SAGYNGALIY AIDARBAYEV,
PIERRE CHABAL,
ZHULDYZ SAIRAMBAEVA (dir.)

MUTATIONS DE SOCIÉTÉ ET RÉPONSES DU DROIT

PERSPECTIVES FRANCO-ASIATIQUES COMPARÉES

Cultures juridiques et politiques

PIE Peter Lang

Pour leur soutien à la publication, les auteurs remercient le ministère français de l'enseignement supérieur, programme PARCECO, la région Haute Normandie, l'université du Havre, le laboratoire LexFEIM, l'université nationale kazakhe *al-Farabi*, le centre franco-kazakh de droit européen.

Illustration de la couverture : France and Kazakhstan Flags © iStock. Benguhan.

Cette publication a fait l'objet d'une évaluation par les pairs.

Éditions scientifiques internationales
Bruxelles, 2017
Avenue Maurice 1, B-1050 Bruxelles, Belgique
brussels@peterlang.com ; www.peterlang.com

Imprimé en Allemagne

ISSN 2235-1078
ISBN 978-2-8076-0187-1
ePDF 978-2-8076-0188-8
ePUB 978-2-8076-0189-5
MOBI 978-2-8076-0190-1
DOI 10.3726/b10992
D/2017/5678/14

Information bibliographique publiée par « Die Deutsche Nationalbibliothek ». « Die Deutsche Nationalbibliothek » répertorie cette publication dans la « Deutsche Nationalbibliografie » ; les données bibliographiques détaillées sont disponibles sur Internet sous <http://dnb.d-nb.de>.

Table des matières

Remerciements 13

Avant-propos 15
Catherine Troallic

Préface 17

Introduction. La diversité des Droits : une ardente obligation universelle 19
Didier Guével

PARTIE I. MUTATIONS LIÉES AUX NOUVELLES TECHNOLOGIES

Les systèmes judiciaires en France et au Kazakhstan. Les emprunts du Kazakhstan à la France 25
Karimzhan Shakirov, Jeanie Manabaeva

Les mutations de la criminalistique. De la loupe de Sherlock Holmes au portrait-robot génétique 33
Nasreddine El Hage

La base juridique de la lutte contre la fraude dans les réseaux de communication mondiaux 49
Danila Tatarinov

Le contrôle de la personne sur ses données personnelles. L'influence décisive du droit européen 59
Amandine Cayol

Organisations régionales et cybersécurité. Divergences euro-asiatiques à l'ère du numérique 71
Philippe Ch.-A. Guillot

La base juridique de la lutte contre la fraude dans les réseaux de communication mondiaux

Danila Tatarinov

Université nationale Kazakhe al-Farabi
Académie des Sciences de Russie

Après son indépendance en 1991, le Kazakhstan est entré dans la communication mondiale et a lancé une informatisation active de tous les secteurs de la vie publique, afin de contribuer au développement progressif de la société. Cette mondialisation de l'espace d'information s'est mise en place rapidement et se poursuit.

Le développement des technologies de l'information et des réseaux de communication globaux a pourtant contribué à l'émergence de nouveaux crimes liés à leur utilisation mais également à la modification des formes préexistantes de violence. Un genre d'infraction dont l'occurrence a fortement augmenté sous l'influence de ces évolutions est la fraude.

La fraude est le plus souvent associée à l'utilisation de l'*Internet*. Il en existe plusieurs dizaines de formes, en constante évolution. À titre d'illustration : la vente de marchandises inexistantes, l'offre de services inexistants, les demandes de fonds pour des œuvres de charité controversées, les jeux de hasard contrevenant à la réglementation, les ventes aux enchères, les « montages » financiers et la vente de réseaux, les projets d'investissement, les agences matrimoniales fictives, les sollicitations pour prendre part à des fonds ou des actions envers les grands malades, les accidentés, les victimes de catastrophes naturelles, du terrorisme, etc.

Une forme relativement nouvelle de cybercriminalité est l'échange d'informations d'affaires, y compris sur les sites des sociétés concertés, par exemple les prix de marchandises et services, les statistiques financières, la description des services offerts, etc. De telles actions peuvent nuire gravement à leur réputation et leur causer de notables dommages financiers.

Il faut donc mieux appréhender les réactions du droit face à ces nouvelles synergies criminelles, en partant de la définition de la fraude dans les réseaux de communication (I) puis en évoquant le besoin pour le Kazakhstan de

s'inspirer des précisions dont se dotent les pays étrangers dans leur lutte contre cette fraude en réseau (II).

