LAW REFORM COMMISSION

Paper

Changes to Book III of Criminal Code (Incorporation of Provisions on Cybercrime)

[June 2015]

13th Floor, SICOM Building II

Reverend Jean Lebrun Street

Port Louis, Republic of Mauritius

Tel: (230) 212-3816/212-4102

Fax: (230) 212-2132

E-Mail: lrc@govmu.org

URL http://lrc.govmu.org

LAW REFORM COMMISSION

Chairperson	: Mr. Guy OLLIVRY, QC, GOSK
Chief Executive Officer	: Mr. Pierre Rosario DOMINGUE [Barrister]
Members	: Mr. Satyajit BOOLELL, SC [Director of Public Prosecutions]
	Mrs. Aruna D. NARAIN [Parliamentary Counsel]
	Mr. Nicholas F. OHSAN BELLEPEAU [Master & Registrar]
	Mr. Rishi PURSEM, SC [Barrister]
	Mr. Narendra APPA JALA, SA [Attorney]
	Mrs. Wenda SAWMYNADEN [Notary]
	Mrs. Luvishka SEEJORE BILTOO [Law Academic (UoM)]
	Mrs. Daisy Rani BRIGEMOHANE [Civil Society]
	Mr. Navin GUNNASAYA [Civil Society]
Secretary	: Mrs. Saroj BUNDHUN

Law Reform Cadre

Chief Executive Officer	**:** Mr. Pierre Rosario DOMINGUE
Consultant	**:** Professor Robert Louis GARRON
Senior Law Reform Officer	**:** Mr. Sabir M. KADEL
Law Reform Officer	**:** Dr. Goran GEORGIJEVIC

Administrative Support Staff

Secretary	**:** Mrs. Saroj BUNDHUN
Senior Office Management Assistant	**:** Mrs. Marie Roselilette SOOBRAMANIA
Office Management Assistant	**:** Mrs. Neelamani BANSRAM
	: Mrs. Kajal RAMDUT
Senior Office Attendant/Technical Assistant	**:** Mr. Subhas CHUMMUN
Driver/Office Attendant	**:** Mr. Claude François JEAN-PIERRE
	Mr. Naraindranathsingh JANKEE

About the Commission

THE LAW REFORM COMMISSION OF MAURITIUS consists of –

(a) a Chairperson, appointed by the Attorney-General;
(b) a representative of the Judiciary appointed by the Chief Justice;
(c) the Solicitor-General or his representative;
(d) the Director of Public Prosecutions or his representative;
(e) a barrister, appointed by the Attorney-General after consultation with the Mauritius Bar Council;
(f) an attorney, appointed by the Attorney-General after consultation with the Mauritius Law Society;
(g) a notary, appointed by the Attorney-General after consultation with the Chambre des Notaires;
(h) a full-time member of the Department of Law of the University of Mauritius, appointed by the Attorney-General after consultation with the Vice-Chancellor of the University of Mauritius; and
(i) two members of the civil society, appointed by the Attorney-General.

Under the direction of the Chairperson, the Chief Executive Officer is responsible for all research to be done by the Commission in the discharge of its functions, for the drafting of all reports to be made by the Commission and, generally, for the day-to-day supervision of the staff and work of the Commission.

The Secretary to the Commission is responsible for taking the minutes of all the proceedings of the Commission and is also responsible, under the supervision of the Chief Executive Officer, for the administration of the Commission.

The Commission may appoint staff on such terms and conditions as it may determine and it may resort to the services of persons with suitable qualifications and experience as consultants to the Commission.

Executive Summary

Paper on Changes to Book III of Criminal Code (Incorporation of Provisions on Cybercrime)
[June 2015]

The Commission has reviewed our law on cybercrime from a comparative and international perspective. In this Paper, the Commission is recommending the incorporation in our Criminal Code of provisions, inspired by French Penal Code, relating, *inter alia*, to Fraudulent access to a computer system, Violations of the operation of a computer system, Import, possession, supply, sale or provision of a breach equipment to a computer system, Identity theft or use of data to identify any third party, and Pornographic exploitation of the image of a minor. These new provisions would reinforce our current law.

Changements au Livre III du Criminal Code
(Infractions contre la Cybercriminalité)

PROPOSITIONS D'AMENDEMENTS AU CODE PÉNAL POUR RENFORCER LA LUTTE CONTRE LA CYBERCRIMINALITÉ

Introduction

Un rapport du gouvernement français sur la lutte contre la cybercriminalité du 25 février 2005 nous rappelle que la liberté sur internet « ne saurait être absolue, dès lors que les contenus peuvent porter atteinte à la sécurité et, notamment, à la dignité ou à l'intégrité physique des personnes »[1]. Cette piqure de rappel est salutaire, puisqu'en effet, bien (trop) souvent, les gens ont tendance à penser que sous couvert d'un supposé anonymat, cachés derrière leurs écrans d'ordinateurs ou de tablettes, ils peuvent se laisser aller à tenir n'importe quel propos ou avoir n'importe quel comportement, et qu'ils n'auront pas à en subir les conséquences. Si en effet longtemps les nouvelles technologies en général, et l'internet en particulier, ont été un domaine de non-droit, tel n'est plus le cas, et ce quel que soit le pays. Certes, en fonction des pays dont il est question, la législation n'est pas la même, mais tous sont d'accord pour dire que les infractions liées à l'essor de la technologie ne peuvent rester impunies.

Le droit mauricien en cela ne fait pas exception et incrimine différents comportements directement ou indirectement liés aux nouvelles technologies et que, par commodité de langage, nous qualifierons de cybercriminalité. Ce sont ces lois spéciales que nous allons d'abord examiner dans une première partie (I), avant de passer en revue différentes études menées sur cette matière à l'étranger (II). Dans une troisième partie, nous nous consacrerons à proposer des amendements dans notre Code pénal (III) afin de pallier les manquements dont il est présentement l'objet et affermir ainsi notre arsenal législatif en matière de cybercriminalité. Enfin, dans la dernière partie (IV), nous verrons comment les nouvelles dispositions s'articulent avec les lois spéciales existantes régissant la cybercriminalité.

