La responsabilité pénale en cas de cyberattaques : une approche comparée des droits belge et international

Auteur : Demoulin, Laura
Promoteur(s) : Franssen, Vanessa
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit, à finalité spécialisée en droit privé
Année académique : 2024-2025
URI/URL : http://hdl.handle.net/2268.2/23643

LIÈGE université
Droit, Science Politique
& Criminologie

Département de Droit

La responsabilité pénale en cas de cyberattaques : une approche comparée des droits belge et international

Laura DEMOULIN

Travail de fin d'études

Master en droit à finalité spécialisée en droit privé

Année académique 2024-2025

Recherche menée sous la direction de :

Madame Sofie ROYER

Professeure invitée

RESUME

Dans une société digitalisée qui est la nôtre, il est important de connaître, tant sur le plan national que sur les plans européen et international, les enjeux que pose la responsabilité pénale en cas de cyberattaques dirigées contre des personnes, physiques ou morales, et des États. Dans cette perspective, les cyberattaques vont être étudiées de manière à déterminer les contours de ce concept complexe et les effets qui s'y rapportent.

D'une part, dans une perspective répressive, certains instruments juridiques consacrés par le droit international, le droit de l'Union européenne et le droit pénal belge vont être comparés afin de déceler si le droit de l'Union européenne et le droit national répondent bel et bien aux exigences établies par le droit international. D'autre part, nous étudierons les mécanismes mis en place pour prévenir ce cyberphénomène.

Enfin, la question des conséquences sur nos droits fondamentaux va être posée. L'exposé traitera ainsi du droit à la vie privée, de la protection des données personnelles et de la liberté d'expression.

REMERCIEMENTS

En premier lieu, mes remerciements les plus sincères vont à Madame Royer. Sa disponibilité, ses conseils et son accompagnement m'ont été précieux dans la réalisation de ce travail de fin d'études.

Je remercie également mes proches ainsi que ma famille pour le soutien apporté tout au long de mes études. L'aventure n'aurait pas été la même sans vous à mes côtés.

Enfin, il me tient à cœur de mettre à l'honneur ma mère et ma grand-mère, qui n'ont jamais cessé de croire en moi.

TABLE DES MATIERES

Introduction

L'ère du numérique appelle à la prudence et à la vigilance. Dans une société du XXIe siècle où la digitalisation et la numérisation sont en pleine explosion, les criminels se voient contraints d'innover au vu des nouvelles opportunités émergeantes face à eux. Par l'évolution d'internet et par l'essor des nouvelles technologies de l'information et de la communication (TIC), de nouvelles portes s'ouvrent pour ces personnes désireuses de commettre l'impensable. En effet, rapidement, de nouveaux phénomènes répréhensibles ont vu le jour et un besoin de légiférer et de trouver des solutions juridiques s'est vite fait ressentir, tant sur le plan national que sur les plans européen et international[1].

Par la formule *infraction pénale commise par le biais d'internet*, nous entendons, plus largement, le concept de *cybercriminalité*. La cybercriminalité vise le plus souvent « *les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement internet* »[2]. Notons d'ores et déjà que cette notion recouvre notamment les *cyberattaques*, faisant l'objet du présent travail d'analyse.

Compte tenu de l'ampleur actuelle de la cybercriminalité et de la sophistication accrue des cyberattaques, le droit se trouve être confronté à des défis majeurs. Le renforcement de la cybersécurité est dès lors essentiel pour préserver la paix dans le cyberespace[3]. Pour cette raison, nous allons tenter de répondre à la question suivante, celle-ci reprenant divers axes d'analyse : « *Le droit apporte-t-il une réponse adéquate face aux conséquences croissantes des cyberattaques, en assurant une réponse nationale et européenne conforme aux prescrits internationaux, en encadrant la responsabilité des acteurs concernés, en privilégiant la prévention, tout en protégeant les droits fondamentaux ?* ».

Comme nous le verrons dans la première partie de cette étude, le concept de cyberattaque, du fait de sa nature hybride, est complexe à définir. Néanmoins, nous nous efforcerons de répondre à la première sous-question suivante : « Quels sont les impacts, voire les conséquences, des cyberattaques d'un point de vue économique et social ? ».

On ne peut ignorer que les cyberattaques peuvent viser des entreprises, des personnes physiques et des États du monde entier. Il était donc évident qu'un cadre juridique devait être établi à une échelle ne se limitant pas au niveau national, afin de permettre une coopération entre les États touchés par ces attaques. Un parallèle va donc pouvoir être établi entre, d'une part, le cadre légal établi au niveau international, notamment avec la Convention sur la cybercriminalité, dite la Convention de Budapest, mais aussi avec les différents règlements et directives mis en place par l'Union européenne et, d'autre part, le cadre légal établi en droit

---

[1] M. WATIN-AUGOUARD, « Préface », O. de MAISON ROUGE, *Les cyberisques. La gestion juridique des risques à l'ère immatérielle*, Paris, LexisNexis, 2018, p. XXV.

[2] F. DECHAMPS et C. LAMBILOT, « Partie I : Concepts et législation – Titre I : phénomène de la cybercriminalité », *Cybercriminalité : état des lieux*, F. Dechamps, O. Bogaert et C. Lambilot (dir.), Bruxelles, Anthemis, 2016, p. 21.

[3] M. WATIN-AUGOUARD, « La sécurité privée et la cyberdélinquance internationale », *Les aspects internationaux de la sécurité privée*, C. Aubertin et X. Latour (dir.), mare & martin, 2016, p. 160 ; M. WAUTELET, *Les cyberconflits. Internet, autoroutes de l'information et cyberespace : quelles menaces ?*, Bruxelles, GRIP, 1998, p. 5 à 15.

belge par le biais de l'adoption de diverses lois et par certaines dispositions consacrées par le Code pénal belge. Par conséquent, une des sous-questions centrales qui va être abordée et résolue, sous le spectre de l'approche comparative, est la suivante : « Le droit belge et le droit de l'Union européenne répondent-ils suffisamment aux exigences posées par la Convention de Budapest ? ».

Une sous-question de recherche complémentaire, mais tout aussi fondamentale, concernant la responsabilité pénale, va être posée. Cette question s'articule ainsi : « La responsabilité pénale des États et des entreprises peut-elle être engagée dans le cas où ces acteurs se rendraient coupables d'une cyberattaque ? ». La question de la responsabilité pénale relève, en effet, d'une importance capitale en droit pénal, et ce afin d'imputer les comportements répréhensibles à son auteur et de lui infliger les sanctions pénales susceptibles de s'appliquer au vu des faits établis. Dans ce contexte, nous décrirons ce phénomène.

Concernant la prévention en cette matière, il semble tout aussi important de répondre à l'interrogation suivante : « Quels sont les mécanismes mis en œuvre, dans le domaine de la cybersécurité, pour lutter contre les cyberattaques ? Ceux-ci sont-ils efficaces ? ».

En dernier lieu, la question « Les droits fondamentaux des citoyens sont-ils protégés en cas de cyberattaque ? » va être posée afin de décrire et d'évaluer les effets néfastes que peuvent avoir ces infractions pénales sur les droits fondamentaux des individus.

Une approche comparative est jugée pertinente dans le cadre de cette analyse pour favoriser la mise en perspective des différents systèmes juridiques, qu'il s'agisse du droit international, du droit de l'Union européenne ou du droit national. Une approche descriptive semble également considérablement judicieuse en ce qu'il apparaît opportun de décrire le phénomène des cyberattaques, les conséquences et les effets qui en découlent, le cadre légal instauré à différentes échelles, le phénomène de responsabilité pénale au regard de la cybercriminalité, les actes préventifs ainsi que le niveau d'atteinte aux droits fondamentaux.

La réflexion s'articulera autour de plusieurs parties complémentaires.

Dans un premier temps, le concept de cyberattaque va être défini et une catégorisation des différents types de cyberattaques sera effectuée. Les conséquences de ces dernières seront également étudiées pour une meilleure compréhension du phénomène.

Dans un second temps, le cadre légal répressif va être étudié. Les instruments juridiques adoptés par le droit international et par le droit de l'Union européenne vont être discutés. Ensuite, les différents crimes informatiques, considérés comme des cyberattaques, vont être mis à la lumière du Code pénal belge.

Dans un troisième temps, l'examen portera sur les personnes morales et sur l'État. D'une part, nous aborderons la responsabilité pénale d'une personne morale en cas de cyberattaque. D'autre part, la responsabilité internationale de l'État, en cas de cyberattaque, sera étudiée.

Dans un quatrième temps, nous explorerons, dans une vision préventive, les différents mécanismes prévus pour lutter contre la cybercriminalité. En effet, la cybersécurité a un grand rôle à jouer dans cette lutte acharnée contre la cybercriminalité.

En dernier lieu, des questions sur le droit à la vie privée, plus précisément sur la protection des données personnelles, et sur la liberté d'expression seront posées. En effet, dans le cas

où une cyberattaque se produit, il arrive que des données soient volées, ce qui peut constituer une violation du droit à la vie privée.

Enfin, une conclusion critique, ayant pour objectif de synthétiser la réponse à ces questions, achèvera l'analyse.

Titre 1. Les cyberattaques

Comme annoncé, cette première partie s'attèlera à poser les contours du concept complexe de *cyberattaque*. Certaines de ces attaques feront l'objet d'un approfondissement et les possibles conséquences seront mises en évidence. Cela paraît essentiel de commencer par ces considérations afin de pouvoir, ensuite, envisager la responsabilité pénale qui peut en découler.

Chapitre 1. Notion de cyberattaque

À l'heure actuelle, la cyberattaque, aussi appelée *attaque informatique*, représente une nouvelle menace, à une échelle internationale, pour les différents gouvernements et entreprises. En effet, ces derniers, détenant des informations sensibles, craignent pour la sécurité de leurs données et redoutent amèrement un dysfonctionnement de leurs divers systèmes informatiques[4].

Force est de constater que, malencontreusement, la Belgique est un pays considéré comme nettement plus à risque et hautement vulnérable face à ces potentielles cyberattaques car celui-ci est réputé comme considérablement dépendant des technologies de l'information et de la communication (TIC). Les nouvelles technologies sont omniprésentes dans notre société, aussi bien dans le secteur public que privé et contribuent notablement à la productivité du pays, ce qui n'est pas pour nous déplaire. Néanmoins, il est relativement important de garder à l'esprit les nombreux dangers et risques existants depuis le développement croissant de ces technologies[5].

Pour une meilleure compréhension de la notion de *cyberattaque*, une distinction fondamentale est à prendre en considération afin de délimiter les enjeux juridiques de ce concept. En effet, la cyberattaque, présentant une nature hybride, doit être différenciée selon qu'elle se produit dans le cadre d'une cyberguerre ou selon qu'elle ait lieu dans un contexte de cybercriminalité[6]. Ce présent travail se contentera d'étudier la cyberattaque en tant que cybercrime.

D'une part, précisons brièvement, tout d'abord, dans quelles circonstances intervient une cyberattaque s'inscrivant dans le cadre d'une cyberguerre. En temps de conflit armé ou en temps de paix, certains actes dommageables peuvent être entrepris par un État dans un but d'attenter aux systèmes informatiques d'un autre État[7]. Par ailleurs, dans ce sens, le Département de la défense américain a défini la cyberattaque comme suit : « *un acte hostile qui utilise les ordinateurs ou les réseaux d'ordinateurs ou systèmes informatisés, et qui vise à*

---

[4] M. BENATAR et M. FONTAINE, « Cyber-attaques : aperçu du cadre juridique national », *Questions juridiques d'actualité en lien avec la défense / Actuele juridische vraagstukken met betrekking tot defensie*, N. Angelet *et al*. (dir.), Bruxelles, die Keure / la Charte, 2017, p. 311.

[5] M. BENATAR et M. FONTAINE, *ibidem*, p. 311.

[6] M. BENATAR et M. FONTAINE, *ibidem*, p. 319 ; M. GRANGE et A-T. NORODOM (dir.), *Cyberattaques et droit international. Problèmes choisis.*, Paris, A. Pedone, 2018, p. 18.

[7] M. BENATAR et M. FONTAINE, *ibidem*, p. 319 ; M. BENATAR, "The use of Cyber force : Need for Legal Justification ?", *Goettingen Journal of International Law I*, 2009, 3, p. 379.

altérer et/ou détruire les systèmes critiques cybernétiques de l'adversaire, sa valeur ou ses fonctions »[8].

