



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

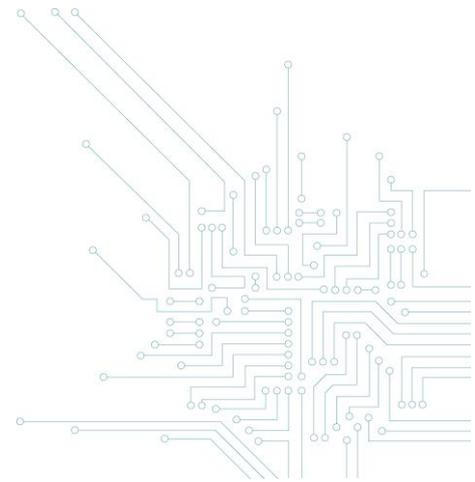
[info@ccb.belgium.be](mailto:info@ccb.belgium.be)  
[www.ccb.belgium.be](http://www.ccb.belgium.be)



.be

UNDER THE AUTHORITY  
OF THE PRIME MINISTER

<b>A. Table des matières</b>	
<b>B. L'application du droit pénal belge</b>	<b>4</b>
<b>C. L'intrusion dans un système informatique</b>	<b>5</b>
<i>Section 1. L'intrusion externe</i>	5
<i>Section 2. L'intrusion interne</i>	12
<i>Section 3. Les circonstances aggravantes de l'intrusion</i>	16
<i>Section 4. La politique de divulgation coordonnée des vulnérabilités et l'intrusion</i>	18
<b>D. La violation de données informatiques</b>	<b>21</b>
<i>Section 1. Les éléments constitutifs matériels</i>	22
<i>Section 2. Élément moral</i>	23
<i>Section 3. Les circonstances aggravantes</i>	23
<i>Section 4. La mise à disposition de moyens pour faciliter la violation de données</i>	24
<i>Section 5. La tentative</i>	25
<i>Section 6. La politique de divulgation coordonnée des vulnérabilités et la violation de données informatiques</i>	25
<b>E. Le faux en informatique et la fraude informatique</b>	<b>26</b>
<i>Section 1. Le faux en informatique et l'usage de faux en informatique</i>	26
<i>Section 2. La fraude informatique</i>	29
<i>Section 3. La politique de divulgation coordonnée des vulnérabilités, le faux en informatique et la fraude informatique</i>	31
<b>F. Les infractions relatives au secret des communications</b>	<b>31</b>
<i>Section 1. Infractions relatives au secret des communications non accessibles au public et des données d'un système informatique</i>	31
<i>Section 2. Les actes préparatoires</i>	34
<i>Section 3. Le recel de communications illicitement obtenues</i>	36
<i>Section 4. La tentative</i>	37
<i>Section 5. Le secret des communications électroniques</i>	38
<i>Section 6. La politique de divulgation coordonnée des vulnérabilités et les communications</i>	44
<b>G. Respect des autres dispositions légales</b>	<b>46</b>
<i>Section 1. Les notions liées aux données à caractère personnel</i>	47
<i>Section 2. Qualification juridique du rôle du participant</i>	50
<i>Section 3. Les conséquences pour le contenu de la CVDP</i>	51
<b>H. Références juridiques</b>	<b>54</b>



**Avertissement :**

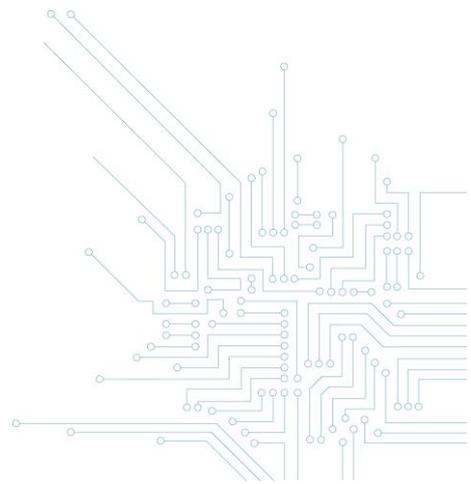
***Le présent guide vise à exposer les concepts, les objectifs, les questions juridiques et les bonnes pratiques liées à l'adoption de politiques de divulgation coordonnée des vulnérabilités (ou Coordinated Vulnerability Disclosure Policies – « CVDP ») dans l'état actuel de la législation en Belgique – 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 Intigrity (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<sup>1</sup>.

