Octopus Interface – Coopération contre le cybercrime
Strasbourg, 11-12 juin 2007

APERÇU DES STRATÉGIES NORMATIVES ITALIENNES DE DROIT MATÉRIEL AU SUJET DE LA LUTTE À LA CYBERCRIMINALITÉ ET DES APPLICATIONS JURISPRUDENTIELLES CORRESPONDANTES. COMPARAISON AVEC LES DISPOSITIONS CONTENUES DANS LA CONVENTION DE BUDAPEST

Par Carlo Sarzana di S.Ippolito, Italy

Préambule

L'Italie, après la France, a été le premier Pays en Europe qui a mis sur pied une loi bien construite pour la répression des infractions informatiques, en modifiant son propre Code Pénal et de Procédure Pénale. Il s'agit de la loi 23.12.1993, n. 547 à qui, par la suite, d'autres lois sont venues s'ajouter, lesquelles, en certains domaines, tendaient à la répression des comportements illicites à propos dudit piratage informatique (décr. législ. 29.12.1992, n. 518, modifié par la loi 18.08.2000 n. 248 et, enfin, par la loi 22.5.2004 n. 128), de la protection des données personnelles (loi 31.12.1996 n. 675 et modifications suivantes) de la soi disant pédophilie télématique (loi 3.8.1998 n. 269 modifiée par la loi n. 11.8.2003 n. 228 et, enfin, par la loi 6 février 2006 n. 38). La place accordée à la note présente ne permet que de renseignements concis, même s'il s'agit d'un sujet désormais tellement ample qu'il mériterait des commentaires détaillés et des traités, surtout pour ce qui concerne l'utilisation illégale des nouveaux technologies. On se bornera, donc, à exposer synthétiquement la législation italienne (celle qui existe et celle *in fieri*) au sujet du droit pénal matériel, avec des esquisses aussi à des dispositions italiennes qui regardent des hypothèses qui ne sont pas conçues dans la Convention: cela pour rendre le plus possible complete cette exposition.

1) Article 2 de la Convention: accès illégal

Dans le système pénal italien il existe l'article 615 ter, ayant comme titre "accès abusif à un système informatique ou télématique". La norme en question punit l'accès abusif à un système informatique ou télématique, ou la contrainte à y demeurer contre la manifestation, expresse ou implicite, de la volonté de l'ayant-droit.

Cette norme trouve sa place dans le domaine des infractions contre la inviolabilité de domicile parce que, comme il a été observé par la Rapport au projet de loi qui est devenu en suite la loi n. 547 du 1993, les systèmes informatiques ou télématiques constituent une extension idéale de la zone de respect qui appartient à la personne intéressé, garantie par l'article 14 de la Constitution et pénalement protégée, en ce qui concerne ses aspects les plus essentiels et traditionnels, des articles 614 et 615 du Code Pénal.

À ce propos, il faut observer que le législateur, en définitive, a introduit dans le Code Pénal l'idée, totalement inédite, de "domicile informatique". D'autre part, en suivant les indications suggérées par le Conseil de l'Europe [voir Racc. n. 89 (R)] 9, la tutelle est limitée aux systèmes informatiques et télématique protégés par des mesures de sécurité, puisque l'existence de mesures pareilles constitue la preuve visible de la volonté du titulaire d'exclure de l'accès les " tierss.".

L'adverbe "abusivement" contenu dans la norme visée à l'article 615 ter constitue, selon la doctrine (Picotti), une clause de illicéité spéciale, introduite par la législation prévue par la loi cite n. 547 de 1993 à selon le modele de l'infraction de violation de domicile, visée à l'article 614 du Code Pénal, donc la norme peut être interprétée en considérant le traitement traditionnel relativement aux qualités spécifiques en l'espèce.

En réalité, la disposition a voulu attribuer, comme il ya dit en precedence, au domaine informatique et télématique la protection déjà reconnue au domicile traditionnellement conçu, comme il est explicitement affirmé,nous l ,avons deya remarquè , dans la relation gouvernementale à ladite n. 547/1993.

Au sujet de la réglementation mentionnée il a y eu beaucoup de decisions jurisprudentielles et de pris de position opposées dans la doctrine, surtout en ce qui concerne la nouvelle definition de domicile informatique et la qualité de l'existence des mesures de protection, comme condition de punibilitè,,.

À propos de la qualité des mesures de sécurité, comme la théorie générale du droit l'a soutenu, ces mesures, prévues dans l'article mentionné, sont citées non pas pour sa propre efficacité qui a force d'exclure, plutôt pour sa propre capacité purement déclarative d'une volonté contraire à l'accès au système; elles sont le "signaux" extérieur de l'exploitation concrète du *jus excludendi alios*, et il s'agit du même phénomène si l'on prend en considération la violation de domicilie "classique", pour laquelle l'art. 614 c.p. demande que l'introduction illégale dans l'appartement d'autrui arrive " contre la volonté exprimée ou tacite en l'habitation d'autrui " de celui qui a le droit de l'exclure. "

On va analyser, donc, les décisions jurisprudentielles à ce sujet. Tout d'abord, il

faut souligner que la première décision à ce sujet de la Cour de Cassation Pénale Chambre VI – est celle n. 3067 et remonte au 4 octobre 1999 par qui on énonce qu'avec la prévision de l'art. 615-ter c.p., introduit lors de la loi 23 décembre 1993, n. 547, le législateur a assuré la protection du "domicile informatique" en qualité de lieu idéale (mais aussi physique où les données informatiques sont contenues) qui releve de la sphère individuelle, en qualité de bien protégé aussi constitutionnellement. Cependant – la Cour a encore adfirmé – l'art. 615-ter c.p. ne se limite pas à proteger seulement les contenus personnels des données recueillies dans les systèmes informatiques protégés, mais il donne une tutelle plus ample qui se concrétise dans le *jus excludendi alios,* quel que soit le contenu des données contenues dans l/ordinqteur , pourvu qu'il soit relatif à la sphère de la pensée ou à l'activité, du travail ou pas, de l'usager; il s'ensuite de là que la tutelle de la loi s'étend aux aspects économique-patrimoniaux des données si le titulaire du *jus excludendi* est une personne physique, morale, ou un particulier ou un public, ou une autre personne.

Par le même arret la Cour a aussi analysé le problème du concours entre le crime de accès illégal et celle de fraude informatique, en admettant la possibilité puisque, d'après la Court, il s'agit d'infractions totalement différentes, la seconde desquelles prévoit nécessairement la manipulation du système, élément constitutif qui n'est pas nécessaire pour la consommation du premier.