[1] Notes bleues de Bercy, 2005, n° 289

Maurice, depuis quelques années déjà, connait un essor de ce type de criminalité. En effet, pour la seule année 2012, on ne recense pas moins de 87 cas d'infractions tombant sous *l'Information and Communication Technologies Act* et 49 cas tombant sous le *Computer Misuse and Cybercrime Act*. Le réseau social Facebook, lui, dont sont friands de nombreux Mauriciens, a donné lieu à 53 cas d'infractions de cybercriminalité[2].

Il convient cependant avant toute chose d'esquisser une définition de ce qu'est la cybercriminalité ; celle-ci s'entend de l'ensemble des infractions pénales qui sont commises *via* les réseaux informatiques, notamment, sur le réseau Internet. Elle cible tout autant l'atteinte aux biens[3] que l'atteinte aux personnes[4].

[2] http://www.lemauricien.com/article/dangers-dinternet%C2%A0-mefiez-vous%C2%A0

[3] Par exemple, la fraude à la carte bancaire sur Internet sans le consentement de son titulaire, la vente par petites annonces ou aux enchères d'objets volés ou contrefaits, encaissement d'un paiement sans livraison de la marchandise ou autres escroqueries en tout genre, piratage d'ordinateur; gravure pour soi ou pour autrui de musiques, films ou logiciels.

[4] Par exemple, diffusion d'images pédophiles, de méthodes pour se suicider, de recettes d'explosifs ou d'injures à caractère racial, diffusion auprès des enfants de photographies à caractère pornographique ou violent, atteinte à la vie privée.

(I) Les lois spéciales à Maurice consacrées à la cybercriminalité

Le Code pénal mauricien, en l'état, garde le silence sur les infractions liées à la cybercriminalité ; cela ne signifie pas que le droit mauricien ignore cette catégorie d'infractions. En effet, ce sont les lois spéciales qui régissent cette matière, en l'occurrence l'*Information and Communication Technologies Act* et le *Computer Misuse and Cybercrime Act*. Cette dernière a été inspirée par la Convention sur la cybercriminalité de Budapest de 2001, que nous examinerons dans la deuxième partie.

Relevons toutefois que certains types de comportements délictueux qui utilisent les nouvelles technologies pour se concrétiser, peuvent être réprimés par le biais de l'escroquerie[5]. Nous pensons par exemple à toute transaction bancaire effectuée en ligne à un prix onéreux, sans retour du bien, ou encore au *phishing*[6], au *ransomware*[7], voire à l'escroquerie dite « 419 »[8], de tels procédés constituant des « manœuvres » à même de caractériser l'escroquerie.

[5] Sec. 330 Code pénal mauricien.
[6] C'est une technique ayant comme but de dérober à des individus leurs identifiants de connexion et mots de passe ou leurs numéros de cartes bancaires.
[7] Apparu à l'origine en Russie, c'est un logiciel malveillant qui chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Il peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent.
[8] D'origine nigériane, cette escroquerie abuse de la crédulité des victimes en utilisant les messageries électroniques (courriels principalement) pour leur soutirer de l'argent.

(1) Information and Communication Technologies Act

L'*Information and Communication Technologies Act* prévoit, en sa **section 46**, plusieurs infractions liées à la cybercriminalité. Ainsi, aux termes de cette section, commet une infraction toute personne qui :

(a) par une forme quelconque d'émission, de rayonnement, d'induction ou autre effet électromagnétique, nuit au fonctionnement d'un service d'information et de communication, y compris à un service de télécommunication ;

(b) avec l'intention de frauder ou pour empêcher l'envoi ou la remise d'un message, prend un message d'information et de communication, y compris un message de télécommunication de l'employé ou agent d'une licence ;

(c) avec l'intention de frauder, s'empare d'un message à partir d'un lieu ou d'un véhicule utilisé par un titulaire dans l'exercice de ses fonctions ;

(d) vole, dissimule ou détruit un message ;

(e) volontairement ou par négligence omet ou retarde la transmission ou la livraison d'un message ;

(f) falsifie un message ou transmet ou alors fait usage d'un message sachant qu'il a été falsifié ;

(g) sciemment envoie, transmet ou fait transmettre un message faux ou frauduleux ;

(h) utilise un service d'information et de communication, y compris un service de télécommunication, -

pour la transmission ou la réception d'un message qui est gravement offensant, ou est de nature indécente, obscène ou menaçante ; ou

dans le but de causer des ennuis, des inconvénients ou une anxiété inutile à toute personne ;

pour la transmission d'un message qui est de nature à mettre en danger ou compromettre la défense de l'État, la sécurité publique ou l'ordre public ;

(i) malhonnêtement obtient ou fait usage d'un service d'information et de communication, y compris un service de télécommunication, avec l'intention d'éviter le paiement de toute taxe ou redevance applicable ;

(j) au moyen d'un appareil ou périphérique connecté à une installation maintenue ou exploitée par un titulaire de permis –

frustre le titulaire de droits ou frais à bon droit payable pour l'utilisation d'un service ;

provoque la titulaire à fournir un service à une autre personne sans le paiement par toute autre personne de la redevance ou une taxe appropriée ; ou

installe ou fait installer frauduleusement un accès à une ligne de télécommunication ;

(k) Volontairement endommage, interfère avec, enlève ou détruit une installation ou un service d'information et de communication, y compris l'installation ou service de télécommunications maintenu ou exploité par un titulaire de permis ;

(l) établit, maintient ou exploite un réseau ou un service sans autorisation ou en violation des termes ou conditions d'un permis ;

(m) sans l'approbation préalable de l'Autorité, importe un équipement capable d'intercepter un message ;

(n) dévoile un message ou des informations relatives à un tel message à toute autre personne autrement que –

conformément à la présente loi ;

avec le consentement de chaque expéditeur du message et chaque destinataire visé du message ;

aux fins de l'administration de la justice, ou

autorisé par un juge ;

(o) sauf autorisation expresse de la présente loi ou autorisé par un juge, intercepte, autorise ou permet à une autre personne d'intercepter, ou accomplit tout acte ou toute chose qui lui permettrait ou permettrait à une autre personne d'intercepter, un message passant sur un réseau ;

(p) de toute autre manière enfreint la présente loi ou des règlements pris en vertu de la présente loi.

