

RAPPORT NATIONAL ROUMAIN*

George ANTONIU, Florin STRETEANU

A. Champ d'application

Les spécialistes roumains en droit pénal ont les mêmes convictions que la société d'aujourd'hui se transforme rapidement et que l'information et la connaissance sont devenus les ressources-clés de la société d'information, affectant à la fois la structure sociale et politique de la société et de L'État ainsi que la fonction, la structure et le contenu du système de la justice pénale. On peut dire que nous assistons à une vraie révolution avec un impact social redoutable sur les organisations sociales dont fait partie le système de justice pénale.

En ce qui concerne la Roumanie, toutes ces transformations de la société sont au début, y compris le remplacement de la structure de l'autorité traditionnelle par une méthode alternative de contrôle de la société (à savoir la transition de L'État-nation à L'État – réseau).

Dans cette lumière, nous allons répondre aux problèmes abordés dans ce rapport national.

B. Criminalisation

(1) Les intérêts juridiques protégés

Vu la diversité des textes d'incrimination en la matière, la valeur sociale protégée doit être identifiée par rapport à chaque catégorie d'infractions. Ainsi, les diverses lois adoptées par le législateur roumain protègent l'intégrité des systèmes informatiques, des systèmes de traitement de données et la confidentialité des données.

(2) Des exemples typiques de lois pénales relatives à/aux :

(a) attaques contre les systèmes d'information :

Selon l'art.42 de la Loi nr.161/2003, (1) *l'accès sans droit à un système informatique est puni de 3 mois à 3 ans d'emprisonnement ou d'une amende.*

(2) *Le fait visé par le paragraphe (1) commis dans le but d'obtenir des données informatiques est puni de 6 mois à 5 ans d'emprisonnement.*

(3) *Lorsque les faits visés par les paragraphes (1) et (2) sont commis en violation des mesures de sécurité la peine est l'emprisonnement de 3 à 12 ans.*

(b) une violation des systèmes d'information personnels

Voir les textes indiqués ci-dessus. En plus, l'art. 43 de la même Loi érige en infraction pénale punie de 2 à 7 ans d'emprisonnement, *l'interception sans droit de données informatiques, effectuée lors d'une transmission non publique, à destination, en provenance ou à l'intérieur d'un système informatique.* La même peine est prévue pour l'interception des émissions électromagnétiques provenant d'un système informatique, contenant des données informatiques qui ne sont pas publiques.

* 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) la falsification et la manipulation des données stockées numériquement

Selon l'art.48 de la Loi n.161/2003, *l'introduction, l'altération ou l'effacement sans droit de données informatiques, ou le fait de rendre inaccessibles, sans droit, ces données, engendrant des données non authentiques, dans l'intention qu'elles soient utilisées à des fins légales comme si elles étaient authentiques est puni de 2 à 7 ans d'emprisonnement.*

(d) la diffusion de virus informatiques

Selon l'art.45 de la Loi n.161/2003, *la perturbation grave et sans droit au fonctionnement d'un système informatique, par l'introduction, la transmission, la modification, l'effacement, la détérioration des données informatiques ou en rendant inaccessibles ces données informatiques est puni de 3 à 15 ans d'emprisonnement.*

(e) infractions liées aux identités virtuelles des utilisateurs

Il n'y a pas des textes spéciaux en la matière mais on peut utiliser les autres incriminations existantes (altération des données informatiques, fraudes informatiques etc.).

(f) la criminalisation de la création et de la possession de certaines images virtuelles, la violation du droit d'auteur dans la sphère virtuelle.

En droit roumain il y a une incrimination spéciale relative à la pornographie enfantine. Selon l'art.52 de la Loi n.161/2003 est puni de 3 à 12 ans d'emprisonnement *la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique, l'offre, la mise à disposition, la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique, le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ou la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.*

En même temps, la Loi n.8/1996 contient des incriminations relatives à la protection du droit d'auteur. Par exemple, l'art.139-8 de la Loi érige en infraction pénale punie de 1 à 4 ans d'emprisonnement ou d'une amende la mise à la disposition y compris par le biais de l'Internet ou d'autres réseaux informatiques et en l'absence du consentement des titulaires des droits, des œuvres ou des produits concernés par le droit d'auteur, par les droits voisins ou par les droits reconnus aux fabricants des bases de données, de sorte que le public puisse avoir accès à ces œuvres ou produits au lieu et au moment de son choix.