La différence entre les deux hypothèses on peut la tirer, en outre – d'après la Court – par la différence des biens juridiques protegès, de l'élément subjectif et de la prévision de la possibilité de commettre le crime d'accès illégal seulement vis_a_vis des systèmes protégés, qualité qui ne se trouve pas dans le crime de fraude informatique.

L'opinion de la Cour a été confirmée par un autre arret de la Court /Chambre Pénale V du 7 novembre - 6 décembre 2000 n. 1675, d'après qui l'art. 615 ter alinéa 1 c.p. punit non seulement celui qui s'introduit abusivement dans un système informatique ou télématique mais aussi celui qui " y demeure contre la volonté explicite ou tacite de celui qui a le droit de l'exclure ". Il s'ensuite de là que la violation des dispositifs de protection du système informatique **n'acquit pas d'importance en soi**, mais seulement comme manifestation d'une volonté opposée à celle de celui qui dispose légitimement du système.

Il ne s'agit pas donc d'un délit caractérisé par l'effraction des systèmes de protection – la Cour a dit – parce qu'il n'aurait pas d'importance la conduite de celui qui, après qu'il est entré légitimement dans le système informatique, y demeure contre la volonté du titulaire. Il s'agit d'un délit caractérisé, en effet, de la

contravention aux dispositions du titulaire, comme il arrive dans le délit de violation de domicile, qui a notamment été le modèle de ce nouveau cas d'espèce pénal, et en effet beaucoup de gens a cru y reconnaître, parfois même d'une manière critique, la tutelle d'un "domicile informatique".

La Cour a continué en disant qu'il faut que l'accès au système informatique ne soit pas permis à tous, comme parfois il arrive surtout quand il s'agit de systèmes télématique. Donc il faut retenir que, dans le but de définir le délit, il acquit de l'importance chaque mécanisme de sélection des personnes qui peuvent accéder au système informatique, aussi quand il s'agit d'instruments extérieurs au système et de pure organisation, en tout ce que destinés à régler l'entrée même dans les pièces où les installations sont gardées. D'autre partie, la ressemblance au cas d'espèce de la violation de domicile doit porter à penser qu'il commette ce délit aussi celui qui, autorisé à l'accès dans un but déterminé, utilise le titre de légitimation dans un but différent, et, donc, ne respecte les conditions à qui était subordonné l'accès.

En ce qui concerne la seconde partie de l'article 615 ter, c'est-à-dire au cas de celui-ci qui demeure dans le système contre la volonté, exprimée ou tacite, de la part du titulaire du droit de veto, cette hypothèse a determinè beaucoup de discussions dans la doctrine.

Récemment un juge (Tribunal Viterbe – Montefiascone – jugement du 5 juillet 2005) a affirmé que cela ne constituait pas un accès illégal aux termes de l'article 615 ter: la conduite d'un employé, autorisé à l'usage du système informatique, qui avait consulté des données relatives à un domaine différent par rapport à celui-ci de sa propre compétence, en l'absence d'une interdiction explicite d'accéder à ce domaine spécifique et en l'absence de buts personnels ou d'autrui, étrangères à l'organisme d'appartenance.

Ledit jugement remarque qu'il s'agirait d'autre chose dans le cas de la permanence dans un système protégé de la part d'un sujet autorisé à accéder tout exceptionnellement, pour le déroulement d'une fonctionne déterminée: par exemple, au cas du technicien chargè par le responsable informatique d/ effectuer une intervention sur le système comme une réparation, l'installation de logiciel ou d'autres opérations semblables. Dans un cas de ce type le consentement du titulaire du système à l'accès laisse totalement non préjugée la nécessité de discrétion sur les données, en étant évident que l'autorisation accordée ne s'étend pas à la prise de connaissance du matériel contenu dans le système, à part le cas où cela se rende étroitement fonctionnel au déroulement des opérations demandées. Aussi dans ce cas il serait donc pénalement considérable la

permanence au moment où l'agent ne sortît pas du système une fois terminé le devoir qui lui avait été confié: la permanence constitue en effet un danger pour la discrétion des données, en pouvant l'agent profiter de la situation pour acquérir des renseignements qu'il ne possède pas. Différemment par rapport à l'hypothèse précédente, la désapprobation du titulaire à la permanence dans le système de la part d'une tierce personne, initialement autorisée à l'accès, il sera normalement tacite, puisque il est implicite dans une autorisation conditionnée sans équivoque au déroulement d'un travail spécifique et occasionnelle.

2) Interception illégale

L'interception illégale est prévue dans le système italien par trois articles du Code Pénal et c'est-à-dire par l'article 617 quater (interception, empêchement ou interruption illicite de communications informatiques ou télématiques) de l'article 617 quinquies (installation d'appareillages aptes à intercepter) empêcher ou interrompre des communications informatiques ou télématiques), par l'article 617 sexies (falsification, altération ou suppression de communications informatiques ou télématiques).L/article s/occupe de l/interception ,ecc.
des communications susmentionnées. Il a pu prevu aussi le cas de celui qui révèle "par l'intermédiaire de n'importe quel moyen et d'information au public" le contenu des communications en question. Des circonstances aggravantes spécifiques sont prévues parmi lesquelles aussi la circonstance relative à celui qui exerce, même abusivement, le métier de détective privé.
L'article suivant punit l'installation d'appareils aptes à intercepter, empêcher ou interrompre des communications relatives à un système informatique ou télématique c'est-à-dire des communications entre plus systèmes: des circonstances aggravantes spécifiques sont prévues ici aussi.
Le contrefaction, l'altération ou la suppression du contenu de communications informatiques ou télématiques, même si occasionnellement intercepté, sont prévues par le troisième article. Afin qu'on puisse définire coupable et punissable une personne il faut qu'elle se tache du dol spécifique ou qu'elle lasse qu'autrui en utilise. Par ce genre de dol on se réfère au but de procurer à soi ou à autrui un avantage ou d'apporter à d' autrui un dommage.
Ladite loi n. 547 du 1993 complète ou modifie les dispositions de loi dans le but de effectuer un rapprochement entre les modifications prévues pour le code de droit matériel et celles prevue pour le droit procedural de façon à consentir à l'Autorité Judiciaire légitimement de disposer l'interception du flux de communications

relatives aux systèmes informatiques ou télématiques c'est-à-dire qu'il y a entre plusieurs systèmes. Il a été ainsi inséré, après l'art. 266 du c.p.p., relatif aux interceptions normales, l'art. 266 bis qui porte comme titre "interception de communications informatiques" ou "télématiques" selon lequel dans les délits indiqués dans l'art. 266 (il s'agit, en générale, de délits graves), ainsi dans les délits commis à travers l'emploi de technologies informatiques ou télématiques elles sont permises toujours les interceptions relatives. En conséquence il y a des parties de l'art. 268 qui ont aussi été mises à jour, relatives à l'exécution des opérations d'interception.

