CYBERCRIMINALITÉ : ÉNONCÉ DU CAS PRATIQUE ET SYNTHÈSE DES RÉPONSES

Maud OLINET

Doctorante à l'Université de Paris I
Chargée d'enseignement à l'Université de Marne-la-Vallée

Espace virtuel qu'aucune frontière ne délimite, qu'aucun fleuve ne borne et qu'aucun pouvoir central ne régente, l'Internet est avant tout un nouvel espace d'expression humaine, un espace qui est celui de la liberté où chacun peut agir, s'instruire et s'exprimer.

Cet espace n'est naturellement pas celui du droit. Extraterritorialité et rapidité des réseaux, fugacité et volatilité des données, anonymat, communication quasiment instantanée à un coût modéré, complexité croissante, le cyberespace est aussi un terrain de prédilection pour les délinquants : il réunit pratiquement tous les ingrédients pour réaliser le crime parfait !

De nombreux délits se sont multipliés, ils menacent autant les individus que les entreprises ou les États. Une enquête dans les milieux d'affaires aux États-Unis a révélé que 85 % des entreprises sondées ont été victimes d'actes de piratage. Aux États-Unis, le Pentagone, à lui seul, a enregistré en un an plus de 22 000 agressions électroniques contre ses systèmes et le FBI a recensé 5 000 infrastructures « extrêmement vulnérables » à la criminalité informatique capable selon son nouveau directeur Ronald L. Dick de « déstabiliser l'économie entière d'un pays ».

Ce réseau planétaire suscite dès lors autant d'attirances que de craintes. C'est pourquoi, avant que ce nouvel espace de civilité ne devienne aussi un champ d'action privilégié du crime organisé, la lutte contre la cybercriminalité est devenue un objectif européen incontournable. Face à l'Internet, vecteur et cible d'une criminalité polymorphe, qui, par nature, ignore les frontières, les États membres de l'Union européenne ne peuvent pas lutter seuls et doivent faire converger leurs efforts. L'Union européenne se veut un réel espace de liberté, de sécurité et de justice, et non un espace virtuel ou de non-droit.

Ciblant son étude sur ces différents caractères spécifiques à la cybercriminalité — principalement l'extraterritorialité — ainsi que sur les infractions clés en la matière que sont le *hacking* et le piratage, le cas pratique suivant a été soumis aux chercheurs afin d'analyser la réalité des sanctions dans chaque système juridique.

Nicky et Marcel, co-présidents de l'association GRO.T.I.US (Groupement des Terreurs Internationales des Universités), en vacances au Portugal, n'ont pas révisé leur examen de droit pénal [1]. *Afin de réussir leur dernière année universitaire, ils entreprennent de prendre connaissance du sujet de leur examen.*

A cette fin, Nicky et Marcel, experts en informatique, déjà condamnés pour les mêmes faits l'année précédente à l'étranger, accèdent, sans autorisation, par le biais de leur ordinateur portable, au réseau intranet de leur université. Le sujet d'examen y étant stocké, ils copient ce dernier sur une disquette. Afin de fêter la fin de leur scolarité, Nicky et Marcel, introduisent en outre un programme dans ce réseau qui détruira toutes les données présentes dans ce système informatique le soir de leur examen. Comme le prévoit la charte fondatrice de l'association GRO.T.I.US., Nicky et Marcel distribuent le sujet de l'examen à tous les membres de leur association.

Soupçonnés par les services de police, Nicky et Marcel avouent avoir commis ces faits.

L'étude comparée des 11 réponses [2] à ce cas pratique a permis de réaliser une synthèse et de dégager des recommandations au regard de la Proposition de Décision-cadre du 19 avril 2002 relative aux attaques visant les systèmes d'information et de la Convention sur la Cybercriminalité du Conseil de l'Europe [3].

De ces diverses réponses se dégagent des éléments pour notre réflexion commune autour de deux axes : d'une part, la répression de la cybercriminalité dans chaque système juridique national et, d'autre part, l'incidence des condamnations pénales étrangères sur ces systèmes juridiques. Au fur et à mesure de la présentation des réponses seront déduites différentes propositions.