(3) **Définition des éléments des infractions**

En général le législateur roumain préfère la description de l'acte prohibé (*l'interception, l'introduction, l'altération, l'effacement de données informatiques* etc.) plutôt que la référence aux conséquences. Pourtant, la référence aux conséquences n'est pas exclue dans certains cas (fraude informatique – *le fait de causer un préjudice patrimonial à autrui...* – art.49 de la Loi n.161/2003).

Le législateur a inclus aussi dans les réglementations internes quelques définitions des termes employés, reprises en général de la Convention sur la cybercriminalité. Par exemple, selon l'art.35 de la Loi n.161/2003:

- par l'expression «données informatiques» on entend toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;

- par l'expression «système informatique» on entend tout dispositif ou ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent un traitement automatisé de données, en exécution d'un programme.

Il y a des définitions pareilles pour d'autres expressions, telles : fournisseurs de services, données relatives au trafic, traitement automatisé de données etc.

(4) Responsabilité pénale à l'égard de certaines cyber-infractions ne visant que certains groupes particuliers d'auteurs et / ou de victimes

En règle générale les infractions prévues par la loi pénale roumaine n'ont pas un sujet qualifié de sorte qu'elles peuvent être commises par toute personne.

En ce qui concerne les victimes il n'y a non plus, en général, des restrictions. Parfois il y a quand même des exceptions, comme il est pour le cas de la pornographie enfantine ou de certaines incriminations relatives aux droits d'auteur.

(5) Responsabilité pénale pour les actes commis par négligence ou imprudence

Comme il s'agit des infractions commises par action, la règle inscrite dans l'art.19 al.(2) du Code pénal est applicable. Selon ce texte, une action commise de façon non-intentionnelle n'est punissable que dans le cas où la loi en dispose expressément. Comme les dispositions légales applicables en matière de criminalité informatique ne font aucune référence aux actions commises par imprudence ou négligence, ce type de comportements reste impuni.

(6) Y a-t-il des différences spécifiques entre la définition de la cyber-infraction et celle des infractions «traditionnelles»?

Non. En général les infractions informatiques sont définies dans la loi pénale roumaine de la même façon que les infractions dites «traditionnelles».

C. Technique législative

(1) Problèmes spécifiques relatives au principe de la légalité

En général les textes d'incrimination existantes en droit roumain répondent aux exigences du principe de légalité, y compris aux exigences de prévisibilité. En même temps, les termes utilisés sont dans la plupart des cas définis par la même loi. On doit mentionner pourtant que le législateur, soucieux de respecter le principe de l'intervention minimale, recourt parfois à des termes qui laissent une large marge d'appréciation au juge (perturbation grave etc.).

(2) Comment la législation évite-t-elle des effets de craintes excessives par rapport à l'utilisation légitime des TCI ou d'internet ?

Malgré le fait que le législateur a choisi parfois des formules un peu larges pour les textes d'incrimination, ces textes sont appliqués de façon assez stricte par les juridictions roumaines ce qui exclut les craintes excessives par rapport à l'utilisation légitime des TCI ou d'internet.

(3) Comment la législation pénale évite-elle de devenir obsolète du fait de la rapidité des innovations technologiques?

En droit roumain la plupart des incriminations relatives à la criminalité informatique ont été adoptées en 2002-2003 et les textes ont subi peu de modifications depuis leurs adoption. En revanche, les formules un peu larges, inspirées

par la Convention de Budapest facilite l'adaptation des textes aux évolutions technologiques. En général on évite les références aux réglementations administratives pour «actualiser» les textes pénaux. Il n'y a pas, croyons-nous, le péril de devenir obsolète par rapport à la rapidité des innovations technologiques.

D. Mesure de la criminalisation

(1) Incrimination des actes préparatoires

En droit roumain les actes préparatoires ne sont pas punissables sauf dans le cas où le législateur les a assimilés aux actes d'exécution (tentative) ou les a érigé en infractions autonomes. En cette matière on retrouve quelques actes préparatoires incriminés de façon autonome. Ainsi, selon l'art.46 de la Loi n.161/2003 :

(1) Est puni d'emprisonnement de 1 à 6 ans :

- a) la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou la mise à la disposition sous toute autre forme, sans droit, d'un dispositif ou d'un programme informatique conçu ou adapté dans le but d'accomplir l'une des infractions prévues par les art.42-45 ci-dessus;
 - b) la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou la mise à la disposition sous toute autre forme, sans droit, d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou à une partie d'un système informatique, dans le but d'accomplir l'une des infractions prévues par les art.42-45 ci-dessus;
- (2) De la même peine est punie la possession sans droit d'un dispositif, d'un programme informatique, d'un mot de passe, d'un code d'accès ou de données informatiques similaires prévues par l'alinéa 1er dans le but d'accomplir l'une des infractions prévues par les art.42-45 ci-dessus.