Maintenant il faut dire que, lors des scandales relatifs à des interceptions illégales en particulier effectuées par des sujet qui appartenaient à la société téléphonique Telecom, le Gouvernement a présenté un décret loi spécial le 22 septembre 2006 n. 259 qui porte comme titre "Dispositions urgentes au sujet des normes qui concernent les interceptions téléphoniques, converti en loi 20.11.2006 n. 28."

La disposition se limite à modifier l'article 240 du c.p.p. en disposant que le M. P. décide immédiatement de tenir secrets et gardés, en endroit protégé, des supports et des documents qui concernent les données et les contenus de conversations ou de communications relatives au trafic téléphonique et télématique, illégalement formé ou acquis, puis en indiquant la procédure pour la destruction.

La normative prévoit un nouveau type de crime en disposant que "quiconque consciemment détient les actes, les supports ou les documents dont la destruction ait été disposée aux termes de l'article 240 c.p.p., il est puni d'une peine de réclusion de 6 mois jusqu'à 4 ans.

La détention de 1 à 5 ans est appliquée dans le cas où le fait est commis par un public officiel ou par un responsable de public service.

3. Article 4 - Atteinte à l'intégrité des données et article 5 - Atteinte à l'intégrité des systèmes

Les hypothèses mentionnées plus haut sont actuellement prevues dans l'article 420 c.p. (atteinte aux installations d'utilité publique) et de l'article 635 bis (endommagement de systèmes informatiques et télématique).

Par la loi n. 547 le législateur a remplacé l'article 420 précédent afin d'étendre la tutelle aux systèmes informatiques ou télématique d'utilité publique c'est-à-dire aux données, renseignements ou programmes ici contenu ou à eux pertinents. L'hypothèse de crime est construite comme délit d'atteinte c'est-à-dire "à la consommation anticipée" dont le moment de la réalisation coïncide avec le mettre

en étant l'action directe à endommager ou détruire les "objets" indiqués. Selon la Rapport au projet de loi, il doit s'agir de systèmes, données, etc., qui appartiennent à des sujets publics ou privés qui ont une complexité et une importance de manière à se faire qu'une atteinte aux mêmes devient source de danger immédiat pour l'ordre public ou pour les intérêts socio-économiques de la collectivité.

À son tour, l'article 635 bis prévoit les hypothèses de celui qui détruise ou rende inutilisables, en tout ou en partie, des systèmes informatiques ou télématiques d'autrui, c'est-à-dire des programmes, des renseignements ou des données qui appartiennent à autrui. Il s'agit d'hypothèse criminelle particulière par rapport à celle de l'endommagement commun (art. 635).

Il faut dire que le projet de loi relatif à la ratification de la Convention de Budapest, présenté par le Ministre de la Justice et approuvé par le Conseil des Ministres le 11 mai 2007, en cours de publication pour la présentation aux Chambre, il prévoit quelques modifications aux articles susmentionnés, modifications déterminées, comme on lit dans la rapport au projet de loi citée, par une nécessité de symétrie par rapport au système de la Convention qui distingue nettement l'endommagement de l'intégrité des données de l'endommagement de l'intégrité du système et discipline les deux hypothèses en articles distincts, le 4 et le 5, et de l'opportunité d'introduire une discipline pénale différenciée à selon que l'objet de la tutelle, des renseignements, des données et des programmes informatiques aient ou n'aient pas d'importance publicitaire.

Les modifications proposées sont les suivante:

l'article 635 - bis du code pénal est remplacé par le suivant: "L'article 635-bis, Endommagement de renseignements, données et programmes informatiques, Sauf que le fait constitue le plus grave délit, quiconque détruit, détériore, efface, altère ou supprime renseignements, données ou programmes informatiques d'autrui est puni, à la plainte de la victime , d'une peine de réclusion de six mois à trois ans. Si recourent l'une ou plusieurs circonstances visées au second alinéa de l'article 635, c'est-à-dire si le fait est commis par abus de la fonctionne d'opérateur du système, la peine est de la réclusion d'un à quatre ans et on procède d'office."

Après l'article 635-bis du code pénal on a ajouté les suivants:

"Article 635-ter, Endommagement de renseignements, données et programmes informatiques utilisés de l'État ou d'autre organisme public ou de toute façon d'utilité publique,

Sauf que le fait constitue le plus grave délit, quiconque détruit, détériore, efface, altère ou supprime renseignements, données ou programmes informatiques utilisés

de l'État ou d'autre organisme public ou de toute façon d'utilité publique, il est puni d'une peine de réclusion d'un à cinq ans. S'il recourt une ou plusieurs circonstances visées au second alinéa de l'article 635, c'est-à-dire si le fait est commis avec abus de la qualité d'opérateur du système, la peine est de la réclusion de deux à sept ans.

Article 635-quater (Endommagement de systèmes informatiques et télématique)

Sauf que le fait constitue le plus grave délit, quiconque, par les conduites visées à l'article 635-bis, c'est-à-dire à travers l'introduction ou la transmission de données, renseignements ou programmes, il rend inutilisables, en tout ou en partie, des systèmes informatiques ou télématique d'autrui ou il en compromet gravement le fonctionnement il est puni d'une peine de réclusion d'un à cinq ans. S'il recourt une ou plus que les circonstances visées au second alinéa de l'article 635, c'est-à-dire si le fait est commis avec abus de la qualité d'opérateur du système, la peine est de la réclusion de deux à sept ans."

4) Article 6 – Abus de dispositifs

L'hypothèse citée plus haut est actuellement prevue dans le système italien par le texte des articles 615 quater et de l'article 615 quinquies c.p..

Le premier qui a comme titre "Détention et diffusion illégale de codes d'accès aux systèmes informatiques ou télématique" punit l'acquisition illégale de n'importe quelle manière (donc, aussi s'il s'agit d'une élaboration autonome), et la diffusion de codes d'accès à systèmes informatiques ou télématiques protégés par des mesures de sécurité. Pour la définition du crime il faut le dol spécifique, consistant dans le but de procurer un profit à soi ou à d'autres personnes ou d'apporter à d'autres personnes un dommage. Aux hypothèses décrites plus haut sont comparées la reproduction, communication et remise de codes, mots clé ou autres moyens aptes à l'accès frauduleux, ou de toute façon illicite, à un système informatique ou télématique ou la fourniture d'indications ou d'instructions aptes au but.