I. LA RÉPRESSION DE LA CYBERCRIMINALITÉ PAR LES DROITS NATIONAUX : L'ÉTUDE COMPARÉE DE 11 SYSTÈMES JURIDIQUES

Distinguons l'étude comparée des incriminations et des sanctions spécifiques à la cybercriminalité abordées dans le cas pratique, de l'examen plus général de la responsabilité pénale des personnes morales.

---

[1] Nicky et Marcel sont des ressortissants de votre pays, et leur université se situe dans votre pays.

[2] Angleterre, Belgique, Espagne, Finlande, France, Grèce, Italie, Pays-Bas, Pologne, Russie, Slovénie.

[3] Proposition de Décision-Cadre du Conseil relative aux attaques visant les systèmes d'information présentée par la Commission européenne (2002/0086(CNS), 19 avr. 2002) ; Convention sur la cybercriminalité du Conseil de l'Europe (S.T.E. nº 185, ouverte à la signature le 23 nov. 2001).

A. — *Étude comparée des incriminations*

Le hacking — L'accès illégal est l'infraction fondamentale qui crée une atteinte à la sécurité, c'est-à-dire à la confidentialité, l'intégrité et la disponibilité, des systèmes et données informatiques.

Huit pays sur onze incriminent l'accès intentionnel et sans autorisation dans un système informatique ainsi que la Proposition de Décision-cadre et la Convention sur la cybercriminalité [4].

Seuls l'Espagne, les Pays-Bas ainsi que la Pologne ne l'incriminent pas. Peut être estiment-ils que l'incrimination de la simple intrusion ne crée pas nécessairement des risques ? Pour autant, le simple fait de s'introduire dans un système informatique sans autorisation implique la prise de connaissance des données présentes dans ce système, données confidentielles, personnelles, industrielles ou étatiques.

Trois pays — la Grèce, l'Italie, la Slovénie — ainsi que la Proposition de Décision-cadre exigent des conditions supplémentaires, principalement que le système soit sécurisé, pour qu'on puisse parler d'infraction [5]. Notons que la Convention du Conseil de l'Europe réserve également ce droit à un État [6].

Les particuliers comme les entreprises et les organismes publics doivent pouvoir diriger, exploiter et contrôler leurs données et leurs systèmes sans perturbation. C'est pourquoi, il est souhaitable que tous les systèmes juridiques incriminent l'accès intentionnel et sans autorisation dans un système informatique protégé par des mesures de sécurité conformément à la Proposition de Décision-cadre du Conseil de l'Union Européenne.

Les atteintes à l'intégrité des données informatiques — Tous les onze systèmes ainsi que l'Union Européenne et le Conseil de l'Europe incriminent les atteintes intentionnelles portées à l'intégrité de données informatiques [7]. Seule la Grèce n'incrimine pas spécifiquement les atteintes portées à des données informatiques.

---

[4] Angleterre (sect. 1 du Computer Misuse Act de 1990), Belgique (art. 550 *bis* § 3 1° du Code pénal), Finlande (chap. 38, Sect. 8 du Code pénal, 21 avr. 1995/578), France (art. 323-1 du Code pénal), Grèce (art. 323-4 du Code pénal), Italie (art. 615 *ter* du Code pénal), Russie (art. 272 du Code pénal), Slovénie (art. 225 § 2 du Code pénal), Proposition de Décision-Cadre du Conseil relative aux attaques visant les systèmes d'information (art. 3), Convention sur la cybercriminalité (art. 2).

[5] En Grèce, est exigée la violation d'interdictions ou de mesures de sécurité ; en Italie, est exigé que le système informatique soit protégé par des mesures de sécurité ; en Slovénie, est exigée en sus l'utilisation indue des données issues de ce réseau ; la Proposition de Décision-cadre exige soit que le système fasse l'objet de mesures de protection particulière, soit une intention spécifique de porter préjudice ou d'obtenir un avantage économique.

[6] L'article 2 de la Convention sur la cybercriminalité précise qu'une partie peut exiger par exemple que l'infraction soit commise en violation des mesures de sécurité ou dans l'intention d'obtenir des données informatiques.