D'autre part, il est ensuite nettement intéressant d'étudier plus en détail le cas où la cyberattaque serait issue de la cybercriminalité et serait donc considérée comme un cybercrime. La cyberattaque, envisagée comme relevant de la cybercriminalité, constitue un comportement privé appréhendé et criminalisé dans des législations nationales et dans des instruments internationaux[9].

À cet égard, il semble à présent pertinent de déterminer les contours du concept de cybercriminalité. La cybercriminalité, plus communément appelée « *criminalité du XXIe siècle* », reflète une partie considérable du contentieux pénal belge et international[10] et se voit attribuer différentes définitions de par son évolution constante. Par exemple, Jean-Luc Putz a tenté de définir cette notion de manière à ce que soient couvertes « *tant les infractions commises contre les installations informatiques que celles commises au moyen des nouvelles technologies de l'information* »[11]. Myriam Quemener a, quant à elle, dans sa propre définition, ajouté que la *tentative,* de commettre des infractions pénales, au moyen ou contre un système d'information et de communication, était aussi sanctionnée[12].

Nous pouvons, de plus, préciser que certains auteurs s'accordent à dire que la cybercriminalité « *intègre toute forme de malveillance électronique effectuée à l'aide des technologies informatiques et de télécommunication (téléphone, cartes à puces…). Qu'il s'agisse de fraude, d'escroquerie, d'extorsion, de vandalisme ou de harcèlement par exemple, les comportements malveillants ou criminels exploitent les caractéristiques d'Internet et portent préjudice aux internautes, aux organisations et à la société* »[13].

En réalité, aucune organisation internationale ou européenne n'a pris soin de définir la cybercriminalité de manière complète, précise et uniforme au vu des difficultés prévisibles qui pouvaient se présenter. À titre d'illustration, les lois belges, du 28 novembre 2000 relative à la criminalité informatique et du 3 aout 2012 portant assentiment à la Convention de Budapest, « *ne la définissent pas de manière précise et se contentent de se référer brièvement à la convention sur la cybercriminalité, ou de la citer* »[14]. D'ailleurs, une étude menée, dans le cadre de la résolution 65/230, par un groupe intergouvernemental d'experts de l'Assemblée générale des Nations Unies, a mis en lumière le fait que définir la cybercriminalité ne présente pas une grande utilité en fonction du contexte auquel elle se rattache[15].

---

[8] L.-E. PANETTA, « Section 2 : L'avènement des cyberattaques », *Cyberattaques et droit international public : de la négociation entre Etats à l'intégration des acteurs privés pour parvenir à la cyberpaix ?*, L. Baudin (dir.), Paris, L'Harmattan, 2023, p. 60 ; D. VENTRE, Cyberattaque et cyberdéfense, Collection Cyberconflits et cybercriminalité, Paris, Hermès science publications : Lavoisier, 2011, p. 34.

[9] M. BENATAR et M. FONTAINE, *op. cit*., p. 319.

[10] M. WATIN-AUGOUARD, « La sécurité privée et la cyberdélinquance internationale », *op. cit.*, p. 160.

[11] J.-L. PUTZ, « Introduction », *Cybercriminalité*, 1e éd., Windhof, Larcier Luxembourg, 2019, p. 14.

[12] J.-L. PUTZ, *ibidem,* p. 14 ; M. QUEMENER, *Le droit face à la disruption numérique*, Gualino, 2018, n° 195.

[13] P. CLOUNER, « Chapitre 7. Approche du Centre pour la Cybersécurité Belgique en matière de protection des personnes (vulnérables) dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, H. Jacquemin et M. Nihoul (dir.), Bruxelles, Larcier, 2018, p. 208.

[14] F. DECHAMPS ET C. LAMBILOT, *op. cit.*, p. 21.

[15] F. DECHAMPS ET C. LAMBILOT, *op. cit.*, p. 22.

Nous arrivons finalement à la conclusion suivante : une adaptation réelle et efficace du droit international est nécessaire afin de répondre aux problématiques posées par la cybercriminalité et par la cyberguerre[16].

Chapitre 2. Catégorisation des cyberattaques

Les cyberattaques ont la particularité de prendre les formes les plus diverses. Afin de délimiter l'exposé, focalisons-nous sur les deux formes suivantes que peuvent prendre les cyberattaques, à savoir le phishing et le malware.

a. Phishing (hameçonnage)

Le phishing est considéré comme une technique d'ingénierie sociale. Par *ingénierie sociale*, nous entendons plus précisément le fait pour un délinquant d'abuser de la confiance et de l'ignorance de certaines personnes afin d'obtenir de celles-ci des données et informations cruciales. Ces techniques d'ingénierie sociale visent donc à exploiter « *l'aspect humain et social de la structure à laquelle est lié le système informatique visé* »[17]. Les lieux publics, tels que les transports en commun, les restaurants et les hôtels en sont souvent la cible première du fait de leur grande exposition aux publics les plus divers. Par ailleurs, les délinquants parviennent à leurs fins en exploitant les failles humaines, qu'il s'agisse de l'inexpérience des utilisateurs des systèmes informatiques, de la compassion ressentie par ces derniers due à une certaine manipulation ou encore de la pression psychologique endurée[18].

Le phishing, en tant que tel, est un grand vecteur de la cybercriminalité et est très souvent utilisé comme cyberattaque de première ligne[19]. Il semblerait que le pays le plus touché soit les États-Unis, suivi de la Russie[20].

Nous pouvons définir le phishing comme étant « *une technique qui consiste à envoyer un mail semblant provenir par exemple d'un site d'établissements financiers, pour inciter l'internaute à fournir les codes d'accès et mots de passe, prétextant un renforcement des contrôles de sécurité* ». Le destinataire reçoit un mail paraissant légitime, mais qui, en réalité, vise à conduire ce dernier « *vers des sites Web imitant à s'y méprendre des sites légitimes* »[21]. En effet, la personne ciblée par la mail de phishing, autrement dit la *victime*, peut également être amenée à télécharger une pièce jointe contenant un logiciel malveillant, ou encore à cliquer sur un lien qui la conduira vers un site Web frauduleux, conçu pour compromettre ses données personnelles et/ou infecter son dispositif informatique. En général, l'unique but recherché est la soustraction d'argent[22].

---

[16] A.-T NORODOM, "Avant-propos", *Internet et le droit international*, Paris, A. Pedone, 2014, p. 7.

[17] M. QUEMENER, « Chapitre 2. Analyse des cyberfraudes », *Établissements financiers & cyberfraudes*, Paris, Revue Banque Édition, 2011, p. 38.

[18] M. QUEMENER, *ibidem*, p. 39.

[19] P. CLOUNER, « Chapitre 7. Approche du Centre pour la Cybersécurité Belgique en matière de protection des personnes (vulnérables) dans l'environnement numérique », *op. cit*., p. 215 ;

[20] M. QUEMENER, « Chapitre 2. Analyse des cyberfraudes », *op. cit*., p. 40.

[21] M. QUEMENER, « Chapitre 2. Analyse des cyberfraudes », *op. cit*., p. 39.

[22] P. CLOUNER, *op. cit.*, p. 215 ; SPF ECONOMIE, « Phishing : ne mordez pas à l'hameçon », disponible sur https://news.economie.fgov.be/248457-phishing-ne-mordez-pas-a-l-hamecon, 1 avril 2025 ;

Il n'existe pas de cible parfaite au phishing. Malheureusement, toute personne, peu importe son état physique ou mental, son âge, son milieu, peut en être victime[23]. La négligence de la victime sera appréciée par les juridictions compétentes afin de déceler sa part de responsabilité[24]. Pour l'année 2024, le SPF Économie a enregistré près de 2.300 signalements quant à des tentatives de phishing, avec un préjudice financier dépassant les 5.6 millions d'euros[25]. Toutefois, ces données semblent bien en dessous de la réalité car, en 2022, le service d'information du Centre pour la Cybersécurité de Belgique avait déjà recensé 5.973.239 courriels de signalement quant à des faits de phishing. Le Centre pour la Cybersécurité de Belgique avait d'ailleurs relaté que 39.8 millions d'euros avaient été dérobés en 2022 en Belgique suite aux attaques de phishing[26].

Afin d'y voir plus clair, précisons tout de même que, d'une part, généralement, les délinquants utilisent des URL ressemblant étrangement à des URL de sociétés déjà existantes, et ce dans un but de tromper les utilisateurs. D'autre part, il existe des délinquants qui choisissent d'exploiter une simple adresse IP, ne prenant même pas la peine de créer un URL semblable à celui d'une société déjà existante. La longévité d'un site internet frauduleux de ce type est très limitée car celui-ci est, fort heureusement, rapidement détecté par les autorités compétentes[27].

Notons également qu'il existe des variantes au phishing, chacune exploitant des moyens de communication différents pour tromper les victimes. Le *smishing*, par exemple, fait appel aux SMS, en lieu et place de l'e-mail, pour rediriger la victime vers des sites frauduleux ou récupérer des données personnelles et sensibles. Le *vishing*, quant à lui, utilise la voix, par le biais d'appels téléphoniques, pour inciter la personne ciblée à « *saisir des données personnelles sur de faux sites web* ». Le *quishing* est une forme plus récente où des QR codes sont exploités à des fins frauduleuses. Par le scan de QR codes, les victimes sont redirigées vers des sites de phishing ou invitées à procéder à un paiement. Il est par ailleurs possible que des logiciels malveillants soient installés sur les appareils de la victime par ce processus illégal. Enfin, le *spoofing* consiste à usurper une adresse e-mail déjà existante, de manière à ce que le courriel semble émaner de l'expéditeur légitime[28].

ENISA, « ENISA THREAT LANDSCAPE 2024 », disponible sur https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf, septembre 2024.

[23] P. CLOUNER, *op. cit.*, p. 215.

[24] Trib. entr., Bruxelles (néerl.), 29 juin 2023, *R.G.D.C.*, 2024, liv. 9, p. 516 ; Civ. Bruxelles (fr.) (11e ch.), 18 février 2025, *J.T.*, 2025, liv. 7018, p. 218.

[25] SPF ECONOMIE, « Phishing : ne mordez pas à l'hameçon », disponible sur https://news.economie.fgov.be/248457-phishing-ne-mordez-pas-a-l-hamecon, 1 avril 2025.

[26] WALLONIE-BRUXELLES INTERNATIONAL, « Le phishing, principale porte d'entrée des cybercriminels », disponible sur https://www.wbi.be/fr/actualites/phishing-principale-porte-dentree-cybercriminels, 7 novembre 2023.

[27] M. QUEMENER, « Chapitre 2. Analyse des cyberfraudes », *op. cit.*, p. 40.

[28] SPF ECONOMIE, « Phishing : ne mordez pas à l'hameçon », disponible sur https://news.economie.fgov.be/248457-phishing-ne-mordez-pas-a-l-hamecon, 1 avril 2025.

b. Malware

Le malware, dénommé *logiciel malveillant* ou *virus,* tire son nom de la fusion des mots « *malicious* » et « *software* » et a, pour objectif majeur, l'obtention de données personnelles confidentielles. Il constitue une forme de cyberattaque en ce qu'il est conçu délibérément pour compromettre la confidentialité, l'intégrité ou la disponibilité d'un système informatique, que ce soit un ordinateur, un serveur, un smartphone ou une tablette. « *Lorsqu'un appareil est infecté par un logiciel malveillant, vous pouvez être confronté à un accès non autorisé, à des données compromises ou à un verrouillage de cet appareil, à moins de payer une rançon* »[29]. Le malware peut lui-même revêtir diverses formes, dont l'étude de certaines suivra dans les prochaines lignes.

1. Les chevaux de Troie

Le cheval de Troie est un malware qui, d'apparence, paraît légitime. En effet, l'utilisateur, sans aucune once de méfiance, télécharge des fichiers paraissant légitimes, alors que ceux-ci constituent des chevaux de Troie. Ceux-ci sont très néfastes en ce qu'ils peuvent causer divers désagréments[30]. Lorsque des chevaux de Troie sont téléchargés, ils peuvent : « *télécharger et installer des logiciels malveillants supplémentaires, tels que des virus ou des vers, utiliser l'appareil infecté dans le cadre d'une escroquerie de type fraude au clic, enregistrer les frappes et les sites web que vous visitez, envoyer des informations (mots de passe, détails de connexion et historique de navigation, par exemple) sur l'appareil infecté à un pirate malveillant* », et encore céder le contrôle de l'ordinateur infecté à un pirate[31].