I. Concept et définition juridique de la fraude dans les réseaux de communication mondiaux

Afin de lutter contre ce type de crime, il est nécessaire, tout d'abord, de se référer à la définition de la fraude dans les réseaux de communication mondiaux. Traditionnellement, les crimes commis dans ces réseaux se divisent en deux grands groupes :

- les crimes contrevenant directement au fonctionnement normal du réseau et des ordinateurs connectés : accès non autorisé à des données informatiques, interception illégale de partage de données informatiques non destinées à un accès commun, interférences avec le fonctionnement du système, interférence avec les données, etc.;
- les crimes « traditionnels », pour la commission desquels les systèmes informatiques et de communication agissent comme un moyen technique : par exemple, la distribution de pornographie juvénile, les violations des droits d'auteur et des droits connexes, etc.

On invoquera ici la définition de la fraude prévue par la législation du Kazakhstan. L'article 190 du Code Pénal kazakhstanais dispose que la fraude est la « déprédation de la propriété d'autrui ou l'acquisition des droits à la propriété d'autrui par la tromperie ou l'abus de confiance. »[1]

Sur la base de cette définition, il est possible d'identifier les principaux signes de fraude suivants :

- cet acte est déterminé par le législateur comme déprédation de la propriété de quelqu'un d'autre ou l'acquisition de droits à la propriété d'autrui ;
- l'attribut obligatoire de ce crime, sa qualification, est son mode de réalisation : la tromperie ou l'abus de confiance.

Il est logique de supposer que la fraude liée aux réseaux de communication mondiaux relève des mêmes attributs, avec, en sus, une caractéristique propre, à savoir un instrument de commission du crime : le réseau de communication globale lui-même. Il en ressort que, selon la classification ci-dessus, des crimes commis dans les réseaux de communication mondiaux, ressortent du second type de fraudes.

La doctrine juridique russe offre un point de vue différent. Selon A.L. Asipenka, l'on ne peut ignorer le fait que, dans l'usage frauduleux des

[1] Code pénal de la République du Kazakhstan du 3 juillet 2014, art. n° 226-V (modifié et complété en date du 24/11/2015) http://online.zakon.kz/Document/?doc_id=31575252.

réseaux de communication, le caractère des crimes commis peut changer qualitativement. Par exemple, l'*Internet* permet aux criminels, en un seul appel, d'atteindre des centaines ou milliers de victimes simultanément, fournissant un lien vers le mode automatique tout en conservant facilement l'anonymat.

> La nature particulière de la fraude au sein du réseau de communication mondial apparait dans la nécessité d'une formation spéciale des enquêteurs, des agents, des juges et d'autres autorités d'application de la loi pour détecter, enquêter, combattre et prévenir ces actes illicites et poursuivre ceux qui les ont commis. La spécificité de cette catégorie de crimes se fait sentir constamment quant à la procédure pour les traiter.[2]

Cette position, différente de la nôtre, se reflète dans le projet de loi fédérale « Sur les amendements au Code pénal de la Fédération de Russie et d'autres actes législatifs de la Fédération de Russie », projet approuvé par le Conseil de la Fédération le 28 novembre 2012. Son principal but est de caractériser la fraude selon son mode de commission. En particulier, ce projet de modification du Code pénal sera complété par l'article 1596 « La fraude dans le domaine de l'informatique », qui définit la fraude informatique comme « la déprédation de la propriété d'autrui ou l'acquisition des droits de la propriété d'autrui par l'ajout, la suppression, le blocage, la modification des informations de l'ordinateur ou l'interférence avec le fonctionnement des moyens de stockage, de traitement ou de transmission de données informatiques ou de réseaux d'information et de télécommunications »[3].

Selon cet article, la fraude dans le domaine informatique renvoie au premier groupe de crimes dans la classification ci-dessus. À notre avis, cependant, l'utilisation du terme « fraude » dans ce cas est incorrecte. Selon l'article de T. Tropin *Fraude informatique : les questions de qualification et technique législative*, un signe de fraude est un transfert volontaire de biens des victimes ou de leurs droits sous l'influence de la fraude ou l'abus de confiance[4]. Si la « fraude informatique » est commise par « tromperie » informatique, à savoir, la manipulation de données informatiques, il est peu probable que dans cette situation le système informatique transfère la propriété « volontairement » ou puisse agir comme une « victime ».