Pour cela, il suffit qu'un des éléments constitutifs matériels ou aggravants matériels<sup>2</sup> 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<sup>3</sup> et de la législation européenne<sup>4</sup>, 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.

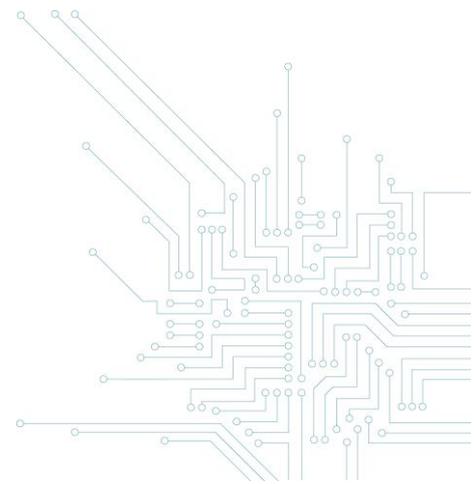
---

<sup>1</sup> Cass., 23 janvier 1979, *Pas.*, I, 1979, p. 582 ; Cass., 4 février 1986, *Pas.*, I, 1986, p. 664.

<sup>2</sup> Et non simplement intentionnels.

<sup>3</sup> Convention sur la Cybercriminalité du Conseil de l'Europe, faite à Budapest le 23 novembre 2001, entrée en vigueur le 1<sup>er</sup> juillet 2004.

<sup>4</sup> 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<sup>5</sup>

### Section 1. L'intrusion externe

L'article 550 *bis*, § 1<sup>er</sup> 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

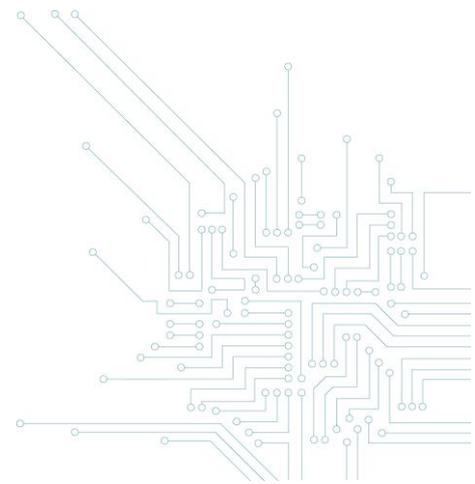
###### a) Un système informatique

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 »<sup>6</sup>. 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

---

<sup>5</sup> 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.

<sup>6</sup> 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<sup>7</sup>.

On peut également se référer à la directive européenne 2013/40/EU du 12 août 2013 relative aux attaques contre les systèmes d'information<sup>8</sup>, 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<sup>9</sup> ;
- 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.

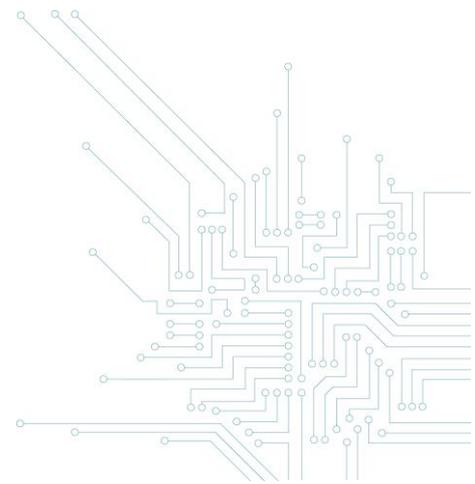
Le concept de système informatique dépasse donc celui du simple ordinateur personnel mais vise au sens large toutes les formes de systèmes traitant des données : une tablette électronique, un GPS, un smartphone, une montre électronique, un réseau, un serveur, un routeur, un décodeur, une télévision connectée,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

---

<sup>7</sup> *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p.12.

