INTERNATIONAL JOURNAL OF DIGITAL AND DATA LAW

REVUE INTERNATIONALE DE DROIT DES DONNÉES ET DU NUMÉRIQUE

ISSN 2553-6893

IMODEV
LES ÉDITIONS

Vol. 9 - 2023

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

Droits d'utilisation et de réutilisation

Licence Creative Commons – Creative Commons License -

CC-**BY-NC-ND**

Attribution
Pas d'utilisation commerciale – Non Commercial
Pas de modification – No Derivatives

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons CC-BY-NC-ND :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-BY-NC-ND:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

LA LUTTE CONTRE LA CYBERCRIMINALITÉ SUR LE DARKNET : L'EXEMPLE DU PIRATAGE INFORMATIQUE ET DU RECEL DE DONNÉES À CARACTÈRE PERSONNEL

par **Sophie EVERARTS DE VELP**, Avocate au barreau de Bruxelles.

Depuis quelques années, force est de constater la croissance exponentielle de la cybercriminalité. Les attaques ne cessent de se développer, devenant plus sophistiquées, ciblées, massives, et souvent non détectées[1]. En 2021, la Police Fédérale belge a fait état de près de 48 000 infractions liées à la criminalité informatique (accès non autorisé à un système informatique[2], fraude informatique[3], faux en informatique[4], etc.), contre 35 000 en 2019[5]. Ainsi, l'accès non autorisé à un système informatique[6] (ou en anglais, *hacking*) et recel de données[7], sont devenus monnaie courante : Les pirates informatiques ou *hackers*[8] regorgent d'ingéniosité pour vendre de plus en plus de données volées. Cette contribution vise à comprendre les différentes notions qui s'y rapportent, les techniques utilisées, les raisons, sanctions et solutions pour protéger notre vie privée.

Dans un premier temps, nous infiltrerons l'univers du darknet qui possède un lien fort avec ces infractions, afin de mieux comprendre comment y accéder et comment l'utiliser. Dans un second temps, nous développerons la notion de donnée à caractère personnel et analyserons leur portée sur Internet et la protection par le règlement général sur la protection des données[9] (« RGPD ») en cas d'accès non autorisé à un système informatique. Ensuite, nous explorerons la législation belge

[1] ENISA, *Threat Landscape 2020*, consulté en ligne le 5 juillet 2022, disponible sur [https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends].
[2] Art. 550 *bis* du Code Pénal.
[3] Art. 504 *quater* du Code Pénal.
[4] Art. 210 *bis* du Code Pénal.
[5] Police Fédérale de Belgique, *Statistiques policières de criminalité*, consulté en ligne le 26 décembre 2022, disponible sur : [https://www.stat.policefederale.be/assets/pdf/crimestat/nationaal/rapport_2021_trim4_nat_belgique_fr.pdf].
[6] Art. 550 bis du Code Pénal.
[7] Art. 550 bis §7 du Code Pénal.
[8] *Dictionnaire Larousse*, consulté en ligne le 6 juillet 2021 : « Personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique ».
[9] 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.

encadrant ces infractions. Par la suite, nous tenterons de comprendre les motivations des cybercriminels, entre gain d'argent facile, chantage, lancement d'alerte ou usurpation d'identité. Nous nous poserons également la question de la levée de l'anonymat sur Internet, et les conséquences qui en découlent concernant la recherche des cybercriminels.

§1 – Le Darknet

A) Notions

Internet est souvent comparé à un iceberg. D'une part, la partie émergée de ce dernier fait référence à la partie visible d'Internet, accessible via les moteurs de recherche, il s'agit du *surface web*. D'autre part, les contenus non indexés par les moteurs de recherche forment le *deepweb* (la partie immergée de l'iceberg). Le darknet fait référence à la face sombre d'Internet, comprise dans le *deepweb*, où la cybercriminalité est très présente. En effet, on estime à plus de 90% des activités sur Internet se déroulent sur le *deepweb* et darknet.

Naviguer dans le darknet n'est pas illicite par nature. Ce n'est qu'à partir du moment où quelqu'un y commet une infraction, par exemple pour acheter ou vendre des biens illicites, il agit illégalement et, par conséquent, tous les articles du Code pénal sont susceptibles de s'appliquer.

A contrario, l'anonymat renforce la protection de la vie privée, une de nos libertés fondamentales[10]. Le darknet est souvent utilisé pour échapper à une surveillance ou pour contourner la censure dans certains pays, pour pouvoir agir en tout anonymat. En particulier, certains pays qui ne pas accès à l'entièreté des sites internet ou services existants (Facebook, Whatsapp, etc.). L'utilisation d'un VPN[11] et du darknet permet aux citoyens de ces pays d'accéder à la totalité des sites censurés étant donné que leur réelle localisation est cachée des autorités locales, en profitant d'un certain anonymat.

B) Accès

Divers accès sont possibles pour arriver sur le darknet, le plus connu et utilisé restant TOR. Ce dernier est l'abréviation de « *The Onion Router* », en référence à son mode de fonctionnement. En effet, les données y sont chiffrées et envoyées à travers de nombreux points de relais dans le monde entier, afin d'en camoufler le contenu, l'expéditeur et la localisation. TOR a été créé dans les années '90 aux USA par le US Naval Research Laboratory (armée américaine) et est désormais sous licence libre

[10] Art. 22 de la Constitution belge et Article 8 Convention européenne des Droits de l'Homme.