On le constate, cette section permet d'incriminer un large éventail de comportements liés aux technologies nouvelles de la communication.[9]

[9] Voir, par rapport à la sous-section (h), *Police v Goodeeal*, 2011 INT 256 ; *Police v Ramasawmy* 2011 INT 241.

(2) Computer Misuse and Cybercrime Act

Selon la **Section 3**, toute personne qui exécute une fonction sur un système informatique, sachant que l'accès qu'il tend à sécuriser est non-autorisé, commet une infraction.

La **Section 4** dispose que toute personne qui essaie d'accéder à un système informatique afin d'y accéder à un programme ou des données dans le but de commettre une infraction sous une autre loi, sera poursuivie.

La **Section 5** dispose elle en substance que toute personne qui, par tous moyens, en connaissance de cause sécurise l'accès à tout système informatique dans le but d'obtenir, directement ou indirectement, des services d'ordinateur, ou intercepte ou fait intercepter, directement ou indirectement, toute fonction de, ou des données dans un système informatique, commet une infraction.

La **Section 6**, quant à elle, incrimine le fait de modifier sans autorisation les données au sein d'un système informatique.

Quant à la **Section 7**, elle incrimine toute personne qui, sans autorisation légale ni excuse légitime, accomplit un acte qui provoque directement ou indirectement une dégradation, une défaillance, l'interruption ou l'obstruction du fonctionnement d'un système informatique, ou un déni de l'accès à, ou l'altération de tout programme ou les données enregistrées dans le système informatique.

Selon la **Section 8**, toute personne qui communique sciemment un mot de passe, code d'accès, ou tout autre moyen d'avoir accès à tout programme ou de données au sein d'un système informatique pour tout gain illicite, à des fins illégales, ou sachant qu'il est susceptible de causer un préjudice à une personne, commet une infraction.

La **Section 9**, elle, érige en infraction le fait de fabriquer sciemment, vendre, procurer l'utilisation, importer, distribuer ou rendre accessible autrement, un système informatique ou tout autre dispositif, conçu ou adapté principalement pour le but de commettre une infraction en vertu des Sections 3 à 8.

Enfin, la **Section 10** dispose que toute personne qui provoque frauduleusement une perte de biens à une autre personne par le biais de toute introduction, altération, effacement ou suppression de données, ou toute interférence avec le fonctionnement d'un système informatique, avec l'intention de se procurer pour lui-même ou une autre personne, un avantage, se rend coupable d'une infraction.

(II) Les différentes conventions et législations relatives à la cybercriminalité

Comme il a été dit plus haut, la loi mauricienne intitulée *Computer Misuse and Cybercrime Act* a été inspirée, pour partie, de la Convention du Conseil de l'Europe sur la cybercriminalité 2001 [Convention de Budapest].

(1) Convention sur la cybercriminalité de Budapest

C'est le premier traité international adopté qui tente d'aborder les crimes informatiques et les crimes liés à Internet en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations. Il contient également une série de pouvoirs et procédures tels que la recherche de réseaux informatiques et l'interception légale. Son principal objectif, énoncé dans le préambule, est de poursuivre une politique pénale commune destinée à protéger la société contre la cybercriminalité, notamment en adoptant une législation appropriée et la stimulation de la coopération internationale.

La Convention est le produit de quatre années de travail par des experts européens et internationaux. Elle a été complétée par un protocole additionnel faisant de toute publication de propagande raciste et xénophobe par le biais de réseaux informatiques une infraction pénale. Actuellement, le cyberterrorisme est également étudié dans le cadre de la Convention.

La Convention vise principalement à :

- Harmoniser les éléments criminels de fond du droit interne des infractions et des dispositions connexes dans le domaine de la cybercriminalité ;
- Fournir des pouvoirs nationaux au droit pénal procédural nécessaires pour l'enquête et la poursuite de ces infractions ainsi que d'autres infractions commises au moyen d'un système informatique ou la preuve par rapport à ce qui est sous forme électronique ;
- Mettre en place un régime rapide et efficace de la coopération internationale.

Les infractions suivantes sont définies par la Convention : l'accès illégal, l'interception illégale, l'ingérence de données, l'interférence du système, abus de dispositifs, falsification informatique, fraude informatique, les infractions liées à la pornographie juvénile et les infractions au droit d'auteur et des droits voisins.

Il énonce également des questions de droit procédural comme la conservation rapide de données stockées, la conservation et divulgation partielle des données de trafic, des ordres de production, la recherche et la saisie des données informatiques, la collecte en temps réel des données de trafic, et l'interception des données de contenu. En outre, la Convention contient une disposition sur un type spécifique de l'accès transfrontalier aux données informatiques stockées qui ne nécessite pas l'assistance mutuelle (avec consentement ou lorsqu'elles sont accessibles au public) et prévoit la mise en place d'un réseau 24/7 pour garantir une assistance rapide parmi les parties signataires.

(2) Commonwealth Model Law sur la cybercriminalité

Maurice faisant partie du *Commonwealth,* elle ne peut faire fi de la *Commonwealth Model Law* sur la cybercriminalité de 2002. C'est un modèle de loi sur la criminalité informatique développé par le *Commonwealth*. Il constitue un effort par les pays du *Commonwealth* d'harmoniser leur législation pénale liée à l'informatique avec la Convention sur la cybercriminalité. La loi modèle sert d'exemple de principes communs que chaque pays peut utiliser pour adapter la législation-cadre compatible avec les autres pays du *Commonwealth.*

Dans ses grandes lignes, notre loi est conforme à ce *Commonwealth Model Law*. Cela n'est guère étonnant puisqu'il s'inspire lui-même de la Convention de Budapest, qui, comme nous l'avons dit, a influencé la rédaction de notre *Computer Misuse and Cybercrime Act*.