Le second article a comme titre "Diffusion de programmes directs à endommager ou interrompre un système informatique." Cette article punit le comportement de celui qui communique ou remet un programme informatique rédigé par lui même ou par d'autres personnes, qui a comme but ou comme effet l'endommagement d'un système informatique ou télématique, c'est-à-dire des données ou des programmes en lui contenu ou à lui pertinents, c'est-à-dire l'interruption, total ou

partielle, ou l'altération de son fonctionnement.
Il s'agit des soi disant programmes virus, terme à considérer de façons ample . c'est-à-dire qui inclue aussi les soi disants worms (pas destructifs).
En Italie la première décision concernant explicitement l'introduction d'un virus a été celle du Tribunal de Bologna du 22.12.2005.
Le cas concernait des individus qui, en concours parmi eux, en créant un programme virus nommé VieriKa, transmis par voie informatique au fournisseur Tiscali et, par celui-ci, à environ 900 usagers du fournisseur, ils s'étaient introduits dans les systèmes informatiques de ces utilisateurs en acquérant des données, aussi réservées, contenues dans leur ordinateur personel - entre qui des listes d'adresses de courrier électronique - à l'insu des personnes en question et, ils avaient en outre, à travers le virus en question, endommagé les programmes contenu dans les ordinateurs personnels atteints, en compromettant le fonctionnement correct.
Selon le jugement en question, le crime de diffusion de programmes visant à endommager ou interrompre un système informatique pouvait concourir avec cet accès illégal à un système informatique ou télématique et le dol de ce dernier cas d'espèce on le déduisait du dol relatif au premier crime.
À ce propos, il faut rappeler qu'aussi en Italie ils se sont vérifiés des cas du soi disant netstrike. Il s'agit d'une nouvelle forme d'attaque aux sites, principalement institutionnels, réalisée dans le but d'une protestation politique ou syndical dont le fondement est une invitation de la part des organisateurs, addressè vers une masse d'utilisateurs possesseurs d'accès Internet et d'un logiciel de navigation, à diriger leur "modem" vers une spécifique URL à une heure précise et, plusieurs fois, de manière telle à occuper un site WEB jusqu'à le rendre inutilisable, au moins pour la durée de la mobilisation.
En relation à l'attaque mené le 28 février 2002 contre le site du Ministère de la Justice, la Procuration de la République de Bologna a ouvert une enquête vis-à-vis des organisateurs du netstrike, accusés du délit visé à l'article 617 quater et à l'article 615 quinquies.

5) Article 7 – Falsification informatique

Dans le système pénal italien cette hypothèse est prévue par l'article 491 bis du c.p., comme l'introduit la loi n. 547 du 1993, qui a comme titre: "Documents informatiques."
Par l'article en question il a été inséré dans chef III du titre II du livre II du c.p.,

relatif à la fausseté en actes, une nouvelle prévision qui étend aux faussetés concernant un document informatique, les dispositions au sujet de faux en acte public ou en écriture privée (articles de 476 à 491 c.p.). La deuxième partie de l'article en question contient la définition de document informatique valable dans le domaine pénal: s'agit d'un "quelconque support informatique contenant des données ou des renseignements qui ont une efficacité en tant que preuves ou des programmes destinés spécifiquement à être élaborés."

Au sujet de la falsification informatique il faut citer un arret récente et important de la Suprême Cour (Jugement Chambre Pénal V - 25 mars 2005 - n. 11930) qui, en suivant quelques précédents de 2001, a soutenu qu'aussi en l'absence de la règle visé à l'art. 491 bis introduite par la loi mentionnée n. 547, le délit de faux informatique résultait déjà puni sur la base la normative existant au sujet du faux, en énonçant les suivantes: principes

Extrait de sentence 1

L'archives informatique d'une Administration Publique il faut le considérer comme un registre, constitué par un matériel pas en papier, tenu par un sujet public, avec la conséquence que la conduite du functionnaire que, dans l'exercice de ses fonctions et en faisant usage des supports techniques de l'administration publique, crée un document faux informatique destiné à rester dans la mémoire de l'ordinateur commet une falsification dans un acte public, selon le cas matériel ou idéologique, n'a pas d'importance la circonstance que aucun document en matériel de papier n'ait été imprimé.

Extrait de sentence 2

Il n'y a pas d'argumentations littéraux, logiques ou de système qui empêchent d'inclure dans la prévision de l'art. 476 c.p. ou en celle de l'art. 479 c.p. la conduite du functionnaire que dans l'exercice de ses fonctions crée un document informatique en substance ou formellement faux. Aussi à travers l'instrument informatique, en vérité, l le functionnaire peut créer un document représentatif d'actes ou de faits, destiné à donner cette certitude à la tutelle de laquelle les règles pénales sont préposées.

Extrait de sentence 3

Malgré les diversités structurales qui caractérisent le document informatique et la conduite relative qui le réalise, par rapport au document écrit et à la conduite qui le réalise, l'art. 491 c.p bis. ne peut pas se définir étroitement innovant pour une raison de genre littéral. Et en effet l/ampleur incontestable de la formulation des articles 476 et 479 c.p. impose de reconnaître que l'insertion de données faux dans l'archives d'un organisme public de la part d'un employé ayant le titre nécessaire

est punissable aux termes des susmentionnées règles qui incriminent, aussi si réalisé en époque précédente par rapport à l'entrée en vigueur de l'art. 491 c.p bis..

Une autre arret important , en outre , a été celle de la Suprême Cour, Chambre V Pénale, du 14 décembre 2005 n. 45313 selon qui il commet le délit visé aux articles 476, 490, 491 c.p bis. l'agent de la Police municipal qui a la fonction de service d'insertion de données dans le système de verbalisation informatique et qui efface les documents informatiques relatifs à la prédisposition des procès-verbal de vérification de violation des règles du code de la route. La Cassation a jugé sans importance la circonstance selon qui les données archivées, objet d'altération, étaient présent aussi sur des supports en papier, en valorisant la définition de "documents informatiques" contenue dans l'art. 491 c.p. bis.. Selon la Suprême Cour, en effet, "la norme concerne l'hypothèses dans laquelle le système informatique est soutenu par support en papier et celle-ci dans laquelle il substitue le même, en incluant, dans les deux cas les deux articulations distinctes du cas d'espèce pénal: l'hypothèse selon qui la falsification concerne directement les données ou les renseignements qui possèdent déjà en soi, une importance en tant que preuves et l'hypothèse selon qui la falsification concerne par contre des contextes de programmes spécifiquement destinés à élaborer des données et des renseignements, comme il est prescrit par la dernière partie de la même règle."

