CENTRE FOR
CYBER SECURITY
BELGIUM

GUIDE SUR LES POLITIQUES DE DIVULGATION COORDONNEE DE VULNERABILITES

PARTIE I : BONNES PRATIQUES

COORDINATED VULNERABILITY DISCLOSURE POLICIES -"CVDP"
RESPONSIBLE DISCLOSURE POLICIES -"RD"

CENTRE POUR LA CYBERSECURITE BELGIQUE
Rue de la Loi, 16
1000 Bruxelles

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

A. TABLE DES MATIERES

CENTRE FOR
CYBER SECURITY
BELGIUM

<u>Avertissement</u> :

Le présent guide vise à exposer les concepts, les objectifs, les questions juridiques et les bonnes pratiques liées à l'adoption de politiques de divulgation coordonnée de vulnérabilités (ou Coordinated Vulnerability Disclosure Policies – « CVDP ») dans l'état actuel de la législation en Belgique – voir les exemples fournis sur le site du CCB.

L'attention des lecteurs est attirée sur le fait que les documents élaborés par le CCB ne constituent nullement une modification des règles légales existantes. L'accès non autorisé au système informatique d'un tiers, même avec de bonnes intentions est une infraction pénale.

Le participant à une CVDP doit être conscient qu'il ne bénéficie pas d'une exclusion générale de responsabilité lorsqu'il participe à une telle politique : il doit agir avec précaution et respecter scrupuleusement toutes les conditions de la politique, ainsi que les dispositions légales applicables.

** Shutterstock - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

B. INTRODUCTION

I. Contexte

L'importance croissante des systèmes d'information au sein de nos sociétés augmente considérablement le risque d'être confronté à des incidents liés à la sécurité de ceux-ci. Ces incidents peuvent, par exemple, avoir pour conséquence d'affecter la disponibilité d'un service fourni, l'intégrité, l'authenticité, ou la confidentialité de données. L'usage grandissant d'objets connectés à internet accroît encore plus les conséquences éventuelles d'un incident.

Parmi les causes de ces incidents, l'existence de vulnérabilités constitue un risque majeur. Celui-ci est toutefois inhérent au processus de développement, d'utilisation et de mise à jour de ces systèmes. Compte tenu de l'ampleur et de la technicité de ce problème, il apparaît illusoire de croire que tous les fabricants ou responsables de systèmes d'information pourront être en mesure d'y remédier seuls.

Une organisation peut choisir de faire appel soit à une entreprise particulière pour vérifier la sécurité de ses systèmes d'information (via un audit de sécurité par exemple), soit de manière publique à des personnes bien intentionnées (« *hackers éthiques* ») qui souhaitent contribuer à l'amélioration de la sécurité de ces technologies en identifiant les vulnérabilités existantes et en aidant à les résoudre.

II. Notions

A. *Une politique de divulgation coordonnée de vulnérabilités*[1] *(CVDP)* est un ensemble de règles préalablement déterminées par une organisation responsable de systèmes d'information autorisant des participants[2] (ou « *hackers éthiques* ») à rechercher, avec de bonnes intentions, de potentielles vulnérabilités dans ses systèmes, ou à lui transmettre toute information pertinente à ce sujet. Ces

[1] Dénommé également « politique de divulgation responsable » : le choix du terme divulgation « coordonnée » plutôt que « responsable » nous paraît préférable dans la mesure où il évite toute confusion avec les notions légales de responsabilité et il insiste sur le caractère réciproque du processus.

[2] Il peut s'agir, par exemple, de chercheurs en cybersécurité ou des utilisateurs. Les participants peuvent éventuellement être soumis à une sélection par un tiers de confiance (« coordinateur »).

règles, généralement rendues publiques sur un site internet, permettent de fixer un cadre juridique à la collaboration entre l'organisation responsable et les participants à la politique. Elles doivent notamment assurer la confidentialité des informations échangées et encadrer, de manière responsable et coordonnée, une éventuelle divulgation des vulnérabilités découvertes.

Ainsi, la notion de « divulgation » ne doit pas être comprise comme impliquant nécessairement une communication publique de la vulnérabilité mais plutôt une communication du participant vers l'organisation responsable. Si la divulgation de la vulnérabilité par le participant à l'organisation responsable est obligatoire, la divulgation publique de la vulnérabilité (par le participant ou l'organisation concernée) est, en revanche, facultative dans le cadre d'une CVDP.

B. ***Une vulnérabilité*** [3] est un défaut ou une faiblesse, une erreur de conception[4] ou de mise en œuvre[5], une absence de mise à jour au regard des connaissances techniques actuelles et qui peut compromettre la sécurité de technologies[6] de l'information. Une vulnérabilité peut conduire potentiellement à un événement inattendu ou indésirable, et être exploitée par des tiers malveillants en vue de violer l'intégrité, l'authenticité, la confidentialité, la disponibilité d'un système[7] ou d'endommager.

[3] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, p. 14, point 2.2, www.enisa.europa.eu/publications/vulnerability-disclosure.

[4] Par exemple, une erreur ou un oubli dans la conception d'un système ou d'un protocole qui le rendent intrinsèquement vulnérable.

[5] Par exemple, une erreur au cours de l'implémentation, de la configuration ou de l'exploitation.

[6] Par exemple, un système, un réseau, un procédé, un programme, une application, un service, un protocole ou un composant.

[7] ou des informations qu'il contient.

C. ***Une organisation responsable*** est une personne physique ou morale, gestionnaire, propriétaire, vendeur ou fabricant, d'un système ou d'un produit liés aux technologies de l'information et qui est, à ce titre, responsable de la sécurité et du bon fonctionnement de celui-ci.

D. ***Le participant à une CVDP[8] (ou « hacker éthique »)*** est une personne bien intentionnée qui souhaite contribuer, avec l'autorisation de l'organisation responsable, à l'amélioration de la sécurité de systèmes d'information. Celui-ci peut, par exemple, réaliser des tests d'intrusion ou utiliser d'autres méthodes pour vérifier la sécurité de systèmes d'information. Il s'oppose au *hacker* qui utilise ses compétences pour tenter d'accéder à un système sans autorisation et avec de mauvaises intentions[9]. Le participant entend quant à lui avertir le responsable du système d'information, ou un coordinateur, des éventuelles vulnérabilités découvertes afin de les éliminer.

E. ***Un coordinateur*** est un personne physique ou morale qui sert d'intermédiaire entre le participant et l'organisation responsable d'un système d'information en fournissant une assistance logistique, technique et juridique, ou encore d'autres fonctions[10], afin de faciliter leur collaboration. A défaut de coordinateur désigné dans la politique, ce rôle peut être joué par le Centre pour la Cybersécurité Belgique (vulnerabilityreport@cert.be).

F. ***Un programme de récompense pour la découverte de vulnérabilités (*ou *bug bounty)[11]*** vise l'ensemble des règles définies par une organisation responsable pour octroyer des récompenses aux participants qui identifieraient des vulnérabilités dans les technologies qu'elle utilise. Cette récompense peut prendre la forme d'une somme d'argent, de cadeaux ou d'une reconnaissance publique (classement parmi les meilleurs participants, publication, conférence, etc.). Il s'agit d'une forme de politique de divulgation coordonnée de vulnérabilités, qui prévoit l'octroi d'une récompense

[8]communément dénommé en anglais «white hat », par référence au fait que les héros dans les films de western américains portaient traditionnellement un chapeau blanc.
[9] Communément dénommé en anglais « black hat », par référence au fait que les bandits dans les films de western américains portaient traditionnellement un chapeau noir.
[10] Par exemple, un rôle d'évaluateur des rapports de vulnérabilités ou de médiateur.
[11] En anglais, « vulnerability rewards program » ou « bug bounty program ».

pour le participant, en fonction du nombre, de l'importance ou de la qualité des informations transmises. Cette forme de politique est plus attrayante pour les éventuels participants et offre souvent de meilleurs résultats pour les organisations. L'organisation peut notamment faire appel à une plate-forme de *bug bounty* qui lui offre une assistance technique et administrative pour la gestion de son programme de récompense pour la découverte de vulnérabilités (rôle de coordinateur).

III. Objectifs

a. Offrir un cadre juridique permettant une collaboration utile, loyale, efficace, légale et à budget maîtrisé

Lorsqu'une organisation fait appel à un prestataire externe déterminé pour vérifier la sécurité de ses systèmes d'information, elle conclut avec lui un contrat d'audit de sécurité qui peut inclure la réalisation de tests d'intrusion (en anglais : *penetration test* ou « *pentest* ») simulant l'attaque de personnes mal intentionnées en vue de démontrer les vulnérabilités existantes. Dans ce cas, les obligations juridiques réciproques des parties sont, en principe, définies dans une convention particulière ou des conditions générales[12].

Cela n'est toutefois pas le cas, par défaut, lorsqu'une organisation souhaite collaborer avec des personnes indéterminées (*participant*s ou *hackers éthiques*) qui seraient susceptibles d'identifier des vulnérabilités dans ses systèmes d'information. Il n'existe alors pas de cadre contractuel précis entre les parties. Dans ce cas de figure, il s'avère nécessaire pour l'organisation de fixer préalablement à toute collaboration ses attentes et les obligations juridiques des participants.

La politique de divulgation coordonnée de vulnérabilités constitue, à ce titre, une forme de contrat d'adhésion dans lequel toutes les dispositions contractuelles sont fixées par l'organisation responsable

[12] L'organisation responsable pourrait également confier ces tâches à certains de ses employés. Les obligations respectives des parties seront alors définies par un règlement interne spécifique ou dans le règlement général de travail.

et ensuite acceptées par le participant lorsque celui-ci décide librement de participer au programme mis en place.

L'adoption d'une telle politique clarifie la situation juridique des participants en leur permettant de prouver, moyennant le respect des conditions énoncées dans la politique, l'existence d'une autorisation préalable d'accès aux systèmes informatiques concernés et dès lors l'absence d'une intrusion illicite (*voir Guide sur les politiques de divulgation coordonnée de vulnérabilités. Partie II : Aspects légaux*).

Cette collaboration peut procurer de manière loyale et licite à l'organisation responsable des informations sur les vulnérabilités de ses systèmes, en lui permettant d'agir de manière appropriée et en temps opportun. Celle-ci permet ainsi de prévenir efficacement ou de limiter, dans la mesure du possible, les risques et les dommages potentiels que pourraient lui causer ces vulnérabilités.

La politique de divulgation coordonnée de vulnérabilités offre la possibilité de vérifier de manière constante et efficace la sécurité de ses systèmes ou équipements. Bien entendu, l'attractivité et l'efficacité de la politique sont augmentées lorsque l'organisation responsable décide d'accorder des récompenses aux participants en fonction de l'importance et de la qualité des informations fournies (dans le cadre d'un programme de récompense pour la découverte de vulnérabilités ou *bug bounty*[13]).

Même lorsque l'organisation octroie des récompenses et fait appel à un coordinateur externe (plate-forme de *hacking éthique*), les coûts liés à la mise en place d'une politique de divulgation coordonnée de vulnérabilités sont, en général, mieux maîtrisés que ceux liés à la réalisation d'audits par des entreprises externes[14]. En effet, l'octroi d'une récompense dans le cadre d'un bug bounty résulte d'une obligation de résultat dans le chef du participant alors que l'auditeur externe n'est généralement tenu

[13] En dehors d'un programme de récompense pour la découverte de vulnérabilités, l'organisation responsable peut unilatéralement décider d'accorder une récompense (non prévue) au participant à l'issue de la procédure.
[14] Certains coûts sont nécessairement à prévoir, comme par exemple, le coût de l'équipe technique nécessaire à l'analyse des informations fournies par les participants.

qu'à une obligation de moyens. Ce dernier devrait ainsi être rémunéré pour l'ensemble de ses prestations même s'il ne trouve pas de vulnérabilités ou des vulnérabilités mineures à l'issue de ses recherches.

b. Augmenter la sécurité des systèmes d'information et encourager les recherches

En adoptant une politique, l'organisation responsable se donne l'opportunité de recevoir de plusieurs sources des informations sur la sécurité de ses systèmes d'information. Compte tenu de la complexité et de la technicité actuelles de tels systèmes, il s'avère très utile de recourir à une multitude d'experts potentiels plutôt que de faire appel à quelques prestataires externes qui peuvent difficilement être experts dans toutes les technologies utilisées par l'organisation.

En complément à d'autres mesures techniques et organisationnelles, la mise en place d'une telle collaboration peut constituer une mesure appropriée en vue de prévenir les incidents qui compromettraient la sécurité de ses réseaux et systèmes d'information. Elle présente l'avantage indéniable d'identifier les vulnérabilités et d'y remédier avant qu'un incident de sécurité ne se produise.

L'amélioration de la sécurité découle de la correction des vulnérabilités, de la minimisation des risques lié à l'existence de vulnérabilités et d'un processus constant d'évaluation de ces mêmes risques pour les systèmes d'information de l'organisation responsable.

Bien entendu, l'adoption d'une CVDP implique que l'organisation dispose de mesures de sécurité qui puissent être mises à l'épreuve et d'une équipe interne (ou externe) capable d'assurer un suivi des informations reçues des participants.

Outre l'amélioration de la sécurité, de telles politiques peuvent également améliorer les connaissances en matière de cybersécurité et encourager les recherches dans ce domaine. Or, les travaux des

chercheurs permettent d'identifier les nouvelles vulnérabilités, les conditions dans lesquelles elles se produisent, les méthodes pour les éviter et les moyens de les corriger.

c. Assurer la confiance des utilisateurs dans les technologies de l'information

La mise en œuvre d'une CVDP témoigne vis-à-vis du public et des utilisateurs de l'attachement de l'organisation responsable à la sécurité de ses technologies de l'information.

En effet, cette démarche implique l'engagement de traiter les informations fournies par les participants et d'essayer de remédier aux vulnérabilités identifiées, ou à tout le moins d'informer les utilisateurs des risques encourus.

Cet engagement peut par ailleurs constituer un argument marketing et être mis en avant dans la communication de l'organisation. La confiance dans les systèmes d'information est assurément un élément important pour les utilisateurs ou les consommateurs.

d. Garantir la confidentialité

La confidentialité des informations liées à une vulnérabilité dans un système informatique doit être assurée autant que possible.

La divulgation complète d'une vulnérabilité[15], alors que celle-ci existe toujours auprès de nombreux utilisateurs, constitue un risque important de sécurité en matière de technologies de l'information. En

[15] « full disclosure ».

effet, des tiers malveillants pourraient développer et répandre des outils spécifiques pour exploiter cette vulnérabilité.

Il n'est donc pas souhaitable qu'une faille de sécurité soit divulguée au public, avant qu'elle n'ait été corrigée par l'organisation responsable, en lui accordant le temps nécessaire à la résolution du problème, ou avant que l'organisation responsable n'ait pu en informer préalablement les autorités publiques en charge de la sécurité des réseaux et systèmes d'information[16].

La divulgation complète est également susceptible de retarder le déploiement efficace d'une solution à la vulnérabilité en imposant à l'organisation responsable de réagir en situation de crise.

De même, la révélation publique de failles de sécurité peut porter atteinte à la réputation de l'organisation responsable et entamer la confiance des utilisateurs dans les technologies concernées.

En outre, le fait de diffuser ou de mettre à disposition du public des données informatiques, tels que des logiciels ou des instructions, adaptées pour forcer la sécurité de systèmes informatiques peut constituer une infraction[17] ou engager la responsabilité civile de celui qui a publié les informations[18] (*voir Guide – partie II Aspects légaux*).

Par voie de conséquence, la divulgation publique d'informations sur une vulnérabilité doit être réalisée avec beaucoup de précaution et de manière coordonnée avec l'organisation responsable.

---

[16] En Belgique, ce rôle est principalement joué par le Centre pour la Cybersécurité Belgique (CCB) qui peut, le cas échéant, informer les organisations d'intérêt vital (autorités publiques, opérateurs de services essentiels, fournisseurs de service numérique, infrastructures critiques, etc.).
[17] Art. 550 *bis*, § 5 du Code pénal.
[18] Art. 1382 du Code civil.

De son côté, l'organisation responsable se doit de réagir dans un délai raisonnable en implémentant une solution ou à tout le moins en informant les utilisateurs des systèmes d'information concernés par la vulnérabilité. En effet, l'organisation pourrait, par exemple, voir sa responsabilité engagée pour avoir laissé dans l'ignorance ses clients quant à l'existence de la vulnérabilité (voir ci-après point e).

Il peut s'avérer également particulièrement utile, lorsque les risques principaux de sécurité sont écartés, de publier les informations sur les vulnérabilités découvertes et leur résolution, dans un contexte adéquat[19], afin de faire progresser les recherches en sécurité informatique.

L'intérêt d'une CVDP réside donc dans l'établissement d'un cadre juridique qui renforce la confidentialité et encadre au mieux une éventuelle divulgation publique.

e. Renforcer le respect des obligations légales en matière de sécurité des technologies de l'information

La mise en œuvre d'une politique de divulgation coordonnée permet de prouver les efforts de l'organisation pour le respect de ses obligations légales de sécurité de ses réseaux et systèmes d'information : Règlement général sur la protection des données UE n°2016/679 (« RGPD »), 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 (« loi NIS »), règles de responsabilité civile, Code de droit économique, etc.

Tout d'abord, l'article 32 du RGPD prévoit que le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, en tenant compte de l'état des connaissances, des coûts de mise en

[19] Par exemple, dans une publication scientifique ou dans un rapport technique diffusé au sein des chercheurs en sécurité informatique.

œuvre, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques (dont le degré de probabilité et de gravité varie).

La disposition précise que le responsable du traitement et le sous-traitant peuvent utiliser notamment :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Dans sa recommandation relative aux mesures de sécurité à respecter afin de prévenir les fuites de données (n°01-2013), la Commission de la protection de la vie privée (devenue aujourd'hui l'Autorité de protection des données) rappelle l'importance de documenter, auditer et améliorer aussi souvent que nécessaire les mesures de sécurité de l'information[20].