Le *Model Law* ne fournit pas de définition des termes « *access* » ou « *unauthorized* » ; ainsi, il faudrait se tourner vers les meilleures pratiques internationales pour interpréter ces termes. Toutefois, et c'est à saluer, la loi-modèle introduit les deux niveaux de *mens rea* pour les infractions, à savoir, celui de l'intention, mais également d'imprudence. Cela permet de s'assurer que les infractions ne soient pas surqualifiées en raison de l'absence d'infractions avec un seuil plus bas.

Cependant, cette loi-modèle exclut certaines infractions qui pourtant sont couvertes par la Convention de Budapest, et qui sont notamment la falsification électronique, la fraude électronique, la protection de copyright digital ou encore la responsabilité des personnes morales. Fort heureusement, mis à part la responsabilité pénale des personnes morales, notre loi en la matière permet d'incriminer les infractions ci-dessus mentionnées.

(3) UNODC Study on Cybercrime

Selon le document de **l'Office des Nations unies contre la drogue et le crime**,[10] la façon dont est définie la cybercriminalité dépend le plus souvent de l'objectif visé dans le contexte où ce terme est utilisé. Un nombre limité d'atteintes à la confidentialité, à l'intégrité et à la disponibilité des données ou des systèmes informatiques constituent l'essentiel de la cybercriminalité. Cependant, d'autres agissements tels que l'utilisation d'ordinateurs pour réaliser un gain ou porter un préjudice, financier ou autre, y compris certaines formes d'usurpation d'identité et les atteintes aux contenus informatiques (qui relèvent tous de la « cybercriminalité » prise dans un sens plus large) ne facilitent pas les efforts visant à définir juridiquement ce terme dans sa globalité. Les principaux actes de cybercriminalité doivent être définis. Cependant, une « définition » de la cybercriminalité n'est pas aussi utile dans d'autres contextes, par exemple pour fixer la portée des pouvoirs spéciaux en matière d'enquête et de coopération internationale, où il vaut mieux privilégier les preuves électroniques de l'infraction, quelle qu'elle soit, plutôt qu'un concept étendu et artificiel de « cybercriminalité ».

De plus, l'UNODC considère que la législation des pays doit couvrir tous les domaines, notamment l'incrimination, la procédure, la compétence, la coopération internationale et la responsabilité des fournisseurs de services Internet.

D'après les experts qui ont rédigé le document, le droit international des droits de l'homme constitue une arme aussi bien offensive que défensive puisqu'il oblige à la fois à incriminer (de façon limitée) les formes d'expression extrêmes et à protéger les autres formes. Certaines limites à la liberté d'expression, notamment celles interdisant l'incitation au génocide, les propos haineux constituant une incitation à la discrimination, à l'hostilité ou à la violence, l'incitation au terrorisme et la propagande en faveur de la guerre, s'imposent donc aux États qui sont partis aux instruments internationaux pertinents relatifs aux droits de l'homme. Les autres disposent d'une certaine marge d'appréciation pour déterminer les limites des formes d'expression acceptables compte tenu de leurs cultures et de leurs traditions juridiques. Néanmoins, à partir d'un certain point, le droit international des droits de l'homme s'appliquera. Par exemple, lorsqu'il s'agira d'appliquer à des propos tenus en ligne des dispositions pénales sur la diffamation, l'outrage à l'autorité et les propos injurieux, il sera difficile de démontrer que les sanctions sont proportionnées, appropriées et le moins intrusives possibles. Lorsqu'un contenu est illégal dans un

[10] UNODC, *Comprehensive Study on Cybercrime* (2013).

pays, mais qu'il est légal de le produire et de le diffuser dans un autre, les États devront cibler leur riposte pénale sur les personnes accédant à ce contenu qui relèvent de leur juridiction et non sur le contenu si celui-ci a été produit à l'étranger.

Ils considèrent également que les enquêtes policières sur la cybercriminalité nécessitent de recourir à une combinaison de techniques tant traditionnelles que nouvelles. Bien que certaines activités d'enquête puissent être menées dans le cadre des pouvoirs habituels, de nombreuses règles de procédure convenant à une approche territoriale et matérielle sont inadaptées dans le contexte du stockage électronique de données et des flux de données en temps réel.

Enfin, ils mettent l'accent sur la coopération internationale qui comprend, en matière pénale, l'extradition, l'entraide judiciaire, la reconnaissance mutuelle des jugements étrangers et la coopération informelle entre polices. En raison de la nature transitoire des preuves électroniques, la collaboration pénale internationale dans le domaine de la cybercriminalité suppose que des réponses rapides soient apportées et que des mesures d'enquête spécialisées telles que la conservation de données informatiques puissent être demandées. Le recours aux formes traditionnelles de coopération reste prédominant pour obtenir des preuves extraterritoriales dans des affaires de cybercriminalité.

(4) L'infraction de vol d'identité vue par l'UNODC

En 2007, l'UNODC a publié une étude sur la fraude et l'abus et la falsification d'identité (E / CN.15 / 2007/8 et Add. 1, 2 et 3) commandée par l'UNODC et soumise à la Commission des Nations Unies sur la prévention du crime et la justice pénale à sa seizième session conformément à la résolution n° 2004/26 du conseil économique et social. Il y avait deux principales réalisations de cette étude. Tout d'abord, elle a adopté une approche large de la notion de crime lié à l'identité pour couvrir toutes les formes de comportement illicite impliquant l'identité, y compris la fraude d'identité et le vol d'identité. Ensuite, elle a examiné les crimes liés à l'identité à partir d'une nouvelle perspective de justice pénale qui traite des crimes liés à l'identité comme des infractions pénales distinctes, plutôt que de simplement criminaliser les autres infractions en utilisant de fausses identités.

Se fondant sur les conclusions et recommandations de cette étude, l'UNODC a publié le Manuel sur la criminalité liée à l'identité en 2011[11]. L'objectif principal du Manuel est de définir une gamme d'options et de considérations à prendre en compte lors de traiter les questions nationales de justice pénale relatives aux crimes liés à l'identité, y compris les défis spécifiques dans le domaine de la coopération internationale et des partenariats potentiels entre les secteurs publics et privés. Le manuel est destiné à être utilisé par les législateurs, les décideurs, les procureurs et les praticiens de l'application des lois, ainsi que d'autres parties prenantes non gouvernementales.