Actuellement, dans le cas de « fraude dans le domaine de la technologie informatique », la victime peut ne rien savoir sur la transmission de

[2] Osipenko A.L., *La lutte contre la criminalité dans les réseaux informatiques mondiaux : expérience internationale*, Norma, 2004.

[3] Projet de loi fédérale n° 53700-6 « Sur les amendements au Code pénal de la Fédération de Russie et d'autres actes législatifs de la Fédération de Russie » http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n = 100289.

[4] Tropin T., « *Fraude informatique* » : *les questions de qualification et technique législative*, L'édition Corporative « Svizainvest », juillet 2006.

biens, ni sur le droit de propriété. Selon Brazhnik S.D., « chaque terme utilisé dans le droit pénal doit être défini, avoir la même valeur dans tous les actes juridiques et utiliser pour la formulation des éléments du crime apparentés. »[5] Dans ce cas, les termes « fraude » et « fraude dans le domaine des technologies informatiques » sont semblables seulement en cela que, dans leurs éléments du crime, une partie du vol de la propriété d'autrui ou de l'attribution des droits de la propriété d'autrui sont présents. Il convient d'exclure du champ d'application de la notion de « fraude sur un réseau de communication mondial » la déprédation de la propriété d'autrui ou de l'acquisition des droits à la propriété d'autrui par l'ajout, la suppression, le blocage ou la modification d'informations de l'ordinateur ou l'interférence avec le fonctionnement des moyens de stockage, de traitement ou de transmission de données informatiques ou de réseaux d'information et de télécommunications.

Nous rejoignons ici l'avis de N. A. Selivanov et d'un certain nombre de chercheurs occidentaux, parmi eux D. Parker, qui pensent que tous les crimes commis avec l'utilisation de réseaux de communication mondiaux, y compris la fraude, ne sont qu'une autre forme de crimes traditionnels, qui présentent l'utilisation d'outils spécifiques par les criminels pour parvenir aux buts illégaux.

II. Expérience de pays étrangers pour préciser la fraude dans les réseaux de communication mondiaux

La fraude dans le réseau mondial de communication est un problème mondial, puisque ce climat de haute technologie ne connaît pas de frontières. Les premiers États qui ont commencé à lutter contre ce problème ont été les États non membres de la CEI. Cela est dû au fait que, chez eux, le développement de la technologie de pointe a commencé plus tôt et a été plus rapide que dans l'ancienne Union soviétique. Pour cette raison, aujourd'hui, l'expérience de ces pays dans le domaine de la prévention, de la suppression et de l'investigation de ces crimes est supérieure ; et l'on devrait s'y référer.

1) le cas de pays occidentaux : un arsenal codifié

Le Code pénal de la République d'Autriche dispose que « les actes criminels contre la propriété d'autrui » comprennent (section 6, §148a) « l'utilisation frauduleuse de traitement des données ». Cet élément du crime établit : « (1) Quiconque, avec l'intention de s'enrichir abusivement

[5] Brazhnik S.D. et Kruglikov L.L., *Crimes dans le domaine de l'information informatique : Problèmes de technique législative*. Résumé de thèse pour le grade de candidat des sciences juridiques. Spécialité 12.00.08. Droit pénal et criminologie ; Droit pénal exécutif, Izhevsk, 2002.

ou d'enrichir des tiers, nuit à la propriété d'autrui par changement de données protégées automatisées grâce à la création de programmes, l'entrée, l'altération, la destruction, ou la dissimulation de données, ou autrement influence le cours du traitement des données, sera puni… (2) Quiconque commet cet acte, comme commerce ou à la suite d'actes de dommages au-delà de 2.000 €, est passible de la peine… »[6]. Cet élément du crime est assez vaste, en vertu du présent paragraphe et couvre également le vol de haute technologie, mais cet article contient tous les éléments nécessaires pour traduire en justice l'auteur de la fraude sur un réseau. En plus de cet article, le Code pénal autrichien contient (§146) la « Fraude », (§147), la « Grave fraude » et (§148) la « Fraude sous forme de commerce. » Comme on le voit, le législateur autrichien a précisé la fraude informatique dans des articles distincts.