Afin de mieux appréhender ce logiciel malveillant, citons deux types de chevaux de Troie. Il existe, par exemple, le programme malveillant *Qbot*. Celui-ci vise au vol de données financières et est bien connu dans le domaine bancaire depuis 2007. De plus, le programme malveillant *TrickBot* a été identifié en 2016. Ce dernier a également été créé pour subtiliser des données bancaires, mais « *est devenu un programme malveillant modulaire et multiétape*

---

[29] X, « Quels sont les différents types de programmes malveillants ? » disponible sur https://www.kaspersky.fr/resource-center/threats/types-of-malware, *s. d.*, consulté le 8 mars 2025 ; MICROSOFT, « Qu'est-ce qu'un logiciel malveillant ? » disponible sur https://www.microsoft.com/fr-be/security/business/security-101/what-is-malware, *s. d.*, consulté le 8 mars 2025 ; X, « Malware ou logiciel malveillant : définition et solutions de protection » disponible sur https://www.cyber-cover.fr/guides/assurance-cyber-risques/les-types-de-cyber-risques-5-exemples-dattaques-malveillantes/malware-ou-logiciel-malveillant-definition-et-solutions-de-protection, *s. d.*, consulté le 8 mars 2025 ; P. CLOUNER, *op. cit*., p. 213.

[30] X, « Quels sont les différents types de programmes malveillants ? » disponible sur https://www.kaspersky.fr/resource-center/threats/types-of-malware, *s. d.*, consulté le 8 mars ; X, « Malware ou logiciel malveillant : définition et solutions de protection » disponible sur https://www.cyber-cover.fr/guides/assurance-cyber-risques/les-types-de-cyber-risques-5-exemples-dattaques-malveillantes/malware-ou-logiciel-malveillant-definition-et-solutions-de-protection, *s. d.*, consulté le 8 mars 2025.

[31] MICROSOFT, « Qu'est-ce qu'un logiciel malveillant ? » disponible sur https://www.microsoft.com/fr-be/security/business/security-101/what-is-malware, *s. d.*, consulté le 8 mars 2025 ; M. QUEMENER, « Chapitre 2. Analyse des cyberfraudes », *op. cit*., p. 35.

qui fournit à ses opérateurs une suite complète d'outils pour mener à bien de nombreuses cyberactivités illégales »[32].

2. Les keyloggers

Un keylogger est un enregistreur de frappe, c'est-à-dire « *un logiciel espion qui enregistre les touches frappées sur le clavier d'un ordinateur sous certaines conditions et les transmet par le réseau internet* »[33]. Une fois de plus, ce logiciel malveillant est exploité dans un but d'obtention d'informations confidentielles, qu'elles soient bancaires ou non. « *Certains peuvent enregistrer les URL visitées, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur* »[34].

3. Les vers

Le ver informatique se reproduit et se propage de manière autonome dans le système informatique[35]. Ainsi, il est en mesure d'infecter rapidement tous les serveurs et ordinateurs vulnérables présents sur le réseau. Ses inconvénients sont multiples : espionnage de l'ordinateur infecté et ralentissement de ce dernier, facilité offerte aux pirates pour s'introduire dans l'ordinateur concerné, destruction de données stockées, plantage du système informatique et bien d'autres[36].

4. Le ransomware

Le ransomware, communément appelé en français *rançongiciel*, est une attaque qui vise un grand nombre d'organisations dans le monde. Depuis le commencement de la guerre en Ukraine, nous remarquons que les institutions et municipalités belges sont de plus en plus impactées par des attaques de ce type. Les secteurs de l'industrie, des soins de santé, de l'éducation, du droit, de la finance et des banques sont considérés comme davantage à risque[37].

Plus concrètement, les ransomwares sont des programmes malveillants qui consistent à extorquer une victime en bloquant ou en supprimant l'accès à des données, applications et outils lui appartenant, tant qu'une rançon n'a pas été versée[38]. À titre d'illustration, nous

---

[32] X, « Quels sont les différents types de programmes malveillants ? » disponible sur https://www.kaspersky.fr/resource-center/threats/types-of-malware, *s. d*., consulté le 8 mars 2025.

[33] M. QUEMENER, « Chapitre 2. Analyse des cyberfraudes », *op. cit*., p. 36 et 37.

[34] M. QUEMENER, « Chapitre 2. Analyse des cyberfraudes », *op. cit*., p. 37.

[35] G. VAN DAELE, « Cyberrisques : un fléau jamais bien loin », *Assur. présent*, liv. 3, Kluwer, 2023, p. 9.

[36] M. QUEMENER, « Chapitre 2. Analyse des cyberfraudes », *op. cit*., p. 37 ; X, « Quels sont les différents types de programmes malveillants ? » disponible sur https://www.kaspersky.fr/resource-center/threats/types-of-malware, *s. d*., consulté le 8 mars 2025 ; MICROSOFT, « Qu'est-ce qu'un logiciel malveillant ? » disponible sur https://www.microsoft.com/fr-be/security/business/security-101/what-is-malware, *s. d*., consulté le 8 mars 2025 ; X, « Malware ou logiciel malveillant : définition et solutions de protection » disponible sur https://www.cyber-cover.fr/guides/assurance-cyber-risques/les-types-de-cyber-risques-5-exemples-dattaques-malveillantes/malware-ou-logiciel-malveillant-definition-et-solutions-de-protection, *s. d*., consulté le 8 mars 2025.

[37] CENTRE FOR CYBERSECURITY BELGIUM, « Miser sur la cybersécurité. Rapport CCB 1/1/2023 – 30/9/2023 » disponible sur https://ccb.belgium.be/sites/default/files/2024-10/CCB%20REPORT%202023_FR.pdf, *s. d*., consulté le 9 mars 2025.

[38] MICROSOFT, « Qu'est-ce qu'un logiciel malveillant ? » disponible sur https://www.microsoft.com/fr-be/security/business/security-101/what-is-malware, *s. d*., consulté le 8 mars 2025 ; O. de MAISON

pouvons citer deux types de ransomware, le *ransomware Locker* et le *ransomware Crypto*. D'une part, le premier empêche l'utilisateur d'utiliser des options de base de son ordinateur. D'autre part, le second a pour unique but le chiffrement de données sensibles sans avoir égard aux simples fonctionnalités de l'ordinateur[39].

Un exemple significatif est celui de l'individu qui reçoit un courriel avec des pièces jointes de la part de l'escroc. L'ouverture des pièces jointes par la victime entrainera aussitôt le téléchargement et l'installation du ransomware. Ainsi, le logiciel malveillant va pouvoir crypter l'ensemble des fichiers présents sur le disque dur de l'ordinateur de la victime. C'est ensuite que la victime recevra un message lui imposant une rançon dans un temps imparti, faute de quoi l'accès à son ordinateur restera bloqué. Il va de soi que les escrocs ont la possibilité d'augmenter le prix et/ou de supprimer certaines parties des fichiers à mesure que le temps passe. Il importe tout de même de garder à l'esprit que le paiement de la rançon n'assure pas le déblocage de l'ordinateur et desdits fichiers. De plus, rien ne garantit formellement que le virus a bien été évincé de l'appareil[40].

Chapitre 3. Conséquences potentielles des cyberattaques

Plusieurs effets sont perceptibles lorsqu'une cyberattaque est intentée. Comme nous le savons, le vol, l'extorsion, la manipulation physique, la perte de données, les vols d'identité, la paralysation des systèmes informatiques et bien d'autres conséquences peuvent voir le jour[41].

De plus, et bien malheureusement, des interruptions d'activité professionnelle peuvent avoir lieu lorsque la cyberattaque y est liée. De ce fait, des conséquences économiques lourdes sont à prévoir en raison des pertes financières causées. En effet, à titre d'exemple, une entreprise victime d'une telle attaque verrait très probablement son chiffre d'affaires chuter de manière significative et manquerait certainement des opportunités commerciales sérieuses. De plus, l'entreprise victime supporterait de nombreux coûts en raison de la remise à jour de ses systèmes informatiques affectés. En sus, il est important de souligner que les clients de l'activité en question seront en mesure de réclamer des dommages et intérêts du fait du préjudice subi. La réputation se détériorera en ce même sens et la mauvaise publicité se laissera percevoir. La confiance ne tiendra plus qu'à un fil, de sorte que les partenariats se

---

ROUGE, « Introduction. De la cyberdélinquance à la cyberguerre », *Les cyberrisques. La gestion juridique des risques à l'ère immatérielle*, 2e éd., Paris, LexisNexis, 2024, p. 7 ; J. TRULLEMANS, « Phénomène des ransomware », *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, C 380, p. 542.

[39] P. CLOUNER, *op. cit.*, p. 217.

[40] SPF ECONOMIE, « Votre ordinateur est bloqué et vous devez payer une rançon pour le débloquer (ransomware) » disponible sur https://economie.fgov.be/fr/themes/protection-des-consommateurs/stop-arnaques/formes-darnaques/vous-avez-recu-un-message/votre-ordinateur-est-bloque-et, *s. d.*, consulté le 9 mars 2025.

[41] P. CLOUNER, *op. cit.*, p. 220 ; X, « Conséquences d'une cyberattaque » disponible sur https://www.cyberimpact.eu/consequences-dune-cyberattaque, *s. d.*, consulté le 9 mars 2025 ; X, « Quelles sont les conséquences d'une cyberattaque sur une entreprise ? » disponible sur https://www.cnfce.com/dossier/consequences-cyberattaque-entreprise-interview-expert-cybercriminalite, 4 octobre 2022.

feront rares. Enfin, des sanctions peuvent être endossées lorsqu'il y a une quelconque violation de la protection des données et de la vie privée. En ce même sens, lorsque l'entreprise victime est reconnue responsable, celle-ci devra également essuyer des dépenses supplémentaires[42].

Titre 2. Répression

La présente seconde partie de ce travail se consacrera à l'étude du dispositif répressif encadrant les cyberattaques lorsqu'elles s'inscrivent dans un contexte de cybercriminalité. En effet, le cadre légal offert par le droit international va être analysé, ainsi que ceux prévus par le droit de l'Union européenne et le droit belge.

Comme annoncé en amont dans la table des matières et dans l'introduction, la prévention fera l'objet d'une quatrième partie. Il est alors légitime de s'interroger sur les raisons pour lesquelles le régime répressif est analysé préalablement au régime préventif. En effet, il apparaît évident que la prévention précède la répression. Cependant, analyser la répression au préalable permet d'établir les infractions existantes et le droit en vigueur de manière à percevoir ensuite le rôle que doit jouer la prévention dans un tel contexte.

Chapitre 1. Droit international

Les deux législations qui vont être abordées sous ce chapitre présentent une politique aussi bien répressive que préventive. Néanmoins, nous pouvons estimer qu'elles s'inscrivent davantage dans une logique répressive.

1. La Convention de Budapest, réponse du Conseil de l'Europe face à la cybercriminalité

La Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001 constitue « *le premier instrument de droit international conventionnel contraignant spécifiquement élaboré pour lutter contre la criminalité informatique* »[43]. Cette convention a été ratifiée par 78 États, comprenant aussi bien des États membres du Conseil de l'Europe que des États non membres[44]. En effet, sur la base de l'article 36 de ladite Convention, les États qui ne sont pas membres du Conseil de l'Europe peuvent tout de même y adhérer. En sus, précisons que, par le biais de l'article 37 de cette dernière, le Comité des ministres peut inviter des États tiers à

---

[42] W. JUSTERS, "Cyber Security at Sea", *I.H.T. – C.I.T. – I.T.T.*, 2017/4, p. 481 ; X, "Cyberattaque en entreprise : quels sont les risques ?" disponible sur https://www.entreprises.cci-paris-idf.fr/web/pme/cyberattaque-en-entreprise-quels-sont-les-risques-, s. d., consulté le 12 mars 2025 ; X, « Quelles sont les conséquences d'une cyberattaque sur une entreprise ? » disponible sur https://www.cnfce.com/dossier/consequences-cyberattaque-entreprise-interview-expert-cybercriminalite, 4 octobre 2022 ; X, « Conséquences d'une cyberattaque » disponible sur https://www.cyberimpact.eu/consequences-dune-cyberattaque, *s. d.*, consulté le 9 mars 2025.

[43] O. LEROUX, « Chapitre IX. Criminalité informatique », *Les infractions – Volume 1*, 2e éd., Bruxelles, Larcier, 2016, p. 446.

[44] Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, *S.T.E.*, n°185.

la rejoindre. De cette façon, ladite Convention régionale est appliquée hors territoire européen et vise une communauté d'États provenant du monde entier, tels que le Canada, les États-Unis, le Japon, le Brésil, le Sénégal et bien d'autres encore. Ceci fait témoignage de l'intérêt que suscite cet instrument au-delà des frontières[45].