[11] http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

(III) Propositions d'Amendements au Code pénal mauricien

Nous le constatons, fort heureusement, Maurice n'est pas dépourvu d'un arsenal législatif pour combattre la cybercriminalité. En vue de le renforcer, il nous parait opportun d'inclure dans notre code pénal des dispositions relatives aux atteintes aux systèmes de traitement automatisé de données.

La rédaction des incriminations de cybercriminalité est un exercice délicat ; en effet, l'infraction doit être définie de manière assez extensive pour que l'évolution de la technologie ne la rende pas obsolète, ou tout du moins insuffisante, tout en prenant garde de respecter le principe de légalité qui exige clarté et précision.

Pour ce faire, nous nous sommes inspirés des dispositions du Code pénal français en la matière, en l'occurrence des articles 323-1 et suivants, introduits en 1988 par la loi Godfrain, relative à la fraude informatique, et qui concernent notamment la suppression ou modification de données (art 323-1, al. 1) ou encore la tentative d'infraction sur un STAD[12] (323-7).

Ainsi, il est proposé de rajouter un Chapitre III au Titre II relatif aux infractions contre les individus, et qui s'intitulerait : « **Des atteintes aux systèmes de traitement automatisé de données** » [nouvelles sections 369A à 369I].

[12] Système de traitement automatisé de données ; les tribunaux interprètent de manière extensive cette notion : le réseau France Telecom est un système, le réseau Carte bancaire aussi, un disque dur, un radiotéléphone, un ordinateur isolé, un réseau local.

369A Accès frauduleux à un système de traitement automatisé de données Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'une peine d'emprisonnement ne dépassant pas deux ans et d'une amende ne dépassant 100 000 roupies. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine d'emprisonnement ne peut dépasser trois ans et 150 000 roupies d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à un emprisonnement ne dépassant pas cinq ans et à 200 000 roupies d'amende. Art. 323-1 Code pén. Fr.	**369A Fraudulent access to a computer system** Fraudulently accessing or remaining within all or part of an automated data processing system is punished by imprisonment not exceeding two years and by a fine not exceeding 100,000 rupees. Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence cannot exceed three years' imprisonment and a fine of 150,000 rupees. When the offenses in the first two paragraphs have been committed against an automated processing system of personal data implemented by the State, the penalty is increased to imprisonment not exceeding five years and a fine of 200,000 rupees.

Explications

Concernant la nouvelle **section 369A**, l'accès frauduleux est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données tout en sachant qu'elle ne possède pas l'autorisation requise. Cette disposition vise à sanctionner ici le *hacker* classique, c'est-à-dire celui qui s'introduit dans les systèmes par des moyens illégaux sans toutefois détruire les données ni utiliser les informations données, parfois dans le seul but de faire savoir qu'il existe des failles de sécurité, par opposition au *cracher*, c'est-à-dire celui qui détruit[13]. La distinction du *hacker* et du *cracher* n'est toutefois pas évidente en pratique[14]. Pour ce qui est des caractères du maintien, ils peuvent être très divers, allant du maintien dit « actif », qui consiste à utiliser les possibilités de traitement du système au-delà de ce qui est autorisé, par exemple en effectuant une copie de données qui ne peuvent en principe qu'être consultées visuellement, jusqu'au maintien dit « inoffensif », qui consiste en une simple « promenade » dans le système en dehors de tout préjudice pour le « maître du système ». Les conséquences du maintien ne sont pas prises en considération par le texte d'incrimination (sous réserve des dispositions de l'alinéa 2 de la nouvelle Section 369A). Il en résulte que l'infraction peut prendre la forme d'un délit d'abstention consistant dans le fait de ne pas mettre fin à son branchement dans le système dès que l'on se rend compte de son erreur, mais aussi d'un délit d'action. Le maintien dans le système de traitement automatisé des données relève du délit continu.

[13] http://en.indian-ocean-times.com/Mauritius-A-computer-hacker-of-35-years-old-had-planted-the-online-site-of-the-government-is-fined_a1166.html

[14] Ainsi, un arrêt de la cour d'appel de Paris du 28 janvier 2010(CA Paris, pôle 4, ch. 11, 28 janv. 2010 : JurisData n° 2010-001050 ; Dr. pén. 2010, chron. 10, n° 19, obs. A. Lepage) retient, outre le délit de participation à un groupement formé ou à une entente établie en vue de la préparation d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 du Code pénal, celui d'accès et de maintien frauduleux dans un système de traitement automatisé de données avec cette circonstance aggravante que ledit accès a eu pour résultat la modification ou la suppression des données, à l'encontre de douze « hackers » qui, profitant d'une faille de la base de données du serveur, s'étaient introduit sur le site internet www.drogues.gouv.fr et y avait remplacé le communiqué annonçant la campagne nationale contre la banalisation de l'usage du cannabis par un texte intitulé « Le cannabis, j'en ai fumé ! » accompagné d'une photographie représentant une molécule de cannabis.

369B Atteintes au fonctionnement d'un système de traitement automatisé de données Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni d'une peine d'emprisonnement ne dépassant pas cinq ans et d'une amende ne dépassant pas 200 000 roupies. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à un emprisonnement ne dépassant pas sept ans et à une amende ne dépassant pas 500 000 roupies. Art. 323-2 Code pén. Fr.	**369B Violations of the operation of a computer system** Obstructing or interfering with the functioning of an automated data processing system is punished by imprisonment not exceeding five years and a fine not exceeding 200,000 rupees. When this offense has been committed against an automated processing system of personal data implemented by the State, the penalty is increased to imprisonment not exceeding seven years and a fine not exceeding 500,000 rupees.