De la même manière, les lignes directrices pour la sécurité de l'information de données à caractère personnel de l'ancienne Commission de la protection de la vie privée mentionnaient que « le responsable de traitement se doit régulièrement d'organiser un audit de qualité concernant la sécurité de l'information des données à caractère personnel et de prendre des mesures de gestion visant à garantir la confidentialité et l'intégrité des données »[21].

[20] Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données (n°01-2013), www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf, p. 3, point 6.

[21] Commission de la protection de la vie privée, *Lignes directrices pour la sécurité de l'information de données à caractère personnel*, (version 2.0 déc. 2014), pp. 20 et 27, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Richtsnoeren_CBPL_V%202%200%20FR_TRA.pdf.

Or, la mise en œuvre d'une CVDP est une mesure technique et organisationnelle, parmi d'autres mesures, appropriée pour démontrer les efforts du responsable de traitement pour, d'une part, garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes de ses systèmes de traitement[22] et, d'autre part, tester, analyser et évaluer régulièrement l'efficacité des mesures de sécurité du traitement[23]. Les standards techniques internationaux en matière de sécurité des technologies de l'information conseillent d'ailleurs explicitement la mise en œuvre d'une CVDP (voy. par exemple : les normes internationales ISO/IEC 29147[24] et 30111[25]).

L'organisation responsable peut ainsi s'appuyer sur sa CVDP pour démontrer, auprès des autorités de contrôle, ses efforts pour évaluer et gérer les risques liés aux vulnérabilités des systèmes d'information de l'organisation concernée.

Dans le même ordre d'idée, une CVDP peut permettre au responsable de traitement d'être mieux informé sur les éventuelles violations de données à caractère personnel et d'évaluer celles qui doivent, dans les meilleurs délais, faire l'objet d'une notification à une autorité de contrôle[26] ou d'une communication à une personne physique[27].

---

[22] Art. 32 (1), point b du RGPD.
[23] Art. 32 (1), point d du RGPD.
[24] ISO/IEC 29147:2018 Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité (https://www.iso.org/standard/72311.html).
[25] ISO/IEC 30111:2019 Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité (https://www.iso.org/standard/53231.html).
[26] Art. 33 du RGPD prévoit que le responsable du traitement doit notifier les violations de données à caractère personnel 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. Le sous-traitant doit également notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.
[27] Art. 34 du RGPD impose que le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

Ensuite, l'article 20 de la loi NIS impose que l'opérateur de services essentiels (« OSE ») prenne « les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information dont sont tributaires ses services essentiels. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité physique et logique adapté aux risques existants, compte tenu de l'état des connaissances techniques ».

L'OSE doit également prendre « les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services »[28].

Les mesures de sécurité sont définies par la loi NIS comme permettant à un système de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles[29]. Pour adopter les mesures nécessaires et proportionnées aux risques[30], il est nécessaire d'identifier les risques d'incidents et d'en limiter l'impact sur la sécurité des réseaux et des systèmes d'information.

En l'occurrence, la mise en œuvre d'une CVDP offre la possibilité pour un OSE ou un fournisseur de service numérique de mieux connaître les éventuelles vulnérabilités et les menaces susceptibles d'apparaître dans ses réseaux et systèmes d'information afin de répondre de manière adéquate aux exigences de la loi NIS.

---

[28] Art. 20 de la loi NIS ; voy. également l'art. 33 de la loi NIS pour les mesures de sécurité des fournisseurs de service numériques (FSN) – par exemple, les fournisseurs de service d'informatique en nuage (« cloud »).
[29] Art. 6, 9° de la loi NIS.
[30] Art. 6, 15° de la loi NIS définit le risque comme « toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ».

En outre, le Règlement européen sur la Cybersécurité (« Cyber Security Act »)[31] prévoit qu'un schéma européen de certification de cybersécurité doit comprendre au moins les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment[32] dans des produits TIC[33], services TIC[34] et processus TIC [35].

Le Règlement impose ainsi au fabricant ou au fournisseur de produits TIC, services TIC ou processus TIC certifiés de mettre à la disposition du public les informations de contact du fabricant ou du fournisseur et les méthodes acceptées pour recevoir des informations concernant des vulnérabilités de la part d'utilisateurs finaux et de chercheurs dans le domaine de la sécurité[36].

Par ailleurs, la responsabilité civile (contractuelle ou extra-contractuelle) d'une organisation responsable peut être engagée lorsqu'une faille de sécurité de ses technologies a causé un dommage à un tiers[37].

Enfin, l'organisation responsable qui vend des systèmes d'information est tenue de garantir ses clients contre les défauts cachés ou les défauts de conformité des biens vendus[38]. Elle peut également être tenue, en qualité de producteur d'un produit (bien corporel) ou d'un service, de la sécurité de ses

[31] 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.
[32] Art. 54, 1, m du Règlement sur la Cybersécurité.
[33] Un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information (art. 2, 12 du Règlement sur la Cybersécurité).
[34] Un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information (art. 2, 13 du Règlement sur la Cybersécurité).
[35] Un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance (art. 2, 14 du Règlement sur la Cybersécurité).
[36] Art. 55, 1, c du Règlement sur la Cybersécurité.
[37] Art. 1382 du Code civil.
[38] Voy. art. 1641 et 1625 du Code civil pour la garantie contre les vices cachés ou art. 1649 *bis* et s. du Code civil sur la garantie contre les défauts de conformité pour les ventes à des consommateurs.

produits et services[39]. La conformité à cette obligation générale de sécurité peut être évaluée en prenant en compte des normes nationales ou internationales, des codes de bonne conduite en vigueur dans le secteur concerné, de l'état actuel des connaissances et de la technique, et la sécurité à laquelle les consommateurs peuvent raisonnablement s'attendre[40].

C. BONNES PRATIQUES

Actuellement, il existe de nombreuses entreprises qui appliquent déjà, en Belgique, des politiques de divulgation coordonnée des vulnérabilités et font appel à des plates-formes de « bug bounty ».

Deux standards internationaux ISO/IEC existent en matière de CVDP : ISO/IEC 29147[41] et ISO/IEC 30111[42]. Le premier décrit la procédure de divulgation d'une vulnérabilité, tandis que le second aborde les processus de traitement de la vulnérabilité renseignée. Ces deux standards décrivent un modèle complet des différents aspects d'une CVDP.

L'ENISA (Agence de l'Union européenne pour la Cybersécurité) a également publié des recommandations sur les bonnes pratiques relatives à la mise en place d'une CVDP[43].

[39] Voy. art. IX.2 et s. du Code de droit économique.
[40] A défaut de normes harmonisées européennes.
[41] ISO/IEC 29147:2018 Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité (https://www.iso.org/standard/72311.html).
[42] ISO/IEC 30111:2019 Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité (https://www.iso.org/standard/53231.html).
[43] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure; Art . 6 (1), b du Règlement (UE) 2019/881 charge d'ailleurs l'ENISA d'assister les États membres de l'Union et les institutions européennes, pour établir et mettre en œuvre, sur une base volontaire, des politiques en matière de divulgation des vulnérabilités.

** Colored-security-background-flat-design Free licence - Designed Freepik - 2020*

I. Contenu d'une CVDP

a. Personnes habilitées

La politique doit être adoptée par les personnes ou les organes pouvant valablement représenter l'organisation responsable et non, par exemple, par un membre de l'équipe informatique sans être valablement mandaté pour ce faire[44]. En effet, les autorisations prévues dans le cadre de la politique

[44] Sous réserve de la théorie du mandat apparent ou du principe général de droit du respect dû aux anticipations légitimes d'autrui.

de divulgation coordonnée doivent nécessairement provenir d'une personne habilitée à cette fin par le titulaire des droits sur le système ou l'équipement concerné[45].

b. Publicité

La publicité donnée à la politique de divulgation responsable est un élément important de son succès[46]. Son contenu doit ainsi être facilement accessible aux participants potentiels, de préférence sur le site internet de l'organisation responsable. Pour ce faire, l'existence de la CVDP devrait être reprise de manière claire et visible sur le site internet de l'organisation responsable (par exemple avec un onglet spécifique ou une sous-section qui contient le contenu complet de la politique)[47]. A ce propos, il existe des propositions de standardisation visant à localiser la CVDP d'une organisation dans un fichier nommé « security.txt » à un endroit connu de l'arborescence de chaque site internet[48] ou des extensions pour navigateur internet qui permettent de renseigner les sites internet qui disposent d'une CVDP[49].

En cas de recours à un programme de récompense pour la découverte de vulnérabilités via une plate-forme de bug bounty, il convient aussi de faire figurer le contenu complet de la CVDP sur cette plate-forme[50].

La CVDP devrait être rédigée dans toutes les langues utilisées par le site internet et dans la mesure du possible aussi en anglais. Il peut s'avérer utile également de mettre un lien à d'autres endroits vers la

[45] Celui-ci est, par défaut, le propriétaire du système.
[46] Pour éviter de commettre une infraction (accès non autorisé à un système d'information), il est nécessaire que la politique de divulgation coordonnée existe préalablement à toute démarche accomplie par le participant. La meilleure façon d'éviter des doutes sur l'existence ou non d'une politique de divulgation coordonnée des vulnérabilités est d'en assurer la publicité. (voir partie II. Aspects légaux). Il est toutefois possible à l'organisation d'avoir une CVDP non publique et limitée à certains participants préalablement sélectionnés (voir notamment certains bug bounty privés).
[47] Par exemple : https://www.[organisation].be/security ou /disclosurepolicy ou encore /vulnerability-policy.
[48] Voy. le projet https://securitytxt.org/
[49] Voir par exemple, l'extension YesWeHack VDP Finder pour Chrome et Firefox.
[50] Par exemple, www.intigriti.be; www.yeswehack.com; www.bugcrowd.com; www.hackerone.com.

page dédiée à la CVDP (par exemple, dans la rubrique aide du programme, dans le mode d'emploi, dans la licence d'utilisation, etc.).

Enfin, il est important pour l'organisation responsable d'informer ses éventuels sous-traitants du contenu de sa CVDP et d'adapter si besoin ses contrats de sous-traitance.

c. Point de contact

L'organisation responsable doit désigner dans sa politique un point de contact vers lequel toutes les informations relatives aux vulnérabilités peuvent être envoyées. A cet effet, une adresse de courriel spécifique pourrait être dédiée à cet effet[51]. Dans le même ordre d'idée, l'organisation responsable doit s'assurer que les courriels reçus par d'autres adresses de courriel [52] soient bien redirigés en interne vers ce point de contact.

L'utilisation d'un formulaire en ligne est aussi intéressant pour recevoir les informations relatives aux vulnérabilités découvertes. Ce procédé offre l'avantage d'automatiser l'encodage, le traitement des données et l'envoi d'un accusé de réception.

De plus, il peut être utile de mentionner les coordonnées de téléphone du service ou de la personne compétente pour traiter les notifications relatives aux vulnérabilités informatiques.

Enfin, il faut préciser clairement les informations à fournir par le participant (voir ci-après, la partie II Procédure).

[51] Comme par exemple : vulnerabilitypolicy@organisation.com; security@organisation.com; csirt@organisation.com; support@organisation.com; security-alert@organisation.com, etc.
[52] Par exemple, info@organisation.com ou contact@organisation.com.

d. Sécurité et confidentialité des communications

Il s'agit d'une question primordiale car il faut éviter au maximum les risques de fuites des informations liées aux vulnérabilités, en garantissant au mieux la confidentialité et l'intégrité des communications.

L'utilisation d'un mode de communication sécurisé est donc hautement recommandé. Celui-ci peut consister à utiliser un moyen pour chiffrer les données[53], créer un portail internet sécurisé[54] ou au moins protéger les documents par un mot de passe[55]. Dans les modalités de communication recommandées aux participants, l'organisation responsable doit donc tenir compte tout spécialement de la sécurité de celles-ci[56].

e. Description des obligations réciproques

1. Champ d'application de la politique

L'organisation responsable doit définir explicitement le champ d'application de sa politique de divulgation coordonnée : quels sont les sites, les produits, les équipements, les services, les systèmes ou les réseaux concernés où sa politique est applicable.

Idéalement, l'organisation responsable devrait veiller à rendre applicables les règles de sa CVDP à ses différents systèmes d'information et à ses engagements contractuels (fournisseurs, clients, sous-traitants, personnel, etc.).

---

[53] Par exemple, Transport Layer Security (TLS) ou son prédécesseur Secure Sockets Layer (SSL) , Secure Multipurpose Internet Mail Extensions (S/MIME), et Pretty Good Privacy (PGP).
[54] en HTTPS ou par un chiffrement dans le navigateur internet.
[55] Le mot de passe étant transmis idéalement à l'organisation responsable par le participant par un autre moyen de communication (téléphone, sms, application de messagerie, autre adresse de courriel, etc.).
[56] Par exemple, fournir la clé publique et le fingerprint de son point de contact pour communiquer de manière chiffrée ou sécuriser en HTTPS son formulaire en ligne.

Dans le cas contraire, la CVDP devrait expressément lister les systèmes d'information appartenant à des tiers et qui seraient exclus du champ d'application de la politique (en l'absence d'autorisation de ces tiers). En cas de doute sur les limites de la CVDP, il convient pour le participant de solliciter préalablement l'accord de l'organisation responsable avant de poursuivre ses recherches.

Egalement, la CVDP devrait mentionner clairement que les recherches du participant sur des systèmes d'information non explicitement inclus dans le cadre de la politique pourraient entraîner des poursuites judiciaires à son encontre (par le ministère public, l'organisation responsable ou des tiers à la CVDP).

2. Conditions de la politique

L'existence même d'une politique de divulgation coordonnée des vulnérabilités, ou d'un programme de bug bounty, implique nécessairement l'octroi au participant d'une autorisation d'accès au système informatique au moins tacite[57]. De même, le participant dispose, en principe, d'une autorisation d'introduire ou de tenter d'introduire des données informatiques dans le système concerné (*voir le Guide – Partie II Aspects légaux*).

L'organisation responsable doit néanmoins mentionner clairement, dans sa politique de divulgation coordonnée, les conditions dans lesquelles les participants peuvent accéder au système informatique, tenter d'introduire ou de modifier des données. Les actions qui sont ou non permises doivent être identifiées, sans ambiguïté sur base des finalités poursuivies.

L'autorisation de modifier ou de supprimer des données informatiques[58] dépend de la manière dont la politique de divulgation coordonnée des vulnérabilités est rédigée. Lors de la rédaction d'une telle politique, l'organisation responsable devra évaluer les avantages, les conditions particulières imposées et les risques encourus afin d'autoriser ou non ces actions. Il devrait être mentionné que le participant doit respecter strictement les conditions de la politique quant à la modification et la suppression de

[57] En fonction du libellé exact de ses dispositions, la politique de divulgation coordonnée des vulnérabilités contiendra des dispositions pouvant être qualifiées d'autorisations soit expresses, soit tacites.
[58] ou de tenter de telles actions.

données informatiques, à défaut de quoi il se rendrait coupable d'une infraction de violation de données informatiques.

A titre d'exemple, il est une bonne pratique d'interdire le recours à des attaques par déni de service distribuée (DDoS) ou par ingénierie sociale, l'installation de logiciels malveillants ou de virus, le vol de mot de passe, le « phishing » par courriel, le spamming, la suppression ou le changement de données/paramètres du système, etc.

La CVDP devrait exclure explicitement les tentatives intentionnelles[59] d'intercepter, d'enregistrer ou de prendre connaissance de communications non accessibles au public ou de communications électroniques[60]. Néanmoins, il pourrait être admis que le contenu d'une communication soit révélé, de manière strictement fortuite, aux participants dans le cadre de la recherche des vulnérabilités[61].

De même, il devrait être mentionné que le participant ne peut utiliser, détenir, révéler ou divulguer des communications non accessibles au public ou des données d'un système informatique dont il ne peut raisonnablement ignorer qu'elles ont été obtenues illégalement.

Il devrait être interdit aussi pour le participant d'installer ou de faire installer un appareil permettant l'interception, la prise de connaissance ou l'enregistrement d'une communication non accessible au public, sauf s'il peut démontrer qu'il agit sans l'intention d'utiliser l'appareil concerné aux fins précitées, soit avec le consentement de tous les participants à la communication, soit en participant lui-même à la communication.

3. Notification

La CVDP doit préciser clairement les informations souhaitées du participant lors de la notification d'une vulnérabilité : type de la vulnérabilité, détails de la configuration, opérations effectuées, outils utilisés,

[59] Ce qui est différent d'une interception fortuite (voir Guide Partie II Aspects légaux).
[60] Sauf l'hypothèse plutôt rare où le participant disposerait du consentement de tous les participants ou participerait lui-même à la communication électronique.
[61] Voy. le secret des communications électroniques (loi du 13 juin 2005).

date des tests, preuves, adresse IP ou URL du système affecté, capture d'écran, coordonnées de contact, etc.

4. Proportionnalité

De manière générale, le participant doit s'engager dans ses actions à respecter le principe de proportionnalité, c'est-à-dire de ne pas perturber la disponibilité des services fournis par le système et de ne pas faire usage de la vulnérabilité au-delà de ce qui est strictement nécessaire à la démonstration de la faille de sécurité. Son attitude doit rester proportionnée : si la démonstration est établie à petit échelle, il n'est pas nécessaire de l'étendre plus loin.

Si cela n'est pas nécessaire à la démonstration de l'existence de la vulnérabilité informatique, l'utilisation des données à caractère personnel par le participant doit être expressément exclue.

En outre, la politique de divulgation coordonnée doit mentionner clairement que les participants ne peuvent détenir plus longtemps que nécessaire les données de l'organisation responsable, dont d'éventuelles données à caractère personnel. Toutes les données personnelles collectées par le participant devraient être supprimées immédiatement. Si cela s'avère nécessaire de conserver ces données encore pendant un certain temps, le participant doit veiller à ce que ces données sont conservées en toute sécurité durant cette période.