Le Code pénal de la République fédérale d'Allemagne aborde (§ 263a) « La fraude informatique », à la section 22. Il dispose : « (1) Quiconque agit dans le but d'obtenir des avantages patrimoniaux illégaux pour lui-même ou pour une tierce personne et porte ainsi préjudice à la propriété d'autrui en modifiant le résultat du traitement informatique des données, en élaborant des programmes malveillants, en utilisant des données incorrectes ou incomplètes, en appliquant des données illégalement ou en affectant ce processus et toute autre action illégalement, sera puni… »[7]. L'article (2) du même paragraphe contient une référence au § 263 (« Fraude »), en évoquant, dans un § 2-7, respectivement, les circonstances aggravantes de la fraude simple et la fraude informatique.

Dans le droit pénal de la Confédération suisse, l'article 143 dispose que « L'acquisition abusive de données », engage la responsabilité pénale de celui « qui, dans le but de s'enrichir ou enrichir quelqu'un illégalement, acquière des données pour lui-même ou une autre personne, recueillies ou transmises par voie électronique ou autrement d'une manière similaire, si ces données ne lui sont pas destinées et spécialement protégées contre un accès non autorisé… »[8]. De plus, l'article 147 précise « [l]'abus frauduleux visant à modifier le traitement de données » en soulignant que « [c]elui qui, dans le but de s'enrichir ou enrichir un autre illégalement par l'utilisation abusive de données ou, semblablement, d'affecter le processus de traitement ou de communication des données, engendre de ce fait un dommage de

[6] Serebrennikov A.V., *Le Code pénal de l'Autriche*, trad. et avant-propos. Miroir, 2001, 144 p.

Shestakova D.A., *Le Code pénal de l'Allemagne*, trad., Legal Press Center, 2003, 524 p.

[8] Serebrennikova A.B., *Le Code pénal de la Suisse*, trad. de l'allemand, Legal Press Center, 2002, 350 p.

propriété à autrui ou masque directement le terme des dommages matériels, sera puni… »[9].

Ces règles montrent bien que le crime est considéré comme constitué à la fois par une acquisition de données protégées et par l'impact sur le traitement ou la transmission de données, même sans acception de s'enrichir, et avec l'aide d'une personne ou non. Ces deux articles figurent dans la deuxième partie du code pénal suisse intitulé « Des actes criminels contre la propriété ». Clairement, l'appropriation de la propriété est, également par informatique, le fait d'une intrusion et d'une captation.

Aux États-Unis, où la lutte contre la cybercriminalité a commencé tôt, la législation établit clairement (*18th Act*, §1030) la responsabilité des crimes dans le domaine de l'information par ordinateur. Les actions décrites dans cet *Act* reprennent les dispositions de la loi sur la fraude informatique et les abus d'utilisation des ordinateurs adoptée en 1986. Selon l'article (a) du paragraphe, il y a responsabilité pour fraude dès lors que l'utilisation d'un ordinateur est effectuée par un accès avec intention frauduleuse, notamment afin d'obtenir quelque chose de valeur au moyen de la fraude, y compris l'utilisation illégale de temps de connexion pour un coût supérieur à cinq mille dollars pour une année, sans paiement pour l'utilisation des réseaux informatiques et des serveurs[10].

Le Code criminel suédois punit pour fraude toute personne qui, par la tromperie, induit quelqu'un à commettre ou ne pas commettre un acte qui implique un avantage pour le défenseur et l'expose à des dommages, ou pour celui qui est représenté par ce dernier : également celui qui, par voie de l'attribution des informations incorrectes ou incomplètes, ou par l'importation de programmes ou de déclarations, ou par tout autre moyen, influence illégalement le résultat d'un traitement automatique de données ou tout autre traitement automatisé similaire, et qui entraîne des avantages. L'auteur de l'infraction doit alors compenser les pertes de toute autre personne[11].

Dans ce cas, très clairement, le champ d'application de l'article est largement ouvert à la fraude utilisant la haute technologie et à la déprédation commis par les mêmes moyens. De manière générale, l'arsenal mis par les législateurs occidentaux à la disposition des juridictions et des juges est très précis et permet une approche répressive déterminée.

[9] *Idem.*

[10] US Code. Title 18. Site Justitia.com, http://law.justia.com/codes/us/2010/title18/parti/chap47/sec1030/.

[11] Code pénal de la Suède, 1962. portail juridique russe : Constitutions.ru/http://constitutions.ru/archives/5705.

2) le cas de pays d'Eurasie : une codification déjà importante

Les États d'Asie et d'Eurasie élaborent également une codification envers la lutte contre la cybercriminalité, avec néanmoins une expérience plus récente et encore perfectible.