[11] Réseau privé assurant l'anonymat et la sécurité des informations échangées en ligne.

depuis 2004. La technique qu'utilise TOR permet une réelle sécurisation et anonymisation de l'information et *a fortiori* une meilleure protection de la vie privée. Concrètement, TOR fait passer les données sur un réseau distribué de nœuds dans le monde entier. En créant ce chemin aléatoire, cela empêche la prise de connaissance de l'adresse IP et dès lors de l'emplacement physique de l'utilisateur. TOR comprend de nombreuses pages proposant des services illégaux (drogues, armes, contenu pédopornographique, vente de données volées, etc.) auxquelles on accède en utilisant le navigateur et des noms de domaines terminant par «.onion»[12].

C) Criminalités sur le darknet

Selon l'ONU la cybercriminalité comprend « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes d'information et des données qu'ils traitent* »[13]. Nombreux sont les sites du darknet qui prennent la forme de forums idéologiques et de grands marchés de substances illégales, sur lesquels on commerce en tout anonymat par le biais de cryptomonnaies intraçables[14]. Ainsi, les recherches les plus effectuées sont liées à des activités illégales telles que l'achat de drogues (20%) ou d'armes (15%), la visualisation d'images pédopornographiques (20%), dont la plupart sont effectuées aux USA (pour un montant estimé à 5 milliards de dollars américains) ou au Royaume-Uni (2,5 milliards de dollars américains)[15].Une autre activité lucrative qui se développe de manière exponentielle sur le darknet est celle du recel de données à caractère personnel volées souvent par le biais d'un piratage informatique[16].

§ 2 – LE PIRATAGE INFORMATIQUE OU ACCÈS NON AUTORISÉ À UN SYSTÈME INFORMATIQUE

A) Notions

L'accès non autorisé à un système informatique, ou *hacking*, est érigé en infraction par le Code pénal. Cette pratique désigne le fait de s'introduire dans le système informatique de quelqu'un à son

[12] Noms de domaine utilisés sur le darknet.
[13] Congrès des Nations Unis pour la prévention du crime et le traitement des délinquants, *Délits liés à l'utilisation d'un réseau informatique*, 2000, Vienne, consulté en ligne le 28 juillet 2021, disponible sur : [https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_F.pdf].
[14] L'exemple le plus connu est celui du forum « Silk Road » qui est dorénavant fermé. ; Pour plus d'informations concernant les cryptomonnaies : Voy. *infra*.
[15] CCIC, *DarkNet : les nouveaux défis sociétaux, juridiques, technologiques et éthiques*, 14 septembre 2017, Siège de l'UNESCO, consulté en ligne le 19 juillet 2021, disponible sur : [https://ccic-unesco.org/darknet-le-cyber-espace-non-visible/].
[16] G. MOUNIER, *Enquêtes internationales et poursuites des cybercriminels – Etat des lieux des défis juridiques*, *Obs. Bxl.*, 2016/3, n° 105, p.14.

insu, sans disposer de l'autorisation requise[17]. L'élément moral consiste à savoir que l'accès se fait sans autorisation. Ce piratage peut être interne[18] ou externe[19]. À cela, plusieurs circonstances aggravantes peuvent être ajoutées : la reprise de données volées[20], l'utilisation du système piraté[21], la survenue d'un dommage[22] au système informatique ou aux données qui sont traitées[23], ainsi qu'une intention frauduleuse[24]. Notons que la tentative d'accès non autorisé à un système informatique est sanctionnée au même titre que le piratage informatique même[25] et que l'ordre de d'accéder à un système informatique sans autorisation[26], ainsi que la récidive[27] sont également condamnables. Nombreuses de ses dispositions ont été implémentées par la loi belge du 28 novembre 2000 relative à la criminalité informatique[28].

Notons qu'en 2001, la Convention sur la cybercriminalité[29] est signée à Budapest par de nombreux pays et constitue le premier traité international en la matière. L'article 2 précise que

> « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un

---

17 M.-A. BEERNAERT *et al., Les infractions : les infractions contre les biens* (volume 1), Bruxelles, Larcier, 2008, p. 410 ; L'article 550bis du Code Pénal mentionne « Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six euros à vingt-cinq mille euros ou d'une de ces peines seulement ».

18 Art. 550bis §2 du Code Pénal ; Un hacking est considéré comme interne lorsqu'il est commis par une personne ayant accès au système informatique mais qui a outrepassé les limites de son autorisation ; Corr. Louvain, 15 juin 2010, *T. Strafr.*, 2011/4, p. 270-273 ; C.C., 24 mars 2004, n°51/2004 ; Cass., 5 janvier 2011, R.G. n° F.10.1094.F. ; Cass., 24 janvier 2017, *R.W.*, 2017-2018/11, p. 415-416 ; C.E. (8 e chambre), 31 mars 2020, n° 247.360.

19 Art. 550*bis*, § 1er, alinéa 1er du Code pénal ; Un hacking est externe lorsqu'une personne qui n'y est pas autorisée, accède ou se maintient dans un système informatique ; C.C., 24 mars 2004, n°51/2004 ; Corr. Bruxelles (40 ech.), 08 janvier 2008, *J.T.*, 2008/19, n° 6311, p. 337-338 ; Corr. Anvers, 10 novembre 2014, *T. Strafr.*, 2015/2, p. 94-96 ; Civ. Dendermonde, 14 mai 2018, *Ac&M*, 2018-2019/1, pp. 80-87.