5. Confidentialité

L'un des éléments essentiels d'une politique de divulgation coordonnée doit être le respect de la confidentialité : le participant doit s'abstenir de partager ou de divulguer les informations récoltées avec des tiers, sans l'accord explicite de l'organisation responsable[62].

[62] A nouveau, sous réserve d'une diffusion restreinte aux autorités compétentes en matière de Cybersécurité.

De même, toute révélation ou divulgation par le participant de données informatiques, de données de communication ou de données à caractère personnel à des personnes tierces à l'organisation responsable doit être expressément exclue, sauf autorisation préalable de l'organisation responsable.

Le texte de la politique de divulgation coordonnée devrait mentionner que l'objectif de la politique n'est pas de permettre la prise de connaissance intentionnellement du contenu de données informatiques, de données de communication ou de données à caractère personnel et qu'une telle prise de connaissance ne pourrait intervenir que de manière fortuite et incidente dans le cadre de la recherche de vulnérabilités dans les technologies concernées.

6. Exécution de bonne foi

L'organisation responsable du système d'information doit s'engager à exécuter de bonne foi sa politique de divulgation coordonnée et de ne pas poursuivre en justice, au civil ou au pénal, le participant qui en respecte les conditions.

De son côté, le participant doit être dénué d'intention frauduleuse, de dessein de nuire, de volonté de faire usage ou de provoquer un dommage au système visité ou encore à ses données. Cela vaut également pour les systèmes tiers situés en Belgique ou à l'étranger.

S'agissant des dispositifs permettant de commettre une violation de données informatiques, le participant pourrait élaborer, détenir ou mettre à disposition de tels dispositifs dans le cadre de la participation à une politique de divulgation des vulnérabilités. Ces actions ne sont pas illicites tant qu'elles sont justifiées par des fins légitimes de recherches de vulnérabilités avec l'accord de l'organisation du responsable du système informatique concerné.

7. Traitement de données à caractère personnel

L'objet d'une CVDP n'est pas d'effectuer intentionnellement des traitements de données à caractère personnel mais il est possible que le participant doive, même de manière fortuite, traiter des données à caractère personnel dans le cadre de ses recherches de vulnérabilités.

Or, le traitement de données à caractère personnel a une portée large et inclut notamment la conservation, la modification, l'extraction, la consultation, l'utilisation ou la communication de toute information pouvant se rapporter à une personne physique identifiée ou identifiable. Le caractère « identifiable » de la personne ne dépend pas de la simple volonté d'identification de celui qui traite les données mais de la possibilité d'identifier, directement ou indirectement, la personne à l'aide de ces données (par exemple : une adresse de courriel, numéro d'identification, identifiant en ligne, adresse IP ou encore des données de localisation).

Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement[63].

Dès lors que la CVDP constitue une forme de contrat d'adhésion qui lie le hacker éthique à l'égard de l'organisation responsable, il s'avère nécessaire d'y préciser les obligations des parties en matière de traitements de données à caractère personnel, notamment les finalités et les moyens essentiels des éventuels traitements effectués dans le cadre de cette politique (*voir Guide – partie II Aspects légaux)*.

8. Délais de procédure

Il est recommandé de fixer des délais clairs à respecter pour chaque étape du processus, notamment pour l'envoi d'un accusé de réception au participant, la communication d'information complémentaire, les investigations, le développement d'une solution, la réponse au participant, l'octroi d'une récompense ou une éventuelle publication. Toutefois, il faut laisser une possibilité de flexibilité des délais, en fonction de la complexité de la vulnérabilité, du nombre de systèmes affectés, de l'urgence ou de la gravité d'une situation.

9. Communication continue

[63] Art. 4, 7) du RGPD.

Une bonne collaboration passe par une communication continue et efficace. Les renseignements fournis par le participant peuvent, en effet, s'avérer très utiles pour identifier la vulnérabilité, y apporter une solution. Il est donc important d'accuser réception de ses envois, de le tenir informé des suites données à sa notification, de lui rappeler le contenu de ses obligations et de lui préciser les prochaines étapes de la procédure.

Par ailleurs, l'intervention d'un coordinateur (désigné de préférence dans la CVDP) ou d'une plate-forme proposant des récompenses pour la découverte de vulnérabilités peut faciliter l'établissement et le maintien d'une relation constructive entre les parties ou éventuellement garantir l'anonymat du participant.

En l'absence de réaction de l'une des parties ou du coordinateur désigné, les parties peuvent toujours faire appel au Centre pour la Cybersécurité Belgique (vulnerabilityreport@cert.be).

10. Octroi d'une récompense

L'octroi d'une récompense ou d'une reconnaissance publique[64] par l'organisation responsable augmente l'attractivité de la CVDP pour les participants et offre souvent de meilleurs résultats pour les organisations. Il peut même s'agir d'un simple cadeau symbolique : par exemple, un t-shirt, un autocollant ou une tasse spécifique.

Dans le cadre d'un programme de récompense pour la découverte de vulnérabilités (ou bug bounty), la récompense est fixée en fonction du nombre, de l'importance ou de la qualité des informations transmises.

[64] classement parmi les meilleurs participants, publication, conférence, etc.

Il est essentiel que la nature de cette récompense soit préalablement et clairement fixée par l'organisation responsable dans sa politique. Toute demande de récompense en dehors des conditions définies par la CVDP pourra ainsi être assimilée à une tentative illicite d'extorsion.

L'organisation peut utilement avoir recours à une plate-forme de *bug bounty*[65] qui coordonnera avec elle les aspects techniques et administratifs de son programme de récompense.

11. Eventuelle divulgation publique

L'éventuelle divulgation de la vulnérabilité doit se réaliser de manière coordonnée et synchronisée entre les parties, afin de fournir un temps suffisant à l'organisation responsable pour résoudre le problème et informer préalablement les opérateurs critiques affectés.

Lorsqu'une vulnérabilité est identifiée dans un programme, un composant, un protocole ou un format fourni par un fournisseur tiers, l'organisation responsable doit l'en informer directement et ce avant toute divulgation publique.

Il en va de même lorsque la vulnérabilité identifiée risque d'affecter de manière plus large d'autres organisations utilisant une technologie similaire ou lorsque le composant informatique affecté est fourni par l'organisation responsable à d'autres organisations (par exemple, via des licences d'utilisation). Dans ces cas, il est alors indispensable qu'un rapport sur la vulnérabilité et sa solution soit diffusé aux parties concernées afin de leur donner l'occasion de se protéger.

En cas de divulgation publique, le rapport relatif à la vulnérabilité et la solution devraient être diffusés, idéalement, en même temps.

L'organisation responsable devrait proposer différents moyens d'informer et de protéger ses utilisateurs : par exemple la mise à jour automatique du système, la publication d'avis de sécurité sur

[65] Par exemple : www.intigriti.com (plate-forme basée en Belgique); www.yeswehack.com (plate-forme basée en France); www.yogosha.com; www.hackerone.com (plate-forme basée aux USA).

son site internet, la diffusion par courriel avec un lien vers une page internet dédiée, communication de ces informations à son réseau de vendeurs, etc.

Dans l'hypothèse d'une vulnérabilité qui concernerait également d'autres organisations, l'organisation responsable se doit d'en informer, en tout état de cause, le Centre pour la Cybersécurité Belgique (vulnerabilityreport@cert.be), même si elle ne souhaite pas que la vulnérabilité soit divulguée publiquement.

** tech-support-concept. Free licence. Designed by macrovector / Freepik (2020)*

CENTRE FOR CYBER SECURITY BELGIUM

II. Procédure

a. Découverte

Lorsqu'un participant découvre des informations relatives à une vulnérabilité potentielle, celui-ci devrait, dans la mesure du possible, réaliser au préalable des vérifications permettant de confirmer l'existence de la vulnérabilité et d'identifier les éventuels risques encourus.

Ensuite, il devrait transmettre à l'organisation responsable, au minimum, les informations techniques suffisantes pour permettre la confirmation de cette faille et fournir ses coordonnées de contact. Ces éléments pourraient être complétés en fonction des spécifications de la politique de divulgation coordonnée ou du contenu du formulaire en ligne de l'organisation responsable.

b. Notification

Le participant devrait notifier, dans les plus brefs délais, les informations techniques au point de contact ou au coordinateur désigné par l'organisation responsable, en utilisant des moyens de communication sécurisés.

Lorsqu'elle reçoit une notification, l'organisation responsable devrait envoyer au participant, dans les plus brefs délais, un accusé de réception avec la référence interne de celle-ci et la prochaine étape de la procédure.

Cet accusé de réception serait l'occasion pour l'organisation responsable de rappeler le contenu de sa politique de divulgation coordonnée, ou à tout le moins de transmettre un lien vers celle-ci, et de demander d'éventuelles informations complémentaires.

Il est notamment intéressant de demander si le participant aurait déjà signalé ce problème à d'autres organisations responsables.

c. Investigation

La phase d'investigation permet à l'organisation responsable de reproduire l'environnement et le comportement signalé afin de vérifier les informations communiquées.

Il convient de tenir informé de manière régulière le participant des résultats des investigations et des suites données à la notification.

Durant ce processus, les parties doivent veiller à faire le lien avec des rapports de sécurité similaires ou connexes, à évaluer le risque et la gravité de la vulnérabilité, et à déterminer les éventuels autres produits ou systèmes affectés.

d. Déploiement d'une solution

L'objectif de la politique de divulgation est de permettre le développement et de déploiement d'une solution afin de faire disparaître la vulnérabilité du système informatique.

Sauf si celle-ci est légalement ou contractuellement tenue de le faire, l'organisation responsable demeure libre du choix de développer une solution et de la mettre en œuvre.

Bien entendu, le choix de ne pas résoudre une faille de sécurité avérée pourrait, le cas échéant, engager la responsabilité civile de l'organisation responsable si un dommage devait en résulter pour un tiers[66].

Dans la mesure du possible, la solution devrait être mise au point au plus tard dans les 90 jours calendrier.

Ces délais devraient être raccourcis au strict minimum en cas de mise en danger des utilisateurs des systèmes impactés ou de risques pour la protection des données à caractère personnel. Si

[66] Indépendamment même de l'existence ou non d'une politique de divulgation responsable.

l'organisation est incapable de résoudre le problème immédiatement, le système informatique en question devrait alors être mis hors service complètement à titre temporaire.

Cependant, la chaîne d'approvisionnement (*supply chain*) et la multiplicité des interdépendances entre les systèmes d'information peuvent compliquer le délai nécessaire à l'élaboration d'une solution et son déploiement.

Durant cette phase, l'organisation responsable (ou son prestataire) doit mener, d'une part, des tests positifs pour vérifier que la solution fonctionne correctement et, d'autre part, des tests négatifs pour s'assurer que la solution ne perturbe pas le bon fonctionnement des autres fonctionnalités existantes.

Lorsque la solution est prête et que la vulnérabilité concerne également d'autres organisations, celle-ci doit être transmise prioritairement et avant toute divulgation publique au CCB (vulnerabilityreport@cert.be).

L'organisation responsable devrait respecter un délai raisonnable à partir de cette transmission avant une éventuelle divulgation générale aux utilisateurs, afin de permettre aux opérateurs d'intérêt vital (opérateurs de services essentiels NIS, infrastructures critiques, administrations publiques, etc.) d'implémenter prioritairement la solution.

e. Eventuelle divulgation publique

Sauf obligation légale particulière, la divulgation publique d'une vulnérabilité n'est pas une étape obligatoire d'une CVDP. En effet, le participant et l'organisation responsable peuvent convenir de ne pas divulguer publiquement l'existence de la vulnérabilité. Cela pourrait être le cas si celle-ci s'avère trop difficile ou impossible à résoudre, ou si sa résolution impliquera des coûts démesurés en comparaison avec les éventuels risques encourus.

Cela doit toutefois rester l'exception dans la mesure où l'objectif d'une CVDP est d'améliorer la sécurité et la transparence vis-à-vis des utilisateurs. Certaines obligations légales imposent, par

ailleurs, l'organisation responsable informe les utilisateurs des systèmes d'information[67] ou les personnes physiques concernées par une violation de données à caractère personnel[68].

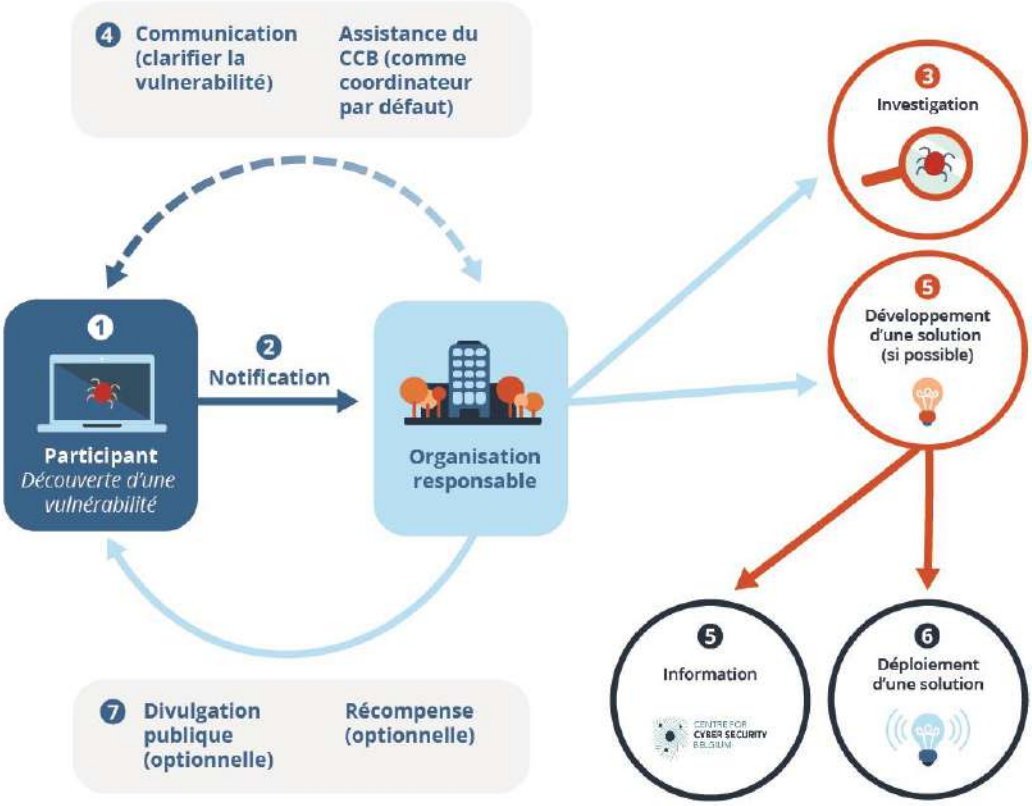
En tout état de cause, les informations relatives à une vulnérabilité qui concernerait également d'autres organisations devraient être divulguées au moins au CCB (vulnerabilityreport@cert.be).

Si la vulnérabilité est rendue publique, l'organisation responsable fixe, en coordination avec le participant, les modalités de sa publication. Idéalement, les informations sur la vulnérabilité et sa solution devraient être diffusés simultanément. Il est recommandé à l'organisation responsable d'informer ses clients par la publication d'un avis de sécurité via son site internet ou d'autres moyens de communication (courriel, lettre d'information, mise à jour du système, etc.).

L'organisation responsable devrait également informer les autres organisations probablement aussi concernées par la même vulnérabilité. L'éventuelle interdépendance des systèmes d'information ou la chaîne d'approvisionnement peut impliquer une coordination plus large de l'éventuelle divulgation.

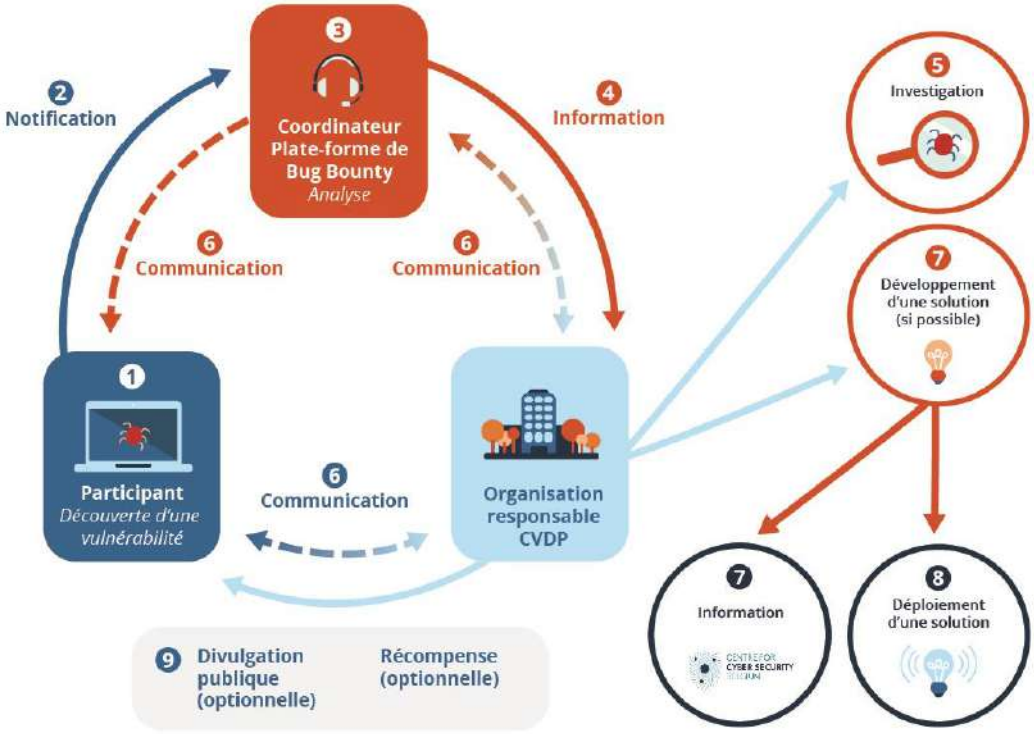
Il convient aussi de recueillir les commentaires des utilisateurs sur le déploiement de la solution et de prendre les mesures correctives nécessaires pour régler les éventuels problèmes posés par la solution, notamment de compatibilité avec d'autres produits ou services.