Explications

Pour ce qui de la nouvelle **section 369B**, elle distingue deux types de comportements : non seulement le fait d'entraver le fonctionnement d'un système de traitement automatisé de données, mais encore celui d'en fausser le fonctionnement. Pour ce qui est du concept de « fonctionnement », il doit ici se concevoir de façon étendue pour englober non seulement ce qui dépend du système d'exploitation, mais encore tous les services que l'on peut attendre des divers programmes d'application. L'infraction de cette nouvelle section relève de l'infraction intentionnelle, qui ne nécessite cependant pas la démonstration d'une intention de nuire. Elle suppose simplement que l'auteur soit conscient de l'entrave qu'il apporte au système ou du fait qu'il fausse le fonctionnement du système. Le plus souvent, la preuve de l'élément moral se déduit des faits, notamment lorsque ceux-ci ont été réitérés.

369C Atteintes aux données contenues dans un système de traitement automatisé de données Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni d'une peine d'emprisonnement ne dépassant pas cinq ans et d'une amende ne dépassant pas 200 000 roupies. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à un emprisonnement ne dépassant pas sept ans et à une amende ne dépassant pas 500 000 roupies d'amende. Art. 323-3 Code pén. Fr.	**369C Interference with data in a computer system** The fraudulent introduction of data into an automated data processing system or the fraudulent deletion or modification of the data that it contains is punished by imprisonment not exceeding five years and a fine not exceeding 200,000 rupees. When this offense has been committed against an automated processing system of personal data implemented by the State, the penalty is increased to imprisonment not exceeding seven years and a fine not exceeding 500,000 rupees.

Explications

S'agissant de la nouvelle **section 369C**, l'incrimination vise encore une fois deux types de comportement : le fait d'introduire frauduleusement des données et le fait de supprimer ou de les modifier frauduleusement. L'introduction de données peut être présentée comme l'incorporation de caractères informatiques nouveaux sur un support du système ; la suppression, quant à elle, peut consister en une atteinte physique à l'intégrité des données, par exemple par « écrasement » ou « effacement », ou encore prendre la forme d'un déplacement hors du système. Le délit d'atteinte frauduleuse aux données présume une intention coupable. L'auteur doit avoir exécuté son forfait en sachant que ce qu'il introduit, supprime ou modifie n'est pas autorisé et en voulant cependant le résultat d'atteinte aux données contenues dans le système. Cette intention coupable peut se déduire des actes accomplis, les prévenus ayant nécessairement conscience de la fraude. Cependant, il n'est pas nécessaire que l'agent soit animé d'une intention de nuire. Ainsi, le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données contenues dans un système de traitement automatisé caractériserait le délit prévu par la nouvelle section 369C, sans qu'il soit nécessaire que ces modifications ou suppressions émanent d'une personne qui n'a pas un droit d'accès au système, ni que leur auteur soit animé de la volonté de nuire. Commet donc ce délit le chef comptable d'une chambre de commerce qui modifie les données qui avaient été enregistrées de manière définitive dans le système automatisé de comptabilité dont il avait la charge[15].

[15] Cass. crim., 8 déc. 1999, Bull. crim. 1999, n° 296 ; JCP G 2000, IV, 1369 ; Dr. pén. 2000, comm. 53, note M. Véron

369D Importation, détention, offre, cession ou mise à disposition d'un équipement d'atteinte aux systèmes de traitement automatisé des données Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les sections 369A à 369C est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. Art. 323-3-1 Code pén. Fr.	**369D Import, possession, supply, sale or provision of a breach equipment to computer systems** A person who, without lawful authority, imports, possesses, offers, transfers or makes available any equipment, instrument, computer programme or information created or specially adapted to commit one or more of the offences prohibited by sections 369A to 369C, is punished by the penalties prescribed for the offence itself, or the one that carries the heaviest penalty.

Explications

La nouvelle **Section 369D** a pour dessein de sanctionner, à titre autonome, un acte de complicité par fourniture de moyens. Autrement dit, cette nouvelle disposition aspire ici à permettre la répression du complice qui apporte son assistance dans la préparation d'une fraude informatique, indépendamment d'un fait principal punissable. Elle vise également à lutter contre la prolifération des virus sur les réseaux informatiques. Ainsi la nouvelle incrimination permet-elle de sanctionner l'importation, l'offre, la cession, la détention ou la mise à disposition de virus informatiques, sans qu'il soit besoin que ledit virus ait été introduit frauduleusement dans un système de traitement automatisé de données.

369E Participation à un groupe formé ou à une entente établie en vue de commettre des fraudes informatiques La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les sections 369A à 369D est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. Art. 323-4 Code pén. Fr.	**369E Participation in a group formed or association established with a view to committing computer fraud** Participating in a group or conspiracy established with a view to the preparation of one or more offences set out under sections 369A to 369D, and demonstrated by one or more material actions, is punished by the penalties prescribed for offence in preparation, or the one that carries the heaviest penalty.

Explications

La nouvelle **Section 369E** se fait fort d'incriminer spécifiquement l'organisation préalable à la commission des infractions prévues par ces sections. L'incrimination suppose toutefois que soit rapportée la preuve de la réunion d'un groupement ou d'une entente, dans le but de préparer une infraction de fraude informatique, laquelle doit se trouver concrétisée par un fait matériel. Il importe donc peu que l'entente ou le groupement soient juridiquement structurés, par exemple en association ou société, ou soient de pur fait.

369F Peines lorsque le système a été mis en œuvre par l'Etat Lorsque les infractions prévues aux sections 369A à 369D ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à un emprisonnement ne dépassant pas dix ans et à une amende ne dépassant pas 750 000 roupies. Art. 323-4-1 Code pén. Fr.	**369F Penalties when data is implemented by the State** When the offenses under sections 369A to 369D were committed by organized gangs and against an automated processing system of personal data implemented by the State, the penalty is increased to imprisonment not exceeding ten years and to a fine not exceeding 750,000 rupees.

Explications

Concernant la nouvelle **Section 369F**, elle ne fait qu'ériger en circonstance aggravante les infractions susmentionnées, puisque la bande organisée implique un plus grand danger contre l'ordre public et l'État.