Le code pénal de la République populaire de Chine prévoit (article 287) la responsabilité pour « utilisation d'un ordinateur afin de prendre possession d'argent par la fraude ou la déprédation par corruption et détournement de fonds publics, pour appropriation par déprédation de secrets d'État et la commission d'autres crimes ». Les sanctions pour ces infractions y sont également énoncées. L'article 266 du code est consacré à la fraude simple, évoquant le « détournement de la propriété publique et de la propriété privée par la fraude sur une assez grande échelle », et la fraude aggravée – commise à grande échelle dans des circonstances aggravantes, et les actes commis à grande échelle dans des circonstances particulièrement aggravantes[12].

Aux Philippines, la loi sur l'abus informatique (2000) fournit des indices de la fraude. Son paragraphe (c) de l'article 4 voit comme but de commettre une fraude le fait d'accéder intentionnellement à un ordinateur protégé sans autorisation ou, au-delà de cette résolution, afin d'obtenir des informations importantes, si la fraude et la réception de l'information sont réalisées uniquement à l'aide d'un ordinateur, ou si les dommages causés par l'utilisation de l'ordinateur ne dépasse pas cinquante mille pesos pour une année. Le paragraphe (f) du même article criminalise l'intention délibérée de commettre une fraude par la transmission de mots de passe ou d'autres informations au moyen desquelles l'on peut obtenir un accès non autorisé à un ordinateur, un réseau informatique, un système informatique, un serveur ou à une base de données. Le sous-alinéa 1-ii du paragraphe (h) interdit d'accepter les virus informatiques électroniques ou, dans le but de propager le virus, d'effectuer un accès non autorisé, de modifier, d'endommager ou détruire tout ordinateur, réseau informatique, logiciel, système informatique, programme informatique, serveur ou base de données à des fins de commettre une fraude ou contrôler l'obtention par la tromperie de demandes frauduleuses[13].

L'évolution historique du Kazakhstan demeure proche, au plan du système juridique de l'État, de celle des anciennes républiques soviétiques, dont la plupart sont aujourd'hui membres de la Communauté des États indépendants. Ces États ont également pris des mesures pour lutter contre la criminalité informatique.

[12] Code pénal de la République populaire de Chine 1997, portail juridique russe : http://law.edu.ru/norm/norm.asp?normID=1247252&subID=100110722,100110731,100110742,100110836,100111905#text.

[13] Kosachkin A.D., *Loi pénale des pays étrangers*. Partie spéciale : manuel Cameron, 2004, 528 p.

Le Code pénal de la République du Belarus, au chapitre « Crimes contre la propriété et les modèles d'activité économique » contient un chapitre 24 intitulé « Crimes contre la propriété ». Dans ce chapitre, en plus de l'article 209, qui traite de la « Fraude », et de l'article 212, qui traite de la « [d]éprédation par l'utilisation de la technologie informatique », sont visées les infractions constitutives de « déprédation de biens par altération des informations traitées dans un système informatique, sauvegardées sur un support de stockage ou transmises par les réseaux de données, ou par l'introduction de fausses informations dans le système informatique ». Dans le même temps, une note du chapitre 24 précise que « la déprédation s'entend de l'acquisition gratuite illicite intentionnelle de la propriété d'autrui ou de son droit de propriété par le vol, le brigandage, le banditisme, l'extorsion, la fraude, l'abus de pouvoir, le détournement, la malversation ou l'utilisation de la technologie informatique »[14].

La méthode de commission de la déprédation est importante. Introduire de fausses informations dans un ordinateur est un indicateur de fraude à l'aide de systèmes informatiques. Le législateur biélorusse a opté pour une règle d'attribution de la déprédation distincte, par usage de matériel informatique par lequel elle est commise. Il s'agit donc bien d'un type de fraude, bien que le terme « fraude » ne soit pas utilisé dans l'article.

Le code pénal de l'Ukraine (article 190, section VI) traite des « [c]rimes contre la propriété », ainsi que de la fraude traditionnelle. Il qualifie également de crime toute « fraude commise à grande échelle, ou par le biais de transactions illégales en utilisant la technologie informatique » (article 190, section IV). La première partie de l'article donne une définition de la fraude : « l'acquisition de la propriété d'autrui ou l'achat par la fraude ou par abus de confiance ». Une personne qui commet l'acte prévu par cette section IV de l'article 190 est « punissable d'un emprisonnement de trois à huit ans ». La commission d'une fraude simple est passible d'une amende pouvant aller jusqu'à cinquante fois le salaire d'un citoyen ordinaire ou un maximum de 240 heures de service communautaire, ou une punition correctionnelle consistant à travailler jusqu'à deux ans, ou une restriction de liberté jusqu'à trois ans[15]. Cet article fonctionne dans la pratique, comme le confirment les médias.