[67] Voir les règles de responsabilité contractuelle et extra-contractuelle notamment.
[68] Art. 34 du RGPD.



1. Le participant trouve une vulnérabilité dans le cadre d'un CVDP.
2. Le participant informe l'organisation responsable sur la base des détails de la CVDP.
3. L'organisation responsable analyse la vulnérabilité.
4. Communication continue entre le participant et l'organisation responsable afin de clarifier la vulnérabilité. L'assistance du CCB (en tant que coordinateur par défaut) peut être demandée s'il y a un manque de communication lors de ce processus.
5. 5 Une solution est élaborée (si possible). Dans le cas où la vulnérabilité peut également affecter d'autres organisations, l'organisation responsable en informe le CCB.
6. L'organisation responsable déploie la solution auprès de ses utilisateurs ou clients.
7. La divulgation publique peut être discutée et une récompense peut être accordée sur la base de la CVDP.

** Designed by CCB and Intigriti - 2020*



1. Le participant trouve une vulnérabilité dans le cadre d'un CVDP.
2. Le participant informe l'organisation responsable par l'intermédiaire d'un coordinateur, par exemple une plateforme de bug bounty, sur la base des détails de la CVDP.
3. Le coordinateur analyse la vulnérabilité.
4. Après validation, le coordinateur informe l'organisation responsable.
5. L'organisation responsable analyse la vulnérabilité.
6. 6 Communication continue entre le participant et l'organisation responsable afin de clarifier la vulnérabilité, si souhaité à travers le coordinateur.
7. 7 Une solution est élaborée (si possible). Dans le cas où la vulnérabilité peut également affecter d'autres organisations, l'organisation responsable en informe le CCB.
8. L'organisation responsable déploie la solution auprès de ses utilisateurs ou clients.
9. La divulgation publique peut être discutée et une récompense peut être accordée sur la base de la CVDP.

** Designed by CCB and Intigriti - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

D. REFERENCES

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure et *Economics of Vulnerability Disclosure*, 2018, www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

CENTRE FOR EUROPEAN POLICY STUDIES (CEPS), *Software vulnerability disclosure in Europe. Technology, Policies and Legal Challenges, Report of a CEPS Task Force, 2018,* www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges

GLOBAL CONFERENCE CYBER SPACE, *Best practice guide Responsible Disclosure*, 2015, www.gccs2015.com/sites/default/files/documents/BestPracticeRD-20150409_0.pdf

INTERNET ENGINEERING TASK FORCE (IETF) - CHRISTEY S. & WYSOPAL C., *Responsible Vulnerability Disclosure Process*, 2002, https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00 (www.circl.lu/pub/responsible-vulnerability-disclosure)

ORGANIZATION FOR INTERNET SAFETY, *Guidelines for responsible disclosure*, 2004, www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf

SOFTWARE ENGINEERING INSTITUTE, *The CERT Guide to Coordinated Vulnerability Disclosure, 2013 (updated in 2019)* https://vuls.cert.org/confluence/display/CVD

NATIONAL CYBER SECURITY CENTRE (NL), *Leidraad Coordinated Vulnerability Disclosure (Coordinated Vulnerability Disclosure: the Guideline),* 2019, //english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline et *Policy for arriving at a practice for Responsible Disclosure*, 2013

CIO PLATFORM NEDERLAND - CEG INFORMATION SECURITY, *Coordinated Vulnerability Disclosure. Model Policy and Procedure*, 2016, www.cio-platform.nl/en/publications et *Coordinated Vulnerability Disclosure 1.4. Implementation guide*, 2016, www.cio-platform.nl/en/publications

ISO/IEC 29147:2018 Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité (https://www.iso.org/standard/72311.html)

ISO/IEC 30111:2019 Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité (https://www.iso.org/standard/53231.html)

CENTRE FOR CYBER SECURITY BELGIUM

GUIDE SUR LES POLITIQUES DE DIVULGATION COORDONNEE DES VULNERABILITES
PARTIE I : LES BONNES PRATIQUES

Ce document et ses annexes ont été élaborés par le Centre pour la Cybersécurité Belgique (CCB), administration fédérale créé par l'arrêté royal du 10 octobre 2014 et sous l'autorité du Premier Ministre.

Le CCB décline toute responsabilité éventuelle en lien avec le contenu de ce document.

Les informations fournies :
• sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières ;
• ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points.

Éd. Responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur
Rue de la Loi, 16
1000 Bruxelles

Dépôt légal :
D/2020/14828/012

2020

CENTRE FOR CYBER SECURITY BELGIUM

GUIDE SUR LES POLITIQUES DE DIVULGATION COORDONNEE DES VULNERABILITES

PARTIE II : LES ASPECTS LEGAUX

COORDINATED VULNERABILITY DISCLOSURE POLICIES -"CVDP"
RESPONSIBLE DISCLOSURE POLICIES -"RDP"

CENTRE POUR LA CYBERSECURITE BELGIQUE
Rue de la Loi, 16
1000 Bruxelles

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

A. Table des matières

CENTRE FOR CYBER SECURITY BELGIUM

<u>Avertissement</u> :

Le présent guide vise à exposer les concepts, les objectifs, les questions juridiques et les bonnes pratiques liées à l'adoption de politiques de divulgation coordonnée des vulnérabilités (ou Coordinated Vulnerability Disclosure Policies – « CVDP ») dans l'état actuel de la législation en Belgique – voir les exemples fournis sur le site du CCB.

L'attention des lecteurs est attirée sur le fait que les documents élaborés par le CCB ne constituent nullement une modification des règles légales existantes. L'accès non autorisé au système informatique d'un tiers, même avec de bonnes intentions demeure une infraction pénale.

Le participant à une CVDP doit être conscient qu'il ne bénéficie pas d'une exclusion générale de responsabilité lorsqu'il participe à une telle politique : il doit agir avec précaution et respecter scrupuleusement toutes les conditions de la politique, ainsi que les dispositions légales applicables.

Designed by CCB and Intigriti (2020)

B. L'application du droit pénal belge

L'application du droit pénal belge dépend, principalement, de la localisation de l'infraction. Selon la théorie de l'ubiquité objective, une infraction est localisée dans le lieu de la réalisation de l'action et dans le ou les lieux de l'apparition de son résultat[1].

Pour cela, il suffit qu'un des éléments constitutifs matériels ou aggravants matériels[2] d'une infraction se soit réalisé sur le territoire belge, sans qu'il soit nécessaire que l'infraction ait été entièrement commise en Belgique. Ainsi, le droit pénal belge pourra s'appliquer lorsque soit l'auteur a posé des actes matériels en Belgique, soit le système informatique ou les données sont localisés en Belgique, ou soit encore les éventuels dommages sont survenus en Belgique.

Dans ce contexte, les règles décrites dans le présent guide pourront s'appliquer si l'auteur se trouve en Belgique lors de sa participation à la politique de divulgation coordonnée ou si le système informatique visité est localisé en Belgique.

En raison des règles communes de la Convention de Budapest sur la cybercriminalité[3] et de la législation européenne[4], certains éléments de la présente analyse juridique en Belgique peuvent être transposables à d'autres pays, notamment en Europe. Néanmoins, il convient à chaque fois de s'assurer auprès des autorités nationales compétentes que cela est bien le cas.

---

[1] Cass., 23 janvier 1979, *Pas.*, I, 1979, p. 582 ; Cass., 4 février 1986, *Pas.*, I, 1986, p. 664.
[2] Et non simplement intentionnels.
[3] Convention sur la Cybercriminalité du Conseil de l'Europe, faite à Budapest le 23 novembre 2001, entrée en vigueur le 1er juillet 2004.
[4] Directive 2013/40/UE du Parlement européen 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., 14 août 2013.

C. L'intrusion dans un système informatique[5]

Section 1. L'intrusion externe

L'article 550 *bis,* § 1er du Code pénal sanctionne celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient.

1. Les éléments constitutifs matériels

1.1. L'accès ou le maintien dans un système informatique

a) Un système informatique

La loi du 28 novembre 2000 relative à la criminalité informatique, qui a introduit l'article 550 *bis* dans le Code pénal, n'a pas défini ce qu'il fallait entendre par « système informatique »[6]. Les travaux préparatoires de la loi décrivent néanmoins les notions d'une part, de « système informatique » comme tout système permettant le stockage, le traitement ou la transmission de données et d'autre part, de « données » comme des représentations de l'information, indépendamment de leur forme

[5] Il nous semble préférable d'utiliser ici le terme d'intrusion plutôt que celui de « hacking » car dans le domaine informatique le « hacking » ne s'identifie pas entièrement à la notion de piratage informatique illégal et peut aussi viser des activités effectuées avec l'autorisation du responsable du système informatique. La notion d'intrusion signifie, elle, bien le fait de pénétrer dans un système informatique ou une partie du système, sans y avoir été autorisé.

[6] Sur ce point, l'imprécision du législateur semble intentionnelle afin d'éviter que les concepts ne soient trop rapidement dépassés par l'évolution des technologies de l'information : en ce sens, *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 12. ; Le législateur belge a tenu compte de l'évolution rapide de la technologie lors de l'élaboration de la loi du 28 novembre 2000 relative à la criminalité informatique de sorte que la terminologie de la loi est neutre d'un point de vue technologique : *Doc. Parl.*, Ch. Repr., 2003-2004, n°1284/001, p. 5.

matérielle (électromagnétique, optique ou autre), pouvant être stockées, traitées et transmises par le biais d'un système informatique[7].

On peut également se référer à la directive européenne 2013/40/EU du 12 août 2013 relative aux attaques contre les systèmes d'information[8], qui apporte une définition à ces deux notions :

- le « système informatique » est un dispositif ou un ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci[9] ;
- les « données informatiques » sont une représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système d'information exécute une fonction.

Le concept de système informatique dépasse donc celui du simple ordinateur personnel mais vise au sens large toutes les formes de systèmes traitant des données : une tablette électronique, un GPS, un smartphone, une montre électronique, un réseau, un serveur, un routeur, un décodeur, une télévision connectée, l'ordinateur de bord d'un véhicule, un terminal de paiement électronique, une carte à puce, etc.

[7] *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p.12.
[8] J.O., 14 août 2013 ; Voy. également les définitions de l'art. 1 de la Convention sur la Cybercriminalité du Conseil de l'Europe, faite à Budapest le 23 novembre 2001, entrée en vigueur le 1er juillet 2004 et approuvé par la Belgique (loi du 3 août 2012, *M.B.* du 21 novembre 2012, p. 69092).
[9] Ces éléments figurent également dans la définition de « réseau et système d'information » de la directive 2016/1148 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 (directive NIS).

b) L'accès ou le maintien

N'étant pas définies par le Code pénal ou les travaux parlementaires, les notions d'accès ou de maintien doivent être comprises dans le sens que leur donne le langage courant, sans exiger l'usage d'une technique particulière.

La notion d'accès implique un acte positif d'intrusion traduisant avec certitude la volonté de pénétrer dans le système informatique[10], sans nécessairement requérir des manipulations informatiques complexes[11] : il suffit, par exemple, d'exécuter une commande permettant la mise en route d'un système, l'ouverture d'un programme, la recherche d'un fichier ou le défilement d'un texte.

S'agissant d'une intrusion, l'auteur de l'infraction agira, généralement, de l'extérieur du système via une infrastructure de télécommunications et en déjouant des mesures de sécurité.

La notion d'accès ne requiert cependant pas qu'il y ait eu introduction, modification ou suppression de données dans le système informatique.

Le maintien envisage notamment l'hypothèse d'une personne qui accède par inadvertance (sans s'en rendre compte) à un système informatique sans autorisation et qui s'y maintient néanmoins après s'en être aperçu. Il peut s'agir également de la situation où une personne maintient son accès au système alors que son autorisation d'accès est expirée (par l'écoulement du temps ou par la fin de l'exercice d'une fonction)[12].

[10] Le terminal informatisé d'un système de transaction bancaire constitue, au sens de cette disposition, un système informatique : Corr. Termonde, 14 mai 2007, *T. Strafr.*, 2007, p. 403.
[11] Corr. Anvers, 10 novembre 2014, *T. Strafr.*, 2015, p. 94.
[12] Par exemple, le maintien d'une connexion au système informatique d'une entreprise par un ancien employé.

c) La protection du système informatique

L'infraction n'exige pas que l'accès ou le maintien dans un système informatique ait été commis suite à l'effraction du système ou au fait d'avoir déjoué des mesures de sécurité (mot de passe, firewall, identification, chiffrement, etc.). L'absence de mesures de protection du système informatique n'empêche donc pas l'existence d'une intrusion externe.

Au cours des travaux parlementaires, ce choix a été justifié par le fait que la notion d'effraction impliquerait, d'une part, un certain nombre de complications pratiques (la détermination d'un niveau requis de protection et la nécessité de révéler les systèmes de protection lors de l'établissement de la preuve) et, d'autre part, s'avèrerait probablement sans objet en raison de la standardisation croissante des protections des systèmes[13].

Une intrusion externe peut donc consister simplement à utiliser un réseau sans fil non sécurisé pour se connecter à internet, sans l'autorisation du gestionnaire de ce réseau[14].

d) Le dommage causé au système informatique

Il n'est pas requis que l'accès ou le maintien ait occasionné un dommage au système informatique. Un simple risque suffit, même s'il ne se réalise pas[15]. En effet, l'intrusion externe est considérée par le législateur comme « un délit de mise en danger punissable en tant que tel, quels que soient les intentions malveillantes particulières ou les effets atteints ».

Le législateur a voulu sanctionner pénalement en tant que tel le simple accès non autorisé dans un système informatique. Ainsi, la simple prise de connaissance du contenu, des paramètres de

[13] *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 17.
[14] Corr. Termonde, 14 novembre 2008, *T. straf.*, 2009, p. 114.
[15] Conformément à l'art. 550 *bis,* § 3, 3° du Code pénal, l'existence d'un dommage constituera néanmoins une circonstance aggravante de l'infraction.

fonctionnement ou de sécurité d'un système informatique tiers, même sans les altérer ou les endommager, peut constituer une infraction.

1.2. L'absence totale d'autorisation

La notion d'autorisation n'est pas précisée par le Code pénal de sorte que celle-ci doit, selon les principes d'interprétation en matière pénale, être entendue dans le sens usuel que lui prête le langage courant. En l'espèce, il s'agit de la permission accordée à autrui, par une personne habilitée d'accéder à ou de se maintenir dans le système informatique concerné.

Concrètement, deux situations peuvent se rencontrer : soit une personne s'introduit consciemment dans un système informatique alors qu'elle ne dispose d'aucune autorisation, même partielle, d'y accéder, soit une personne accède à un système informatique par inadvertance, ou sciemment après l'expiration de son autorisation, et s'y maintient néanmoins sans titre ni droit.

L'intrusion externe est une infraction instantanée de sorte que celle-ci existe dès le moment où l'individu accède ou se maintient dans le système informatique sans autorisation. L'autorisation éventuellement donnée postérieurement aux faits ne fait donc pas disparaître l'existence d'une infraction pénale.

Pour être valable, la permission d'accéder ou de se maintenir dans un système informatique doit nécessairement provenir d'une personne habilitée à cette fin par le titulaire des droits sur le système, à savoir le responsable de ce dernier[16]. C'est au responsable du système et à ses délégués qu'incombe, en définitive, la tâche d'accorder, de retirer et de fixer les conditions d'une telle habilitation. Cette autorisation peut être expresse autant que tacite, pour autant que celle-ci soit certaine.

[16] En fonction de la structure de l'organisation, cette personne pourra, par exemple, être le propriétaire du système, le dirigeant de l'organisation, le responsable informatique ou le conseiller en sécurité de l'information.

a) L'autorisation expresse

L'autorisation expresse consiste pour le gestionnaire du système informatique à habiliter explicitement une personne physique ou morale déterminée à accéder à son système informatique, par exemple, pour y mener des opérations de maintenance, des tests de sécurité ou de mise à jour de programmes. Cette habilitation expresse figure, généralement, dans des dispositions contractuelles ou dans des documents internes de l'organisation.

Lorsqu'une organisation conclut un contrat d'audit de sécurité impliquant la réalisation de tests d'intrusion[17], elle autorise expressément l'accès au moins à une partie de son système informatique. Dans cette hypothèse, le prestataire, spécialiste en sécurité informatique, dispose d'un accès autorisé et ne doit pas craindre de poursuites pénales pour hacking externe.

b) L'autorisation tacite

L'autorisation tacite va, quant à elle, résulter des circonstances particulières de la cause. Par exemple, l'exercice d'une fonction pour le compte d'une entreprise, qui implique nécessairement l'accès aux moyens informatiques de celle-ci pour accomplir ses tâches, même en l'absence d'une habilitation explicite[18].

Dans le même ordre d'idée, une habilitation tacite peut résulter de l'existence d'un système informatique mis sans ambiguïté à la disposition du public [19].

---

[17] Contrat de « pentesting ».
[18] Toutefois, l'employé recevra souvent de son employeur un identifiant et un mot de passe autorisant explicitement l'accès au système informatique.
[19] Par exemple, un réseau sans fil dans un espace public et sans mot de passe (« hotspots »), un ordinateur ou réseau sans fil d'un établissement mis à disposition de ses clients, une caisse de paiement automatisé, un kiosque d'enregistrement des bagages par les passagers dans un aéroport, etc.