Il convient de noter que figurent les principaux objectifs du présent instrument dans le rapport explicatif de la Convention sur la cybercriminalité. En effet, cette dernière tend « *1) à harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité, 2) à fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique et, 3) à mettre en place un régime rapide et efficace de coopération internationale* »[46]. Cette convention crée donc une obligation positive, dans le chef des États l'ayant ratifiée, d'instaurer des mesures nationales visant à assurer son effectivité[47].

Malheureusement, force est de constater que, malgré l'objectif de la Convention de Budapest d'harmoniser les législations de droit domestique et de se diriger vers une coopération internationale, il existe toujours de fortes disparités entre les droits nationaux. En effet, nous relevons des écarts significatifs entre les lois nationales qui intègrent et transposent la Convention de Budapest dans leur droit interne respectif. Cela s'explique par le fait que « *certaines pratiques sont caractérisées juridiquement de manière différente d'un pays à l'autre. Il s'agit entre autres de la caractérisation juridique des actes préparatoires à la commission d'une infraction comme l'écriture d'un acte malveillant (malware). Dans certains pays européens, cet acte préparatoire ne suffit pas à caractériser une tentative punissable. Alors que dans d'autres, produire un code malveillant dont la seule utilité est de contrôler un botnet peut justifier l'ouverture d'une enquête* »[48].

Cet écart entre les droits nationaux profitent aux criminels les plus rusés. Ceux-ci vont, à l'évidence, profiter de ce manque de coordination entre les États pour organiser leurs activités illicites dans les États aux législations les plus permissives. À titre d'illustration, il importe de reconnaitre que « *les infrastructures criminelles digitales sont hébergées dans les pays qui ont les périodes de conservation des données les plus courtes ou dans lesquels les autorités ne sont pas susceptibles de coopérer avec d'autres pays* »[49]. Il semblerait donc nécessaire de remédier aux nombreuses lacunes existantes afin d'assurer une réponse juridique efficace et harmonisée face à la cybercriminalité transnationale[50].

---

[45] S. TURGIS, « Les valeurs du conseil de l'Europe appliquées à internet », *Droits et souveraineté numérique en Europe*, A. Blandin (dir.), Bruxelles, Bruylant, 2016, p. 27.

[46] Rapport explicatif de la Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, *S.T.E.*, n°185 ; S. KWASNY, « Lutte contre la cybercriminalité et le respect des droits de l'homme : les instruments du Conseil de l'Europe », *Internet et le droit international*, Paris, A. Pedone, 2014, p. 345.

[47] O. LEROUX, *op. cit.*, p. 447.

[48] G. MOUNIER, « Enquêtes internationales et poursuites des cybercriminels – Etat des lieux des défis juridiques », *Obs. Bxl*., 2016/3, n° 105, p. 16.

[49] G. MOUNIER, *ibidem*, p. 16.

[50] S. KWASNY, *op. cit.*, p. 346.

Il n'en demeure pas moins que quatre catégories d'infractions sont identifiées dans la Convention étudiée. En premier lieu, sont reconnues les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques. En deuxième lieu, sont consacrées les infractions informatiques. Troisièmement, figurent les infractions se rapportant au contenu et dernièrement, les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes sont considérées. Cette catégorisation est, pour ainsi dire, relativement lacunaire en raison du fait qu'il n'existe pas de critère isolé permettant de faire une distinction claire et précise entre chaque catégorie d'infraction. Compte tenu du fait que les catégories se chevauchent les unes avec les autres, il va de soi que certaines infractions peuvent appartenir à plusieurs catégories à la fois[51].

Par suite de ces lacunes présentées, certains auteurs ont privilégié une division en 3 catégories d'infractions, à savoir les crimes contre l'intégrité de la personne, les crimes économiques et les crimes contre la collectivité[52]. Une autre partie de la doctrine, quant à elle, différencie les infractions eu égard à l'évolution de la cybercriminalité. Le moment de leur apparition dans l'histoire détermine la catégorie dont l'infraction ressort, de sorte qu'une distinction est opérée entre les usages problématiques qui ne sont pas criminalisés, les crimes traditionnels qui existaient déjà avant l'apparition d'internet et les crimes innovateurs qui ne peuvent être réalisés que grâce aux technologies de l'information et à internet. Toutefois et malencontreusement, ces deux catégorisations ne reprennent pas la distinction opérée sur la base de l'informatique en tant que sujet, objet ou moyen de perpétration de l'infraction[53]. Rajoutons tout de même qu'un auteur a opéré une troisième distinction entre deux formes de cybercriminalité, et ce dans un souci de simplification. Il y aurait, d'après ses propos, la cybercriminalité portant atteinte aux réseaux et la cybercriminalité exploitant les réseaux afin de porter atteinte aux droits des personnes[54].

Concernant les actes qualifiés de répréhensibles en matière de cybercriminalité, un groupe d'experts de l'Assemblée générale des Nations Unies a réalisé une étude qui a permis d'identifier 15 actes :

- « *Accès illégal à un système informatique ;*
- *Accès illégal à des données informatiques ;*
- *Interception ou acquisition illégale des données informatiques ;*
- *Atteinte à l'intégrité des données ou à l'intégrité du système ;*
- *Production, distribution ou possession d'outils informatiques malveillants ;*
- *Violation de la vie privée ou de la protection des données ;*

---

[51] F. DECHAMPS et C. LAMBILOT, « Partie I : Concepts et législation – Titre II : cybercriminalité et outils juridiques », *op. cit.*, p. 26 et 27 ; M. CHAWKI, « L'individu face à la cybercriminalité », *Droit pénal et nouvelles technologies*, J.-P. Céré, J. M. Rascagnères et E. Vergès (dir.), Paris, L'Harmattan, 2015, p. 41.

[52] B. DUPONT, F. GAUDREAU et F. PRATES, « La cybercriminalité : état des lieux et perspectives d'avenir », *Droits de la personne : La circulation des idées, des personnes et des biens et capitaux*, Actes des journées strasbourgeoises 2012 organisées par l'Institut canadien d'études juridiques supérieures, Cowansville, Yvon Blais, Cowansville, 2013, p. 415 à 442.

[53] F. DECHAMPS et C. LAMBILOT, « Partie I : Concepts et législation – Titre II : cybercriminalité et outils juridiques », *op. cit.*, p. 27.

[54] M. CHAWKI, *op. cit.*, p. 42.

- *Fraude ou falsifications informatiques ;*
- *Usurpation d'identité numérique ;*
- *Atteintes au droit d'auteur et aux marques par voie informatique ;*
- *Envoi massif ou contrôle de l'envoi massif de messages non sollicités (spams) ;*
- *Actes informatiques causant un préjudice personnel ;*
- *Actes informatiques à caractère raciste ou xénophobe ;*
- *Production, diffusion ou possession de pornographie enfantine par voie informatique ;*
- *Sollicitation en ligne d'enfants à des fins sexuelles (grooming) ;*
- *Actes informatiques visant à faciliter les infractions terroristes* »[55].

Certains pays pénalisent les infractions qu'ils associent à la criminalité informatique, tandis que d'autres choisissent de ne pas les incriminer[56].

En définitive, il paraît évident, au vu de ce qui est susmentionné, que les cyberattaques sont visées par la Convention de Budapest en ce qu'elles constituent manifestement un acte répréhensible pouvant rentrer dans le champ de la cybercriminalité. Il importera toutefois de s'attacher à répondre à la question suivante : « *est-ce que le droit de l'Union européenne et le droit belge respectent le contexte posé par la Convention de Budapest ?* ».

À cet égard, précisons d'emblée que la Belgique a adopté une loi du 3 août 2012 afin de porter assentiment à la Convention sur la cybercriminalité[57], dite la Convention de Budapest. Il ressort d'ailleurs du document parlementaire relatif au projet de loi présenté au Sénat que la législation belge était, en grande majorité, conforme aux prescrits dictés par la Convention[58].

2. La Convention des Nations Unies contre la cybercriminalité, une avancée majeure récente ?

Depuis peu et après une longue période de négociations, un nouvel outil international a vu le jour en matière de cybercriminalité, constituant un progrès significatif. Il s'agit de la Convention des Nations Unies contre la cybercriminalité. Le 24 décembre 2024, celle-ci a été adoptée par les 193 États membres des Nations Unies à la suite d'un consensus, et ce dans un but premier de renforcer la coopération internationale pour la lutte contre certaines infractions[59]. Son contenu se calque fortement sur celui de la Convention de Budapest[60]. La Convention des Nations Unies permettra « *de renforcer la coopération internationale entre des États qui ne sont aujourd'hui pas partie aux mêmes instruments régionaux en apportant*

---

[55] F. DECHAMPS et C. LAMBILOT, « Partie I : Concepts et législation – Titre II : cybercriminalité et outils juridiques », *op. cit.*, p. 28.

[56] F. DECHAMPS et C. LAMBILOT, *ibidem*, p. 29.

[57] Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, approuvé par la loi du 3 août 2012, *M.B.*, 21 novembre 2012.

[58] Projet de loi portant assentiment à la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, *Doc.*, Sén., 2011–2012, n°5-1497/1. Document parlementaire n°5-1497/1.

[59] NATIONS UNIES, « La Convention sur la cybercriminalité, pour un monde numérique et physique plus sûr » disponible sur https://news.un.org/fr/story/2024/12/1151706, 25 décembre 2024.

[60] CONSEIL DE L'EUROPE, « Conventions sur la cybercriminalité : La Convention de Budapest et le projet de traité des Nations Unies » disponible sur https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1fb99, 27 août 2024.

plus de cohérence entre les système juridiques et en offrant de nouveaux mécanismes de coopération »[61].

L'Organisation internationale de police criminelle, à savoir Interpol, précise que cette Convention répond au besoin d'apporter des garanties face à l'augmentation et la complexité accrue des cyberattaques émergeantes dans le monde entier. La mise à jour des bases juridiques quant à la cybercriminalité demeurait indispensable[62] et nous espérons que ce nouvel instrument fera ses preuves au gré des années à venir. À cet égard, précisons qu'il découle de l'article 64 de ladite Convention que celle-ci « *est ouverte à la signature de tous les États à Hanoï en 2025, puis au Siège de l'Organisation des Nations Unies, à New-York, jusqu'au 31 décembre 2026* »[63]. Il semblerait qu'aucune date précise n'ait été communiquée. Concernant son entrée en vigueur, le traité ne s'appliquera qu'après que quarante États en soient devenus parties[64].

Chapitre 2. Droit de l'Union européenne

Au niveau de l'Union européenne, les cyberattaques sont visées dans différents instruments. Signalons d'ores et déjà que certains actes normatifs élaborés par l'Union européenne seront étudiés ultérieurement dans la partie consacrée à la prévention en ce qu'ils concernent davantage la cybersécurité. À présent, concentrons-nous sur deux normes juridiques édifiantes en cette matière qui, de manière générale, semblent conformes à la Convention de Budapest.

1. Deux instruments significatifs de droit dérivé

Le premier instrument qui retiendra notre attention est la Directive 2013/40/UE relative aux attaques contre les systèmes d'information, remplaçant la Décision-cadre 2005/222/JAI[65]. Celle-ci s'inspire considérablement de la Convention de Budapest et reprend pour ainsi dire ses idées[66]. Elle a également pour objectif d'harmoniser la cybercriminalité et privilégie une approche de sécurisation des systèmes d'information[67]. Plus particulièrement, « *la directive fixe les règles minimales concernant la définition des infractions pénales et les sanctions en*

---

[61] A. GERY et A.-T. NORODOM, « ONU : adoption d'une convention sur la lutte contre la cybercriminalité » disponible sur https://www.leclubdesjuristes.com/international/onu-adoption-dune-convention-sur-la-lutte-contre-la-cybercriminalite-8783/, 16 janvier 2025.

[62] INTERPOL, « Interpol salue l'adoption de la Convention des Nations Unies contre la cybercriminalité » disponible sur https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2024/INTERPOL-salue-l-adoption-de-la-Convention-des-Nations-Unies-contre-la-cybercriminalite, 23 décembre 2024.

[63] Art. 64 de la Convention des Nations Unies contre la cybercriminalité.

[64] Art. 65 de la Convention des Nations Unies contre la cybercriminalité.

[65] Directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, *J.O.U.E.*, L 218/8, 14 août 2013.

[66] D. FLORE et S. BOSLY, « Chronique de droit pénal européen », *J.D.E.*, 2018/5, n°249, p. 199 à 206.