20 Art. 550*bis*, § 3, 1° du Code pénal.

21 Art. 550*bis*, § 3, 2° du Code pénal.

22 Même non-intentionnellement.

23 Art. 550*bis*, § 3, 3° du Code pénal.

24 Art. 550*bis*, § 2 du Code pénal.

25 Art. 550*bis*, § 4 du Code pénal.

26 Art. 550*bis*, § 6 du Code pénal.

27 Art. 550*bis*, § 8 du Code pénal.

28 Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B*, 03 février 2001.

29 Convention sur la cybercriminalité, 23 novembre 2001, Budapest, disponible sur [https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf] ; Son protocole additionnel a été signé à Strasbourg le 28 janvier 2003 et est disponible sur [https://rm.coe.int/1680081610].

> système informatique connecté à un autre système informatique »[30].

À cette époque, le droit belge est déjà en grande partie conforme avec les dispositions de la Convention de Budapest.
En outre, force est de constater que le caractère intentionnel prévu par le Convention de Budapest se retrouve dans l'élément moral de l'infraction prévue à l'article 550*bis*, du fait de savoir que l'accès se fait sans autorisation. L'élément moral de cette infraction a fait l'objet de nombreux débats lors de l'adoption de l'article 550 *bis*. En effet, le paragraphe 1er de cette disposition lors du premier projet de loi[31] ressemblait à celui que nous pouvons trouver actuellement dans le Code pénal. Le Sénat a ensuite proposé un amendement, en ne maintenant l'incrimination que pour le piratage informatique commis avec une intention particulière mais

> « Ceci aurait pour effet que le hacking qui se limiterait à la violation d'un système informatique par exemple pour tester un système de sécurité ne serait plus punissable. Cela ouvrirait la voie à toutes sortes d'abus, qui mettraient en danger la sécurité des systèmes informatiques »[32].

C'est pour ces raisons qu'un contre-amendement a été proposé afin de restaurer l'article initialement prévu. L'exposé des motifs du projet de loi explique qu'

> « il ne nous paraît pas opportun de décider de ne pas poursuivre une catégorie de "chevaliers blancs, qui pirateraient les réseaux informatiques animés de nobles intentions". Le piratage est en effet une pratique mettant en danger la sécurité et l'intégrité des réseaux. Nous recommandons dès lors que la loi prévoie explicitement la possibilité de poursuivre ce type d'infractions. Le présent amendement s'inscrit ainsi dans le droit fil de la tendance internationale visant à incriminer l'introduction volontaire et illicite dans un système informatique »[33].

Plus concrètement, illustrons notre propos par le *phishing* ou hameçonnage qui consiste à imiter une page web pour permettre au cybercriminel de voler des identifiants. Il constitue la technique la plus répandue pour voler des données[34]. D'après le rapport de 2020 de la Police fédérale[35], 7 424 faits ont été enregistrés en

---

30 Art. 2 de la Convention sur la cybercriminalité.
31 Projet de loi relatif à la criminalité informatique, 19 octobre 2000, *doc.parl.* disponible sur :
https://www.lachambre.be/doc/flwb/pdf/50/0213/50k0213011.pdf#search=%22550bis%20%2050k,49k%20%3Cin%3E%20keywords%22
32 *Idem.*
33 *Idem.*
34 Anti-Phishing Working Group, *Phishing activity trends report 2021*, consulté en ligne le 12 août 2021, disponible sur :
[https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf].
35 Police fédérale de Belgique, *Statistiques policières de criminalité*, consulté en ligne le 26 décembre 2022, disponible sur :

Belgique, à savoir trois fois plus qu'en 2019. Nous pouvons également citer le piratage de comptes (e-mails, réseaux sociaux, bancaires, etc.), le *doxing*[36] ou encore le *swatting*[37]. Ces méthodes constituent des exemples de la forme que pourrait prendre un piratage informatique. Elles ne sont pas reprises telles quelles dans le Code pénal mais peuvent se comprendre comme un accès non autorisé à un système informatique tombant sous le champ d'application de l'article 550 bis.

B) Données à caractère personnel

Les données à caractère personnel[38] sont toutes les informations se rapportant directement ou indirectement à une personne vivante identifiée ou identifiable[39]. En cas d'anonymisation ou pseudonymisation qui permettrait d'identifier à nouveau une personne, ces données constitueraient encore des données à caractère personnel et sont couvertes par le RGPD[40]. *A contratrio*, les données à caractère personnel rendues anonymes de telle manière que la personne ne soit pas ou plus identifiable ne relèvent plus du champ d'application du RGPD. Cependant, pour qu'une donnée soit véritablement rendue anonyme, le processus d'anonymisation doit être irréversible[41].

L'intérêt de la distinction entre anonymisation et pseudonymisation se trouve dans le fait que les données anonymisées ne tombent pas dans le champ d'application du RGPD car elles ne sont plus considérées comme des données à caractère personnel et qu'on ne peut a priori pas retrouver l'identité de l'individu[42]. Au contraire, les données pseudonymisées sont toujours considérées comme des données à caractère personnel. En cas de jeux de données mixtes, dans lesquels sont liées les données à caractère personnel et les données à caractère non-personnel, le RGPD s'applique.

La directive (UE) 2019/1024 sur les données ouvertes et la réutilisation des informations du secteur public[43] propose une

[http://www.stat.policefederale.be/statistiquescriminalite/rapports/].

[36] Où les données personnelles sont divulguées publiquement pour porter préjudice et se venger.

[37] Où la victime est dénoncée comme un dangereux criminel pour le faire arrêter par des forces d'intervention armées, comme le Swat aux États-Unis.

[38] Pour plus d'informations, voy. C. DE TERWANGNE et K. ROSIER (dir.), *Le règlement général sur la protection des données (RGPD/GDPR)*, 1e éd., Bruxelles, Larcier, 2018, pp. 60 et s.