Evidemment, le propriétaire du système informatique et ses représentants légaux disposent, par nature, d'une autorisation d'accès au moins tacite au système informatique concerné, tant que ceux-ci peuvent valablement se prévaloir de ces qualités.

Par contre, l'autorisation tacite disparaît dès le moment où prend fin la fonction exercée pour le compte de l'entreprise, le caractère public de l'accès, la mise à disposition des clients ou le droit de propriété. Le maintien ou l'accès dans le système informatique ultérieurement sera alors considéré comme une intrusion.

2. Elément moral

2.1. La volonté d'accès au système et la connaissance de l'absence d'autorisation

L'infraction nécessite simplement la volonté consciente et libre d'accéder à un système informatique ou de s'y maintenir alors que l'on sait ne pas y être autorisé. L'article 550 *bis* du Code pénal ne requiert pas d'intention spéciale, comme par exemple une intention frauduleuse ou le dessein de nuire. L'intrusion ou le maintien volontaire et non autorisé dans un système informatique suffit pour réaliser l'infraction. A l'inverse, l'intrusion qui est la conséquence d'une inadvertance, d'une inattention, d'une erreur de manipulation ou d'une maîtrise insuffisante de l'outil informatique (la personne ayant agi de bonne foi) n'est pas constitutive d'une infraction (si celle-ci n'est pas suivie d'un maintien dans le système informatique en connaissance de cause).

L'intrusion volontaire (non autorisée) visant la poursuite d'un mobile honorable, comme par exemple la recherche de failles de sécurité informatique dans un système informatique tiers, est bien constitutive d'une infraction[20]. En effet, le législateur a entendu sanctionner toute intrusion, sauf

[20] Corr. Hasselt, 21 janvier 2004, *Lim. Rechtsl.*, 2005, p. 133 ; *Computerr.,* 2004, liv. 3, p. 131 : par exemple, le fait pour un utilisateur de vérifier la sécurité du système de PC banking de sa banque, de découvrir qu'il est possible de réaliser des opérations susceptibles de préjudicier les utilisateurs du système (comme télécharger les listes des bénéficiaires de virement d'autres utilisateurs, modifier les numéros de compte bancaires de ces listes et de remettre ainsi la liste modifiée sur leur

involontaire, dans un système informatique sans se préoccuper de l'intention de l'intrus[21]. L'objectif est de protéger autant que possible la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui y sont stockées, traitées ou transmises.

Le fait pour l'intrus d'être bien intentionné ou d'avoir reçu une approbation postérieure aux faits du responsable du système informatique ne constitue donc pas une cause de justification excluant une potentielle condamnation pénale pour intrusion externe. Il est vrai qu'il serait facile pour des intrus d'invoquer de prétendus motifs bienveillants après le début des poursuites à leur égard et qu'il serait difficile de vérifier ceux-ci *a posteriori*.

La jurisprudence a ainsi confirmé que l'intrusion externe dans le simple but de vouloir vérifier si les mesures de sécurité informatique d'un concurrent pour la protection de ses données sont aussi peu fiables que les siennes constitue bien un délit[22].

L'intention frauduleuse de l'auteur intervient néanmoins comme une circonstance aggravante de l'infraction, laquelle va alourdir la peine infligée[23].

Section 2. L'intrusion interne

L'article 550 *bis*, § 2 du Code pénal vise celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique.

---

disque dur, en permettant des virements vers d'autres numéros de comptes que ceux des bénéficiaires) et d'en avertir sa banque, n'est pas une situation élusive de l'existence d'une infraction ; Corr. Eupen, 15 déc. 2003, *R.D.T.I.*, 2004, p. 61 et note O. LEROUX ; Corr. Louvain, 15 juin 2010, *T. Strafr.*, 2011, p. 270 ; Corr. Termonde, 25 mai 2007, *T.G.R.*, 2007, p. 351 et s.

[21] Corr. Bruxelles, 8 janv. 2008, *J.T.*, 2008, p. 337.

[22] Corr. Eupen, 15 déc. 2003, *R.D.T.I.*, 2004, p. 61.

[23] Art. 550 *bis,* § 1er, al. 2 du Code pénal.

1. Les éléments constitutifs matériels

1.1. L'existence d'une autorisation partielle

L'intrusion interne suppose l'existence, préalablement à la commission de l'infraction, d'une autorisation partielle d'accès au système informatique concerné[24]. En l'absence d'autres précisions du Code pénal, l'autorisation doit être entendue dans son sens courant, à l'instar de la notion d'autorisation visée pour l'intrusion externe (*supra*).

En effet, la nature et l'étendue du pouvoir d'accès à un système informatique ne sont, en principe, pas déterminées par le législateur mais laissées au pouvoir d'appréciation du propriétaire du système, étant le mieux placé pour déterminer qui reçoit le pouvoir d'accès et dans quelles limites[25].

Les limites posées à l'autorisation d'accès peuvent, par exemple, être « spatiales », c'est-à-dire liées à certaines portions interdites du système informatique, ou « fonctionnelles », c'est-à-dire liées à certaines opérations ou certaines catégories de données interdites sur l'ensemble du système. La restriction ne fait aucun doute lorsque, par exemple, le système est assorti pour accéder à certaines données ou programmes d'un processus d'identification préalable[26].

La finalité pour laquelle une personne reçoit une autorisation d'accès à un système informatique ne constitue pas, sauf mention explicite contraire du responsable du système, une limite à ce droit d'accès. On ne peut considérer qu'une personne aurait outrepassé son droit d'accès, au sens de l'article 550 *bis*, § 2 du Code pénal, au simple motif qu'elle aurait détourné ce pouvoir de sa finalité[27]. Par voie de conséquence, l'auteur qui utilise son droit d'accès à un système informatique pour des fins

[24] Corr. Louvain, 15 juin 2010, *T. Strafr.*, 2011, p. 270 : le tribunal a estimé que le fait d'être client d'une banque et de pouvoir accéder au système de pc banking ne donne pas la qualité de personne autorisée au système informatique de la banque.
[25] C.A., 24 mars 2004, n°51/2004, B.4.3, p. 7.
[26] Corr. Bruxelles, 8 janv. 2008, *J.T.*, 2008, p. 337.
[27] Cass., 24 janvier 2017, P.16.0048.N, *www.cass.be.*

privées alors qu'il a reçu une autorisation d'accès pour des fins professionnelles déterminées ne commet pas une intrusion interne.

La notion vise tant les personnes bénéficiant d'une habilitation partielle permanente, comme celle octroyée au personnel d'une entreprise, que les personnes bénéficiant d'une habilitation partielle limitée dans le temps, comme celle accordée temporairement à un consultant d'une société extérieure spécialisée en sécurité informatique.

Si l'autorisation partielle préalable se présente souvent dans le cadre de liens contractuels, cette notion n'implique pas nécessairement l'existence d'un pouvoir de subordination, d'un lien hiérarchique ou d'un rapport contractuel entre le donneur d'autorisation et le bénéficiaire.

1.2. Le dépassement de l'autorisation

L'infraction existe dès l'instant où l'auteur outrepasse ses droits d'accès pour pénétrer ou se maintenir dans une partie du système informatique à laquelle il n'était pas ou plus autorisé à accéder au moment de l'infraction[28].

Cette hypothèse vise entre autres la situation d'un employé qui s'est vu accordé un pouvoir d'accès partiel au serveur de son entreprise pour accomplir ses tâches mais outrepasse les limites qui lui ont été imposées.

Comme pour l'intrusion externe, l'intrusion interne ne doit pas nécessairement avoir entraîné de dommage au système visité pour être sanctionnée.

[28] Voy. Cass., 5 janvier 2011, P.10.1094.F., www.cass.be : la constatation que les personnes poursuivies avaient le droit d'accéder aux données litigieuses, lorsqu'ils en ont demandé et obtenu la copie, exclut le dépassement du pouvoir d'accès incriminé par l'article 550 *bis*, § 2, du Code pénal.

2. Elément moral

2.1. La volonté d'outrepasser son autorisation

L'infraction nécessite la volonté d'accéder, intentionnellement et en connaissance de cause, à une partie du système informatique ou de s'y maintenir alors que la personne sait qu'elle outrepasse ainsi ses pouvoirs d'accès au système informatique.

2.2. L'intention spéciale : frauduleuse ou le dessein de nuire

Le simple fait d'entrer sans autorisation dans certaines parties du système informatique, par exemple par simple curiosité, n'est pas sanctionnée pénalement. L'intrusion doit être motivée par une intention spéciale, consistant à la poursuite d'un but lucratif illicite (fraude) ou de malveillance (dessein de nuire), pour constituer une infraction. Par exemple, cela pourrait être le cas d'un employé qui, bénéficiant de l'accès à une partie du réseau de l'entreprise, excède cette autorisation pour accéder au programme comptable et y faire des opérations bancaires non autorisées ou encore commercialiser certaines données pour son propre compte[29].

Le législateur a justifié cette différence, avec l'infraction d'intrusion externe, par le fait que les tiers qui ne disposent d'aucune autorisation d'accès mettraient plus en danger la sécurité du système informatique qu'une personne bénéficiant d'une autorisation partielle[30]. De plus, les travaux parlementaires ont rappelé que le responsable du système disposait d'autres sanctions (civiles, disciplinaires ou contractuelles) contre le bénéficiaire d'une autorisation partielle qui aurait été outrepassée sans intention frauduleuse ou malveillante[31].

[29] *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/004, p. 6.
[30] *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 16.
[31] *Doc. parl.*, Sén., 1999-2000, 2-392/3, p. 6 ; *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 16.

Section 3. Les circonstances aggravantes de l'intrusion

L'article 550 *bis*, § 3 du Code pénal prévoit un certain nombre de circonstances aggravantes communes aux deux infractions liées à l'intrusion.

1. La reprise des données

La première circonstance aggravante est la reprise, de quelque manière que ce soit, de données stockées, traitées ou transmises par le système informatique visité[32]. Il s'agit du fait de s'accaparer, en original ou en copie, des données informatiques extraites du système visité afin de pouvoir, le cas échéant, les réutiliser[33]. La formulation utilisée « de quelque manière que ce soit » est très large de sorte qu'elle peut viser le fait d'imprimer, d'envoyer par courriel, de copier sur un support, de transférer dans un système de sauvegarde en nuage, de faire une capture d'écran, etc[34]. Le législateur visait ici notamment à lutter contre le vol de secrets d'entreprise dans le cadre d'espionnage industriel[35].

La notion de « reprise » des données semble nécessiter, enfin, un élément moral, résultant d'une démarche volontaire de l'auteur de récupérer ces données et non du simple enregistrement automatique de données par le système informatique utilisé pour commettre l'intrusion.

---

[32] Corr. Termonde, 14 mai 2007, *T. Strafr.*, 2007, p. 403.
[33] Ce comportement est parfois qualifié de « bitnapping », en référence au kidnapping de données.
[34] Il faut préciser toutefois que cette disposition ne vise pas le fait d'emporter matériellement le support sur lequel étaient imprimées ou stockées (par exemple, le vol de données imprimées, d'un disque dur ou d'une clé USB) des données informatiques, qui constitue lui une autre infraction, à savoir le vol du support lui-même.
[35] *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p.17; lorsque c'est un travailleur qui agit pour voler des secrets d'affaires de son employeur, celui-ci pourrait aussi être poursuivi pour le délit de communication de secrets de fabrique visé à l'art. 309 du Code pénal.

2. L'utilisation du système visité

La seconde circonstance aggravante est l'usage quelconque d'un système informatique appartenant à un tiers ou le fait de se servir du système informatique pour accéder au système informatique d'un tiers. D'une part, la disposition vise l'utilisation de la capacité du système informatique visité, en entraînant une limitation temporaire des possibilités d'utilisation d'autres utilisateurs (par exemple, le vol de temps ou de bande passante)[36]. D'autre part, elle concerne le fait d'accéder à un autre système informatique via le système visité, utilisé comme base de relais pour une attaque informatique en faisant croire que l'attaque provient d'un système intermédiaire[37].

Les deux situations visées supposent bien un élément moral, à savoir que l'auteur ait volontairement et, en connaissance de cause, eu l'intention de faire usage du système informatique à ces fins. Cet élément exclut, par exemple, la situation où la réduction de la capacité du système informatique découlerait, de façon imprévue, de l'intrusion.

3. Le dommage au système informatique ou aux données

La troisième circonstance aggravante consiste à causer un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui y sont stockées, traitées ou transmises, ou au système ou aux données informatiques d'un tiers.

Cela englobe tout type de dommage, qu'il soit matériel (détérioration physique du système, de câbles ou de périphériques) ou immatériel (engorgement préjudiciable du système, indisponibilité) au système informatique visité ou à ses données.

---

[36] *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 17.

[37] 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 », *op. cit.*, p. 639 ; Par exemple, il pourrait s'agir de l'utilisation du système informatique dans un réseau « botnet », c'est-à-dire dans un groupe d'ordinateurs infectés (« zombies ») et contrôlés à distance par un pirate informatique afin d'attaquer d'autres systèmes informatiques en dissimulant l'origine véritable de l'attaque.

Dans ce cas de figure, le dommage peut avoir été causé intentionnellement ou involontairement de sorte qu'aucun élément moral n'est requis dans le chef de l'auteur[38].

Section 4. La politique de divulgation coordonnée des vulnérabilités et l'intrusion

Comme exposé précédemment, l'infraction d'intrusion externe dans un système informatique existe, même lorsque l'auteur n'a pas d'intention malveillante, ne déjoue pas des mesures de sécurité, n'utilise pas le système visité, ne reprend pas des données et ne cause pas de dommage au système ou aux données. Les bonnes intentions du participant à une CVDP ne suffissent donc pas pour éviter l'existence de cette infraction pénale.

Toutefois, l'intrusion externe n'existe que lorsque le participant ne dispose pas d'une autorisation de l'organisation responsable d'accéder à son système informatique. Dès lors que le participant agit dans le cadre d'une autorisation, il n'y a pas d'intrusion externe.

Or, une politique de divulgation coordonnée des vulnérabilités ou un programme de récompenses des vulnérabilités contient une telle autorisation, soit expresse, soit tacite.

L'adoption d'une politique de divulgation coordonnée des vulnérabilités, en ce compris un programme de récompenses, constitue de facto au moins une autorisation tacite et certaine. En effet, celle-ci précise les modalités de collaboration entre une organisation responsable du système informatique considéré et des participants disposés à l'informer sur les vulnérabilités de son système informatique. Cette collaboration implique nécessairement une habilitation d'accéder au système informatique concerné ou de s'y maintenir, dans le but d'en améliorer la sécurité et sous respect des conditions

[38] La survenance de cette circonstance doit néanmoins être prévisible pour l'auteur et un lien de causalité doit exister entre celle-ci et la commission de l'infraction principale ; Le dommage causé intentionnellement découlant de l'introduction, de la modification ou de la suppression de données donnera, le cas échéant, lieu à une autre infraction, celle de violation de données informatiques visée à l'art. 550 *ter* du Code pénal.

préalablement définies. Même si le destinataire précis de l'habilitation n'est pas connu au moment de l'adoption de la politique de divulgation coordonnée, il s'agit là bien d'une autorisation, accordée unilatéralement par le responsable du système informatique, aux personnes souhaitant participer à son programme de divulgation coordonnée.

Eu égard au principe de légalité, le droit pénal est d'interprétation restrictive, ce qui a pour corollaire que le juge est tenu, en cas de doute sur la portée des termes répressifs utilisés, d'en limiter le champ d'application. L'absence d'autorisation, au sens de l'article 550 *bis* du Code pénal, devrait dès lors être interprétée dans un sens strict, c'est-à-dire dans l'hypothèse où aucun acte ne pouvait légitimement laisser croire aux tiers que l'organisation responsable autorisait l'accès à son système informatique. Lorsque l'organisation responsable a délibérément et sciemment adopté une politique de divulgation coordonnée, il existe une volonté préalable et claire de celle-ci d'autoriser l'accès, moyennant le respect des conditions définies, à son système informatique. Il faut préciser également qu'une partie de la jurisprudence soutient une interprétation extensive des dispositions favorables au prévenu, ce qui pourrait également être le cas de la notion d'autorisation. En ce qu'elle est favorable à l'auteur des faits et exclut l'existence d'une infraction, l'autorisation devrait être interprétée comme inhérente à l'adoption d'une politique de divulgation coordonnée.

L'intérêt d'une politique de divulgation coordonnée réside donc dans le fait d'exclure, pour autant que les conditions énoncées par l'organisation responsable soient respectées, une des conditions constitutives matérielles de l'infraction d'intrusion externe, à savoir l'absence totale d'autorisation. Le participant qui participe à une telle politique et en respecte les conditions ne commet donc pas d'intrusion externe.

Quant au participant qui est bénéficiaire d'une autorisation partielle d'accès à un système informatique, celui-ci ne commet pas une infraction d'intrusion interne lorsqu'il recherche, avec de bonnes intentions, des failles de sécurité dans des portions de ce système qui ne lui sont pas autorisées d'accès. Aussi longtemps que le participant outrepasse son pouvoir d'accès sans intention frauduleuse ou dans le but de nuire, il n'y a effectivement pas d'intrusion interne, pénalement sanctionnée.

Même si une politique de divulgation coordonnée des vulnérabilités a pour vocation de s'appliquer principalement aux personnes extérieures à l'organisation responsable et qui ne disposent pas de

pouvoir d'accès au système informatique, celle-ci pourrait, le cas échéant, également encadrer le comportement de participants internes à l'organisation et bien intentionnés. A défaut de règles contractuelles visant ces situations ou en cas de lacunes de celles-ci, une politique de divulgation coordonnée de l'organisation responsable pourrait, en effet, être utilement appliquée par les parties. L'intérêt d'une telle politique ne se limite donc pas aux seules personnes ne disposant pas de liens juridiques avec l'organisation responsable.