[67] A. BRUNI, « Chapter 11. Promoting Coherence in the EU Cybersecurity Strategy », *Security and Law*, A. Vedder *et al.* (dir.), Cambridge, Intersentia Ltd, 2019, p. 260.

matière d'attaques contre les systèmes d'information » et vise à renforcer la prévention tout en optimisant la coopération entre les autorités judiciaires[68].

Il est important de préciser que les définitions, établies par la directive en son article 1, sont majoritairement identiques à celles prévues par la Convention de Budapest. Toutefois, certains changements sont opérés et quelques précisions sont ajoutées. À titre d'illustration, la Convention de Budapest parle de « système informatique » alors que la directive fait référence au « système d'information ». Ajoutons que cette directive, par son article 9, énonce les sanctions prévues de manière plus précise que la Convention de Budapest. En effet, des prescrits quant à des peines d'emprisonnement sont établis par la directive et doivent être respectés par les États membres. La Convention de Budapest, quant à elle, n'impose pas de seuils minimaux pour les sanctions pénales et laisse ainsi une grande et large marge d'appréciation aux États parties. De plus, l'article 13 de la directive instaure une procédure d'urgence, nettement plus aboutie, « *au cours de laquelle l'autorité compétente doit indiquer dans les huit heures suivant la réception d'une demande d'assistance la forme et le délai estimé pour la réponse, au moins lorsque celle-ci sera satisfaite* ». Enfin, l'article 14 de la directive invitent les États à adopter un système d'enregistrement, de production et de communication quant aux infractions qui seraient commises sur leur territoire. Les données récoltées par les États devront par la suite être transmises à la Commission afin qu'un rapport consolidé soit communiqué aux organes qualifiés et compétents[69].

Ensuite, le deuxième instrument auquel nous pouvons faire allusion est le Règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres[70]. Ce dernier trouve son fondement notamment dans une Décision (PESC) 2019/797 ayant trait à la même thématique[71]. Sur la base de l'article 1 du règlement, nous comprenons que sont visées les cyberattaques de grande ampleur. En effet, sont concernées les cyberattaques « *dirigées contre des pays tiers ou des organisations internationales lorsqu'une action est jugée nécessaire à la réalisation des objectifs de l'UE en matière de politique étrangère et de sécurité commune* ». Dans ce contexte, des sanctions sont ainsi imposées par l'Union européenne[72].

Chapitre 3. Droit pénal belge

Dans ce chapitre, le cadre légal offert par le droit pénal belge va être étudié. Dans notre droit national, il existe, selon moi, trois infractions pouvant être qualifiées de cyberattaques *sensu*

[68] « Attaques visant les systèmes d'information », *Obs. Bxl*., 2014/1, n° 95, p. 60.

[69] A. ALBERINI *et al*., « Chronique de législation 2013 », *Rev. Aff. Eur*., 2014/1, p. 261 ; « Attaques visant les systèmes d'information », *Obs. Bxl*., 2014/1, n° 95, p. 60 et 61.

[70] Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menaces l'Union ou ses États membres, *J.O.U.E.*, L 129 1/1, 17 mai 2019.

[71] Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant les mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, *J.O.U.E*., LI 129/13, 17 mai 2019.

[72] EUR-Lex, « Mesures restrictives de l'Union européenne contre les cyberattaques » disponible sur https://eur-lex.europa.eu/legal-content/FR/LSU/?uri=celex:32019R0796, 18 mai 2022.

stricto, le hacking, le sabotage informatique et la fraude informatique[73]. Nous allons donc procéder à l'étude de chacune de ces infractions et relever si le cadre juridique prévu par notre droit interne respecte les dispositions internationales.

Il me paraît nécessaire de rappeler que le Code pénal de 1867 est toujours d'application en ce que le nouveau Code pénal de 2024 n'entrera en vigueur que le 8 avril 2026. En considération de cela, les dispositions légales actuelles et futures vont être citées pour chacune des infractions analysées et les nouveautés apportées par la nouvelle législation seront soulignées[74].

1. Hacking

Le hacking, ou encore l'*accès non autorisé*, peut être interne ou externe. L'article 550*bis* du Code pénal consacre ces deux formes, l'une étant traitée au premier paragraphe et l'autre étant traitée au deuxième paragraphe[75]. *A contrario*, dans le nouveau Code pénal, les dispositions légales sont différentes selon qu'il s'agisse du hacking externe ou du hacking interne. En effet, l'accès non autorisé externe est consacré à l'article 524, alors que l'accès non autorisé interne est prévu à l'article 525.

a) Hacking externe

La définition du hacking externe n'a pas changé dans le nouveau Code pénal. En effet, sur la base de l'article 524 du nouveau Code pénal, « *l'accès non autorisé externe dans un système informatique consiste, pour une personne sachant qu'elle n'y est pas autorisée, à, délibérément, accéder à un système informatique ou s'y maintenir* »[76]. D'une part, les éléments constitutifs matériels de l'infraction sont l'absence d'autorisation et l'accès ou le maintien dans un système informatique. D'autre part, l'élément constitutif moral de l'infraction est le fait d'avoir agi avec connaissance de cause et volonté. Une intention spéciale n'est pas requise en l'espèce[77]. De plus, dans l'article 524 du nouveau Code pénal, une peine de niveau deux est retenue.

---

[73] Selon moi, le concept de cyberattaque *sensu lato* peut, certainement, englober d'autres infractions consacrées par notre droit pénal belge, toutefois la présente analyse se limitera à l'étude des cyberattaques au sens strict.

[74] Dans la suite des développements, le Code pénal de 1867 sera appelé « Code pénal » et le Code pénal de 2024 sera appelé « nouveau Code pénal ».

[75] F. DUMORTIER, « Chapitre 5. La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilités », *Les obligations légales de cybersécurité et de notifications d'incidents*, F. Dumortier et V. Vander Geeten (dir.), Belgique, Politeia, 2019, p. 220 et 227.

[76] C. pén. art 524.

[77] F. DUMORTIER, *op. cit.,* p. 220 à 225 ; P. CAROLUS *et al*., « Chapitre 3. Criminalité informatique », *Droit pénal des affaires*, 2e éd., Bruxelles, Larcier-Intersentia, 2024, p. 574 et 575 ; O. LEROUX, *op. cit.*, p. 478 à 483 ; V. VANDER GEETEN, « Hacking « éthique » en droit pénal belge », *Société numérique et droit pénal*, D. Flore et V. Franssen (dir.), 1e éd., Bruxelles, Bruylant, 2019, p. 76 à 82 ; J. KERKHOFS et P. van LINTHOUT, « Inleiding tot het materieel en strafprocedureel cyberstrafrecht : uitdagingen voor de advocatuur », *Internet &/@ Recht*, Gand, Larcier, 2013, p. 14 et 15.

b) Hacking interne

La définition du hacking interne n'a, pour ainsi dire, pas non plus changé dans le nouveau Code pénal. L'article 525 de ce même Code fournit la définition suivante : « *l'accès non autorisé interne dans un système informatique consiste pour une personne à, avec une intention frauduleuse ou dans le dessein de nuire, outrepasser son pouvoir d'accès à un système informatique* »[78]. *In casu*, nous remarquons que l'élément moral diffère du hacking externe en ce que la personne a la volonté d'outrepasser son pouvoir d'accès au système informatique, et ce avec une intention spéciale, c'est-à-dire une intention frauduleuse ou dans un dessein de nuire[79]. En outre, l'article 525 du nouveau Code pénal prévoit également une peine de niveau deux.

2. Sabotage informatique

L'article 531 du nouveau Code pénal stipule que « *le sabotage informatique consiste, pour une personne sachant qu'elle n'y est pas autorisée, à, délibérément, de façon directe ou indirecte, introduire dans un système informatique, y modifier ou y effacer des données, ou modifier par tout moyen technologique l'utilisation normale de données dans un système informatique* »[80]. Cette définition reprend précisément les termes énoncé à l'article 550*ter* du Code pénal. Les éléments constitutifs sur le plan matériel sont au nombre de deux, à savoir l'introduction, la modification ou la suppression de données informatiques par tout moyen technologique et l'absence d'autorisation. Quant à l'élément moral, il est nécessaire que la personne ait eu conscience que l'opération était illicite. Une intention frauduleuse n'est toutefois pas requise. La peine, quant à elle, est de niveau deux. À titre d'exemple, il est à relever que le vers, étudié précédemment, est considéré comme un type de sabotage informatique[81].

3. Fraude informatique

La fraude à l'aide d'un système informatique est définie à l'article 488 du nouveau Code pénal comme suit : « *la fraude informatique consiste à chercher à se procurer, pour soi-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique* »[82]. Ce concept est défini identiquement à l'article 504*quater* du Code pénal. Il en découle trois éléments constitutifs, à savoir l'intention frauduleuse, la procuration d'un avantage économique illégal et l'introduction, la modification ou l'effacement des données dans un système informatique[83]. À titre d'exemple, le phishing, faisant l'objet de développements ci-avant, est

---

[78] C. pén. art. 525.

[79] F. DUMORTIER, *op. cit.,* p. 229 ; P. CAROLUS *et al.*, *op. cit.,* p. 576 et 577 ; O. LEROUX, *op. cit.*, p. 485 et 486 ; V. VANDER GEETEN, *op. cit.*, p. 85.

[80] C. pén. art. 531.

[81] F. DUMORTIER, *op. cit.,* p. 239 et 240 ; P. CAROLUS *et al*., *op. cit.,* p. 580 et 581 ; V. VANDER GEETEN, *op. cit.*, p. 97 et 98.

[82] C. pén. art. 488.

[83] P. CAROLUS *et al*., *op. cit.,* p.. 571.

considéré comme une fraude informatique[84]. Enfin, la peine prévue par ledit article 488 est de niveau trois.

4. Conformité à la Convention de Budapest ?

Pour clore cette analyse du droit pénal belge, nous relèverons un réel alignement du droit national sur les exigences posées par la Convention de Budapest. En effet, signalons que le hacking, consacré en droit pénal belge, correspond à l' « accès illégal » sanctionné par l'article 2 de ladite Convention. De plus, le sabotage informatique constitue une consécration de l'article 5 de la Convention en ce que l' « atteinte à l'intégrité du système » est reconnue. La fraude informatique est, par ailleurs, consacrée à l'article 8 de la Convention, de sorte que le droit pénal belge s'y soumet entièrement. Le droit national répond donc à cette nécessité de réprimer ces comportements. Enfin, comme annoncé, ces trois infractions pénales prévoient des peines relevant des niveaux deux ou trois, soit des sanctions effectives, proportionnées et dissuasives, comprenant des peines d'emprisonnement. De cette manière, l'article 13 de la Convention de Budapest est respecté.

Titre 3. De quelques auteurs responsables des cyberattaques

Chapitre 1. Les personnes morales

Tout d'abord, la responsabilité des personnes morales est consacrée à l'article 12 de la Convention de Budapest. Les personnes morales auteurs de cyberattaques peuvent ainsi être tenues responsables. Il est néanmoins difficile d'identifier les réels auteurs compte tenu du caractère technique et de la transnationalité de ces attaques[85].

Le premier paragraphe de l'article 12 précité impose aux États parties de mettre en place une responsabilité des personnes morales pour des infractions qui seraient commises par des personnes qui exerceraient un pouvoir de direction et qui agiraient dans le cadre de ce pouvoir[86]. Il en découle le respect de quatre conditions : la commission d'une infraction définie par la Convention, la commission de l'infraction pour le compte de la personne morale, le pouvoir de direction exercé par la personne auteur et le fait pour cette personne d' « *avoir agi sur la base de l'une de ses compétences – un pouvoir de représentation ou le pouvoir de prendre des décisions ou d'exercer un contrôle* »[87].

Le deuxième paragraphe, quant à lui, « *oblige les États à imposer une responsabilité à une personne morale lorsque l'infraction est commise par l'un de ses employés ou agents agissant dans le cadre de leur pouvoir, si l'infraction a été rendue possible par le fait que la personne*

[84] P. CAROLUS *et al*., *Ibidem*, p. 572.

[85] P. ACHILLEAS, "Entreprises, cyberattaques et responsabilité", *Cyberattaques et droit international. Problèmes choisis*, M. Grange et A-T. Norodom (dir.), Paris, A. PEDONE, 2018, p. 138.

[86] P. ACHILLEAS, *ibidem*, p. 140.

[87] Rapport explicatif de la Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, *S.T.E*., n°185, p. 23.

exerçant un pouvoir de direction n'a pas supervisé l'employé ou l'agent en question »[88]. Nous pouvons nous questionner sur l'absence de supervision requise. À cet égard, le rapport explicatif de la Convention sur la cybercriminalité énonce que l'absence de supervision est supposée lorsqu'aucune mesure appropriée et raisonnable n'a été adoptée dans le but d'empêcher les employés de commettre des actes illégaux pour le compte de la personne morale[89].