[39] Article 4.1 du 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 (RGPD).

[40] Cons. 28 du RGPD et Art. 4.5 du RGPD.

[41] Cons. 26 du RGPD.

[42] Il existe cependant des risques, comme celui de la ré-identification en cas d'anonymisation.

[43] Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, *J.O.U.E*, 26 juin 2019.

définition formelle de l'anonymisation. Selon l'article 2.7 de la directive, on entend par anonymisation :

> « Le processus consistant à changer des documents en documents anonymes qui ne se rapportent pas à une personne physique identifiée ou identifiable, ou le processus consistant à rendre des données à caractère personnel anonymes de telle sorte que la personne concernée ne soit pas ou plus identifiable ».

Différentes techniques existent pour anonymiser les données, par exemple « *par randomisation* »[44] ou « *par généralisation* »[45]. La première consiste à modifier certaines informations dans un jeu de données de telle sorte qu'elles soient moins précises, par exemple en modifiant une date de naissance. La seconde consiste à modifier l'échelle de certaines informations, des jeux de données ou leur ordre de grandeur afin de s'assurer qu'ils soient communs à un ensemble de personnes. Cela pourrait être le cas de dates de naissance qu'on limiterait à l'année de naissance de l'individu[46].
Il est vrai que la notion d'anonymisation est souvent confondue avec la notion de pseudonymisation. Selon l'article 4.5 du RGPD, la pseudonymisation désigne :

> « le traitement de données à caractère personnel de telle sorte que les données à caractère personnel ne puissent plus être attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »[47].

Le groupe de travail Article 29 (remplacé par le Comité européen à la protection des données) soulignait que la pseudonymisation n'était pas une méthode d'anonymisation mais plutôt d'une réduction de la « *possibilité de liaison d'un ensemble de données* »[48] avec l'identité originale d'une personne concernée. La grande différence entre l'anonymisation et la pseudonymisation est donc que l'anonymisation complète ne permet plus d'identifier la personne concernée avec des moyens raisonnables. *A contrario*, il suffit de disposer d'une information initiale supplémentaire (par exemple, une clé pour déchiffrer un fichier crypté) pour identifier la personne dont les données sont pseudonymisées.

---

[44] Cette technique permet de protéger le jeu de données du risque *d'*inférence *;* Voy. Groupe 29, Avis 05/2014 du 10 avril 2014 sur les techniques d'anonymisation, WP216.
[45] Cette technique permet d'éviter l'individualisation d'un jeu de données. Elle limite également les possibles corrélations du jeu de données avec d'autres ; Voy. Groupe 29, Avis 05/2014 du 10 avril 2014 sur les techniques d'anonymisation, WP216.
[46] Groupe 29, Avis 05/2014 du 10 avril 2014 sur les techniques d'anonymisation, WP216.
[47] Art. 4.5 du RGPD.
[48] Groupe 29, Avis 05/2014 du 10 avril 2014 sur les techniques d'anonymisation, WP216.

C) Le piratage informatique comme violation de données à caractère personnel[49]

La protection des données à caractère personnel et la lutte contre l'accès non autorisé aux données en ligne est mené tant au niveau national[50] qu'européen[51].
C'est ainsi que le RGPD, définit une violation de données à caractère personnel comme

> « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données »[52].

Le *hacking* constitue dès lors une violation de données à caractère personnel étant donné son caractère illicite et l'accès sans autorisation à ces informations[53].
Par conséquent, il existe toute une procédure à suivre en cas de piratage informatique de données à caractère personnel. D'une part, le responsable du traitement[54] doit le notifier à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques[55]. D'autre part, si le *hacking* est susceptible d'engendrer un risque élevé[56] pour les droits et libertés d'une personne physique, le responsable du traitement se doit de communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais[57].

---

[49] Pour plus d'informations, voy. F. DUMORTIER, « Chapitre 1 - Les obligations de sécurité et de notification des violations des traitements de données à caractère personnel » in F. DUMORTIER *et al.* (dir.), *Les obligations légales de cybersécurité et de notifications d'incidents*, 1e éd., Bruxelles, Politeia, 2019, p. 11-96.
[50] 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 ; Code Pénal ; Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.*, 3 mai 2019.
[51] RGPD ; 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 (NIS).
[52] Art. 4.12 du RGPD.
[53] Concernant l'obligation de sécurité du RGPD, voy. Dumortier, F., « Chapitre 5. - Une obligation de sécurité axée autour des risques pour les personnes physiques » in Le règlement général sur la protection des données (RGPD/GDPR), 1e édition, Bruxelles, Larcier, 2018, p. 187-196.
[54] Art. 4.7 du RGPD.
[55] Art. 33 du RGPD.
[56] L'évaluation des risques se fait par le biais d'une analyse d'impact, tel que prévu à l'article 35 du RGPD.
[57] Art. 34 du RGPD.