Bien entendu, il est nécessaire de limiter strictement, dans des documents contractuels[39] ou dans la politique de divulgation coordonnée de vulnérabilités, les circonstances dans lesquelles une telle transgression « bienveillante » pourrait avoir lieu et les règles à suivre dans ce cas de figure[40].

Avertissement :

Le participant doit être attentifs également à ne pas poser des actes, sans une autorisation complémentaire, sur des systèmes informatiques ou aux données gérés par des tiers à la politique de divulgation coordonnée de l'organisation responsable.

Les tiers ne sont pas tenus au contenu de la politique de divulgation responsable et pourraient, en effet, entreprendre des actions judiciaires en raison du comportement du participant.

[39] Par exemple, un contrat de travail, une relation statutaire ou un contrat de service.

[40] Il pourrait s'agir de la situation où le bénéficiaire d'une autorisation partielle, par exemple un employé du service informatique, soupçonne raisonnablement l'existence d'une vulnérabilité, d'un virus, d'un vers, d'un cheval de Troie ou d'un logiciel de rançon dans une partie du système auquel il n'est, en principe, pas autorisé à accéder.

D. La violation de données informatiques[41]

L'article 550 *ter* du Code pénal réprime celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique.

[41] Le choix du terme sabotage informatique n'est pas idéal dans la mesure où il induit erronément l'idée de l'existence d'un dommage, ce qui n'est pas un élément constitutif de l'infraction. L'infraction vise de manière plus large la violation de l'intégrité et de l'authenticité de données informatiques.

Section 1. Les éléments constitutifs matériels

1.1. L'introduction, la modification ou la suppression de données informatiques par tout moyen technologique

L'infraction a pour objet l'introduction, la modification, l'effacement de données ou la modification de l'utilisation normale de données par tout moyen technologique dans un système informatique. En substance, cette disposition vise à protéger l'intégrité d'un système informatique ou des données qu'il contient, stocke et transmet, contre les manipulations informatiques au sens large. L'intervention sur le système peut être directe, c'est-à-dire en utilisant un ordinateur directement connecté sur le réseau, ou de manière indirecte, c'est-à-dire par une connexion à distance via un réseau de télécommunications ou un ordinateur intermédiaire.

En pratique, il peut s'agir de l'introduction d'un virus, d'une bombe logique, d'un vers, d'un cheval de Troie, de la suppression ou de la création d'un fichier, du dérèglement d'un système d'exploitation, du cryptage de fichiers, de rendre un disque dur inutilisable ou plus simplement de la modification du mot de passe d'un utilisateur.

Contrairement à ce que l'on pourrait croire, le dommage n'est pas un élément constitutif de l'infraction, mais seulement une circonstance aggravante. Le simple fait de laisser une mention dans le système, tel que « x était ici », constitue une violation de données informatiques. Par contre, l'infraction demeure réalisée, même si l'introduction volontaire de données dans un ordinateur n'a pas atteint son objectif, par exemple en raison d'une défaillance technique.

1.2. L'absence d'autorisation

Il s'agit de punir toute manipulation de données informatiques[42] qui n'a pas été autorisée préalablement par le responsable du système informatique en question. L'autorisation doit porter sur la modification des données dans le système informatique, indépendamment de la question de l'accès autorisé ou non au système informatique.

[42] *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 19.

Section 2. Elément moral

Il faut que l'auteur ait eu conscience d'exécuter une opération illicite. La transmission involontaire, sans le savoir, d'un virus annexé à un courriel ne constitue donc pas une infraction dans le chef de l'expéditeur.

Section 3. Les circonstances aggravantes

1. L'intention frauduleuse ou le but de nuire

Si l'existence d'une intention spéciale dans le chef de l'auteur n'est pas requise pour l'infraction, elle constitue néanmoins une circonstance aggravante[43].

2. Le dommage aux données

Le dommage à des données dans le système informatique concerné ou dans tout autre système informatique est une circonstance aggravante de l'infraction[44]. On vise l'altération des données stockées, transmises ou traitées par le système informatique, par opposition au dommage causé au système lui-même.

3. L'entrave au fonctionnement du système

Cette circonstance aggravante vise la violation de données informatiques qui a pour conséquence d'empêcher, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique[45]. On vise ici la destruction du contenu, une paralysie totale ou partielle du système informatique ou encore un ralentissement. Par exemple, il peut s'agir

---

[43] Voy. les considérations émises sur l'intention spéciale requise pour l'infraction d'intrusion non autorisée interne ; Art. 550 *ter*, § 1 du Code pénal.
[44] Art. 550 *ter*, § 2 du Code pénal.
[45] Art. 550 *ter*, § 3 du Code pénal prévoit un emprisonnement de un an à 5 ans et une amende de 26 € à 100.000 € ou d'une de ces peines seulement; Le fait d'empêcher le bon fonctionnement d'un système informatique est, d'ailleurs, plus sévèrement puni, vu l'importance des systèmes informatiques dans nos sociétés, que le simple fait de causer un dommage à des données.

de l'envoi massif de requêtes de nature à surcharger son serveur ou même des dégâts physiques au système informatique causés à distance. En visant également tout « autre système informatique », cette disposition concerne également l'élaboration ou la diffusion de vers informatiques, lesquels possèdent la faculté de se dupliquer et de se répandre en copie automatiquement au travers des réseaux de communication. Il faut néanmoins qu'il existe un lien de causalité entre l'infraction principale et le dommage prévisible causé.

Section 4. La mise à disposition de moyens pour faciliter la violation de données

Indépendamment de l'infraction de violation de données informatiques, le Code pénal sanctionne aussi celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un dispositif y compris des données informatiques, principalement conçu ou adapté pour permettre la commission des infractions de violation de données informatiques, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique[46].

1. Les éléments constitutifs matériels

L'infraction vise l'élaboration, la détention ou la mise à disposition de dispositifs ou de données informatiques principalement conçus ou adaptés pour commettre une violation de données informatiques. La notion de dispositif est, ici, identique à celle relative aux moyens pour faciliter une intrusion.

2. Elément moral

L'infraction exige un élément intentionnel qui est de savoir que les dispositifs ou les données peuvent être utilisés pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique. L'auteur doit ainsi agir en connaissance de cause et avec la volonté d'élaborer, de posséder ou de mettre à disposition de tels dispositifs[47]. La possession involontaire et ignorée de tels dispositifs n'est, par voie de conséquence, pas constitutive de

[46] Art. 550 *ter*, § 4 du Code pénal.
[47] O. LEROUX, « La Criminalité informatique », *op. cit.*, p. 437.

l'infraction. De même, la seule possession d'un programme qui permet une utilisation tant légitime qu'illégitime ne constitue pas nécessairement une infraction.

A l'instar de l'infraction liée aux hacker tools, le terme « indûment » signifie que la possession ou la mise à disposition intentionnelle mais justifiée par un usage académique[48], scientifique ou professionnel n'est pas pénalement sanctionnée.

Section 5. La tentative

La tentative est punie des mêmes peines que la violation de données informatiques elle-même[49].

Toutefois, la tentative ne sera réalisée que si l'auteur a mis en œuvre non seulement des actes préparatoires mais également des actes d'exécution univoques[50].

Section 6. La politique de divulgation coordonnée des vulnérabilités et la violation de données informatiques

En participant à une politique de divulgation coordonnée des vulnérabilités, le participant dispose, en principe, d'une autorisation d'introduire ou de tenter d'introduire des données informatiques dans le système concerné. Il apparaît effectivement difficile de mener des recherches de failles de sécurité sans tenter au moins d'introduire des données ou d'exécuter des commandes contenant de telles données.

Par contre, l'autorisation de modifier ou de supprimer (ou de tenter de telles actions) des données informatiques dépend de la manière dont la politique de divulgation coordonnée des vulnérabilités est rédigée. Pour éviter de commettre une violation de données informatiques, le participant devra

[48] Par exemple, l'enseignement de la sécurité informatique.
[49] Art. 550 *ter*, § 6 du Code pénal.
[50] Voy. les développements sur la tentative d'intrusion dans un système informatique.

veiller à respecter strictement les conditions de la politique quant à la modification et la suppression de données informatiques.

En fonction du contenu de la politique de divulgation coordonnée des vulnérabilités et du respect par le participant de ces conditions, l'infraction de violation aux données informatiques existera ou non[51].

S'agissant des dispositifs permettant de commettre une violation de données informatiques, le participant pourrait élaborer, détenir ou mettre à disposition de tels dispositifs dans le cadre de la participation à une politique de divulgation des vulnérabilités. Ces actions ne seraient pas illicites tant qu'elles sont justifiées par des fins légitimes, et non indûment, de recherches de vulnérabilités avec l'accord de l'organisation du responsable du système informatique concerné.

A nouveau, le participant devra néanmoins prouver qu'il participe concrètement à une politique existante de divulgation des vulnérabilités et que celle-ci est bien identifiable. La simple intention de participer hypothétiquement et de manière générale à de telles politiques ne suffirait pas.

E. Le faux en informatique et la fraude informatique

Section 1. Le faux en informatique[52] et l'usage de faux en informatique[53]

L'article 210 *bis* du Code pénal punit le faux qui consiste, à introduire dans un système informatique, à modifier ou effacer des données, qui sont stockées, traitées ou transmises par un système informatique, ou à modifier par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là, modifier la portée juridique de telles données[54].

[51] Et elle pourra, le cas échéant, être accompagnée de circonstances aggravantes.
[52] Art. 210 *bis*, § 1er.
[53] Art. 210 *bis*, § 2.
[54] Art. 210 *bis*, § 1 du Code pénal.

Cette disposition sanctionne aussi d'une part, l'usage des données obtenues par un faux en informatique, tout en sachant que celles-ci sont fausses[55] et, d'autre part, la tentative de commettre un faux en informatique[56].

1. Les éléments constitutifs matériels

1.1. Une altération de la vérité par un des modes prévus par la loi (introduction, modification ou suppression de données)

Le faux ne dispose pas d'une définition légale mais la jurisprudence a précisé que celui-ci implique une altération de la vérité susceptible de faire naître, à l'égard de tiers, des droits dont ces derniers seraient dans l'impossibilité pratique de vérifier l'exactitude. Il peut s'agir, par exemple, de la création et de l'utilisation d'une fausse adresse de courriel au nom d'une personne tierce, d'une fausse annonce de vente en ligne ou d'un faux profil sur un réseau social. Les données susceptibles d'être falsifiées doivent donc avoir une portée juridique et s'imposer à la foi publique[57].

Il peut s'agir de fichiers informatiques enregistrés dans le disque dur d'un terminal ou sur un support optique ou numérique (à condition que celui-ci soit exécuté sur un système), ou encore des données en cours de transmission sur un réseau. Par contre, l'altération d'un document papier sur lesquels sont imprimées des données informatiques relève, lui, du faux en écriture.[58]

[55] Art. 210 *bis*, § 2 du Code pénal.
[56] Art. 210 *bis*, § 3 du Code pénal.
[57] *Doc. Parl.*, Ch. Repr., 1999-2000, n°0213/001, p. 10.
[58] Art. 194 et s. du Code pénal.

1.2. Une modification de la portée juridique des données

Pour réaliser l'infraction, il faut que la manipulation de données ait entraîné une modification de la portée juridique de celles-ci. La portée juridique correspond aux données modifiées prises dans leur ensemble et non à une unité. L'altération peut toucher les données informatiques elles-mêmes ou la pensée qu'elles expriment.

Les travaux parlementaires citent, par exemple, la confection de fausses cartes de crédit[59] ou la falsification de cartes de crédit, la création de faux contrats numériques ou la falsification de contrats numériques, ou encore l'introduction dans un système informatique d'un faux numéro de carte de crédit.

2. Elément moral

L'infraction exige une intention frauduleuse ou le dessein de nuire[60]. Ce dol spécial se justifie par l'assimilation du faux en informatique aux autres catégories de faux. L'intention frauduleuse consiste en la volonté de se procurer ou de procurer à autrui un profit ou un avantage illicite. Le dessein de nuire vise, quant à lui, la volonté de nuire à une personne physique ou morale.

De seules erreurs, négligences ou imprudences ne sont dès lors pas suffisantes pour constituer une infraction de faux en informatique.

De même, la réalisation ou l'usage d'un faux en informatique ne sont pénalement pas sanctionnés lorsque l'auteur agit à des fins d'enseignement, scientifiques ou professionnelles.

---

[59] Il s'agit notamment de réprimer la pratique du « skimming », soit la copie illégale des données d'une carte bancaire de paiement, qui réunit souvent les infractions de faux en informatique, de fraude informatique et d'intrusion non autorisée dans un système informatique tiers.
[60] Voy. l'article 193 du Code pénal.

1. La tentative

La tentative de commettre un faux en informatique est aussi incriminée, sans qu'il ne soit nécessaire dès lors qu'un préjudice se réalise effectivement.

La tentative implique néanmoins à la fois des actes préparatoires mais également des actes d'exécution qui ne laissent pas de doute sur l'intention criminelle de l'auteur[61].

Section 2. La fraude informatique

L'article 504 *quater* du Code pénal incrimine celui qui cherche à se procurer, pour lui-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.

1. Les éléments constitutifs matériels

1.1. La manipulation de données

L'infraction implique l'introduction, la modification[62] ou la suppression de données dans un système informatique ou dans le recours à une technologie, quelle qu'elle soit, permettant de modifier l'usage normal de données stockées, traitées ou transmises par un système informatique (voir *supra* le faux en informatique).

[61] Voy. la tentative d'intrusion dans un système informatique.
[62] Par exemple, la modification du solde d'un compte bancaire.

1.2. La poursuite d'un avantage économique illégal

L'infraction n'exige pas l'obtention concrète de l'avantage économique illégal recherché mais simplement la poursuite d'un tel objectif, même si celui-ci n'a finalement pas été obtenu. La fraude informatique est un délit de simple mise en danger ou délit « formel », qui implique seulement de démontrer que le traitement de données était en lien causal avec la poursuite d'un avantage économique illicite. L'avantage économique[63] peut être direct ou indirect et prendre différentes formes : biens matériels, biens immatériels, prestations. Celui-ci peut être à l'avantage de l'auteur ou d'une autre personne.

2. Elément moral

La fraude informatique suppose que l'auteur ait eu non seulement connaissance de commettre volontairement l'infraction mais aussi qu'il ait poursuivi une intention spéciale, à savoir une intention frauduleuse de se procurer pour soi-même ou pour autrui un avantage économique illégal.

3. La tentative

La tentative de fraude informatique est également sanctionnée[64].

A nouveau, la tentative ne sera établie que si le ministère public apporte la preuve de ce que l'auteur a mis en œuvre non seulement des actes préparatoires mais également des actes d'exécution univoques.

---

[63] L'article 504 *quater* exigeait auparavant que l'auteur se procure, pour lui-même ou pour autrui, un avantage patrimonial frauduleux, ce qui n'était pas entièrement conforme avec l'article 8 de la Convention du Conseil de l'Europe sur la Cybercriminalité : *Doc. Parl.*, Ch. Repr., 2003-2004, n°1284/001, p. 6 et 8.

[64] Voy. les considérations relatives à la tentative d'intrusion illicite.

Section 3. La politique de divulgation coordonnée des vulnérabilités, le faux en informatique et la fraude informatique

Le faux en informatique nécessitant une intention frauduleuse ou le dessein de nuire, la participation à une politique de divulgation coordonnée des vulnérabilités exclut pour le participant cette infraction. Dans le même ordre d'idée, le participant à une politique de divulgation coordonnée ou à un programme de récompenses des vulnérabilités ne s'expose, en principe, pas à des poursuites pénales pour fraude informatique, compte tenu de l'absence d'intention frauduleuse dans son chef.

F. Les infractions relatives au secret des communications

Section 1. Infractions relatives au secret des communications non accessibles au public et des données d'un système informatique

L'article 314*bis* du Code pénal punit quiconque qui, intentionnellement et à l'aide d'un appareil quelconque, intercepte ou fait intercepter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des communications non accessibles au public, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications[65].

1. Elément matériel

1.1. L'interception, la prise de connaissance ou l'enregistrement, à l'aide d'un appareil

A défaut d'une définition légale, l'interception, la prise de connaissance ou l'enregistrement d'une communication doivent s'entendre au sens du langage courant. Tout d'abord, l'interception consiste à prendre au passage et par surprise une communication qui est adressée, envoyée ou destinée à quelqu'un autre. Ensuite, la prise de connaissance d'une communication signifie le fait de savoir

[65] Art. 314 *bis*, §1er, 1° du Code pénal.

l'existence et le contenu d'une communication entre des personnes alors que l'on n'est pas destinataire de cette communication. Cette dernière notion a un sens large et s'applique aussi à des formes de communications techniques, comme la transmission électronique de données. Enfin, l'enregistrement vise l'action de fixer des données sur un support matériel local ou à distance[66], afin de pouvoir les utiliser ultérieurement.

L'incrimination du fait d'intercepter une communication vise à punir, outre l'auteur de l'infraction, celui qui en a donné l'ordre[67].

La disposition précise encore que l'interception[68], la prise de connaissance ou l'enregistrement doit intervenir à l'aide d'un appareil quelconque[69]. Cette formule est large mais elle implique nécessairement l'usage d'un matériel d'assistance technique, à défaut les faits ne sont pas punissables. Cela semble être le cas dès le moment où une manipulation informatique est effectuée ou un programme utilisé[70].