Le troisième paragraphe de l'article 12 énonce le principe selon lequel les États préservent le libre choix d'imposer une responsabilité de nature pénale, civile ou administrative[90]. Rappelons toutefois que le paragraphe deuxième de l'article 13 de la Convention sur la cybercriminalité doit être respecté, de sorte que des sanctions effectives, proportionnées et dissuasives doivent être prévues[91].

Enfin, le dernier paragraphe de cette disposition fait mention que les personnes physiques ayant commis l'infraction peuvent également voir leur responsabilité pénale engagée.

Aussi, il me paraît judicieux d'indiquer que l'article 10 de la Directive 2013/40/UE relative aux attaques contre les systèmes d'information prévoit également une responsabilité des personnes morales. Cet article reprend par ailleurs le même contenu que l'article 12 de la Convention sur la cybercriminalité[92]. L'Union européenne est, par conséquent, en parfaite adéquation avec les aspirations du Conseil de l'Europe.

En dernier lieu, relevons que notre droit national prévoit également une responsabilité pénale des personnes morales en son article 5 du Code pénal de 1867. Cette disposition est retranscrite dans les mêmes termes à l'article 18 du nouveau Code pénal[93]. Ainsi, lorsque des infractions qui s'apparentent à des cyberattaques (telles que le hacking, le sabotage informatique ou la fraude informatique) sont commises par ou pour le compte d'une personne morale, celle-ci peut voir sa responsabilité pénale engagée. De plus, le droit belge n'exclut pas non plus la responsabilité pénale des personnes physiques auteurs des mêmes faits ou y ayant participé. Nous pouvons donc également conclure, de manière générale, à une conformité du droit belge avec la Convention sur la cybercriminalité au sujet de la responsabilité des personnes morales.

Chapitre 2. L'État

À présent, concentrons-nous brièvement sur la responsabilité de l'État lorsque ce dernier a commis une cyberattaque. Dans cette hypothèse, ayons à l'esprit que la Convention de Budapest ne s'applique pas en ce que les États ne sont aucunement visés. En effet, comme

---

[88] P. ACHILLEAS, *op. cit.*, p. 140.

[89] Rapport explicatif de la Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, *S.T.E.*, n°185, p. 23.

[90] P. ACHILLEAS, *op. cit.*, p. 140.

[91] Rapport explicatif de la Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, *S.T.E.*, n°185, p. 23.

[92] A. GUINCHARD, "L'entreprise face à la cybercriminalité », *Droit pénal et nouvelles technologies*, J-P. Ceré, J.M. Rascagnères et E. Vergès (dir.), Paris, L'Harmattan, 2015, p. 22 et 23.

[93] V. FRANSSEN, « Le nouveau Code pénal et la responsabilité pénale des personnes morales : une regrettable non-réforme ? », *Rev. Dr. ULiège*, 2024/2, p. 230.

déjà annoncé, cette dernière ne sanctionne que les infractions commises par des personnes physiques ou morales au sens strict[94].

L'État auteur d'une cyberattaque se verra donc sanctionné par des règles de droit international public. On parlera donc de la *responsabilité internationale des États*[95]. Concrètement, « *l'État est non seulement responsable des comportements de ceux qu'il considère comme ses organes, mais il peut également se voir attribuer les agissements de personnes qu'il tient, ou veut faire passer, pour privées* »[96]. Toutefois, il reste relativement difficile d'apprécier si l'acte illicite, en l'espèce la cyberattaque, a été initiée pour le compte de l'État[97].

Titre 4. Prévention

Après avoir étudié le cadre légal et avoir vu que la responsabilité pouvait être engagée dans un but répressif, intéressons-nous à la prévention des cyberattaques. Au vu des faits répréhensibles qui peuvent être commis, il est important de prévoir en amont des solutions afin d'éviter le pire. Pour cette raison, nous allons procéder, à travers cette quatrième partie, à une analyse de la cybersécurité, celle-ci ayant un rôle principalement préventif[98].

Nous remarquons que la cybersécurité est majoritairement traitée au niveau de l'Union européenne, celle-ci prenant son rôle très à cœur de prévenir les cybermenaces potentielles[99]. Par conséquent, nous étudierons dans les développements ci-après les instruments mis en place à cette échelle.

Commençons par évoquer une directive, fondamentale dans ce domaine, qui a été adoptée récemment. Il s'agit de la directive (UE) 2022/2555 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, également dénommée *directive NIS 2*[100]. Celle-ci remplace effectivement la directive (UE) 2016/1148, aussi appelée

---

[94] C. CRÉPET DAIGREMONT, « Responsabilité de l'Etat-auteur d'une cyberattaque », *Cyberattaques et droit international. Problèmes choisis*, M. Grange et A-T. Norodom (dir.), Paris, A. PEDONE, 2018, p. 155 et 156.

[95] C. CRÉPET DAIGREMONT, *Ibidem*, p. 155 et 156.

[96] P. JACOB, « La responsabilité internationale de l'État du fait des cyberattaques », *La souveraineté numérique*, B. Bertrand et G. Le Floc (dir.), 1e éd., Bruxelles, Bruylant, 2024, p. 286.

[97] P. JACOB, *Ibidem*, p. 290.

[98] E. LIEVENS, « Chapter 21. Cybercrime and cybersecurity », *An Introduction to Law & Technology*, E. Lievens, C. Vander Maelen et S. Verschaeve (dir.), Belgique, Owl Press Legal, 2024, p. 400.

[99] E. LIEVENS, *Ibidem*, p. 408.

[100] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), *J.O.U.E.*, L 333/80, 27 décembre 2022.

directive NIS 1[101]. Un règlement d'exécution énonçant les règles relatives à l'application de la directive NIS 2 a également été adopté[102].

La directive NIS 2 a pour objectif d'harmoniser les dispositifs prévus par les États membres dans une perspective de lutte acharnée contre les cybermenaces[103]. Cette nouvelle directive a notamment été adoptée dans une perspective de renforcement de sa politique et laisse par conséquent moins de marge de manœuvre aux États afin de réduire au maximum les risques de cyberattaques[104]. À la lecture de ladite directive NIS 2, nous découvrons, par exemple, que les États ont pour mission de mettre en place une stratégie propre en matière de cybersécurité avec des objectifs déterminés[105], des autorités compétentes en cette matière ainsi que des points de contacts uniques[106] et des centres de réponse aux incidents de sécurité informatique (CSIRT)[107]. La coopération entre ces acteurs est exigée au sein de chaque État membre sur la base de l'article 13 de la directive[108]. Enfin, une coopération internationale est maintenue par le législateur européen[109].

---

[101] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.U.E.*, L 194, 19 juillet 2016 ; M. KNOCKAERT, « Chronique de législation. La cybersécurité », *R.D.T.I.*, 2023/3-4, p. 87.

[102] Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance, *J.O.U.E.*, 18 octobre 2024.

[103] M. KNOCKAERT, « Chronique de législation. La cybersécurité », *R.D.T.I.*, 2023/3-4, p. 88 ; H. VAN SOEST, « Chapitre XIV. Cybersecurity in the European Electricity System : The Role of the NIS2 Directive", *European Energy Law Report XV*, C. Banet et M.-M. Roggenkamp (dir.), 1e éd., Bruxelles, Intersentia, 2025, p. 354 ; Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), art. 5, *J.O.U.E.*, L 333/80, 27 décembre 2022.

[104] E. LIEVENS, *op. cit.*, p. 408.

[105] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), art. 7, *J.O.U.E.*, L 333/80, 27 décembre 2022.

[106] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), art. 8, *J.O.U.E.*, L 333/80, 27 décembre 2022.

[107] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), art. 10, *J.O.U.E.*, L 333/80, 27 décembre 2022.

[108] E. LIEVENS, *op. cit.*, p. 408 et 409.

[109] M. KNOCKAERT, « Chronique de législation. La cybersécurité », *R.D.T.I.*, 2023/3-4, p. 100.

Spécifions que le législateur belge a transposé cette directive NIS 2 par la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique[110]. Nous pouvons, de plus, mentionner l'existence d'un arrêté royal exécutant cette loi du 26 avril 2024[111]. Il en résulte que le droit belge s'est conformé aux exigences retenues par le droit de l'Union européenne.

Ensuite, nous pouvons évoquer le règlement (UE) 2019/881 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications[112]. Il est plus communément appelé « *Cybersecurity Act* ». Ce règlement se charge de déterminer *sensu lato* les contours de l'ENISA et le cadre de certification de la cybersécurité[113]. Ainsi, la prévention est également assurée.

En outre, deux règlements sur la résilience ont été adoptés de manière à prévenir de telles attaques informatiques. D'une part, nous avons le règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier, appelé également le règlement DORA[114]. À la lecture de l'article 3 de ce règlement, nous découvrons une nouvelle définition du concept de *cyberattaque*. Celle-ci est définie comme « *un incident lié aux TIC malveillant causé par une tentative de destruction, d'exposition, de modification, de désactivation, de vol, d'utilisation non autorisée d'un actif ou d'accès non autorisé à celui-ci, perpétrée par un acteur de la menace* »[115]. Notons que l'objectif de ce règlement est d'assurer une protection aux réseaux et systèmes d'information de nombreuses entités financières. La résistance à toute menace impliquant des TIC est le maître-mot[116]. D'autre part, un règlement (UE) 2024/2847 sur la cyberrésilience a également été conçu dans une optique préventive face aux vulnérabilités qui peuvent se présenter en cas de cyberattaques[117].

---

[110] Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 17 mai 2024.

[111] Arrêté royal 9 juin 2024 exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 24 juin 2024 ; Il existe un arrêté royal du 15 décembre 2024 qui modifie l'arrêté royal du 9 juin 2024 exécutant la loi du 26 avril 2024.

[112] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), *J.O.U.E.*, L 151/15, 7 juin 2019.

[113] A. BRUNI, *op. cit.,* p. 272.

[114] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, *J.O.U.E.*, L 333/1, 27 décembre 2022.

[115] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, art. 3, J.O.U.E., L 333/1, 27 décembre 2022.

[116] EUR-Lex, « Résilience opérationnelle numérique du secteur financier » disponible sur https://eur-lex.europa.eu/legal-content/FR/LSU/?uri=CELEX:32022R2554, 10 janvier 2024.

[117] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n°168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience), *J.O.U.E.*, 20 novembre 2024 ; CENTRE FOR CYBERSECURITY BELGIUM,

Ajoutons qu'il existe, depuis peu, un règlement (UE) 2025/38 sur la cybersolidarité[118]. Celui-ci est entré en vigueur le 4 février 2025. Comme nous pouvons nous en douter, le but de ce règlement est de favoriser la solidarité entre les États membres et de renforcer la cybersécurité. À la différence de la directive NIS 2 et du règlement sur la cyberrésilience, cet instrument n'impose aucune obligation aux États. En d'autres termes, ce règlement sur la cybersolidarité est facultatif[119].

Il semble enfin pertinent de relever l'existence du Centre pour la Cybersécurité belge (CCB), s'agissant de l'autorité compétente en matière de prévention de ce cyberphénomène[120]. La mise en place de cette autorité belge a permis la démonstration de son implication à prévenir de tels incidents. Elle « *a pour tâche principale de défendre les réseaux et les systèmes d'informations contre tout événement issu du cyberespace qui pourrait compromettre la disponibilité, l'intégrité et la confidentialité de ces systèmes (tel que le matériel, les logiciels et les infrastructures associées), des réseaux, des données stockées, traitées ou transmises par un système d'information (ordinateur, smartphone, tablette, serveurs) et services qu'ils génèrent* »[121].

Titre 5. Au regard de certains droits fondamentaux

Cette dernière partie a pour objectif de déceler l'impact des cyberattaques sur nos droits fondamentaux, plus particulièrement le droit au respect de la vie privée et le droit à la liberté d'expression. Le droit protège-t-il suffisamment les droits humains des individus ?

Chapitre I. Droit au respect de la vie privée

Différentes législations encadrent ce droit au respect de la vie privée. Nous nous limiterons néanmoins à ne citer que certaines d'entre elles dans un souci de délimitation. À une grande échelle, ce droit au respect de la vie privée est consacré par l'article 8 de la Convention européenne des droits de l'homme, tandis qu'à une échelle plus restreinte, ce droit est inscrit à l'article 22 de la Constitution belge. D'emblée, signalons également que la protection des données personnelles trouve son fondement dans ce droit à la vie privée[122]. Cette

« Règlementation » disponible sur https://ccb.belgium.be/fr/reglementation, *s. d*., consulté le 28 avril 2025.