(2) Criminalisation de la simple possession de certaines données

Comme nous l'avons déjà montré, la législation roumaine criminalise la possession de pornographie enfantine dans un système informatique. Le texte ne fait aucune distinction selon la durée de cette possession. En principe, la possession temporaire suffit pour engager la responsabilité pénale.

De plus, on retrouve en droit roumain un certain nombre d'actes préparatoires érigés en infractions autonomes. Ainsi, l'art.46 de la Loi n.161/2003 punit la possession sans droit d'un programme informatique, d'un mot de passe, d'un code d'accès ou de données informatiques similaires dans le but d'accomplir l'une des infractions prévues par les art.42-45 de la même loi. A son tour, l'art.25 de la Loi nr.365/2002 relative au commerce électronique incrimine, entre autres, la possession des logiciels destinés à servir pour falsifier un instrument de paiement électronique. Des incriminations pareilles on retrouve aussi dans la Loi n.8/1996 sur les droits d'auteur et les droits voisins.

(3) Responsabilité des fournisseurs

La législation roumaine ne contient pas des règles spéciales en matière de responsabilité pénale des prestataires de services d'hébergement ou des fournisseurs d'accès. Leur responsabilité pourrait éventuellement être engagée sur la base des règles générales en matière de participation punissable (en général à titre de complicité). Comme la complicité exige toujours en droit roumain une intention, il est assez difficile d'en faire la preuve.

Il n'y a pas une obligation générale imposée aux fournisseurs d'accès de contrôler les informations qu'ils fournissent ou auxquelles ils offrent accès. Dans certains les propriétaires de certains sites Internet sont obligés à imposer des

restrictions d'accès, (par exemple, les propriétaires des sites pornographiques), mais la méconnaissance de cette obligation constitue une simple infraction administrative.

En ce qui concerne l'obligation de fournir des informations aux autorités, l'art.55 de la Loi nr.161/2003 permet au procureur et au juge de demander aux fournisseurs de services l'accès aux données relatives au trafic ou relatives aux utilisateurs.

(4) *Limites constitutionnelles à la criminalisation en la matière*

La doctrine roumaine a connu très peu des débats relatifs aux limites constitutionnelles de la criminalisation des comportements commis à travers l'Internet. Les discussions sur la liberté d'expression, la liberté de la presse, la liberté d'association, le respect de la vie privée etc., se portent en mêmes termes que pour les infractions commises par la presse écrite.

(5) *Sanctions pénales visant spécifiquement les cybercriminels*

La législation roumaine ne prévoit pas expressément une telle interdiction spéciale. L'art.64 du Code pénal roumain permet au juge d'interdire, pour une durée de 1 à 10 ans, à titre de peine complémentaire, l'exercice de l'activité dont le condamné s'est servi pour commettre l'infraction. Pourtant la jurisprudence n'a jamais utilisé ce texte pour imposer une interdiction d'utiliser l'Internet.

E. *Alternatives à la criminalisation*

(1) *Le rôle du droit pénal par rapport à d'autres moyens*

Le législateur roumain a une préférence manifeste pour le recours au droit pénal en matière de criminalité informatique au détriment du droit administratif. Si on examine le cas des incriminations relatives à l'intégrité des systèmes informatiques, on constate que la loi roumaine a institué des sanctions pénales pour toutes les hypothèses prévues par la Convention de Budapest, même dans le cas où la criminalisation restait facultative (par exemple, pour le simple accès illégal, en l'absence de toute condition supplémentaire).

Bien sûr, la responsabilité pénale exclut toute responsabilité administrative en raison du même fait. En revanche, la responsabilité pénale est assortie d'une responsabilité civile chaque fois que l'infraction pénale a causé un dommage.

(2) *Moyens d'attaques non criminelles utilisés à l'encontre de sites Web*

Dans certains cas l'Autorité Nationale de réglementation en matière de communications électroniques peut demander aux fournisseurs de service le blocage du site Web. Par exemple, selon l'art.14 de la Loi n.196/2003, une telle mesure peut être prise lorsque le propriétaire d'un site Web de caractère pornographique n'a pas pris les mesures nécessaires pour imposer les restrictions d'accès voulues par l'art.7 de la loi.

