une infraction fait l'objet de la confiscation selon l'art 54 al. 4

La confiscation est une mesure de sûreté selon le CPT donc le juge peut confisquer les valeurs patrimoniales alors même qu'aucune personne déterminée n'est punissable.

Le juge peut donc ordonner la confiscation de tout matériel ou équipement utilisé dans la perpétration d'une infraction de pédopornographie en vertu de l'art 54 al.1 et 4 du CPT

Criminalise-t-il:

1. l'accès en connaissance de cause à la pornographie infantile sur internet

2. la transmission de pornographie infantile sur Internet

3. l'exportation de pornographie juvénile sur Internet

4. La possession de pornographie juvénile sur internet dans le but, par exemple, de transmettre, d'exporter ...?

L'art 226 CPT punit la simple possession, de la pornographie infantile. Selon la Cour de cassation turque, l'auteur est punissable même s'il ne possède pas la pornographie infantile à des fins commerciales mais à usage personnel.

Aux yeux de la Cour de cassation, la pornographie enfantine téléchargée et stocké de manière systématique et continue entraîne sa possession. Cependant, le seul fait d'accéder à un site Web et de visionner les images, en connaissance de cause ne suffit pas à caractériser l'infraction prévu par l'article 226-23, alinéa 3, du Code pénal.

iii. Votre droit pénal incrimine-t-il la sollicitation en ligne des enfants à des fins sexuelles via des sites Web de réseaux sociaux et des chats?

L'art. 103/1 CPT incrimine l'abus sexuel sur mineur. Selon cette disposition «l'auteur de tout acte à caractère sexuel sur un mineur de moins de 15ans, ou sur une personne de 15 ans ou plus incapable de comprendre les conséquences juridiques d'un tel acte, est passible de trois à huit ans d'emprisonnement. Le code ne définit pas les actes à caractère sexuel.

Par « *acte à caractère sexuel* », la jurisprudence entend, en effet, un contact physique sans nécessairement une relation sexuelle.

Nonobstant la jurisprudence, d'aucuns considère que l'infraction peut être constitué sans contact même en l'absence de contact de physique. Cela étant les propos, gestes et mimiques d'ordre sexuels adressé au mineur sur les réseaux sociaux sur internet suffit à caractériser l'infraction d'abus sexuel sur mineur.

L'incitation à la prostitution d'un mineur peut être commise par le biais d'internet.

iv. La définition de la pornographie juvénile dans votre code pénal est-elle proche de celle contenue dans les instruments internationaux (par exemple directives de l'UE)?

La Turquie a signé le Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants et l'a ratifié par la loi n°4755 de 2002. Elle signé la Convention sur la cybercriminalité du Conseil de l'Europe en 2010 mais ne l'a pas encore ratifié. Elle fait partie aussi de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels.

Même si la Turquie a érigé en infractions pénales la plupart des actes que les États membres sont invités à interdire conformément aux dispositions du Protocole, aucune définition de la pornographie enfantine n'est adoptée.

Certaines modifications ont été apportées dans la législation turque afin de se conformer notamment à l'art. 8 du Protocole facultatif. L'art. 52/3 et 226 du CPP s'inscrivent dans cette ligne. L'audition d'un mineur victime d'une infraction sexuelle devra faire l'objet d'un enregistrement sonore ou audiovisuel. Un tel enregistrement est en effet de nature à limiter le nombre des auditions de la victime, mais aussi à faciliter l'expression de l'enfant tout en permettant d'y déceler les éléments non verbalisés et de les mémoriser pour la suite de la procédure. Cet enregistrement, est, aux termes de la loi, obligatoire dans toutes les procédures où des mineurs victimes doivent être entendues. L'enfant victime doit être accompagné par des spécialistes lors de son audition.

v. La victimisation secondaire est-elle évitée pour les victimes de pornographie infantile dans votre droit pénal ? Dans des États où la prostitution ou l'apparition dans la pornographie sont punissables sous couvert du droit pénal national, il devrait être possible de ne pas poursuivre ou de ne pas imposer de peines conformément aux lois dans le cas où l'enfant concerné a commis ces actes car il est victime d'exploitation sexuelle ou a été contraint à participer à la pornographie d'enfant. Ceci est-il envisagé par votre droit pénal?