[7] Angleterre (sect. 3 du Computer Misuse Act de 1990), Belgique (art. 550 *ter* § 2 du Code pénal), Espagne (art. 264 du Code pénal), Finlande (chap. 34, Sect. 9a du Code pénal (14 oct. 1999/951), France (art. 323-1, 323-3 du Code pénal), Grèce (art. 222 du Code pénal), Italie (art. 635 *bis* du Code pénal), Pays-Bas (art. 350a § 1 du Code pénal), Pologne (art. 268 § 1 du Code pénal), Russie (art. 273 du Code pénal), Slovénie (art. 225 § 4 du Code pénal), Proposition de Décision-Cadre du Conseil (art. 4), Convention du Conseil de l'Europe (art. 4).

Les manifestations diverses de ces atteintes peuvent se regrouper en deux éléments matériels que six systèmes juridiques [8] ainsi que l'Union Européenne incriminent tous les deux : l'altération, c'est-à-dire la modification de données existantes telle l'endommagement ou la détérioration, incriminée seule par quatre droits nationaux [9] ; la destruction, c'est-à-dire la suppression, l'effacement de données informatiques, incriminée seule par le droit russe.

Huit pays ainsi que la Proposition de Décision-Cadre du Conseil, la Convention du Conseil de l'Europe réservant ce droit à un État, exigent en outre des conditions supplémentaires afin que l'on puisse parler d'infraction : une intention spécifique (Belgique, Proposition de Décision-Cadre), une atteinte au système informatique (Finlande, Italie), l'introduction d'un virus (Slovénie) ou l'utilisation de programmes informatiques (Russie).

Tous les systèmes juridiques nationaux étudiés permettent donc de réprimer les atteintes portées à l'intégrité des données informatiques même si l'on constate certaines divergences entre les incriminations nationales. Conformément à la Proposition de Décision-Cadre du Conseil, doit être assurée aux données informatiques une protection analogue à celle dont jouissent les biens corporels, et doivent être protégés tant les particuliers que les entreprises et les organismes publics relativement à l'intégrité et au bon fonctionnement et usage des données.

L'association de cybercriminels — Mise à part la France qui incrimine l'association de « cybercriminels » constituée en vue de commettre des attaques aux systèmes informatiques, seuls deux pays incriminent par le biais du droit commun une telle association, et deux autres ainsi que la Proposition de Décision-Cadre l'érigent en circonstance aggravante [10].

Les attaques menées contre les systèmes informatiques étant l'objet de hackers constitués en groupements organisés, il serait souhaitable que l'association de cybercriminels soit érigée en circonstance aggravante dans les différents systèmes juridiques à l'instar de la Proposition de Décision-Cadre du Conseil.

B. — *Étude comparée des sanctions*

Les peines encourues relatives au hacking — Sept pays ainsi que la Proposition de Décision-cadre de l'Union Européenne prévoient des peines d'emprisonnement et/ou des peines d'amende pour cette infraction.

Concernant les peines d'emprisonnement, les minima vont de quinze jours à deux ans [11] ; les maxima vont d'un à cinq ans [12].

---

[8] France, Grèce, Italie, Pays-Bas, Pologne, Slovénie.

[9] Angleterre, Belgique, Espagne, Finlande.

[10] Belgique (art. 324 *ter* du Code pénal), Finlande (Circonstance aggravante), France (art. 323-4 du Code pénal), Italie (art. 270 *bis* et 416 du Code pénal), Pologne (art. 65 du Code pénal — circonstance aggravante), Proposition de Décision-Cadre du Conseil (art. 7).

[11] Italie (15 jours), Russie (2 ans).

[12] France (1 an), Grèce (5 ans).

Ces peines d'emprisonnement sont parfois encourues avec des peines d'amende [13], ou ne peuvent être encourues que des peines d'amende [14].

Concernant les peines d'amende, seule la France prévoit un maxima de 15 000 € ; les autres systèmes juridiques prévoient des fourchettes de peine qui s'étendent de 30 € à 250 000 € [15].

Il en ressort une grande diversité des peines encourues pour l'infraction de *hacking*. Si une peine d'emprisonnement est prévue par huit systèmes juridiques, une peine d'amende seule peut être prononcée dans cinq systèmes [16].