Le législateur de la République d'Ouzbékistan a également pris des mesures pour lutter contre la fraude dans les réseaux de communication mondiaux. La méthode est similaire à la façon du législateur ukrainien Le chapitre X du code pénal qui traite de la « [d]prédation de la propriété

[14] Code pénal de la République du Bélarus. Adopté par la Chambre des représentants le 2 juin 1999. Approuvé par le Conseil de la République le 24 juin 1999. Texte en date du 12 mars 2007. Minsk, Amalhteia, 2008, 352 p.

[15] Code pénal de l'Ukraine, 2001. Site « Services juridiques online » : http://yurist-online.com/uslugi/yuristam/kodeks/013/193.php.

d'autrui » contient un article 168 sur la « [f]raude ». Le paragraphe (c) de la partie 2 de cet article précise un indicateur de qualification de la fraude : l'utilisation de l'équipement informatique. La pénalité pour la commission d'un tel acte est une amende de cent à trois cents fois le salaire mensuel minimum, ou un travail correctionnel pouvant aller jusqu'à deux ans, ou un emprisonnement maximal de cinq ans. La fraude est définie dans cet article comme « l'acquisition de la propriété d'autrui ou de droit sur la propriété d'autrui par la tromperie ou l'abus de confiance envers autrui »[16].

Le droit pénal de la République de Lettonie (chapitre XVIII) aborde les « actes criminels contre la propriété ». Son article 177-1, intitulé « [f]raude dans un système de traitement automatisé de données » en donne la définition suivante : « obtentir la propriété d'autrui ou des droits sur celle-ci, ou d'autres avantages exclusifs, par l'introduction dans un système de traitement automatisé de données ou de fausses informations pour influencer l'action de ses ressources ». La personne qui commet l'acte ci-dessus « est punie d'un emprisonnement maximal de cinq ans, ou d'un service communautaire ou d'une amende ne dépassant pas quatre-vingts fois le salaire mensuel minimum »[17].

Ce rapide survol des systèmes des pays d'Asie et d'Eurasie montre que les États en question utilisent deux méthodes pour criminaliser la fraude dans les réseaux mondiaux de communication : le traitement de la fraude dans ces réseaux i) par un article distinct du code pénal ou ii) l'adjonction d'un critère de qualification – la haute technologie informatique.

Le moyen à notre avis le plus efficace est de définir une norme distincte de fraude, dans un réseau mondial de communication, par son propre critère de qualification. L'usage de réseaux de communication mondiaux modifie en effet qualitativement la composition de la fraude, en développant la notion du dol lors de la fraude et en augmentant le degré de danger social du crime. Nous proposons donc de compléter le Code pénal du Kazakhstan en ce sens quant à la fraude commise par l'utilisation des réseaux de communication mondiaux.

En conclusion, il n'existe pas une seule définition, généralement acceptée, de la fraude dans le réseau mondial de communication. On peut seulement mettre en évidence les signes principaux et les plus globaux des tentatives de formulation d'une définition. La fraude dans les réseaux de communication mondiaux est ainsi, selon nous : « le vol de la propriété d'autrui ou la cession des droits à la propriété d'autrui par la tromperie ou l'abus de confiance, commis avec l'utilisation de réseaux de communication mondiaux ». Cette catégorie de

[16] Code pénal de la République d'Ouzbékistan, 1994. Site de « Finmanconsult » : http://fmc.uz/legisl.php?id=k_ug_27.

[17] Code pénal de Lettonie, 1998. Site des lois lettones en russe : http://www.alex-lawyer.lv/kra1.htm.

crimes tombe sous le coup de l'article 177 du Code pénal du Kazakhstan. La différence entre la fraude simple et la fraude dans les réseaux de communication mondiaux est que, dans cette dernière, le signe objectif, l'instrument de commission du crime et la partie subjective du crime coïncident.

La question de la définition et de la consolidation législative de cette catégorie de fraude demeure ainsi ouverte.