§ 3 – LE RECEL DE DONNÉES PIRATÉES

Le piratage informatique et recel de données sont pénalement condamnables, qu'ils soient effectués à titre gratuit ou moyennant paiement[58]. Force est de constater que ces données volées ont souvent une valeur marchande intéressante car elles permettent aux *hackers* d'optimiser leurs campagnes de *phishing*, d'usurpation d'identité, de détournement d'argent ou permettent tout simplement la revente de ces données. Cette valeur peut être facilement trouvée sur Internet. A titre illustratif, selon le Dark Web Price Index[59], en 2022, il est possible d'acheter sur le darknet une carte de crédit volée pour environ 25$, les détails d'un compte PayPal pour 150$, un compte Facebook *hacké* pour 65$, 1000 followers ou likes Instagram pour 5$, un abonnement Netflix d'un an pour 4$ ou encore des bases de données d'un millier d'adresses e-mails pour 10$. Ces montants pour la plupart insignifiants peuvent étonner vu l'impact que leur objet pourrait avoir sur la vie privée et le portefeuille du propriétaire de ses données volées. De surcroît, il a été estimé que le volume du recel de données en 2021 était beaucoup plus important qu'en 2020, les vendeurs de fausses cartes d'identité et de crédit faisant état de ventes de plusieurs milliers d'unités. Certains experts en cybercriminalité affirment que

> « non seulement la quantité, mais la variété des articles à acheter s'est également accrue, comme des comptes cryptographiques piratés et des services Web tels que les comptes Uber »[60].

Bien que l'article 505 du Code pénal incrimine le recel, notre regard se tourne plutôt vers l'article 550 *bis* du Code pénal belge qui traite des infractions contre des systèmes informatiques et des données qui y sont stockées. En effet, la disposition en son paragraphe 7 mentionne que

> « Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement »[61].

---

[58] C. MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *Rev. dr. pén.*, *op.cit.*

[59] Par exemple, le site https://www.privacyaffairs.com/dark-web-price-index-2021/ reprend la valeur de nombreuses catégories de données personnelles en 2021. Consulté le 22 juillet 2021.

[60] *Ibid.*

[61] Art. 550 *bis*, § 7 du Code pénal. ; Pour plus d'informations, voy. V. VANDER GEETEN, « La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilités » in F. DUMORTIER *et al.* (dir.), *Les obligations légales de cybersécurité et de notifications d'incidents*, *op.cit.*, pp. 215-265.

Le recel de donnée*s* piratées constitue une infraction *per se* et peut être poursuivie indépendamment de l'infraction d'accès non autorisé à un système informatique, ceci ayant pour conséquence qu'un receleur de données pourrait être condamné alors même que le pirate informatique serait inconnu[62]. Dans le cas d'utilisations successives des données piratées, chaque cybercriminel pourrait être reconnu comme receleur, pour autant qu'il ait été informé du caractère illicite de la provenance des données. Cependant, l'action ne sera pas considérée comme un recel informatique lorsque l'auteur s'est procuré des données informatiques auprès d'une personne habilitée à y accéder[63].
Ici, l'élément matériel de l'infraction consiste en la détention, la révélation, la divulgation ou l'usage de données, alors que l'élément moral est constitué par la conscience que ces données aient été obtenues à la suite d'un piratage informatique.

§ 4 – LES MOTIVATIONS

A) Motivation financière

Il convient de se poser la question des raisons qui poussent ces individus à commettre de telles infractions. La première qui pourrait venir à l'esprit est celle de l'« argent facile ». L'ENISA confirme cette intuition en estimant dans son rapport de 2020 que pour la majorité des attaques recensées, la motivation est de nature financière[64]. Dans ces cas-ci, l'intention frauduleuse mentionnée comme circonstance aggravante à l'article 550 *bis* du Code Pénal pourrait être retenue.

B) Vengeance et chantage

Outre cette possibilité de gain aisé, d'autres motivations pourraient être évoquées. Tout d'abord, la vengeance et le chantage. Certains *hackeurs* profitent de la faiblesse de leurs victimes pour leurs soutirer de l'argent en indiquant avoir en leur possession leurs données (logins, mots de passe, photo, vidéos, etc.). Par ailleurs, une autre menace grandit, celle des rançongiciels, programmes malveillants permettant aux attaquants de prendre le contrôle à distance d'un ordinateur ou d'un système d'information. Ces logiciels rendent la consultation ou l'utilisation des données impossibles, sans le paiement d'une rançon[65]. Ici

---

[62] J.-P. COLLIN, E.-R. FRANCE, F. ROGGEN et J. SPREUTELS, « Chapitre 5 - La criminalité informatique », *op.cit.*, p. 985 ; O. LEROUX, « Criminalité informatique spécifique », in *Les infractions – Volume 1*, 2e éd., Bruxelles, Larcier, 2016, p. 496.
[63] V. VANDER GEETEN, « Chapitre 5 - La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilités » in F. DUMORTIER *et al.* (dir.), *Les obligations légales de cybersécurité et de notifications d'incidents*, *op.cit.*, p. 237.
[64] ENISA, *Threat Landscape 2020*, consulté en ligne le 5 juillet 2021, disponible sur https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.
[65] *Ibid.*

aussi, l'intention frauduleuse mentionnée comme circonstance aggravante à l'article 550 *bis* du Code Pénal pourrait être retenue.

C) Lancement d'alerte

Ensuite, le phénomène des lanceurs d'alerte mérite d'être évoqué[66]. Le Conseil de l'Europe définit cette notion de lanceurs d'alerte comme étant les personnes qui signalent ou révèlent des informations et actes répréhensibles qu'elles ont constatés dans le secteur public comme dans le secteur privé[67]. Ces actes dénoncés constituent des menaces à l'intérêt général, tels que les faits de corruption, les infractions pénales, les détournements de pouvoirs, les menaces pour l'environnement, la santé publique, la sécurité nationale, les atteintes aux droits de l'homme, aux droits des travailleurs, aux autres droits sociaux, à l'État de droit ainsi que les actes visant à dissimuler toute atteinte de ce type[68]. Ces lanceurs d'alerte, dont les plus médiatisés ont été Chelsea Manning, Julian Assange, Antoine Deltour, ou Edward Snowden, se présentent comme des garde-fous de nos démocraties, garantissant que les détournements nocifs à celles-ci ne restent impunis. La multiplication des lanceurs d'alerte ces dernières années et l'impact des affaires révélées confirme l'importance de leur protection[69].