1.2. Les communications non accessibles au public, auxquelles on ne prend pas part

L'article 314 *bis* du Code pénal précise désormais que les communications visées sont « des communications non accessibles au public » et non plus « des communications ou télécommunications

[66] Par exemple, via un service de sauvegarde en nuage.
[67] *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 8-9.
[68] La disposition n'exige désormais plus que les communications soient interceptées « durant leur transmission ». Les travaux parlementaires expliquent cette adaptation par le fait que les dernières évolutions dans le domaine de l'informatique rendent souvent impossible le fait de déterminer précisément quand une communication est toujours en cours de « transmission » et quand elle est déjà délivrée. En effet, il est difficile de déterminer si un courriel non lu doit être considéré comme une communication délivrée ou comme une communication en cours de transmission : *Doc. Parl.*, Ch. Repr., 2015-2015, n°1966/001, p. 54.
[69] *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 6.
[70] A l'inverse, la simple visualisation directe sur un écran d'ordinateur d'un courriel ou d'une page internet, laissés ouverts et sans manipulation quelconque, échappe à l'infraction.

privées »[71]. Il semble que l'on puisse interpréter cette notion, comme auparavant, en fonction du contexte et des intentions des participants à la communication[72]. Le caractère non accessible au public correspond au fait que les communications ne sont pas destinées à être entendues par d'autres personnes, que les correspondants de la communication[73]. Le caractère professionnel ou non d'une communication n'a, en principe, pas d'incidence pour en apprécier la nature non accessible au public[74].

La communication vise notamment la transmission électronique de données dans des ordinateurs ou des réseaux d'ordinateurs[75]. On vise ici notamment les courriers électroniques.

La disposition incrimine uniquement les personnes qui ne prennent pas part à la communication. A l'inverse, le participant à une communication non accessible au public qui enregistre celle-ci, même à l'insu des autres interlocuteurs, ne commet pas une infraction à l'article 314 *bis* du Code pénal.

1.3. L'absence de consentement des participants

Pour échapper à l'infraction, il faut avoir obtenu au préalable le consentement de tous les participants à la communication électronique et non uniquement de certains d'entre eux. Le consentement des participants peut être exprès ou tacite en résultant d'un ensemble de circonstances, pour autant qu'il

[71] Art. 32 de la loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocale, *M.B.* du 17 janvier 2017, p. 2738 ; Les travaux parlementaires justifient cette modification comme une adaptation terminologie, compte tenu des modifications apportées aux articles 90 *ter* et s. du Code d'instruction criminelle.

[72] *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 6 ; Les travaux parlementaires exposent également que la notion de « communications non accessibles au public » consiste dans des communications ou communications qui ont lieu dans la sphère privée. Il s'agit donc d'une notion globale qui recouvre également les termes anciens de « communications ou télécommunications privées » : *Doc. Parl.*, Ch. Repr., 2015-2015, n°1966/001, p. 53.

[73] *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 7 ; Commission de la protection de la vie privée, Recommandation n°08/2012 du 2 mai 2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail, www.privacycommission.be.

[74] *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 8 et n°843/2, pp. 10 et 36.

[75] En ce sens : *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 7.

soit certain. Certains auteurs ajoutent que ce consentement devrait être donné nécessairement de manière spécifique et individuelle, et non pas être déduit d'un accord préalable contenu, par exemple, dans une clause d'un contrat de travail ou d'un règlement interne. Celui-ci devrait également être obtenu de manière loyale et dans le respect de l'éventuelle finalité annoncée aux participants.

2. Elément moral

L'infraction exige explicitement que l'auteur agisse intentionnellement, c'est-à-dire agir sciemment. Les travaux parlementaires indiquaient clairement qu'une simple coïncidence ou indiscrétion ne suffit pas pour constituer l'infraction[76]. Par voie de conséquence, la découverte purement fortuite de communications non accessibles au public n'est pas punissable. Toutefois, celui qui agit volontairement mais par simple curiosité commet l'infraction[77]. Par exemple, la prise de connaissance fortuite du contenu d'une communication par un technicien lors de la vérification du bon fonctionnement d'un système informatique n'est pas incriminée, sauf s'il a agi intentionnellement par curiosité.

Section 2. Les actes préparatoires

1. L'installation d'un appareil

1.1 Elément matériel

Le Code pénal incrimine l'auteur qui installe ou fait installer un appareil quelconque qui puisse permettre une interception, une prise de connaissance ou un enregistrement illicite de

[76] *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 7.
[77] *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 6.

communications[78]. En effet, il se peut que la personne qui place l'appareil ou le fait placer et celle qui l'emploie ne soit pas nécessairement la même[79].

1.2 Elément moral

L'infraction nécessite que l'auteur agisse avec l'intention de commettre une interception, une prise de connaissance ou un enregistrement illicite.

2. La mise à disposition d'un dispositif

2.1. Les éléments constitutifs matériels

Le législateur réprime celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission d'une interception illicite de communication[80].

La notion de « dispositif » s'entend des moyens d'accès ou d'autres outils qui sont conçus, par exemple, pour altérer, voire détruire des données, ou pour s'ingérer dans le fonctionnement des systèmes, tels que les programmes-virus, ou bien des programmes conçus ou adaptés pour accéder à des systèmes informatiques[81].

[78] Art. 314 *bis*, §1er, 2° du Code pénal.
[79] *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 9.
[80] Art. 314 *bis*, § 2 *bis* du Code pénal.
[81] *Doc. Parl.*, Ch. Repr., 2003-2004, n°1284/001, p. 6.

2.2. Elément moral

Comme pour la mise à disposition de moyens pour faciliter une intrusion non autorisée, l'auteur doit avoir volontairement et en connaissance de cause, élaboré, possédé ou mis à disposition un tel dispositif. Il doit dès lors avoir eu connaissance du fait que le dispositif incriminé a été principalement conçu ou adapté pour permettre une interception, un enregistrement et une prise de connaissance illicite de communications.

Le terme « indûment » signifie néanmoins que la détention ou la mise à disposition de tel dispositif à des fins légitimes telles que scientifiques ou professionnelles en matière de sécurité des systèmes de communications, n'est pas répréhensible.

Section 3. Le recel de communications illicitement obtenues

Le Code pénal sanctionne quiconque détient, révèle ou divulgue sciemment à une autre personne le contenu de communications non accessibles au public ou de données d'un système informatique illégalement interceptées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon[82].

1. Elément matériel

1.1. Le contenu de communications non accessibles au public ou de données d'un système informatique illégalement interceptées ou enregistrées, ou dont on a pris connaissance illégalement

La personne qui reçoit par erreur ou incidemment une communication qui ne lui était pas destinée, ne commet pas l'infraction.

[82] Art. 314 *bis*, § 2 du Code pénal.

1.2. La détention, la révélation, la divulgation à une autre personne ou l'utilisation d'une manière quelconque

Il est renvoyé à propos de ces mêmes notions aux développements consacrés au recel de données informatiques illicitement obtenues.

2. Elément moral

Il faut avoir agi « sciemment », c'est-à-dire volontairement et en connaissance de cause de l'illégalité de l'information obtenue.

Section 4. La tentative

La tentative d'interception illicite de communications non accessibles au public est également sanctionnée[83].

Celle-ci nécessite de prouver la réalisation d'actes préparatoires et d'actes d'exécution qui ne laissent pas de doute sur l'intention criminelle de l'auteur.

[83] Art. 314 *bis*, § 3 du Code pénal ; Voy. Corr. Bruxelles, 8 janvier 2008, *J.T.*, 2008, p. 337, pour un exemple de tentative d'interception de communications avec l'utilisation d'un « keylogger », soit un logiciel mouchard qui récolte l'activité (touches du clavier) d'un ordinateur et les renvoie vers un tiers.

Section 5. Le secret des communications électroniques

L'article 145 de la loi du 13 juin 2005 relative aux communications électroniques sanctionne pénalement différents comportements contraires au secret des communications électroniques, protégé par l'article 124 de cette même loi.

Ces différentes sanctions visent à garantir le caractère confidentiel des informations transmises via un réseau de communications électroniques[84].

1. Les éléments constitutifs matériels

1.1. L'autorisation des personnes directement ou indirectement concernées

Malgré la formule large utilisée par la loi qui laisse à penser que toutes les personnes directement ou indirectement concernées par la communication et par son contenu devraient donner leur consentement[85], il semble néanmoins plus raisonnable de considérer que seules les personnes auxquelles se rattachent, directement ou indirectement la communication, doivent consentir à la prise de connaissance, à savoir l'expéditeur et le ou les destinataire(s). S'agissant de données de connections ou de pages internet consultées, il suffit alors d'obtenir le consentement de l'utilisateur concerné.

[84] *Doc. Parl.*, 2004-2005, n°1425-1426/01, p. 76.

[85] Commission de la protection de la vie privée, Avis n° 8/2004 du 14 juin 2004 sur l'avant-projet de loi relatif aux communications électroniques, p. 7, www.privacycommission.be : la CPVP s'interrogeait sur le fait qu'une personne mentionnée dans le contenu d'un message était indirectement concernée par la communication aux termes de la loi, ce qui était plus étendu que le texte européen.

1.2. La prise de connaissance intentionnelle par une personne de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement[86]

1.2.1. L'information transmise par voie de communication électronique

La loi du 13 juin 2005 fournit une définition indirecte de la notion de communication électronique par les définitions de *service de communications électroniques*, à savoir « le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission, en ce compris les opérations de commutation et de routage, de signaux sur des réseaux de communications électroniques (…) » et de *réseau de communications électroniques*, à savoir « les systèmes de transmission, et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques (…) »[87]. Pour sa part, le Code de droit économique définit le courrier électronique, comme « tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère » [88].

La notion de communication électronique comprend les communications téléphoniques, les courriels, les sms, les messages envoyées par réseau sans fil ou échange de données cellulaires, les connexions à un réseau ou à un système informatique. Cette notion englobe donc les courriels et les données de connexion à l'internet qui permettent d'identifier les sites consultés.

---

[86] Art. 124, al. 1 de la loi du 13 juin 2005 relative aux communications électroniques.
[87] Art. 2, 3° et 5° de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.* du 20 juin 2005, p. 28070.
[88] Loi du 15 décembre 2013 portant insertion du Livre XII, « Droit de l'économie électronique » dans le Code de droit économique, portant insertion des définitions propres au Livre XII et des dispositions d'application de la loi propres au Livre XII, dans les Livres I et XV du Code de droit économique.

La prise de connaissance désigne l'information dans son ensemble y compris le contenu du courrier électronique[89]. En effet, la personne qui a pris connaissance de l'existence d'un courrier électronique et en a fait usage a nécessairement pris simultanément connaissance de son contenu. La prise de connaissance et l'usage du contenu d'un courriel sont liés à la prise de connaissance et à l'usage de l'existence de ce courrier électronique[90]. On peut considérer que l'article 124 de la loi du 15 juin 2005 fait donc obstacle à la prise de connaissance du contenu de la communication électronique.

1.2.2. L'information de toute nature qui ne lui est pas destinée personnellement

La prise de connaissance d'une information de toute nature qui est destinée personnellement à celui qui en prend connaissance ne constitue pas une violation de l'article 124, al. 1 de la loi du 15 juin 2005.

1.3. L'identification intentionnelle des personnes concernées par la transmission de l'information et son contenu

L'article 124, al. 2, interdit l'identification des personnes concernées tant par la transmission que par son contenu. Cela vise tant les données relatives à l'identité de l'expéditeur, du ou des destinataires des messages que celles relatives aux personnes concernées par le contenu (par exemple, celles citées dans le courrier électronique).

[89] Cass., 1 oct. 2009, C.08.0064.N, www.cass.be. La doctrine hésitait à considérer l'article 124 comme visant, outre l'existence d'une information, aussi le contenu de l'information elle-même. Voy. Commission de la protection de la vie privée, Avis n° 8/2004 du 14 juin 2004 sur l'avant-projet de loi relatif aux communications électroniques, p. 6, www.privacycommission.be : « la disposition vise à protéger les communications (contenu et données de trafic) de toute prise de connaissance ou manipulation par une personne autre que les parties à la communication ».
[90] *Ibidem*.

1.4. La prise de connaissance intentionnelle de données en matière de communications électroniques et relatives à une autre personne[91]

Les données relatives aux communications électroniques sont celles qui transitent par réseau telles que l'adresse de courrier électronique de l'expéditeur et du destinataire, l'heure de l'envoi et de la réception, les données de routage, la taille du message, la présence de pièces jointes, etc[92].

La prise de connaissance correspond au fait de connaître l'existence et le contenu de données relatives à une communication électronique entre des personnes alors que l'on n'est pas destinataire de cette communication.

1.5. La modification, la suppression, la révélation, le stockage ou l'usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non[93]

Il est interdit de modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement mais également de celles obtenues de manière fortuite.

2. Elément moral

Cette disposition implique que les actes incriminés doivent intervenir de manière intentionnelle dans le chef de l'auteur de l'infraction. Lorsqu'il est établi que la prise de connaissance d'une communication électronique est intervenue fortuitement, le caractère intentionnel de la découverte fait défaut et l'article 124 de la loi du 13 juin 2005 ne s'applique pas[94]. Une distinction doit dès lors

---

[91] Art. 124, al. 3 de la loi du 13 juin 2005 relative aux communications électroniques.
[92] C.T. Bruxelles, 10 février 2004, R.G. 44002, www.juridat.be.
[93] Art. 124, al. 4 de la loi du 13 juin 2005 relative aux communications électroniques.
[94] C.T., Mons, 8 déc. 2010, *JLMB*, 2011, p. 715 ; *Chron. D.S.*, 2011, p. 399; C.T., Bruxelles, 4 décembre 2007, *J.T.T.*, 2008, p. 179 ; T.T. Liège, 19 mars 2008, RG 360.454, www.juridat.be.

être faite entre la prise de connaissance active d'une communication électronique et la prise de connaissance purement fortuite.

3. Les exceptions prévues par l'article 125 de la loi

L'article 125 de la loi du 13 juin 2005 relative aux communications électroniques prévoit un certain nombre d'exceptions au secret des communications visées à l'article 124 de la même loi et de l'article 314 *bis* du Code pénal. Cette disposition permet entre autres[95] de poser les actes, en principe, prohibés lorsqu'ils sont nécessaires pour vérifier le bon fonctionnement du réseau et pour assurer la bonne exécution d'un service de communications électroniques. En raison des termes généraux de la loi, il semble que cette disposition puisse s'appliquer tant à un réseau public de communications électroniques qu'à un réseau privé.

Pour autant que cela soit justifié par des mesures d'ordres strictement techniques, il est dès lors possible d'accomplir les actes visés à l'article 124. Les informations relatives à des communications électroniques découvertes à cette occasion ne pourraient toutefois être utilisées à d'autre fin que le contrôle du bon fonctionnement du réseau.

4. Les communications électroniques frauduleuses[96]

1. Les éléments constitutifs matériels

Il s'agit de la réalisation, frauduleusement, de communications électroniques au moyen d'un réseau de communications électroniques.

[95] Art. 125, § 1er, 1° de la loi du 13 juin 2005 relative aux communications électroniques prévoit aussi la possibilité d'une dérogation lorsque la loi permet ou impose l'accomplissement des actes incriminés : la commission de la vie privée estime que l'article 16 de la loi du 3 juillet 1978 relative aux contrats de travail constituerait un fondement légal, moyennant le respect de certaines conditions.
[96] Art. 145, § 3, 1° de la loi du 13 juin 2005 relative aux communications électroniques.

2. Elément moral

Outre la volonté d'agir sciemment, cette infraction implique que l'auteur ait eu une intention spéciale, à savoir de vouloir se procurer ou de procurer à autrui un avantage illicite.

3. La tentative et les actes préparatoires[97]

La loi incrimine également la personne qui tente de réaliser frauduleusement des communications électroniques ou installe un appareil quelconque destiné à réaliser de telles communications.

Comme les autres tentatives, celle-ci nécessite de prouver la réalisation d'actes préparatoires et d'actes d'exécution univoques.

5. L'utilisation illicite d'un réseau ou d'un service de communications électroniques[98]

1. Les éléments constitutifs matériels

La loi sanctionne la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques dans un but illicite.

2. Elément moral

L'infraction implique que l'auteur veuille importuner son correspondant ou provoquer des dommages.

[97] Art. 145, § 3, 3° de la loi du 13 juin 2005 relative aux communications électroniques.
[98] Art. 145, § 3 *bis* de la loi du 13 juin 2005 relative aux communications électroniques.

3. La tentative et les actes préparatoires

La loi incrimine aussi la personne qui installe un appareil quelconque destiné à commettre une utilisation illicite d'un réseau ou d'un service de communications électroniques, ainsi que la tentative de commettre celle-ci.

Pour la tentative, il faudra établir que l'auteur ait accompli des actes préparatoires et des actes d'exécution univoques.

Section 6. La politique de divulgation coordonnée des vulnérabilités et les communications

Le participant ne peut intentionnellement intercepter, prendre connaissance ou enregistrer, avec un appareil quelconque, une communication non accessible au public[99]. Cela n'est d'ailleurs pas nécessaire à la mise en œuvre d'une politique de divulgation coordonnée des vulnérabilités.

Cependant, l'interception, la prise de connaissance ou l'enregistrement d'une communication non accessible au public par le participant ne constituera pas une infraction lorsque celle-ci intervient soit de manière fortuite, soit avec le consentement de tous les participants à la communication concernée[100], soit avec la participation du participant lui-même à la communication.

De même, un participant pourrait, sans commettre une infraction, installer ou faire installer un appareil permettant l'interception, la prise de connaissance ou l'enregistrement d'une communication non accessible au public pour autant qu'il agisse soit sans l'intention d'utiliser l'appareil concerné aux

[99] Art. 314 *bis* du Code pénal.
[100] Même si cela serait loin d'être acquis dans de nombreuses situations, il n'est pas exclu que le participant dispose pour les besoins de la politique de divulgation coordonnée du consentement des participants à la communication.

fins précitées, soit avec le consentement de tous les participants, soit en participant lui-même à la communication.

En outre, un participant pourrait élaborer, posséder ou mettre à disposition d'un autre participant un dispositif permettant l'interception, la prise de connaissance ou l'enregistrement d'une communication non accessible au public. Cela ne serait toutefois légitimement justifié que dans le cadre de la participation réelle à une politique de divulgation coordonnée des vulnérabilités. Ce dispositif pourrait, en effet, permettre de démontrer la possibilité d'une prise de connaissance illicite de communications, en raison de vulnérabilités du système informatique.