369G Peines complémentaires Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes : 1° L'interdiction, pour une durée ne dépassant pas cinq ans, des droits civiques, civils et de famille ; 2° L'interdiction, pour une durée ne dépassant pas cinq ans, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ; 3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ; 4° La fermeture, pour une durée ne dépassant pas cinq ans, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; 5° L'exclusion, pour une durée ne dépassant pas cinq ans, des marchés publics ; 6° L'interdiction, pour une durée ne dépassant pas cinq ans, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ; 7° L'affichage ou la diffusion de la décision prononcée Art. 323-5 Code pén. Fr.	**369G Additional penalties** Natural persons convicted of any of the offences provided for under the present Chapter also incur the following additional penalties: 1° forfeiture, for a period not exceeding five years, of civic, civil and family rights ; 2° prohibition to hold public office or to undertake the social or professional activity in the course of which or on the occasion of the performance of which the offence was committed, for a period not exceeding five years; 3° confiscation of the thing which was used or intended for the commission of the offence, or of the thing which is the product of it, with the exception of articles subject to restitution; 4° mandatory closure, for a period not exceeding five years of the business premises or of one or more of the premises of the undertaking used to commit the offences; 5° disqualification from public tenders for a period not exceeding five years; 6° prohibition to draw cheques, except those allowing the withdrawal of funds by the drawer from the drawee or certified cheques, for a period not exceeding five years; 7° public display or dissemination of the decision.

Explications

Pour ce qui est de la nouvelle **section 369G**, il s'agit de peines complémentaires qui s'expliquent à la fois par la gravité et la nature même de l'infraction.

369H Tentative punissable La tentative des délits prévus par les sections 369A à 369D est punie des mêmes peines. Art. 323-7 Code pén. Fr.	**369H Punishable attempt** Attempt to commit the misdemeanours referred to under sections 369A to 369D is subject to the same penalties.

Explications

La nouvelle **Section 369H** concerne la tentative de commettre les délits qu'on a vus plus haut. La répression au titre de la tentative implique une absence de désistement volontaire et un commencement d'exécution, même si dans la pratique, la frontière entre le commencement d'exécution des fraudes informatiques et les simples actes préparatoires à celles-ci peut se révéler poreuse.

369I Usurpation d'identité ou usage de données permettant d'identifier un tiers Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'une peine d'emprisonnement ne dépassant pas un an et d'une d'amende ne dépassant pas 150,000 roupies. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. Art. 226-4-1 Code pén. Fr.	**369I identity theft or use of data to identify any third party** The act of impersonating a third party or make use of one or more data of any kind which allows to identify him in view of disturbing his tranquility or that of others, or harm his honor or his reputation or consideration, is punishable by imprisonment not exceeding one year and a fine not exceeding 150 000 rupees. This offense is punishable by the same penalties when committed on a public online communication network.

Explications

Le vol d'identité a causé des pertes économiques substantielles dans plusieurs pays ; si on s'en tient à l'exemple du Royaume-Uni, le ministère de l'Intérieur estime que la fraude sur l'identité coûte 1,7 milliard de livres à l'économie britannique, soit presque 50 % de plus qu'en 2002. D'après l'APACS, l'Association des services de paiement au Royaume-Uni, la fraude touchant la banque en ligne a doublé au premier semestre 2006 par rapport à l'année précédente. En 2007, l'Office des Nations-unies contre la drogue et le crime (UNODC) a formulé un ensemble de recommandations concernant la criminalité liée à l'identité (Nations unies, 2007) qui appellent les autorités, le secteur privé et la société civile à conjuguer leurs efforts contre le vol d'identité.

On constate donc qu'un droit moderne ne peut garder un silence qui ne saurait être que coupable sur ces questions, tant en ce qui concerne la sécurité des justiciables que la pérennité économique, d'où la proposition de cette nouvelle section dans notre Code pénal. Celle-ci permettrait d'incriminer deux comportements. D'abord, l'usurpation d'identité. Ensuite, l'usage d'une ou de plusieurs données de toute nature permettant d'identifier ce tiers d'autre part. Le rapporteur de ce texte de loi en France a souligné que le terme « identité » devait être compris comme « recouvrant tous les identifiants électroniques de la personne, c'est-à-dire à la fois son nom, mais aussi son surnom ou son pseudonyme utilisé sur Internet »[16].

L'usurpation d'identité d'un tiers ou l'utilisation de données de toute nature permettant de l'identifier est une infraction intentionnelle, le dol général devant ici être complété par un dol spécial. Le premier consiste ici, au regard de ce qui constitue la matérialité de l'incrimination, dans la seule volonté consciente d'usurper l'identité d'un tiers ou de faire usage de données de toute nature permettant de l'identifier. Quant au second, l'usurpation d'identité d'un tiers ou l'utilisation de données de toute nature permettant de l'identifier doit avoir été commise « en vue » de troubler la tranquillité, l'honneur ou la considération.

[16] E. Ciotti, Rapport AN n° 2271, 1re lecture, 27 janv. 2010, p. 112

Il est aussi proposé d'ajouter une nouvelle section 249quater pour combattre la pédopornographie en ligne, avec les systèmes et réseaux informatiques comme supports de l'infraction.

S. 249quater Exploitation à caractère pornographique de l'image d'un mineur Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni d'une peine d'emprisonnement ne dépassant pas cinq ans et d'une amende ne dépassant pas 75 000 roupies. Lorsque l'image ou la représentation concerne un mineur de seize ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation. Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines. Les peines sont portées à un emprisonnement ne dépassant pas sept ans et à une amende ne dépassant pas 100 000 roupies lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques. Le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou	**S. 249quater Pornographic exploitation of the image of a minor** Taking, recording or transmitting a picture or representation of a minor with a view to circulating it, where that image or representation has a pornographic character, is punished by imprisonment not exceeding five years and a fine not exceeding 75,000 rupees. When the image or representation involves a minor of sixteen, the acts are punishable even if they were not committed in view of the dissemination of this image or representation. The same penalty applies to offering or distributing such a picture or representation by any means, and to importing or exporting it, or causing it to be imported or exported. The penalties are increased to imprisonment not exceeding seven years and a fine not exceeding 100,000 rupees where use was made of a communication network for the circulation of messages to an unrestricted public in order to circulate the image or representation of a minor. The fact of habitually consulting or in return of a payment a public online communication service providing such an image or representation, to acquire or stocking such image or representation, by any means whatsoever, is punished by imprisonment not exceeding two years and a fine not exceeding 30 000 rupees.