À cette fin, une directive européenne[70] est entrée en vigueur en 2019. La loi de transposition belge du 28 novembre 2022 entrera en vigueur le 15 février 2023[71]. Ces dispositions permettent la protection des individus qui accèderaient à des données sans autorisation afin de signaler des violations du droit de l'Union, pour autant qu'ils entrent dans le champ d'application matériel et personnel de la directive. Deux conditions supplémentaires viennent s'ajouter pour bénéficier de la protection[72] : d'une part des motifs raisonnables de croire que les informations signalées sur les violations étaient véridiques au moment du signalement et d'autre part qu'il y a eu un signalement (interne, externe ou une divulgation publique). Des conditions complémentaires s'appliquent en cas de divulgation publique : la personne doit avoir des motifs raisonnables de croire que

---

66 Pour plus d'informations, voy. A. LACHAPELLE, *La dénonciation à l'ère des lanceurs d'alerte fiscale*, 1e éd., Bruxelles, Larcier, 2021.

67 Recommandation du 30 avril 2014 du Conseil de l'Europe CM/ Rec(2014)7 du Comité des ministres aux États membres sur la protection des lanceurs d'alerte.

68 Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (Directive lanceurs d'alerte).

69 A. LACHAPELLE, *La dénonciation à l'ère des lanceurs d'alerte fiscale*, *op.cit.*

70 Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (Directive lanceurs d'alerte).

71 Loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé, *M.B.*, 15 décembre 2022.

72 Art. 6 paragraphe 1 de la Directive lanceurs d'alerte.

> « i) la violation peut représenter un danger imminent ou manifeste pour l'intérêt public, comme lorsqu'il existe une situation d'urgence ou un risque de préjudice irréversible; ou ii) en cas de signalement externe, il existe un risque de représailles ou il y a peu de chances qu'il soit véritablement remédié à la violation, en raison des circonstances particulières de l'affaire, comme lorsque des preuves peuvent être dissimulées ou détruites ou lorsqu'une autorité peut être en collusion avec l'auteur de la violation ou impliquée dans la violation »[73].

Cependant, cette directive ne protège dès lors que les individus qui dévoileraient des violations du droit de l'Union et du droit national et non pas les individus qui divulgueraient simplement des données à caractère personnel, sans que ces dernières ne permettent de révéler une atteinte ou droit de l'Union ou au droit national.

Cette situation soulève la question de savoir ce qu'il en est des lanceurs d'alerte qui divulgueraient publiquement des informations et tomberaient sous le champ d'application de la directive, mais qui le feraient également en vue de monnayer ces données de façon malveillante. Bien que la motivation ne soit pas un critère repris dans la directive, elle mentionne indirectement cette possibilité en son article 21 paragraphe 3 en indiquant que

> « les auteurs de signalement n'encourent aucune responsabilité en ce qui concerne l'obtention des informations qui sont signalées ou divulguées publiquement, ou l'accès à ces informations, à condition que cette obtention ou cet accès ne constitue pas une infraction pénale autonome »[74].

Dans l'hypothèse où cette obtention ou cet accès constitue une infraction pénale autonome, la responsabilité pénale continue d'être régie par le droit national applicable. Cela laisse à penser que les lanceurs d'alertes receleurs (à titre onéreux) ne pourraient pas être protégés par la directive, étant donné que la décision de monnayer les données *hackées* constituerait l'intention frauduleuse (dol général) mentionnée dans l'alinéa 2 de l'article 550*bis* § 1 du Code pénal. A partir du moment où l'individu lance l'alerte mais décide de le faire également pour pouvoir en soutirer de l'argent frauduleusement, il conviendrait de ne plus le considérer comme un réel lanceur d'alerte, au sens de la directive.

D) Commission d'autres infractions

Enfin, une autre cause du *hacking* et recel de données serait la facilitation de la commission d'autres infractions, par exemple, la fraude à la carte bancaire (*carding*), l'usurpation d'identité ou

[73] Art. 15 de la Directive lanceurs d'alerte.
[74] Art. 21 par 3 de la Directive lanceurs d'alerte.

spoofing. Cette dernière arnaque consiste à tromper un destinataire d'email en se faisant passer pour un proche, un supérieur ou une entreprise, en visant une personne bien précise et en la poussant à cliquer sur un lien et de fournir ses identifiants ou à envoyer une somme d'argent. Par ailleurs, le vol de données de carte bancaire ou d'autres éléments d'identité permet aux pirates informatiques de pouvoir les vendre sur le darknet à des acheteurs souvent malintentionnés qui souhaiteraient utiliser ces données à caractère personnel pour utiliser l'identité de la victime. En effet, sous couvert d'une fausse identité, de nombreuses escroqueries sont dorénavant possibles : Création de faux comptes de réseaux sociaux pour attirer des profils naïfs et leur soutirer de l'argent ; fausses annonces, achats en ligne, cyberharcèlement, diffusion d'informations diffamatoires, etc. Dans tous ces exemples, l'intention frauduleuse pourrait être retenue comme circonstance aggravante.