La prostitution n'est pas incriminée en droit turc. Cependant, l'incitation à la prostitution constitue une infraction en vertu de l'art 227 al. 1 CPT. Toute personne qui incite un enfant à la prostitution, facilite la prostitution d'un enfant, procure le matériel nécessaire ou sert d'intermédiaire en vue de la prostitution d'un enfant encourt de 4 à 10 ans d'emprisonnement assortis de 5 000 jours-amende. La personne incitée à la prostitution considérée comme victime n'est ni poursuivie, ni punie.

vi. Votre droit pénal incrimine-t-il la pornographie d' « enfant virtuel»? La pornographie d'«enfant virtuel » n'utilise pas de vrais enfants ou d'images d'enfants réellement identifiables. Lorsque l'image n'est pas celle d'un enfant réel mais une combinaison de millions de pixels informatiques fabriqués par un artiste, le gouvernement peut-il interdire cette création dont votre pays est prétendument victime? Veuillez citer la loi applicable et / ou les décisions judiciaires.

Le code pénal turc, en mentionnant expressément, l'utilisation de mineurs, empêche la prise en compte des représentations virtuelles.

Selon l'art 226 al. 7, les dispositions de l'article 226 ne s'appliquent pas aux ouvrages scientifiques et aux œuvres ayant valeur artistique et littéraire à condition que les mineurs ne puissent y avoir accès et n'y figurent pas.

vii. Elément moral: Pour être responsable, la personne doit à la fois avoir l'intention d'entrer dans un site où la pornographie juvénile est disponible et savoir que ce genre d'images peut être trouvé ici. Les sanctions ne devraient pas être appliquées à des personnes qui entrent par inadvertance sur des sites proposant des images pédopornographiques . Est-ce le cas dans le droit pénal de votre pays?

L'infraction d'obscénité (art. 226 CPT) ne peut être commise que de manière intentionnelle.

b. Tout autre objet où la criminalisation dépend de l'utilisation des technologies de l'information et des communications (TIC)

Votre droit pénal incrimine-t-il les situations suivantes? Veuillez citer les lois pertinentes:

1. la création et l'utilisation de l'envoi anonyme et/ou la réception des documents sur les TIC?

2. la cyber-intimidation?

3. le cyber-harcèlement?

4. le cyber-toilettage?

Le cyber intimidation, le cyber harcèlement et le cyber toilettage ne constitue pas une infraction en soi en droit turc. Cependant, il est possible de poursuivre les auteurs desdits actes par les infractions du Code pénal qui correspondent à tels actes : harcelement sexuel (art. 105 CPT), menace (art.106 CPT), chantage (art.107 CPT),violation du secret de la correspondance (art. 132 CPT), violation de la vie privée (art.134 CPT), enregistrement des données personnelles (art.135 CPT), acquisition illégale des données personnelles (art. 136 CPT).

2. Acte - création / adhésion / possession / transfert / distribution publique par les TIC (donner des exemples)

Citer des lois spécifiques qui criminalisent la création (même si elles ne sont jamais utilisées), l'adhésion, la possession (même si elle est seulement privée), le transfert et la distribution publique par internet et par d'autres moyens électroniques de matériaux à côté de ceux déjà mentionnés ci-dessus et ce, en raison précisément d'internet / de l'utilisation de la technologie électronique.

L'art. 226 CPT, calqué sur l'infraction disposé dans le Code pénal allemand incrimine la possession de la pornographie enfantine (le contenu obscène en vertu du texte de la loi).

La possession personnelle ou le stockage des œuvres intellectuelles et artistiques protégées par la loi constitue une infarction en vertu de l'art. 71 de la lois sur la protection de la propriété intellectuelle.

La possession des données est punie indirectement dans les infractions d'acquisition illégale des données personnelles (art. 136 CPT) et le fait de ne pas détruire des données (art. 138 CPT).

(d) La violation des droits de propriété en matière de TIC, y compris la propriété intellectuelle.

Votre droit pénal incrimine-t-il spécifiquement les comportements suivants commis grâce à l'utilisation des TIC?

Veuillez citer les textes légaux de référence.