Par contre, la tentative intentionnelle d'intercepter, d'enregistrer ou de prendre connaissance d'une communication non accessible au public ne pourrait se justifier dans le cadre de la mise en œuvre d'une politique de divulgation coordonnée, sauf si le participant dispose du consentement de tous les participants ou participe lui-même à la communication.

Si le participant pouvait raisonnablement ignorer que le contenu de communications non accessibles au public ou de données d'un système informatique a été obtenu illégalement, il peut les utiliser, détenir, révéler ou divulguer. A l'inverse, le participant qui connaît l'illégalité de l'obtention de telles informations devra strictement s'abstenir de les receler dans le cadre de sa participation à une politique de divulgation coordonnée des vulnérabilités.

Compte-tenu des bonnes intentions du participant, celui-ci ne devrait, en principe, pas réaliser de communications électroniques frauduleuses, ou utiliser illicitement un réseau ou un service de communications électroniques.

Enfin, l'objectif d'une politique de divulgation coordonnée des vulnérabilités n'est assurément pas, de manière intentionnelle, de prendre connaissance ou de modifier des informations, l'identité de communicants ou des données de communications électroniques. Si le participant devait réaliser ces actions, c'est soit de manière fortuite, soit avec le consentement de tous les participants concernés, soit lorsque la communication lui est destinée personnellement. La mise en œuvre d'une politique de

divulgation coordonnée vise, au contraire, à renforcer la confidentialité des communications électroniques échangées par l'organisation responsable.

A notre estime, le participant qui participe à une politique de divulgation coordonnée des vulnérabilités pourrait éventuellement invoquer l'application de l'article 125 de la loi du 13 juin 2015 relative aux communications électroniques qui permet de déroger au secret des communications électroniques. Les actions accomplies par un participant dans le cadre d'une politique de divulgation coordonnée pourrait viser à contrôler le bon fonctionnement d'un réseau ou d'un service de communications électroniques, en ce compris la sécurité de celui-ci.

G. Respect des autres dispositions légales

Au-delà des dispositions en matière de cybercriminalité, les participants à une politique de divulgation coordonnée des vulnérabilités doivent tenir compte d'autres dispositions légales, dont la législation relatives aux traitements de données à caractère personnel[101].

L'objet d'une politique de divulgation coordonnée n'est pas d'effectuer intentionnellement des traitements de données à caractère personnel. Cependant, il est fort probable que l'organisation responsable traite des données des données à caractère personnel soit à titre de responsable du traitement, soit à titre de sous-traitant. Ainsi, le participant pourrait traiter, même de manière fortuite, des données à caractère personnel stockées, traitées ou transmises dans le système informatique concerné. Il peut également s'avérer nécessaire au participant, dans le cadre de ses recherches de vulnérabilités, de devoir traiter des données à caractère personnel pour démontrer l'existence d'une vulnérabilité.

[101] Règlement européen n°2016/679 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 (Règlement général sur la protection des données, ci-après « RGPD ») et abrogeant la directive 95/46/CE, ainsi que les lois belges y afférentes dont la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.* du 10 janvier 2018, p. 989.

Section 1. Les notions liées aux données à caractère personnel

1. Les données à caractère personnel

Les données à caractère personnel, au sens du RGPD, sont toutes les informations se rapportant à une personne physique identifiée ou identifiable. Le caractère identifiable de données résulte du fait que celles-ci peuvent permettre d'identifier une personne physique, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[102]. Le caractère « identifiable » de la personne ne dépend pas de la simple volonté d'identification de celui qui traite les données mais de la possibilité d'identifier, directement ou indirectement, la personne à l'aide de ces données (par exemple : une adresse de courriel, numéro d'identification, identifiant en ligne, adresse IP ou encore de données de localisation).

2. Le traitement

Le traitement de données à caractère personnel a une portée large et inclut « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »[103]. En définitive, la notion de traitement vise presque toutes les opérations qui peuvent être appliquées à des données à caractère personnel.

[102] Art. 4, 1) du RGPD.
[103] Art. 4, 2) du RGPD.

La simple collecte ou la consultation de données à caractère personnel sont ainsi considérées comme un traitement de données à caractère personnel[104].

3. Le responsable du traitement

Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement[105].

La qualité de responsable du traitement découle donc du pouvoir de détermination des finalités du traitement de données à caractère personnel.

3.1. Le pouvoir de détermination

Le pouvoir de détermination consiste pour une entité à pouvoir choisir de traiter des données à caractère personnel pour des finalités qui lui sont propres[106]. La notion de responsable du traitement est une notion fonctionnelle visant à attribuer les responsabilités aux personnes qui exercent une influence de fait et elle s'appuie donc sur une analyse factuelle plutôt que formelle[107].

---

[104] C. DE TERWANGNE, Vie privée et données à caractère personnel, Chap. 3.2 Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution, Bruxelles, Ed. Politeia, p. 23.
[105] Art. 4, 7) du RGPD lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.
[106] C. DE TERWANGNE, Vie privée et données à caractère personnel, Chap. 3.2 Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution, Bruxelles, Ed. Politeia, p. 26.
[107] Groupe de l'article 29, avis 1/2010 sur les notions de responsable du traitement et de sous-traitant, WP 169, p. 10, (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_fr.pdf)

Il s'agit donc d'examiner dans les faits les opérations de traitement afin d'établir les raisons pour lesquelles elles ont lieu et qui a concrètement décidé de les mettre en œuvre.

3.2. La détermination des finalités et des moyens

Les finalités du traitement sont les objectifs recherchés et qui guident les actions de traitement entreprises. Les moyens sont les méthodes techniques ou organisationnelles[108] appliquées pour atteindre les finalités de traitement. Il s'agit, en somme, de déterminer le « pourquoi » et le « comment » des activités de traitement[109].

Ces deux éléments doivent être réunis pour être qualifié de responsable du traitement.

La détermination des moyens doit porter sur les éléments essentiels techniques et organisationnels du traitement (par exemple, les données à traiter, la durée du traitement ou les personnes qui peuvent avoir accès aux données)[110].

4. Le sous-traitant

Le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement[111]. Le sous-traitant agit pour le compte du responsable du traitement en exécutant ses instructions, au moins en ce qui concerne les finalités du traitement et les éléments essentiels des moyens du traitement.

---

[108] C. DE TERWANGNE, *idem*, p. 28.
[109] Groupe de l'article 29, avis 1/2010 sur les notions de responsable du traitement et de sous-traitant, WP 169, p. 14, *idem*.
[110] Ibidem.
[111] Art. 4, 8) du RGPD.

Section 2. Qualification juridique du rôle du participant

La politique de divulgation responsable constitue une forme de contrat d'adhésion qui lie le hacker éthique à l'égard du responsable du traitement[112]. Ainsi, les finalités et les moyens essentiels du traitement de données à caractère personnel sont, en principe, déterminées dans le cadre d'une politique de divulgation coordonnée des vulnérabilités par l'organisation responsable et non par le participant. Dans ce cas, le participant devra respecter les obligations légales en matière de protection des données à caractère personnel en qualité de sous-traitant de l'organisation responsable[113].

L'article 28, §3 (a) du RGPD impose au sous-traitant de traiter les données personnelles conformément aux instructions du responsable du traitement. Il est généralement admis que le traitement confié au sous-traitant puisse néanmoins impliquer « une certaine liberté d'appréciation sur la façon de servir au mieux les intérêts du responsable du traitement, permettant au sous-traitant de choisir les moyens techniques et d'organisation les plus appropriés »[114]. Il peut ainsi se concevoir que le participant jouisse d'une certaine liberté de choix dans les moyens qu'il utilise pour vérifier la sécurité des systèmes d'information de l'organisation responsable. L'organisation responsable détermine quant à elle les systèmes et les services que le participant est autorisé à tester et ceux qui lui sont interdits.

L'article 28, § 1 du RGPD impose au responsable du traitement de mettre en place des procédures de sélection des prestataires de services afin de s'assurer qu'ils présentent des « garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées », notamment en termes de connaissances spécialisées, de fiabilité et de ressources. Dans le cadre d'une CVDP ou d'un programme de récompense pour la découverte de vulnérabilités, l'organisation responsable peut, en effet, limiter la participation à certains hackers éthiques ou exiger de ceux-ci qu'ils reconnaissent avoir

[112] Ou du sous-traitant, si l'organisation responsable a la qualité de responsable du traitement.
[113] L'organisation responsable peut être un responsable du traitement de données à caractère personnel ou elle-même un sous-traitant d'un responsable du traitement.
[114] Groupe de l'article 29, avis 1/2010 sur les notions de responsable du traitement et de sous-traitant, WP 169, p. 27, *idem*.

l'expertise et l'expérience nécessaires afin de tester les systèmes de l'organisation responsable, en ce compris ses éventuelles données de caractère personnel.

Egalement, le responsable du traitement doit pouvoir exercer une certaine surveillance[115] sur l'exécution du service réalisé pour son compte afin de vérifier sa conformité avec le contrat conclu avec le sous-traitant et le RGPD. Le participant doit ainsi collaborer avec l'organisation responsable et pouvoir lui fournir, à sa demande, toutes informations utiles.

Toutefois, le participant pourrait être qualifié de responsable du traitement lorsque les moyens essentiels du traitement de données à caractère personnel ne sont pas suffisamment déterminés dans la CVDP ou si le participant ne respecte pas les instructions de l'organisation responsable. En effet, le participant qui pose des actes de traitement non autorisés (ou traite les données pour d'autres finalités que la recherche de vulnérabilités) devra être qualifié de responsable du traitement puisqu'il déterminera lui-même une autre finalité de traitement et/ou des moyens (essentiels) de traitement.

Section 3. Les conséquences pour le contenu de la CVDP

Il résulte de ce qui précède qu'il est nécessaire de préciser dans la CVDP les obligations des parties en matière de traitements de données à caractère personnel, notamment les finalités et les moyens essentiels des éventuels traitements. Le contenu de la politique devrait ainsi définir l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

L'organisation responsable devrait prévoir dans sa CVDP des règles qui imposent des garanties suffisantes au participant pour la mise en œuvre de mesures techniques et organisationnelles appropriées pour le traitement de données à caractère personnel[116]. Le participant devrait veiller à ce

[115] Groupe de travail Article 29, Avis 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant", WP 169, p.30
[116] Art. 28, § 1er du RGDP.

que ces données soient conservées en garantissant un niveau de sécurité adapté aux risques encourus (de préférence de manière chiffrée) et que ces données soient supprimés immédiatement après la fin du traitement.

De même, le traitement de données à caractère personnel pour une autre finalité que la recherche des vulnérabilités des systèmes, équipements ou produits de l'organisation responsable devrait être exclu.

Le participant devrait également s'engager à informer l'organisation responsable et/ou l'Autorité de protection des données, dans les meilleurs délais après en avoir pris connaissance, de toute perte éventuelle de données à caractère personnel.

La CVDP devrait contenir au moins les engagements suivants du participant [117] :

- ne traiter des données à caractère personnel que sur instruction documentée du responsable du traitement ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ;
- interdire aux personnes physiques agissant sous l'autorité du sous-traitant, qui ont accès à des données à caractère personnel, de les traiter, excepté sur instruction du responsable du traitement[118] ;
- prendre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, compte tenu de l'état des connaissances, des coûts de mise en œuvre et

[117] Voy. notamment les conditions reprises à l'article 28, § 3 du RGDP.
[118] Art. 32 § 4 du RGPD.

de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques[119] ;

- s'assurer de l'autorisation préalable du responsable du traitement pour recruter un autre sous-traitant et imposer à ce dernier le respect du contenu de la politique de divulgation ;

- aider le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits ;

- aider le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD (sécurité, notification de violation, analyse d'impact, consultation préalable), compte tenu de la nature du traitement et des informations à la disposition du participant ;

- notifier au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance[120] ;

- supprimer ou renvoyer[121] toutes les données à caractère personnel, au responsable du traitement au terme de la participation à la politique, et détruire les copies existantes ;

- mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations, dont un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement[122] ;

- exclure l'utilisation des données à caractère personnel pour une autre finalité que la recherche des vulnérabilités du système ou la communication de ces données à des tiers.

[119] Art. 32 § 1er du RGPD.
[120] Art. 33, § 2 du RGPD.
[121] selon le choix du responsable du traitement
[122] Dont le contenu est précisé à l'art. 30, § 2 du RGPD.

H. Références juridiques

DE NAUW A. et KUTY F., *Manuel de droit pénal spécial*, Waterloo, Kluwer, 2014, pp. 1125-1145.
DECHAMPS F. et LAMBILOT C., *Cybercriminalité : Etats des lieux*, Limal, Anthémis, 2016, pp. 26-46.
DEHOUSSE F., VERBIEST T., ZGAJEWSKI T., « La criminalité dans la société de l'information » in *Introduction au droit de la société de l'information*, Bruxelles, Larcier, 2007.
DE VILLENFAGNE F. et DUSOLLIER S., « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *A.M.*, 2001, p. 60-81.
DOCQUIR B., « La loi du 15 mai 2006: nouvelles définitions des infractions en matière de criminalité informatique », *R.D.T.I.*, 2006, pp. 287-294.
EVRARD S., « La loi du 28 novembre 2000 relative à la criminalité informatique », *J.T.*, 2001, pp. 241-245.
HENRION T., *Mémento Droit pénal*, Bruxelles, Kluwer, 2016.
KUTY F., *Principes généraux du droit pénal*, t. 1, *La loi pénale*, Bruxelles, Larcier, 2009.
K. ROSIER, « Le traitement de données dans le cadre des communications électroniques » in X. *Vie privée et données à caractère personnel*, Bruxelles, Politeia.
LEROUX O., « La Criminalité informatique », *Les infractions contre les biens*, Bruxelles, Larcier, 2008, pp. 409-436.
LEROUX O., in X. *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, Bruxelles, Kluwer, 2014, pp. C 362/1-55.
LORENT A., « Destructions et dégradations autres que par incendie ou explosion », *Droit pénal et procédure pénale (DPPP)*, Kluwer, 2006, pp. 119-136.
MEUNIER C., « 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.*, 2001, pp. 611-690.
MEUNIER C., « La loi du 28 novembre 2000 relative à la criminalité informatique *in Actualités du droit des technologies de l'information et de la communication,* CUP, 2001 pp. 37-160.
OMRANI F. et DUMORTIER F., « Chronique de jurisprudence 2009-2011. Criminalité informatique », *R.D.T.I.*, 2012, pp. 198-208.
ROGER FRANCE E., « La criminalité informatique », *Actualités de droit pénal*, Bruxelles, Bruylant, 2005, pp. 101-133.
TULKENS F., VAN DE KERCHOVE M., CARTUYVELS Y. et GUILLAIN C., *Introduction au droit pénal*, 9e éd., Bruxelles, Kluwer, 2010.
DE VILLENFAGNE F., « Chronique de jurisprudence 2002-2008. Criminalité informatique », *R.D.T.I.*, 2010, pp. 9-28.

VANDER GEETEN V., « La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilités » in *Les obligations légales de cybersécurité et de notifications d'incidents*, Politeia, Bruxelles, 2019, pp. 217 et s.
VANDERMEERSCH D., « Eléments de droit pénal et de procédure pénale », La Charte, Bruxelles, 2012.

BAEYENS, E., "Informatica en recht: oude griffels - nieuwe leien", *T. Strafr.,* 2007, pp. 404-407.
DEENE J. en NERINCKX G., "Computercriminaliteit" in *Praktijkboek recht en internet*, Titel II – Hoofdstuk 10, Brugge, Vanden Broele, 2007, pp. 3-43.
DELBROUCK I., "Informaticacriminaliteit", in X., *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, Antwerpen, Kluwer, 2007, I. 42/08-30.
DE HERT, P., "De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?", *T. Strafr.*, 2001, pp. 286-334.
J. DUMORTIER, *ICT-Recht*, Acco, Louvain, 1999, p. 86 et s.
KERKHOFS J. en VAN LINTHOUT P., *Cybercrime 3.0*, Brussel, Politeia, 2019.
KERKHOFS J. en VAN LINTHOUT P., *Cybercrime*, Brussel, Politeia, 2014.
KERKHOFS J. en VAN LINTHOUT P., "Cybercriminaliteit doorgelicht", *T. Strafr.*, 2010, p. 179 et s.
KEUSTERMANS J., F. MOLS en T. DE MAERE, "Informaticacriminaliteit" in *Strafrecht en strafvordering. Commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2010, pp. 65-103.
KEUSTERMANS J. en MOLS F., "De wet van 28 november 2000 inzake informaticacriminaliteit : eerste overzicht", *R-W*, 2001-2002, pp. 721-732.
KEUSTERMANS J. en DE MAERE T., "Tien jaar wet informaticacriminaliteit", *R-W*, 2010-2011, pp. 562-568.
VAN EECKE, P., "De Wet Informaticacriminaliteit", in X., *Elektronische handel, juridische en praktische aspecten*, Heule, UGA, 2004, pp. 369-385.
VANSTEENHUYSE S. et T'JONCK P., "Cybercriminaliteit en privacy" in *Privacy en strafrecht, Nieuwe en grensoverschrijden verkenningen*, Anvers, Maklu, 2007.

CENTRE FOR CYBER SECURITY BELGIUM

GUIDE SUR LES POLITIQUES DE DIVULGATION COORDONNEE DES VULNERABILITES
PARTIE II : LES ASPECTS LEGAUX

Ce document et ses annexes ont été élaborés par le Centre pour la Cybersécurité Belgique (CCB), administration fédérale créé par l'arrêté royal du 10 octobre 2014 et sous l'autorité du Premier Ministre.

Les informations fournies :
• sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières
• ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points.

Éd. Responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur
Rue de la Loi, 16
1000 Bruxelles

Dépôt légal :

D/2020/14828/013

2020