[118] Règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité), *J.O.U.E.*, 15 janvier 2025.

[119] CENTRE FOR CYBERSECURITY BELGIUM, « Règlementation » disponible sur https://ccb.belgium.be/fr/reglementation, *s. d*., consulté le 28 avril 2025.

[120] Arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, *M.B*., 21 novembre 2014, art. 3.

[121] P. CLOUNER, *op. cit*., p. 210 et 211.

[122] Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000 ; Cour eur. D.H., arrêt S. et Marper c. Royaume-Uni, 4 décembre 2008 ; J.-F. HENROTTE et Y. POULLET, « La protection des données (à caractère personnel) à l'heure de l'Internet », *CUP109 – Protection du consommateur, pratiques commerciales et T.I.C.*, J. Laffineur (dir.), Belgique, Anthemis, 2009, p. 206.

considération nous est nécessaire en ce que, lorsqu'une cyberattaque est commise, un risque existe quant aux données personnelles des individus.

Le droit au respect de la vie privée et la protection des données personnelles partagent les mêmes valeurs, à savoir la dignité humaine et l'autonomie personnelle. Toutefois, notons que le droit à la vie privée s'attache à une sphère personnelle, alors que la protection des données personnelles se réfère aux informations sensibles et propres à chacun[123].

Nous ne pouvons pas parler de la protection des données personnelles, sans évoquer le Règlement général sur la protection des données, plus connu sous l'appellation « *RGPD* »[124]. Celui-ci a par ailleurs inspiré le législateur belge en ce qu'il existe une loi belge du 30 juillet 2018 sur le traitement des données personnelles[125].

Tout d'abord, mentionnons que le RGPD protège uniquement les données des personnes physiques[126]. La notion de donnée à caractère personnel est définie à l'article 4 du RGPD comme « *toute information se rapportant à une personne physique identifiée ou identifiable* », alors que la notion de traitement est définie comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel* ». Ces définitions, relativement larges, permettent d'appliquer le RGPD à la grande majorité des situations[127]. De plus, il nous faut ajouter qu'est organisée une responsabilité du responsable du traitement et du sous-traitant. Par conséquent, dans le cas où une cyberattaque se produirait et qu'une personne physique verrait ses données à caractère personnel violées, la responsabilité du responsable du traitement de ses données et la responsabilité du sous-traitant peuvent être engagées[128].

Concrètement, l'article 5. 1, f) du RGPD protège les données à caractère personnel de tout traitement non autorisé ou illicite, et ce par le biais de mesures de sécurité. En effet, comme nous le savons, les données sensibles et personnelles attisent la curiosité des cybercriminels. Pour cette raison, une sécurité accrue doit être garantie par des mesures aussi bien

---

[123] L. KEUNEN et I. MILKAITE, « Chapter 5. The right to privacy and data protection in a digital era », *An Introduction to Law & Technology*, E. Lievens, C. Vander Maelen et S. Verschaeve (dir.), 2e éd., Belgique, Owl Press Legal, 2023, p. 101.

[124] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119/1, 4 mai 2016 ; R. TAMAS, « The data processor's new obligations under the GDPR : a restored balance or a shift of responsabilities ? », *Data Protection & Privacy*. Le GDPR dans la pratique / De GDPR in de praktijk, N. RAGHENO (dir.), Belgique, Anthemis, 2017, p. 75 ; J. LIDDICOAT, « Part II. New Challenges in the Digital Era. Chapter 8. Human Rights and Artificial Intelligence », *Human Rights and the Internet*, Cambridge, Intersentia, 2021, p. 156.

[125] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018 ; L. KEUNEN et I. MILKAITE, *op. cit.*, p. 114 ; F. ERNOTTE, « Chapitre 5 – Données à caractère personnel », *Droit des réseaux sociaux*, 1e éd., Bruxelles, Larcier, 2021, p. 82 et 83.

[126] C. de TERWANGNE, « Titre 2. Définitions clés et champ d'application du RGPD », *Le règlement général sur la protection des données (RGPD/GDPR)*, 1e éd., Bruxelles, Larcier, p. 63.

[127] F. DUMORTIER, « Les obligations de sécurité et de notification des violations des traitements de données à caractère personnel », *Les obligations légales de cybersécurité et de notifications d'incidents*, F. Dumortier et Valery Vander Geeten (dir.), Bruxelles, Politeia, 2019, p. 16 à 20.

[128] C. de TERWANGNE, op. cit., p. 67 et 68.

organisationnelles que techniques[129]. Les données sont ainsi protégées contre les cyberattaques grâce à cette disposition du RDPD. Sur la base de l'article 32 su RGPD, le responsable du traitement et le sous-traitant doivent prendre des mesures de sécurité, sous peine de sanctions[130].

Chapitre II. Droit à la liberté d'expression

La liberté d'expression est un droit fondamental garanti par de nombreux instruments, tels que la Constitution belge, la Charte des droits fondamentaux de l'Union européenne, la Convention européenne des droits de l'homme, le Pacte international relatif aux droits civils et politiques et la Déclaration universelle des droits de l'homme[131].

À titre d'illustration, l'article 10 de la Convention européenne des droits de l'homme consacre la liberté d'expression. Cette disposition maintient que toute personne y a droit. Nous pouvons donc en conclure qu'autant les personnes physiques que morales peuvent revendiquer le bénéfice de ce droit. Une ingérence dans ce droit n'est ainsi permise que si les conditions de légalité, du but légitime et de la nécessité sont respectées[132]. À mon estime, ces conditions ne peuvent être rencontrées lorsqu'une cyberattaque a lieu. En effet, le cyberdélinquant ne peut, selon moi, revendiquer le bénéfice d'une ingérence dans le droit à la liberté d'expression de sa victime.

---

[129] L.-A. NYSSEN, "La conformité des entreprises d'assurance au RGPD", *Bull. ass.*, liv. 2, Kluwer, 2023, p. 150 ; C. de TERWANGNE, « Titre 3. Les principes relatifs au traitement des données à caractère personnel et à sa licéité. Chapitre 1. Principes de base de la protection des données », *Le règlement général sur la protection des données (RGPD/GDPR)*, 1e éd., Bruxelles, Larcier, p. 115.

[130] L. GERARD, « Titre 13. Les sanctions en cas de non-respect du RGPD : vers une plus grande effectivité de la protection des données à caractère personnel ? », *Le règlement général sur la protection des données (RGPD/GDPR)*, 1e éd., Bruxelles, Larcier, 2018, p. 641 ; Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), art. 83, *J.O.U.E.*, L 119/1, 4 mai 2016.

[131] L. STOLLE, « Chapter 4. Freedom of Expression and Digital Technologies », *An Introduction to Law & Technology*, E. Lievens, C. Vander Maelen et S. Verschaeve (dir.), 2e éd., Belgique, Owl Press Legal, 2023, p. 80.

[132] F. ERNOTTE, « Chapitre 3. Liberté d'expression », *Droit des réseaux sociaux*, 1e éd., Bruxelles, Larcier, 2021, p. 42 à 53.

Conclusion

Comme nous avons pu le constater à travers ce présent travail, les cyberattaques représentent une préoccupation certaine pour les différents acteurs de notre société. Divers instruments touchant, de près ou de loin, les cyberattaques ont été adoptés afin de lutter contre ce phénomène préjudiciable. Toutefois, l'ingéniosité des cybercriminels provoque la multiplication des types de cyberattaques, de sorte que ledit phénomène s'étend davantage. Les nouvelles technologies sont de plus en plus innovantes, ainsi les instruments juridiques doivent perpétuellement être mis à jour.

Pour rappel, la question de recherche générale annoncée dans l'introduction était la suivante : « *Le droit apporte-t-il une réponse adéquate face aux conséquences croissantes des cyberattaques, en assurant une réponse nationale et européenne conforme aux prescrits internationaux, en encadrant la responsabilité des acteurs concernés, en privilégiant la prévention, tout en protégeant les droits fondamentaux ?* ». Après avoir suivi l'acheminement de l'exposé, une réponse va être offerte en divisant la question de recherche principale en différentes sous-questions correspondant à chacune des cinq parties de ce travail.

La première partie de ce travail avait pour objectif de dégager les conséquences des cyberattaques après analyse de cette notion. Force est de constater que les conséquences économiques et sociales de cette forme de cybercriminalité, en ce que nous l'avons déterminé, sont multiples. Les cyberattaques peuvent engendrer la commission d'autres infractions, causer des pertes financières importantes, d'autant plus lorsqu'il s'agit d'une entreprise, et avoir des effets psychologiques néfastes.

La deuxième partie du présent travail s'est concentrée sur le cadre légal répressif consacré par le droit international, le droit de l'Union européenne et le droit belge. À travers les éléments rapportés, nous pouvons nettement considérer que la Convention de Budapest impose, d'une certaine façon, la marche à suivre en matière de cybercriminalité. Le droit de l'Union européenne, par sa Directive 2013/40, s'y conforme en grande majorité. De plus, notre droit pénal belge n'a cessé de s'adapter en prévoyant des infractions, en matière de criminalité informatique, assorties de peines adéquates.

Troisièmement, nous avons bien évidemment découvert que la responsabilité pénale des personnes morales pouvait être engagée en cas de cyberattaque commise, de sorte que la répression y en découle. De plus, la responsabilité internationale de l'État auteur peut également être mise en œuvre dans le cadre du droit international public. Cette responsabilité est évidemment encadrée par la loi.

La prévention a fait l'objet d'une quatrième partie. En effet, à cet effet, nous percevons rapidement que la question de la cybersécurité est relativement prise au sérieux, surtout au niveau de l'Union européenne. Assurément, la Convention de Budapest et la nouvelle Convention des Nations Unies contre la cybercriminalité assurent une prévention en ce que la coopération est mise en avant. Néanmoins et selon moi, ces instruments demeurent répressifs avant tout. L'Union européenne, quant à elle, a drastiquement contribué au déploiement de la cybersécurité avec l'adoption de nombreux instruments de droit dérivé. Concernant la question de l'efficacité de ces dispositifs, il reste compliqué selon moi de prétendre à une

réelle efficacité lorsque nous apprenons que ce phénomène est en expansion et que les types de cyberattaques se multiplient au fil du temps.

Enfin, les dernières considérations ont porté sur le droit au respect de la vie privée et le droit à la liberté d'expression. La protection des données personnelles est à cet égard suffisamment protégée depuis l'avènement du RGPD. Des sanctions ont d'ailleurs été mises en place par cet instrument, de manière à garantir les droits fondamentaux des citoyens. De plus, concernant la question plus délicate de la liberté d'expression, celle-ci semble, à mon sens, protégée de manière moindre.

En définitive, le mot de la fin serait prudence. Il est du devoir du législateur de s'adapter aux prochaines avancées dans la matière, de sorte à encadrer la responsabilité pénale des auteurs. Le droit international et les différents droits nationaux se doivent d'être complémentaires afin de vivre en harmonie.

BIBLIOGRAPHIE

Législation

Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001, S.T.E., n°185.

Directive 2013/40/UE du Parlement et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, *J.O.U.E.*, L 218/8, 14 août 2013.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119/1, 4 mai 2016.

Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.U.E.*, L 194/1, 19 juillet 2016.

Règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menaces l'Union ou ses États membres, *J.O.U.E.*, L 129 1/1, 17 mai 2019.

Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant les mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, *J.O.U.E.*, LI 129/13, 17 mai 2019.

Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n°526/2013 (règlement sur la cybersécurité), *J.O.U.E.*, L 151/15, 7 juin 2019.

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n°910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), *J.O.U.E.*, L 333/80, 27 décembre 2022.

Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, *J.O.U.E.*, L 333/1, 27 décembre 2022.

Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences

techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance, *J.O.U.E.*, 18 octobre 2024.

Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n°168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience), *J.O.U.E.*, 20 novembre 2024.

Règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité), *J.O.U.E.*, 15 janvier 2025.

Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 17 mai 2024.

Loi du 3 août 2012 portant assentiment à la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, *M.B.*, 21 novembre 2012.

A.R. du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, *M.B.*, 21 novembre 2014.

Arrêté royal 9 juin 2024 exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 24 juin 2024.

Travaux parlementaires

Projet de loi portant assentiment à la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001, *Doc.*, Sén., 2011–2012, n°5-1497/1. Document parlementaire n°5-1497/1.

Jurisprudence

Cour eur. D.H., arrêt *Rotaru c. Roumanie*, 4 mai 2000.