Les peines encourues relatives aux atteintes aux données informatiques — Tous les systèmes juridiques étudiés prévoient des peines d'emprisonnement et/ou des peines d'amende pour cette infraction.

Concernant les peines d'emprisonnement, les minima vont de trois mois à un an [17] ; les maxima vont de deux ans à cinq ans [18].

Ces peines d'emprisonnement sont encourues avec des peines d'amende dans quatre systèmes juridiques [19], ou ne sont encourues que des peines d'amende pour trois droits nationaux [20].

Concernant les peines d'amende, la France et les Pays-Bas prévoient un maxima de 45 000 € ; les autres systèmes juridiques prévoient des fourchettes de peine dont les minimas vont de 14,4 € à 130 € et les maxima de 7 212,24 € à 375 000 € [21].

Est soulignée ainsi, pour cette infraction, une grande diversité des peines encourues. Si une peine d'emprisonnement peut être prononcée dans tous les systèmes juridiques, une peine d'amende seule peut être prononcée dans quatre systèmes [22].

Les peines encourues relatives à l'association de cybercriminels — Les systèmes juridiques étudiés prévoient des peines d'emprisonnement : des minimas qui s'étendent de trois à quatre ans [23], une peine maximale encourue de sept ans en droit français, la Pologne précisant la possibilité pour le juge de prononcer une peine excédant de moitié celle maximum encourue. Il en ressort une nette aggravation des peines encourues.

Le problème du cumul des peines — Afin de comparer réellement les peines encourues aux peines prononcées et exécutées, il est nécessaire d'exposer les différentes réponses relatives au problème du cumul des peines.

---

[13] Belgique, France, Proposition de Décision-Cadre.
[14] Belgique, Grèce, Russie, Proposition de Décision-Cadre.
[15] Grèce (30 €), Belgique (250 000 €).
[16] Belgique, France, Grèce, Russie, Proposition de Décision-Cadre.
[17] Slovénie (3 mois), Espagne (1 an).
[18] Grèce (2 ans), Belgique (5 ans), Slovénie (5 ans).
[19] Belgique, Espagne, France, Pays-Bas.
[20] Pays-Bas, Pologne, Russie.
[21] Espagne (14,4 € — 7 212,24 €), Belgique (130 € — 375 000 €).
[22] France, Pays-Bas, Pologne, Russie.
[23] Italie (3 ans), Proposition de Décision-Cadre du Conseil (4 ans).

La majorité des systèmes juridiques étudiés prescrit le non-cumul des peines et prévoit que seule la peine la plus élevée sera encourue [24].

Concernant les systèmes juridiques qui prévoient le cumul des peines, certains le font toutefois avec réserve — le droit polonais prévoit le cumul dans la limite du minimum de la plus haute peine imposée et du maximum de la somme de toutes les peines — d'autre sans, comme le droit russe.

Les peines prononcées — Pour six systèmes juridiques [25], est pronostiqué que seules seront prononcées des peines d'emprisonnement : d'un emprisonnement conditionnel en Slovénie à cinq ans et huit mois d'emprisonnement en Italie.

Pour un seul système juridique — la Belgique — est précisé que sera prononcée avec la peine d'emprisonnement une peine d'amende, en l'occurrence de 5 000 €.

Les peines exécutées — Seuls l'Angleterre et la Belgique indiquent les peines qui seront probablement exécutées : trois ans selon le premier, six mois sous réserve des règles de libération anticipée et de la grâce pour le deuxième. Aux fins de comparaison, rappelons en Angleterre que la peine prononcée était évaluée à quatre ans et, en droit belge, la peine encourue est d'un à trois ans d'emprisonnement et/ou de 130 à 250 000 € d'amende, et la peine prononcée évaluée à deux ans et 5 000 € d'amende.

Force est de constater le manque d'informations concernant les peines effectivement exécutées, seuls deux systèmes juridiques les ayant précisées ! Cette carence empêche une analyse comparative approfondie des peines encourues, prononcées et exécutées, et interdit d'en tirer des conclusions qui aboutiraient à des recommandations erronées.