Le projet de loi gouvernemental relatif à la ratification prévoit quelques modifications et intégrations au sujet du faux en informatique: plus précisément à l'article 491-bis, premiers alinéas, du code pénal, la deuxième période est supprimée de "dans un tel but" jusqu'aux mots "destinés" et "les élaborer". Et en outre, après l'article 495 du code pénal, on a ajouté le suivant: "L'article 495-bis, (Fausse déclaration ou attestation à celui qui certifie sur l'identité ou sur ses propres qualités personnelles ou d'autrui). Quiconque déclare ou atteste faussement à celui qui certifie l'identité ou l'état ou d'autres qualités de sa propre personne ou d'autrui, il est puni d'une peine de réclusion jusqu'à un an."

Le rapport au projet de loi de la Convention susmentionné motive les innovations susmentionnées, en affirmant que la modification de l'article 491-bis a été effectuée en considération de l'inadéquation survenue de la définition de document informatique, entendu comme "support d'informatique contenant des données ou des renseignements qui ont une efficacité en tant que preuves ou contenant des programmes destinés à les élaborer". On a décidé d'accueillir, aussi dans le but pénal, la plus ample et correcte notion de document informatique, déjà contenu dans le décret du Président de la République 10 novembre 1997 n. 513 comme "

représentation informatique d'actes, faits ou données juridiquement importants ", en abrogeant la deuxième période de l'art. 491-bis.

6) Article 8 – Fraude informatique

Le code pénal actuellement en viguer prévoit la fraude informatique à l'article 640-ter. Il s'agit d'une hypothèse spéciale d'escroquerie, relative à l'altération du fonctionnement d'un système informatique ou télématique ou à lui pertinent. Plus particulièrement la règle concerne le fait de celui qui, en altérant de n'importe quelle manière le fonctionnement d'un système informatique ou télématique ou en intervenant sans droit de n'importe quelle manière sur des données, des renseignements ou des programmes, contenus dans un système informatique ou télématique, ou à eux pertinents, procure à soi ou à d'autres personnes un profit injuste et par conséquence il cause à autrui un dommage. Aussi cette disposition est spécial par rapport au cas d'espèce d'escroquerie commune, art. 640.
Selon la doctrine (Picotti) le cas d'espèce susmentionné est assez semblable à celui-ci prévue par l'article 8 de la Convention.
Cependant une différence considérable concerne le second événement de consommation de délit prévu par le cas d'espèce italien, le profit injuste pour soi ou pour autrui, absent dans la prévision de la Convention selon qui ça suffit que l'avantage, de nature d'autre part résolument économique, soit objet du dol spécifique de l'agent.
Le droit italien a eu occasion de s'occuper du crime en question, surtout en ce qui concerne la distinction de l'escroquerie informatique de celle commune, prévue par l'art. 640 c.p.) mais aussi en ce qui concerne le moment de consommation du délit.
Selon la Cassation Pénale, Chambre VI, arret du 14.12.1999 n. 3065, le crime de fraude informatique, art. 640-ter c.p.) a la même structure et les mêmes éléments constitutifs de l'escroquerie de laquelle elle diffère seulement parce que l'activité frauduleuse de l'agent ne concerne pas la personne (sujet passif), qui ne vient pas induite en erreur , mais le système informatique de la personne, à travers la manipulation de ce système. Aussi la fraude informatique se réalise dans le moment où l'agent obtient l'injuste profite et, par conséquence, un dommage patrimonial d'autrui. (Dans le cas d'espèce l'agent, en utilisant le système du téléphone fixe installé dans une filiale de la société italienne pour l'exercice téléphonique, par une digitation rapide et ininterrompue de numéros téléphoniques, en partie correspondants à ceux-ci pour qui le standard était qualifié et en partie correspondants aux usages étrangers, il avait réussi à obtenir des liaisons

internationales, en éludant le bloc prédisposé pour les appels internationaux pour qui le système n'était pas qualifié, ainsi en exposant à une situation de dette passive, la société italienne pour l'exercice téléphonique vis-à-vis des organismes étrangers correspondants autorisés à l'exercice téléphonique).
À propos de la forme de la conduite, selon la doctrine, il s'agit d'un crime à la forme libre qui prévoit, alternativement une conduite consistante à l'altération du fonctionnement du système informatique ou télématique c'est-à-dire à une intervention ne pas autorisée (il est possible d'effectuer cela par l'intermédiaire de n'importe quelles modalités en agissant sur les données, les renseignements et les programmes ici contenus).
Toujours à ce sujet, un jugement récent de la Suprême Cour, Chambre II, le 14 septembre 2006, n. 30663 a affirmé que: "Dans le fait de reproduction ne pas autorisée, en copie, de programmes d'entreprises et de données secrètes achevées réalisé par accès au système opérationnel d'entreprise, ils existent les extrêmes pour la définition abstraite du concours entre les délits d'accès illégal à un système informatique ou télématique et de fraude informatique.

7) Article 9 – Infractions se rapportant à la pornographie enfantine

La loi n. 269 du 3 août 1998 a introduit dans le c.p. l'art. 600 ter intitulé "pornographie enfantine", dont le troisième alinéa prévoit le fait de celui qui, par l'intermédiaire de n'importe quel moyen, aussi par voie télématique, distribue, divulgue ou publicise le matériel pornographique prévu par le 1er alinéa, (réalisé, c'est-à-dire, par l'exploitation sexuelle des personnes âgées de mois de ans 18, c'est-à-dire il distribue ou il divulgue des nouvelles ou des renseignements finalisés à la séduction ou à l'exploitation sexuelle des personnes âgées de mois de ans 18. Le 4ème alinéa réprime aussi la pure cession consciente à autrui personne, aussi au titre gratuit, de matériel pornographique produit par l'exploitation mentionnées déjà plusieurs fois.
La loi en question a introduit dans le code .penal . aussi un autre article, le 600 quater intitulé "détention de matériel pornographique", selon lequel est puni quiconque en , au dehors du cas visé à l'art. 600 ter – consciemment – se procure ou dispose de matériel produit par l'exploitation plusieurs fois mentionnée.
La loi prévoit d'importantes innovations d'un point de perspective procédurale au sujet des interceptions, d'activité secret sous couverture , de renvoi des mesures d'arrêt ou de séquestre (articles 12 et 13), etc..
Les dispositions mentionnées plus haut ont été en partie modifiées par la loi

11.08.2003 n. 228 et, surtout, de la loi 6 février 2006 n. 38 qui a comme titre "Dispositions en matière de lutte contre l'exploitation sexuelle des enfants et contre la pédopornographie aussi par le biais d'Internet."