représentation par quelque moyen que ce soit est puni d'une peine d'emprisonnement ne dépassant pas deux ans et d'une amende ne dépassant pas 30 000 roupies. Les infractions prévues à la présente section sont punies d'une peine d'emprisonnement ne dépassant pas dix ans et d'une amende ne dépassant pas 500 000 roupies lorsqu'elles sont commises en bande organisée. La tentative des délits prévus à la présente section est punie des mêmes peines. Les dispositions de la présente section sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image. Article 227-23 Code pénal fr.	The offences set out in the present section are punished by imprisonment not exceeding ten years and by a fine not exceeding 500,000 rupees where they are committed by an organised gang. Attempting to do so is subject to the same penalties. The provisions of the present section also apply to the pornographic images of a person whose physical appearance is that of a minor unless it is proved that the person was over eighteen on the day his picture was taken or recorded.

Explications

La Section 15 de notre *Child Protection Act* fait certes de la prise ou de la distribution d'une photographie « indécente » de mineur une infraction, mais, à notre avis, ne prend pas suffisamment en compte le caractère protéiforme des nouvelles technologies. De plus, le terme « indécent » peut prêter à confusion ; en effet, il s'agit ici d'une « infraction ouverte »[17] parce que le terme « indécent » ne correspond juridiquement à rien de précis et qu'il appartient, en définitive, aux tribunaux, de déterminer dans chaque cas particulier les règles caractéristiques de l'indécence. Enfin, il n'y est question que de « photographies » ou « pseudo-photographies ». Ce sont ces errements que la nouvelle Section 249quater (qui se situerait juste après la section 249ter dévolue aux atteintes sexuelles sur mineur[18]) aspire à rectifier. En effet, avec la nouvelle incrimination, il peut s'agir aussi bien d'un dessin ou d'une sculpture que d'une photographie ou un film. Dans la mesure où le fondement de l'incrimination n'est pas l'atteinte au mineur que constitue la réalisation du support, mais l'attitude de l'agent réalisant une image pornographique à partir de la représentation d'un mineur, celle-ci est aussi coupable que l'œuvre soit réelle ou d'imagination. La simple nudité ne semble pas pouvoir être interprétée comme pornographique[19]. Cela ne veut en aucun cas dire que prendre des photos d'enfants nus serait légal, cela tomberait alors sous la Section 15 du *Child Protection Act*, puisque comme il a été rappelé plus haut, les amendements au Code pénal ne viennent pas se substituer aux lois spéciales, mais les suppléer. Cette nouvelle infraction est un délit intentionnel dont l'élément moral sera établi directement à l'égard de tous ceux qui seront informés de la nature des images fabriquées et diffusées[20].

[17] M.-L. Rassat, Fasc. 20, MISE EN PÉRIL DES MINEURS, JurisClasseur Pénal Code > Art. 227-23 et 227-24, n° 9, 16 Janvier 2015
[18] Voir le document de la LRC : *Paper Changes to Book III of Criminal Code (Offences against Persons)* de mars 2015.
[19] CA Douai, 16 mai 2007, n° 06/04021.
[20] Cass. crim., 10 juill. 1973.

(IV) Articulation des nouvelles dispositions avec les lois spéciales

La question peut se poser quant à l'agencement des nouvelles dispositions avec les lois spéciales qui régissent cette matière au sein de notre droit. Cependant, les nouvelles dispositions dans le Code pénal dont il est question ci-dessus viennent suppléer et s'ajouter aux dispositions existantes dans le *Computer Misuse and Cybercrime Act* et le *Information and Communication Technologies Act*.

a. Computer Misuse and Cybercrime Act

Ainsi, l'on constate que l'expression employée dans la nouvelle Section 369A : « accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données » est plus exhaustive que celle de la Section 3 qui se lit comme suit « *causes a computer system to perform a function, knowing that the access he intends to secure is unauthorised* (…) » et permettra donc d'élargir le champ d'incrimination.

De même, la formule « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données » (nouvelle Section 369B du Code pénal) est plus claire que celle utilisée à la Section 5 de la loi spéciale « *unauthorised access to and interception of computer service* ».
Idem pour ce qui est de la nouvelle Section 369C qui incrimine le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient. Elle englobe plus de faits matériels que la Section 6 de la loi spéciale (« *unauthorised modification of computer material* »).
La même réflexion s'applique quant à la formulation de la nouvelle Section 369D, qui porte sur le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions et qui vient supplémenter la caractérisation de l'infraction qui découle de la Section 4 de la loi spéciale (« *Access with intent to commit offences* »).

Plusieurs des nouvelles infractions qui sont proposées ne trouvent pas d'écho dans le *Computer Misuse and Cybercrime Act*. Il en va ainsi de la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions

(Section 369E). La commission des infractions susmentionnées en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État (Section 369F), n'est, elle non plus, pas traitée dans la loi spéciale. Les peines complémentaires applicables aux personnes physiques ne s'y retrouvent pas non plus. *Idem* en ce qui concerne la tentative punissable des délits en question dont la loi spéciale ne fait pas mention.

b. Child Protection Act

La nouvelle Section 249quater relatif à la pédopornographie trouve un écho à la section 22 de la loi spéciale qui renvoie au *Child Protection Act*. Cependant, cette dernière utilise le vocable de « *indecent* » qui nous parait par trop nébuleux, alors que la nouvelle section emploi un terme qui a l'avantage d'être utilisé dans différentes législations, celui de « pornographique ». De plus, constituerait désormais une infraction le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, ainsi que d'acquérir ou de détenir une telle image ou représentation par quelque moyen.

c. Information and Communication Technologies Act

Les nouvelles sections incriminent essentiellement les atteintes aux systèmes de traitement automatisé de données alors que la Section 46 de l'*Information and Communication Technologies Act* couvre un plus large éventail de comportements liés aux technologies nouvelles de la communication Il ne faut pas voir ces nouvelles sections et la loi spéciale comme étant mutuellement exclusives, mais venant se complémenter.