1. La fraude

L'art. 158 CPT incrimine l'acte d'escroquerie commise en utilisant les systèmes informatiques. Utiliser les systèmes informatiques constitue une circonstance aggravante.

2. La violation de droits de propriété intellectuelle

En outre l'art. 71 de la Loi sur les œuvres intellectuelles et artistiques incrimine l'acte de propager, de changer, de diffuser les œuvres sans la permission préalables de son auteur.

3. L'espionnage industriel

L'art. 239 CPT incrimine la divulgation des secrets commerciaux, bancaires et secrets des clients. L'acte incriminé est de donner aux personnes non-autorisées ou de divulguer les secrets. L'alinéa 2 de cet article prévoit que les informations relatives à l'industrie aussi sont incluses à la protection de cet article.

(e) La criminalisation des actes commis dans le monde virtuel

Votre droit pénal incrimine-t-il la perpétration de crimes commis dans le monde virtuel comme, par exemple, la pédopornographie virtuelle, la violence virtuelle, les graffitis virtuels, la cyber-diffamation, le harcèlement sexuel, le harcèlement au travail lorsqu'ils sont commis sans aucune implication de personnes réelles mais, seulement par des représentations virtuelles? Veuillez citer les textes légaux de référence et fournir des détails.

Le droit pénal turc n'incrimine pas ces types d'actes.

(f) La non-conformité aux infractions

Votre droit pénal incrimine-t-il le refus de coopérer avec les organismes d'application de la loi dans le domaine de la cybercriminalité? L'obligation de coopérer peut-elle avoir pour fonction de retenir et de stocker des informations, pour produire / fournir des informations telles que requis par une ordonnance de

production, de donner accès au cyber-systèmes, d'installer des filtres ou des dispositifs etc. Est-ce que l'obligation de coopération peut également être forcée au moyen de sanctions administratives? Citer la législation pertinente et fournir plus de détails.

(D) Les informations complémentaires facultatives concernant le droit et la pratique (y compris les statistiques)

(1) Les cyber-crimes sont-ils inclus dans la collecte de données sur la criminalité dans votre pays?

À statistiques officielles de l'Institution de statistique turque, on ne peut pas rencontrer l'information sur les cyber-crimes.

(2) Y a-t-il dans votre pays un site Web qui fournit des données et des informations sur l'apparition, la gravité, le coût et plus généralement l'impact de cyber-crimes dans votre pays? Si oui, veuillez fournir l'adresse du site internet.

On peut donner comme exemple les sites d'internet de la police. Les departments sur les infractions informatiques de la police nous donne des informations importantes. (http://www.eskisehir.pol.tr/subeler/kacakcilik/bilisim.asp, http://www.gaziantep.pol.tr/birimdetayoku.aspx?Bid=176&masaadi=Asayis)

A part, on a le site d'internet de l'Association contre les crimes informatiques (www.bsm.org.tr).

Aussi il y a un autre site comme http://privacy.cyber-rights.org.tr.

(3) Les enquêtes sur les victimes dans votre pays comprennent-elles des questions sur les cyber-crimes?

On n'a pas d'information sur ce sujet.

(4) Quel type de criminalité informatique/fraude informatique est le plus souvent recensé dans votre pays?

Le fait d'entrer dans le systeme informatique est plus souvent recensé en Turquie.

(5) Les services d'application de la loi et des poursuites dans votre pays ont-t-ils une unité spécialisée dans les crimes informatiques? Si oui, combien d'agents et des procureurs compte-t-elle?

A part des départements établis au sein de la police sur les cyber-crimes, il y a des départements au sein du parquet.

(6) Est-ce que vous ou une autre faculté de droit dans le pays offre des cours sur la cyber-criminalité? S'il vous plaît, veuillez fournir une adresse de site Web.

Dans l'Université Bahçeşehir on a des cours intitulés « Internet Law ». Dans l'Université Galatasaray et aussi Bahçeşehir, aux cours de droit pénal on traite « les crimes au domaine de l'informatique ».

(7) L'étude de la cybercriminalité est-elle incluse dans la formation et/ou la formation continue des juges, des procureurs et la police?

Dans la formation et/ou la formation continue des juges, des procureurs et de la police inclut aussi l'étude de la cybercriminalité.