(3) *Obligations d'autoprotection des utilisateurs des TIC*

La législation roumaine impose peu de conditions relatives à l'autoprotection des utilisateurs des TIC. En général, les simples utilisateurs ne sont pas obligés à utiliser des moyens de protection, même minimales (logiciel antivirus, mot de passe etc.). Pourtant, l'art.41 de la Loi n.161/2003 impose, aux propriétaires et aux administrateurs des systèmes informatiques dont l'accès est soumis à des restrictions pour certaines utilisateurs, l'obligation de d'informer les utilisateurs sur les conditions légales d'accès et sur les conséquences de l'accès illégal à ces systèmes

informatiques. La méconnaissance de cette obligation constitue une infraction administrative (art.52 de la même Loi). En même temps, l'art.3 de la Loi n.506/2004 impose aux fournisseurs de services de communications électroniques l'obligation de prendre toutes les mesures techniques nécessaires pour garantir le secret des communications.

En revanche, l'absence d'une autoprotection raisonnable ne fournit pas un moyen de défense en cas d'accusation d'accès illégal, car l'art.42 al.1^{er} de la Loi n.161/2003 n'exige pas que l'infraction soit commise en violation des mesures de sécurité, le simple accès illégal étant constitutif d'infraction pénale.

F. Limiter l'anonymat

(1) Réglementations obligeant les fournisseurs de services internet à stocker des données personnelles des utilisateurs

Selon les dispositions de la Loi n.82/2012 qui transpose en droit roumain la Directive 2006/24/CE, les fournisseurs de services Internet sont obligés à stocker pour une période de 6 mois, entre autres, des données relatives à :

- les nom et adresse des abonnés ou des utilisateurs inscrits et le numéro d'identifiant du destinataire prévu de la communication
- les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (protocole internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication
- la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'internet dans un fuseau horaire déterminé, ainsi que l'adresse IP (protocole internet), dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet, ainsi que le numéro d'identifiant de l'abonné ou de l'utilisateur inscrit.

En revanche, les fournisseurs ne sont pas autorisés à conserver des données relatives au contenu de la communication effectuée ou aux informations consultées durant l'accès à l'Internet.

Selon l'art.16 de la loi, les fournisseurs sont obligés à transmettre aux autorités judiciaires, dans un délai de 48 heures, les données conservées sollicitées par ces autorités.

(2) Réglementations limitant le cryptage des fichiers et des messages sur internet

Il n'y a pas des interdictions ou des limitations imposées par la loi en matière de cryptage des fichiers et des messages sur internet. Etant donnée la présomption d'innocence et le privilège contre l'auto-incrimination le suspect ne peut pas être contraint de divulguer les mots de passe qu'il utilise.

G. Internationalisation

(1) Application du droit interne quant aux données introduites sur internet depuis l'étranger

Comme la législation roumaine ne contient pas des règles spéciales en la matière, les principes généraux relatifs à l'application de la loi pénale dans l'espace trouvent application dans ce domaine. Conformément aux dispositions du Code pénal, la loi pénale roumaine est applicable lorsqu'un acte d'exécution ou le résultat de l'infraction a été localisé sur le territoire roumain. Il est donc possible d'attirer la compétence de la loi pénale roumaine à l'égard de certaines données introduites sur Internet depuis l'étranger à la condition qu'un résultat peut être localisé sur le territoire roumain. Dans ce cas-là la compétence de la loi roumaine n'est pas soumise à l'exigence de la «double incrimination».

(2) Influence des instruments juridiques internationaux

L'influence des instruments adoptés sous l'égide du Conseil de l'Europe ou de l'Union Européenne est très importante en droit roumain. Il suffit de rappeler que la principale loi relative à la criminalité informatique reprend de manière fidèle les dispositions de la Convention de Budapest.

(3) Participation aux débats sur l'harmonisation des législations dans le domaine de la cybercriminalité

En général la Roumanie est représentée dans les groupes de travail sur la cybercriminalité au niveau régional ou mondial (Conseil de l'Europe, Union Européenne, ONU).

H. Les développements futurs

La criminalité informatique est devenue une composante importante de la criminalité contemporaine en Roumanie. Notamment les fraudes commises par Internet ou à travers les moyens de paiement électronique ont connu les dernières années une croissance très importante. De plus, une bonne partie de ces infractions sont commises en préjudice des étrangers, ce qui implique un renforcement des mécanismes de coopération judiciaire internationale.