Cette dernière loi a introduit à l'article 600-ter c.p., après le terme "divulgue", l'autre " diffuse", en prévoyant un dernier alinéa selon lequel si le matériel est en quantité considérable la peine vient augmentée.

La loi en question a modifié l'article précédent 604 quater du c.p. relatif à la détention de matériel pornographique en disposant que: "Quiconque, hors des hypothèses prévues par l'article 600-ter, consciemment procure ou détient matériel pornographique réalisé en utilisant des personnes âgées de mois de ans 18, est puni d'une peine de réclusion jusqu'à trois ans et d'une amende qui ne sera pas inférieure à 1.549 euros.

La peine est augmentée au maximum de deux tiers si le fait concerne des quantités considérable de matériel détenu.

La loi en question a aussi introduit une nouvelle prévision et c'est-à-dire l'article 604-quater.1 intitulé "Pornographie virtuelle" selon lequel "les dispositions visées à l'article 600-ter et 600-quater s'appliquent aussi quand le matériel pornographique représente des images virtuelles réalisées en utilisant des images ou des parties d'elles des personnes âgées de mois de ans 18, mais la peine est réduite d'un tiers. L'expression images virtuelles signifie images réalisées par des techniques d'élaboration graphique ne pas associées en tout ou en partie à des situations réelles, dont la qualité de représentation fait apparaître comme vraies des situations qui ne sont pas réelles."

À ce sujet, il faut dire qu'en 2003 une Commission Interministérielle fut nommée, sous la demande du Ministère de la Justice et de celui des Affaires Étrangers, chargée de rédiger un projet de ratification de la Convention.

Le travail de cette Commission, terminé en été de 2004, n'eut pas cependant de suite, probablement dans la perspective de donner préférence au projet de loi au sujet de la pédophilie enfantine. qui avais ètè presentè par le puissant Ministre de les soi disant Pari Opportunità;; La famme avais,en realitè ; la charge de la protection des mineurs,attribuè a elle par le Premier Ministre.. ;

Le texte de la Commission, de toute façon, a été récemment repris par le Ministère de la Justice actuel toutfois en apportant au même quelques modifications et en éliminant quelques prévisions.

On a ainsi éliminée la possibilité d'incriminer la pédophilie putative, c'est-à-dire celle relative à une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite, comme la prévision explicite de la séduction

des mineurs en réseau.
Il ne peut pas se taire, d'autre part, que la doctrine a vivement critiqué cette dernière loi en l'accusant le texte beaucoup d'omissions et d'une rigueur absolument excessive.
En réalité, il n'y a pas dans la loi quelque prévision de soutien possible au pédophile repenti. Il faudrait analyser probablement encore une fois, comme une partie de la doctrine a soutenu/ l'a dit, le monopole de l'action délicate d'opposition a la pedopornogaphie, exclusivement confié à la Police d'État, comme il faudrait prévoir la nécessité de formation spécifique de la part du magistrat qui mène les actions délicates et sous couverture qui comprennent – il faut le remarquer bien - aussi l'ouverture de sites "chouette" pornographique et l'utilisation dans un tel but de matériel pornographique séquestrée précédemment par les forces de l'ordre.
Last but not least, sans aucun doute il faudrait prévoir un contrôle psychologique attentif à l'égard du personnel de la Police qui agit comme agent provocateur.
Avec référence à la loi en question, la doctrine la plus avisée (Manna) a affirmé que le bien juridique protégé par la nouvelle entité de la pornographie virtuelle présente des contours indéfinis et peut s'assimiler à la tutelle de la moralité contre les "répréhensibles" entités des pédopornographes, qui producent aussi dans des but particuliers du matériel pornographique. Par la réforme de 2006 le bien juridique protégé par l'art. 600-quater n. 1 c.p. subit - selon une telle doctrine - un procès de matérialisation puisque on ne protège pas un bien concret (qui est constitué par son contenu) mais la projection des pures valeurs culturelles, politiques et sociales. Des doutes de légitimité constitutionnelle pour la violation du principe du soi disant principe d/offensivitè, peuvent venir soulevés, c'est ce que soutient encore la doctrine en question en relation à tel cas d'espèce dans lequel on veut prévenir la commission d'autres crimes par l'incrimination de comportements qui peuvent en constituer l'introduction sans qu'en concret un mineur vienne effectivement lésé en sa dignité pour la réalisation du matériel pornographique.
Un problème délicat à ce sujet semble avoir été résolu par la Suprême Cour par l arret de la Chambre Pénale II du 22 avril 2004. L arret en question a affirmé que la règle visée l'art. 600-quater (ante modifica) ne punit pas ceux qui simplement visionnent le sites porno et ceux qui, en naviguant dans le réseau Internet, viennent simplement en contact avec des images qui ont un contenu pornographique.
La règle en question punit en réalité ceux qui s'approprient de l'image, en la sauvant et en véhiculant sur le disque dur de l'ordinateur personnel ou sur d'autres supports qui peuvent avoir un interface par rapport à celui-ci, qui en permettent la

vision et de toute façon la reproduction.
Le téléchargement des matériaux pornographiques doit être évidemment conscient et volontaire, car il faut exclure la responsabilité pénale dans les cas dans lequel le matériel retrouvé dans l'ordinateur personnel constitue la trace pure d'une consultation passée du web, créée par les systèmes de sauvetage automatique de l'ordinateur personnel même.
La pris de position jurisprudentielle susmentionnée a été confirmée par un autre arret de la Cassation, Chambre III de 21.9.2005 qui a confirmé la définition du délit en question dans l'hypothèse où, à l'intérieur d'un système informatique, on n'est pas possible de retrouver d'images mais seulement les traces d'une pure et simpleconsultation de sites pédophiles.
Un autre problème délicat a été résolu par le bureau du G.I.P (Juge pour les Enquêtes Préliminaires) près du Tribunal de Perugia (sentence 8 juillet/30 décembre 2003) selon lequel l'envoi de matériel pornographique à un site chouette, c'est-à-dire au agent de police judiciaire qui agit en secret c,est a dir sous couverture (agent provocateur), cela ne constitue pas de crime.
Il faut rappeler maintenant que le Ministre des Télécommunications, de concert avec le Ministre pour les réformes et les innovations dans l'Administration Publique, a émis en date 8 janvier 2007, un décret pour l'obscurcissement des sites pédopornografiques en réalisation de l'article 14-quater inséré par l'article 19 alinéas 1 de ladite loi le 6 février 2006 n. 38.
Finalement, il doit être rappelé que, selon la Cassation et la doctrine prédominante, les notions de pornographie enfantine accueillies par l'art. 600-ter du c.p., doivent t être corréler directement à l'exploitation effective d'un enfant, en chair et en os.

8) Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Le système actuel, art. 171-bis de la loi n. 633 de 1941 comme modifié par le décret n législatif n. 518 de 29.12.1992 et de la loi n. 248 de 18.08.2000, protège explicitement les programmes pour ordinateur.
L'article en question recite: "Quiconque abusivement duplique, pour tirer un avantage, des programmes pour ordinateur ou dans les mêmes buts importe, distribue, vend, détient au but commercial ou d'entrepreneur ou donne en location des programmes contenus en supports qui ne sont pas marqués par la Société italienne des auteurs et éditeurs (SIAE), il fait l'objet de la peine de la réclusion de six mois à trois ans et de l'amende de lires cinq millions à lires trente million. La

même peine s'applique si le fait concerne simplement un quelconque moyen qui permette ou facilite le déplacement arbitraire ou l'escamotage fonctionnel de dispositifs appliqués à la protection d'un programme pour ordinateurs. La peine ne peut pas venir réduite au minimum de deux ans de réclusion et d l'amende à lires trente millions si le fait est de gravité considérable.

"Quiconque, afin d'en tirer un profit, reproduit sur des supports qui ne sont pas marqués SIAE, transfère sur un autre support, distribue, communique, présente ou montre en public le contenu d'une banque de données en violation des dispositions visées aux articles 64-quinquies et 64-sexies, c'est-à-dire qu'il exécute l'extraction ou le réemploi de la banque de données en violation des dispositions visées aux articles 102-bis et 102-ter, c'est-à-dire qu'il distribue, vend ou accorde en location une banque de données, il est fait objet de la peine de la réclusion de six mois à trois ans et de l'amende de euro 2582,26 a 15493. La peine n'est pas inférieure au minimum à deux ans de réclusion et l'amende de euro 15493 si le fait est de gravité considérable.

Le décret loi de 31.11.2005, n. 7 converti en loi n. 43 de 2005 prévoit le fait de celui qui en violation de l'art. 16 de la loi 633/941 dans le but du gain met à disposition du public, en les introduisant dans un système de réseaux télématique, par l'intermédiaire de communications de n'importe quel genre une oeuvre de l'esprit protégée ou une partie d'elle.

9) Article 12 – Responsabilité des personnes morales

La responsabilité administrative des personnes morales est prévue en Italie du Décret Législatif 8/6/2001 n. 231 qui prévoit à l'article 24 la responsabilité de l'organisme pour fraude informatique en dommage de l'État ou d'un organisme public.

L'article en question, qui porte comme titre "perception illégale de distributions, escroquerie en dommage de l'État ou d'un organisme public ou pour l'obtention de subvention publiques , fraude informatique en dommage de l'État ou d'un organisme public" récite: "En relation à la commission des délits visés aux articles 316-bis, 316-ter, 640, alinéa 2, n. 1, 640-bis et 640-ter s'ils sont commis en dommage de l'État ou d'un autre organisme public, du code pénal, il s'applique à l'organisme la sanction pécuniaire jusqu'à cinq-cents parts."

"Si, à la suite de la commission des délits visés à l'alinéa 1, l'organisme a obtenu un profit d'entité considérable ou qu'il lui est dérivé un dommage de gravité spéciale; il faut appliquer la sanction pécuniaire de deux-cents à six-cents parts."

"Dans les cas prévus par les alinéas précédents, ils faut appliquer les sanctions d'interdiction prévues par l'article 9, alinéa 2, lettres c), d), et e)".
Le projet de loi mentionné, relatif à la ratification de la Convention, se propose de compléter le décret législatif n. 231, en insérant l'article 25-septies qui prévoit: "En relation à la commission des délits visés aux articles 420, 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter et 635-quater du code pénal, il faut appliquer à l'encontre de l'organisme la sanction pécuniaire de 100 à 500 parts."
"En relation à la commission des délits visés aux articles 615-quater et 615-quinquies du code pénal il faut appliquer à l'organisme même la sanction pécuniaire jusqu'à 300 parts."
"En relation à la commission des délits visés aux articles 491-bis et 640-quinquies du code pénal, sauf tout ce qui a été prévu par l'article 24 pour les cas de fraude informatique en dommage de l'État ou d'un autre organisme public, il faut appliquer à l'organisme la sanction pécuniaire aux 400 parts."
"Dans les cas de condamnation pour un des délits indiqués dans l'alinéa 1 il faut appliquer les sanctions d'interdiction prévu par l'article 9, alinéa 2, lettre a), b), et c). Dans les cas de condamnation pour un des délits indiqués dans l'alinéa 2 il faut appliquer les sanctions d'interdiction prévu par l'article 9, alinéa 2, lettres b), et e). Dans les cas de condamnation pour un des délits indiqués dans l'alinéa 3 il faut appliquer les sanctions d'interdiction prévu par l'article 9, alinéa 2, lettres c), d), et e)".