§ 5 – PROBLÉMATIQUE DE L'ANONYMAT SUR INTERNET

A) Controverse

Début 2021, le président français Emmanuel Macron avait émis le souhait d'une « *levée progressive de toute forme d'anonymat* »[75]. Quelque temps auparavant lors de l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, il avait déjà annoncé que

> « nos gouvernements, nos populations ne vont pas pouvoir tolérer encore longtemps les torrents de haine que déversent en ligne des auteurs protégés par un anonymat devenu problématique »[76].

Par ailleurs, certains députés français LREM[77] avaient suggéré

> « que soit envisagée l'hypothèse de créer une obligation légale de recueil des pièces d'identité à l'occasion de la création de comptes sur les réseaux sociaux, à l'image de ce qui existe sur d'autres plateformes telles que AirBnb »[78].

Ces propos ont provoqué à un débat houleux entre les différentes parties aux pouvoirs et défenseuses de libertés individuelles.
Bien que ces débats aient eu lieu dans un contexte de cyberharcèlement et de lutte contre le terrorisme et les contenus incitant à la haine, ils posent la question de la levée de l'anonymat sur Internet afin de lutter contre la cybercriminalité. Plus

[75] Discours prononcé devant les maires réunis pour le deuxième acte du grand débat national au Palais des congrès de Souillac, France.
[76] Discours prononcé lors de l'Appel de Paris pour la confiance et la stabilité dans le cyberespace.
[77] Parti politique français La République en marche.
[78] https://www.developpez.com/actu/244523/Des-deputes-LREM-veulent-imposer-une-piece-d-identite-a-la-creation-de-comptes-sur-les-reseaux-sociaux-une-tentative-de-lever-l-anonymat-en-ligne/, consulté le 10 août 2021.

précisément, il s'agit de la facilitation et l'accélération de la levée de l'anonymat en cas de délit.

B) La reconnaissance d'un droit à l'anonymat sur Internet

Mise à part certains professionnels informatiques très prudents, l'immense majorité des internautes sont traçables sur internet grâce à la série d'informations personnelles semées à longueur de navigations, et peuvent être retrouvés, à condition de s'en donner les moyens. L'anonymat sur Internet semble donc illusoire dans la pratique[79].

Cependant, de la jurisprudence européenne reconnaît ce droit à l'anonymat en ligne, en particulier en matière d'adresse IP. Citons l'arrêt Benedik c. Slovénie[80] dans lequel la Cour européenne des droits de l'Homme rappelle qu'elle

> « a déjà reconnu l'aspect de l'anonymat de la vie privée en ligne, en ce qui concerne la nature de l'activité en ligne, à laquelle les utilisateurs participent sans être nécessairement identifiables. Cette conception de l'anonymat de la vie privée est un facteur important à prendre en compte dans la présente évaluation. En particulier, il n'a pas été soutenu que le requérant ait jamais révélé son identité en relation avec l'activité en ligne en question ni qu'il était, par exemple, identifiable par le site Web via un compte ou des données de contact. Son activité en ligne faisait donc appel à un degré d'anonymat élevé, comme le confirme le fait que l'adresse IP dynamique attribuée, même si elle est visible aux autres utilisateurs du réseau, ne pouvait pas être reliée à un ordinateur en particulier sans une vérification de données par le FAI suite à une demande de la police »[81].

Dans cet arrêt, la Cour a également rappelé l'importance de l'anonymat en ligne, permettant de « *promouvoir la libre circulation des idées des informations de manière importante* »[82]. Elle ajoute cependant qu'elle

> « ne perd pas de vue la facilité, l'ampleur et la rapidité de la diffusion des informations sur Internet, ainsi que la persistance des informations une fois divulguées, ce qui peut considérablement aggraver les effets d'un discours illégal sur Internet par rapport aux médias traditionnels »[83].

---

[79] Pour plus d'exemples concrets sur l'absence d'anonymat sur Internet, en particulier en lien avec les GAFAM, voy. E. SCARAMOZZINO, « La fabrication de la publicité de la TV.2.0 face à la protection des données personnelles » in *La télévision européenne face à la TV 2.0 ?*, 1e éd., Bruxelles, Larcier, 2012, pp. 158-162.

[80] Cour eur . D .H ., arrêt Benedik c. Slovénie, 24 avril 2018, req . no 62357/14.

[81] *Idem.*

[82] *Idem.*

[83] Pour plus d'informations sur cet arrêt, voy. E. DELHAISE, A. LACHAPELLE et M. KNOCKAERT, « Chronique de jurisprudence 2018-2020. Criminalité informatique »,

Les individus qui souhaitent rester anonymes utilisent généralement le darknet qui permet cette sécurité. Cependant, le risque d'être retrouvé en cas d'infraction existe. C'est le cas notamment de nombreux cybercriminels mais aussi des gestionnaires de plateformes dédiées à certaines pratiques illégales sur le darknet qui ont été condamnés. Bien que la navigation sur le darknet ajoute une difficulté supplémentaire en cachant l'adresse IP de l'internaute[84], il existe déjà des technologies permettant de retrouver l'individu qui commettrait un délit en ligne. En effet, les moyens techniques des services de police devenant de plus en plus développés, il est désormais possible de retrouver les fournisseurs de ces services, leurs clients et les responsables des sites web ou autres *marketplaces*, qui laissent souvent des indices, sans le vouloir.

C) Vers une levée de l'anonymat et pseudonymat ?