Il convient de relever toutefois, comme l'ont précisé certains rapports, notamment anglais, que le nombre de condamnations prononcées en la matière est très faible [26] : la mesure de cette criminalité est difficilement quantifiable et principalement à cause des réticences des entreprises à dénoncer le fait qu'elles ont été victimes de tels délits, de crainte de voir révélées certaines faiblesses de leur système d'information et que ne soit porté atteinte à leur crédibilité commerciale.

C. — *Étude comparée de la responsabilité pénale des personnes morales*

D'après les réponses au cas pratique, seules la France et la Proposition de Décision-cadre permettent de tenir une personne morale pour responsable pénalement des infractions étudiées commises pour leur compte. La

---

[24] Belgique, Italie, Slovénie, Grèce, France (non-cumul des peines de même nature ; cumul des peines de nature différente).

[25] Angleterre (4 ans), Belgique (2 ans), Finlande, Grèce (3,6 ans), Italie (5,8 ans), Slovénie (emprisonnement conditionnel).

[26] Par exemple, en France, 52 condamnations ont été prononcées en matière d'accès ou de maintien irrégulier dans un système informatique entre 1996 et 1998, alors que 1 151 enquêtes pénales ont été diligentées par la police judiciaire ces trois années (Source : Direction centrale de la police judiciaire, *Évolution de la criminalité informatique*, Document officiel du ministère de l'Intérieur).

situation dans laquelle des personnes morales sont impliquées dans des attaques contre des systèmes d'information n'est donc pas couverte par la majorité des systèmes juridiques étudiés. Or, les entreprises, notamment de commerce électronique, sur lesquelles reposent l'économie européenne, sont particulièrement visées par le *hacking*, l'espionnage industriel commis souvent pour le compte d'autres personnes morales. Elles doivent pouvoir diriger, exploiter et contrôler leur système d'information sans perturbation.

Étant donné que les réseaux de communication et d'information sont devenus un facteur clé du développement économique et sociétal, que la sécurité de ces réseaux est une nécessité pour la croissance du commerce électronique et le fonctionnement de toute l'économie, que la société de l'information sur laquelle repose l'économie actuelle doit être préservée, il est souhaitable que les différents systèmes juridiques instaurent un mécanisme permettant d'engager la responsabilité pénale des personnes morales lorsque ces infractions sont commises pour leur compte et des sanctions appropriées.

II. LA RÉPRESSION DE LA CYBERCRIMINALITÉ A L'ÉTRANGER : SON INCIDENCE SUR LES DROITS NATIONAUX

Il ressort des réponses au cas pratique que la très grande majorité des systèmes juridiques n'accorde officiellement aucune valeur positive aux jugements étrangers : en l'occurrence, dans le cadre de la récidive, la condamnation précédente à l'étranger n'a aucune incidence sur la peine encourue qui n'est donc pas aggravée.

Seul le droit italien semble faire figure d'exception [27]. Toutefois, la plupart des droits nationaux examinés prennent indirectement en compte les condamnations étrangères, au stade du prononcé de la peine, par le biais du pouvoir d'individualisation de la peine par le juge. Il existe cependant une limite pratique à cette possibilité : la connaissance préalable par le juge national de la condamnation antérieure à l'étranger.

Il convient donc sur ce point d'appuyer la recommandation générale sur la valeur des décisions judiciaires portant une condamnation pénale incitant à la mise en place d'un système permettant la connaissance des décisions judiciaires portant une sanction privative de liberté.

En matière de cybercriminalité, les réponses au cas pratique ont révélé d'importantes disparités entre les différents systèmes juridiques étudiés. Le droit pénal de ces États comporte certains vides juridiques et des différences importantes susceptibles d'entraver la lutte contre ce phénomène criminel, notamment la coopération policière et judiciaire.

Le rapprochement des droits pénaux de fond en la matière garantirait que les législations nationales soient suffisamment complètes afin que les attaques contre les systèmes d'information puissent faire l'objet d'enquêtes et ne constituent plus une menace pour la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice.

---

[27] Art. 12 n° 1 du Code pénal.