10) <u>Remarques conclusives</u>

Dans le but de maintenir un caractère exhaustif a ce rapport , il faut dire que dans le système pénal italien, en opposition à la cybercriminalité, des autres réglementations sont prévues, qui ne sont pas visees par la Convention: Ainsi la loi n. 547 de 1993 a partiellement modifié l'article 392 du code .penal . qui concernait l'exercice arbitraire de ses propres raisons avec violence sur les choses. n

ajoutant au texte un troisième alinéa àu moyenn du quel la notion juridique de "violence" sur les choses a été étendue, aux effets de la loi pénale, à des comportements qui concerne les programmes informatiques… plus en particulière le délit en question existe lorsqu'un programme informatique a ètè ; altéré, modifié ou effacé en tout ou en partie ou 'il est empêché ou troublé le fonctionnement d'un système informatique ou télématique sur qui l'agent avance des droits prétendus, même si ces programme se trouvent en la disponibilité d'autrui. Il s'agit de la

"mutilation" ou de l'action directe à rendre inutilisables, aussi seulement partiellement des programmes informatiques, des actions celles-ci réalisées dans le but d'exercer des droits qu'ils auraient pu ou dû être faits valoir devant à un juge. Évidemment, s'il n'existe pas le particulier but de l' "auto-tutelle prétendue, dans le fait ils se relèvent les éléments d'autres types de crimes." De son cotè la loi antiterrorisme du 31/7/2005 n,155 introduit l'article 2-bis dans la loi 2.10.1967 n. 895, énonçant: "Quiconque hors des cas permis par des dispositions de loi ou des règlements dresse une personne ou donne des instructions de n'importe quelle manière, aussi d'une manière anonyme, ou *par voie télématique* sur la préparation ou sur l'usage d'explosifs matériels, d'armes de guerre, d'irritants du rhino-pharynx ou de substances bactériologiques nuisibles ou dangereux et d'autres mécanismes meurtriers, il est puni, sauf que le fait constitue le plus grave délit, d'une peine de réclusion d'un à six ans".

Remarques à propos du Protocole Additionnel à la Convention, relatif à l'incrimination d'actes de nature raciste ou xénophobe commis par le biais d'un système informatique

L'Italie n'est pas signataire du protocole susmentionné et on n'a pas de renseignements en ce qui concerne un revirement possible ou un supplément éventuel de réflexion.

Pour ce qui concerne la situation de l'Italie à propos de la lutte au racisme et à la haine raciale, on se rapporte donc au *paper* présenté par moi-même dans la conférence précédente d'OCTOPUS qui a eu lieu à Strasbourg du 15 au 17 septembre 2004. Il faut ajouter que le Ministre de la Justice a présenté au Conseil des Ministres, qui l'a approuvé en date 25 janvier 2007 (le projet de loi est à présent dans l'attente d'une publication) un projet de loi que prevoit des règles au sujet de la sensibilisation et de la répression de la discrimination raciale, à cause du sexe et de l'identité du genre. Des modifications à la loi 13 octobre 1975 n. 654 – énonçant: " À l'article 3 de la loi 13 octobre 1975, n. 654, et modifications ultérieurs, l'alinéa 1 è substitué par l'alinéa suivant: "Sauf que le fait constitue le plus grave délit, même dans le but de la réalisation de l'article 4 de la Convention, le rappel est a la Convention internationale pour l/eliminationdes toute forme de discrimination raciale) il est puni: a) d'une peine de réclusion jusqu'à trois ans quiconque, de n'importe quelle manière, divulgue des idées fondées sur la supériorité ou sur la haine raciale ou ethnique, ou bien encourage à commettre ou commet des actes de discrimination en raison de la race, de l'origine ethnique, de

l'origine nationale, de la religion ou fondés sur le sexe ou sur l'identité du genre; b) d'une peine de réclusion de six mois à quatre ans quiconque, de n'importe quelle manière, encourage à commettre ou commet de la violence ou des actes d'incitation à la violence en raison de la race, de l'origine ethnique, de l'origine nationale, de la religion ou fondés sur le sexe ou sur l'identité du genre ".

CONCLUSIONS

Il n'y a pas de doute que l'évolution et les applications de plus en plus diffuses de la technologie informatique aient eu comme conséquence parallèle une envahissante et inéluctable dépendance des systèmes de gouvernement de la société et des de la vie sociale par la technologie en question. Parmi les conséquences indésirables d'un processus de ce genre a acquis une importance capitale le phénomène parasitaire de l'utilisation illégale de cette technologie. Les possibilités d'attaque aux centres névralgiques de la société et à ses infrastructures critiques, surtout lorsque elles sont informatisées, depuis longtemps ont attiré l'attention des gouvernements et des principales institutions internationales et ont agrandi la conscience de la vulnérabilité de la "information society" et des dangers potentiels qui menacent l'organisation même, politique et économique, des pays démocratiques de l'occident. Cette vulnérabilité a été bien soulignée récemment dans le Rapport du COE (2004) qui portait sur le crime organisé en Europe et sur la menace du cybercrime. Les bruits à juste raison alarmistes de la relation mentionnée et les "caveat" ci-contenus sont si considérables que, à part ses aspects qui concernent la procédure pénale et qui concernent la criminologie, le problème ne peut plus être ignorer. D'une manière avantageuse et réaliste, cette relation a attiré l'attention sur le besoin d'éduquer les usagers, en les rendant conscients des graves risques inhérents à l'évolution d'une criminalité de ce genre, et sur la nécessité de développer et mettre en place des mesures techniques de protection. Bien que la relation souligne que la réalisation de ces objectifs se porte au delà de l'objet de relation même, cela dit, il n'y a pas de doute que l'activité de lutte contre le dangereux phénomène de la cyberctiminality on ne peut pas le confier seulement à des mesures répressives, et cela parce qu'on sait bien que le gap t entre le droit et la technologie constitue une constante. Et à propos des nouvelles technologies je me réfère aux conséquences et aux répercussions dans le domaine juridique, national et international, et de la privacy, de l'utilisation de nouvelles technologies par exemple la biométrie, le WIFI, le VoIP (système vocal sur l'Internet), la RFID (l'identification par radiofréquence) et aux "lacunes" du cadre juridique traditionnel. Pour en venir au rapport citè, je souligne - entre parenthèses - que, en dehors des

objectifs éclairés par la relation, il y en a d'autres rattachés comme la formation des employés pour ce qui concerne la sécurité des systèmes et la meme ethique informatique, l'étude des implications dans le domaine juridique et de l'organisation de la sécurité informatique. Il semble très important, à mon avis, l'étude des conséquences, même purement juridiques, de l'utilisation énorme de l'intelligence artificielle et de l'utilisation de plus en plus diffuse des robots ainsi que les réflexions sur ll/incidence sur les comportements juridiquement évaluables de la fréquentation des mondes virtuels du genre de "second life" à l'égard desquels il y a une série de problèmes indubitables de attribution de responsabilité empruntée. En conclusion, la pure répression est l'un des aspects de tout ce qui constitue le processus de lutte à la menace du cybercrime: en réalité, il faut avoir un vrai approche multidisciplinaire au phénomène et ici le monde juridique et le monde de la coopération internationale sont sans aucun doute au premier plan.

Carlo Sarzana di S.Ippolito
11 juin 2007