Il convient de mettre en balance la lutte contre la cybercriminalité et la sauvegarde de nos libertés individuelles. Dans son rapport de 1997 sur l'anonymat sur Internet, le Groupe Article 29 posait déjà ce dilemme en affirmant que :

> « d'une part, la possibilité de rester anonyme est essentielle si l'on veut préserver les droits fondamentaux à la vie privée et à la liberté d'expression dans le cyberespace. D'autre part, la faculté de participer à des activités et de communiquer en ligne sans révéler son identité va à l'encontre d'initiatives lancées pour soutenir d'autres activités clés d'intérêt général tels que la lutte contre le contenu illégal et préjudiciable, la lutte contre les délits financiers ou les atteintes au droit d'auteur »[85].

Dès lors, la levée de l'anonymat et du pseudonymat sur Internet constituerait pour certains un outil efficace dans la lutte contre la cybercriminalité. La *Déclaration sur la liberté de la communication sur l'Internet*, en son principe n°7 relatif à l'anonymat dispose qu':

> « afin d'assurer une protection contre les surveillances en ligne et de favoriser l'expression libre d'informations et d'idées, les États membres devraient respecter la volonté des usagers de l'Internet de ne pas révéler leur identité. Cela n'empêche pas les États membres de prendre des mesures et de coopérer pour retrouver la trace de ceux qui sont responsables d'actes délictueux, conformément à la législation nationale, à la Convention de sauvegarde des

R.D.T.I., 2021/1-2, p. 208-209 ; J. HERVEG et J.VAN GYSEGHEM, « La protection des données à caractère personnel en droit européen – Chronique de jurisprudence (2018) », *J.E.D.H.*, 2019/1, p. 35.

[84] Pour plus d'informations sur les adresses IP et leurs protection en droit européen voy. E. DELHAISE, A. LACHAPELLE et M. KNOCKAERT, « Chronique de jurisprudence 2018-2020. Criminalité informatique », *R.D.T.I.*, 2021/1-2, p. 208-209.

[85] Recommandation 3/97 WP 6 du Groupe 29 du 3 décembre 1997, « l'anonymat sur Internet », D/5022/97.

> Droits de l'Homme et des Libertés fondamentales et aux autres traités internationaux dans le domaine de la justice et de la police »[86].

Ainsi, la protection de l'anonymat est une composante vitale de la protection tant du droit à la liberté d'expression que du droit au respect de la vie privée. En particulier, l'anonymat permet à des individus de s'exprimer sans crainte de représailles, ce qui est fondamental en particulier dans les pays où la liberté d'expression est fortement censurée. L'anonymat et le pseudonymat constituent une réelle garantie pour la démocratie, en permettant aux individus de s'exprimer librement.
L'interdiction de cette pratique pourrait mener à une société où chaque prise de parole serait identifiée, surveillée, contrôlée. Il pourrait s'en suivre la création de nombreux cas d'autocensure, par crainte de froisser les opinions de ses proches ou de subir des représailles. Si une interdiction de naviguer sous couvert d'anonymat ou pseudonymat se réalisait, cela signifierait que nul n'aurait le droit de s'exprimer sur Internet sans révéler son identité. Ce qui pourrait entraîner l'obligation pour les internautes de communiquer certaines informations sensibles aux plateformes en ligne, dont certaines sont déjà contestées par rapport à l'exploitation qu'elles font des données à caractère personnel de leurs utilisateurs.
Par ailleurs, nous pouvons constater l'existence d'un réel paradoxe entre la volonté d'être visible sur les plateformes numériques et une volonté d'être anonyme quand on le souhaite. D'une part, nombreux d'entre nous souhaitent être présents sur les réseaux sociaux afin de rester connecté avec ses amis proches ou moins proches, et de les informer par exemple sur nos dernières vacances, achats ou autres éléments de notre vie privée. D'autre part, de plus en plus d'individus prônent un droit à l'anonymat sur Internet, un droit à la vie privée et une protection totale des données à caractère personnel en ligne. Il semble nécessaire que tout un chacun prenne conscience de la quantité immense de données que nous laissons à chacun de nos passages sur un site web et tente s'il le souhaite, de limiter ces traces.

CONCLUSION

Depuis quelques années, nous constatons la croissance exponentielle de la cybercriminalité, dont le piratage informatique et le recel de données font partie. Les cybercriminels regorgent d'ingéniosité pour vendre de plus en plus de données piratées.
À travers cette publication, nous avons tenté de comprendre l'univers du darknet et les infractions qui s'y passent, en

[86] Conseil de l'Europe, *Déclaration sur la liberté de la communication sur l'Internet*, 28 mai 2003, consulté en ligne le 13 août 2021, disponible sur https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805dfbe1.

particulier le piratage informatique de données à caractère personnel et le recel de ces dernières. Nous avons analysé ces notions, ainsi que les motivations des *hackeurs*. Bien que des moyens existent, les pirates sont souvent difficilement identifiables, en particulier sur le darknet où l'anonymisation est facilitée.

Cette notion d'anonymat pose diverses questions auxquelles nous avons tenté de répondre. En particulier, celle de la mise en balance des libertés individuelles avec la lutte contre la cybercriminalité nous a parue intéressante. L'anonymat et le pseudonymat constituent une garantie pour la démocratie, en permettant aux individus de s'exprimer librement. L'interdiction de cette pratique pourrait mener à une société où la prise de parole de chacun serait identifiée, surveillée, contrôlée. Une dérive pourrait être l'augmentation des cas d'autocensure, par crainte de froisser les opinions ou de subir des représailles.

Un vrai débat démocratique ainsi qu'une certaine évolution technique, opérationnelle et législative sembleraient nécessaires afin de déterminer le sort de l'anonymat et du pseudonymat sur Internet et de condamner plus facilement les cybercriminels, en particulier ceux qui se cachent sur le darknet.