Cour eur. D.H., arrêt *S. et Marper c. Royaume-Uni*, 4 décembre 2008.

Trib. entr., Bruxelles (néerl.), 29 juin 2023, *R.G.D.C.*, 2024, liv. 9, p. 516

Civ. Bruxelles (fr.) (11e ch.), 18 février 2025, *J.T.*, 2025, liv. 7018, p. 218.

Doctrine

ALBERINI, A. *et al*., « Chronique de législation 2013 », *Rev. Aff. Eur*., 2014/1, p. 261.

BENATAR, M., "The use of Cyber force : Need for Legal Justification ?", *Goettingen Journal of International Law I*, 2009, 3, p. 379.

BENATAR, M. et FONTAINE, M., « Cyber-attaques : aperçu du cadre juridique national », *Questions juridiques d'actualité en lien avec la défense / Actuele juridische vraagstukken met betrekking tot defensie*, N. Angelet *et al*. (dir.), Bruxelles, die Keure / la Charte, 2017.

BOGAERT, O., DECHAMPS, F. et LAMBILOT, C. (dir.), *Cybercriminalité : état des lieux*, Bruxelles, Anthemis, 2016.

BOSLY, S. et FLORE, D., « Chronique de droit pénal européen », *J.D.E*., 2018/5, n°249, p. 199 à 206.

BRUNI, A., « Chapter 11. Promoting Coherence in the EU Cybersecurity Strategy », *Security and Law*. *Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security,* A. Vedder *et al.* (dir.), Cambridge, Intersentia Ltd, 2019.

CAROLUS, P., *et al*., « Chapitre 3. Criminalité informatique », *Droit pénal des affaires*, 2e éd., Bruxelles, Larcier-Intersentia, 2024.

CERÉ, J.-P., RASCAGNÈRES, J. M. et VERGÈS, E. (dir.), *Droit pénal et nouvelles technologies*, Paris, L'Harmattan, 2015.

CLOUNER, P., « Chapitre 7. Approche du Centre pour la Cybersécurité Belgique en matière de protection des personnes (vulnérables) dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, H. Jacquemin et M. Nihoul (dir.), Bruxelles, Larcier, 2018.

de MAISON ROUGE, O., « Introduction. De la cyberdélinquance à la cyberguerre », *Les cyberrisques. La gestion juridique des risques à l'ère immatérielle*, 2e éd., Paris, LexisNexis, 2024.

DUMORTIER, F. et VANDER GEETEN, V. (dir.), *Les obligations légales de cybersécurité et de notifications d'incidents*, Belgique, Politeia, 2019.

DUPONT, B., GAUDREAU, F. et PRATES, F.,, « La cybercriminalité : état des lieux et perspectives d'avenir », *Droits de la personne : La circulation des idées, des personnes et des biens et*

capitaux, Actes des journées strasbourgeoises 2012 organisées par l'Institut canadien d'études juridiques supérieures, Cowansville, Yvon Blais, Cowansville, 2013.

ERNOTTE, F., *Droit des réseaux sociaux*, 1e éd., Bruxelles, Larcier, 2021.

FRANSSEN, V., « Le nouveau Code pénal et la responsabilité pénale des personnes morales : une regrettable non-réforme ? », *Rev. Dr. ULiège*, 2024/2, p. 230.

GRANGE, M. et NORODOM, A.-T. (dir.), Cyberattaques et droit international. Problèmes choisis, Paris, A. Pedone, 2018.

HENROTTE, J.-F. et POULLET, Y., « La protection des données (à caractère personnel) à l'heure de l'Internet », *CUP109 – Protection du consommateur, pratiques commerciales et T.I.C.*, J. Laffineur (dir.), Belgique, Anthemis, 2009.

JACOB, P., « La responsabilité internationale de l'État du fait des cyberattaques », *La souveraineté numérique*, B. Bertrand et G. Le Floc (dir.), 1e éd., Bruxelles, Bruylant, 2024.

JUSTERS, W., "Cyber Security at Sea", *I.H.T. – C.I.T. – I.T.T.*, 2017/4, p. 481.

KERKHOFS, J. et van LINTHOUT, P., « Inleiding tot het materieel en strafprocedureel cyberstrafrecht : uitdagingen voor de advocatuur », *Internet &/@ Recht*, Gand, Larcier, 2013.

KNOCKAERT, M., « Chronique de législation. La cybersécurité », *R.D.T.I.*, 2023/3-4.

LEROUX, O., « Chapitre IX. Criminalité informatique », *Les infractions – Volume 1*, 2e éd., Bruxelles, Larcier, 2016.

LIDDICOAT, J., « Part II. New Challenges in the Digital Era. Chapter 8. Human Rights and Artificial Intelligence », *Human Rights and the Internet*, Cambridge, Intersentia, 2021.

LIEVENS, E., VANDER MAELEN, C. et VERSCHAEVE, S. (dir.), *An Introduction to Law & Technology*, Belgique, Owl Press Legal, 2024.

MOUNIER, G., « Enquêtes internationales et poursuites des cybercriminels – Etat des lieux des défis juridiques », *Obs. Bxl.*, 2016/3, n° 105, p. 16.

NYSSEN, L.-A., "La conformité des entreprises d'assurance au RGPD", *Bull. ass.*, liv. 2, Kluwer, 2023, p. 150.

PANETTA, L.-E., « Section 2 : L'avènement des cyberattaques », *Cyberattaques et droit international public : de la négociation entre Etats à l'intégration des acteurs privés pour parvenir à la cyberpaix ?*, L. Baudin (dir.), Paris, L'Harmattan, 2023.

PUTZ, J.-L., « Introduction », *Cybercriminalité*, 1e éd., Windhof, Larcier Luxembourg, 2019.

QUEMENER, M., « Chapitre 2. Analyse des cyberfraudes », *Établissements financiers & cyberfraudes*, Paris, Revue Banque Édition, 2011.

QUEMENER, M., *Le droit face à la disruption numérique*, Gualino, 2018, n° 195.

ROSIER, K. et de TERWANGNE, C. (dir.), Le règlement général sur la protection des données (RGPD/GDPR), 1e éd., Bruxelles, Larcier, 2018.

SOCIETE FRANCAISE POUR LE DROIT INTERNATIONAL, *Internet et le droit international*, Paris, A. Pedone, 2014.

TAMAS, R., « The data processor's new obligations under the GDPR : a restored balance or a shift of responsabilities ? », *Data Protection & Privacy*. Le GDPR dans la pratique / De GDPR in de praktijk, N. RAGHENO (dir.), Belgique, Anthemis, 2017.

TRULLEMANS, J., « Phénomène des ransomware », *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, C 380, p. 542.

TURGIS, S., « Les valeurs du conseil de l'Europe appliquées à internet », *Droits et souveraineté numérique en Europe*, A. Blandin (dir.), Bruxelles, Bruylant, 2016.

van DAELE, G., « Cyberrisques : un fléau jamais bien loin », *Assur. présent*, liv. 3, Kluwer, 2023, p. 9.

VANDER GEETEN, V., « Hacking « éthique » en droit pénal belge », *Société numérique et droit pénal*, D. Flore et V. Franssen (dir.), 1e éd., Bruxelles, Bruylant, 2019.

van SOEST, H., « Chapitre XIV. Cybersecurity in the European Electricity System : The Role of the NIS2 Directive", *European Energy Law Report XV*, C. Banet et M.-M. Roggenkamp (dir.), 1e éd., Bruxelles, Intersentia, 2025.

WATIN-AUGOUARD, M., « La sécurité privée et la cyberdélinquance internationale », *Les aspects internationaux de la sécurité privée*, C. Aubertin et X. Latour (dir.), mare & martin, 2016, p. 160.

WATIN-AUGOUARD, M., « Préface », O. de MAISON ROUGE, *Les cyberisques. La gestion juridique des risques à l'ère immatérielle*, Paris, LexisNexis, 2018.

WAUTELET, M., *Les cyberconflits. Internet, autoroutes de l'information et cyberespace : quelles menaces ?*, Bruxelles, GRIP, 1998.

X, « Attaques visant les systèmes d'information », *Obs. Bxl*., 2014/1, n° 95, p. 60.

Autres sources

CONSEIL DE L'EUROPE, « Rapport explicatif de la Convention sur la cybercriminalité » disponible sur https://rm.coe.int/16800ccea4, 23 novembre 2001.

EUR-LEX, « Mesures restrictives de l'Union européenne contre les cyberattaques » disponible sur https://eur-lex.europa.eu/legal-content/FR/LSU/?uri=celex:32019R0796, 18 mai 2022.

X, « Quelles sont les conséquences d'une cyberattaque sur une entreprise ? » disponible sur https://www.cnfce.com/dossier/consequences-cyberattaque-entreprise-interview-expert-cybercriminalite, 4 octobre 2022.

WALLONIE – BRUXELLES INETRNATIONAL, « Le phishing, principale porte d'entrée des cybercriminels », disponible sur https://www.wbi.be/fr/actualites/phishing-principale-porte-dentree-cybercriminels, 7 novembre 2023.

EUR-LEX, « Résilience opérationnelle numérique du secteur financier » disponible sur https://eur-lex.europa.eu/legal-content/FR/LSU/?uri=CELEX:32022R2554, 10 janvier 2024.

ENISA, « ENISA THREAT LANDSCAPE 2024 », disponible sur https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf, septembre 2024.

INTERPOL, « Interpol salue l'adoption de la Convention des Nations Unies contre la cybercriminalité » disponible sur https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2024/INTERPOL-salue-l-adoption-de-la-Convention-des-Nations-Unies-contre-la-cybercriminalite, 23 décembre 2024.

NATIONS UNIES, « La Convention sur la cybercriminalité, pour un monde numérique et physique plus sûr » disponible sur https://news.un.org/fr/story/2024/12/1151706, 25 décembre 2024.

CONSEIL DE L'EUROPE, « Conventions sur la cybercriminalité : La Convention de Budapest et le projet de traité des Nations Unies » disponible sur https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1fb99, 27 août 2024.

X, « Quels sont les différents types de programmes malveillants ? » disponible sur https://www.kaspersky.fr/resource-center/threats/types-of-malware, *s. d.*, consulté le 8 mars 2025.

MICROSOFT, « Qu'est-ce qu'un logiciel malveillant ? » disponible sur https://www.microsoft.com/fr-be/security/business/security-101/what-is-malware, *s. d.*, consulté le 8 mars 2025.

X, « Malware ou logiciel malveillant : définition et solutions de protection » disponible sur https://www.cyber-cover.fr/guides/assurance-cyber-risques/les-types-de-cyber-risques-5-exemples-dattaques-malveillantes/malware-ou-logiciel-malveillant-definition-et-solutions-de-protection, *s. d.*, consulté le 8 mars 2025.

CENTRE FOR CYBERSECURITY BELGIUM, « Miser sur la cybersécurité. Rapport CCB 1/1/2023 – 30/9/2023 » disponible sur https://ccb.belgium.be/sites/default/files/2024-10/CCB%20REPORT%202023_FR.pdf, *s. d.*, consulté le 9 mars 2025.

SPF ECONOMIE, « Votre ordinateur est bloqué et vous devez payer une rançon pour le débloquer (ransomware) » disponible sur https://economie.fgov.be/fr/themes/protection-des-consommateurs/stop-arnaques/formes-darnaques/vous-avez-recu-un-message/votre-ordinateur-est-bloque-et, *s. d.*, consulté le 9 mars 2025.

X, « Conséquences d'une cyberattaque » disponible sur https://www.cyberimpact.eu/consequences-dune-cyberattaque, *s. d.*, consulté le 9 mars 2025.

X, "Cyberattaque en entreprise : quels sont les risques ?" disponible sur https://www.entreprises.cci-paris-idf.fr/web/pme/cyberattaque-en-entreprise-quels-sont-les-risques-, s. d., consulté le 12 mars 2025.

GERY, A. et NORODOM, A.-T., « ONU : adoption d'une convention sur la lutte contre la cybercriminalité » disponible sur https://www.leclubdesjuristes.com/international/onu-adoption-dune-convention-sur-la-lutte-contre-la-cybercriminalite-8783/, 16 janvier 2025.

SPF ECONOMIE, "Phishing : ne mordez pas à l'hameçon », disponible sur https://news.economie.fgov.be/248457-phishing-ne-mordez-pas-a-l-hamecon, 1 avril 2025.

CENTRE FOR CYBERSECURITY BELGIUM, « Règlementation » disponible sur https://ccb.belgium.be/fr/reglementation, *s. d.*, consulté le 28 avril 2025.