<sup>8</sup> 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 1<sup>er</sup> juillet 2004 et approuvé par la Belgique (loi du 3 août 2012, *M.B.* du 21 novembre 2012, p. 69092).

<sup>9</sup> 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<sup>10</sup>, sans nécessairement requérir des manipulations informatiques complexes<sup>11</sup> : 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.

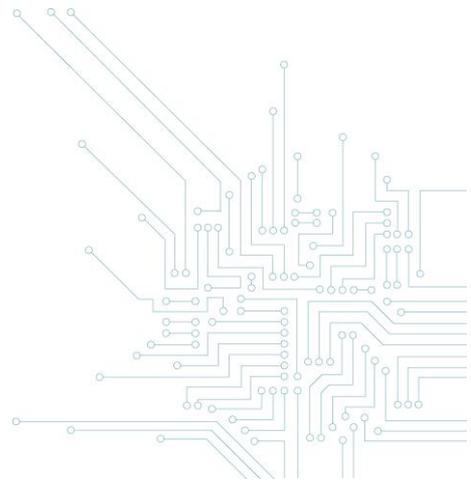
Le maintien envisage notamment l'hypothèse d'une personne qui accède par inadvertance (sans s'en rendre compte) à un système informatique sans autorisation et qui s'y maintient néanmoins après s'en être aperçu. Il peut s'agir également de la situation où une personne maintient son accès au système alors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

---

<sup>10</sup> 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.

<sup>11</sup> Corr. Anvers, 10 novembre 2014, *T. Strafr.*, 2015, p. 94.

<sup>12</sup> 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<sup>13</sup>.

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<sup>14</sup>.

### 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<sup>15</sup>. 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 ».

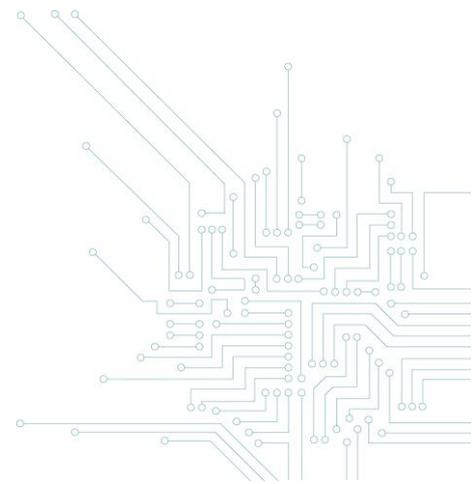
Le législateur a voulu sanctionner pénalement en tant que tel le simple accès non autorisé dans un système informatique. Ainsi, la simple prise de connaissance du contenu, des paramètres de

---

<sup>13</sup> *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 17.

<sup>14</sup> *Corr. Termonde*, 14 novembre 2008, *T. straf.*, 2009, p. 114.

<sup>15</sup> 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.

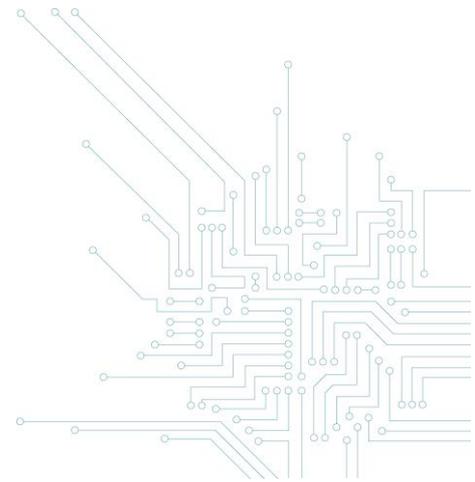
Concrètement, deux situations peuvent se rencontrer : soit une personne s'introduit consciemment dans un système informatique alors qu'elle ne dispose d'aucune autorisation, même partielle, d'y accéder, soit une personne accède à un système informatique par inadvertance, ou sciemment après l'expiration 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<sup>16</sup>. 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.

---

<sup>16</sup> 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<sup>17</sup>, 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<sup>18</sup>.

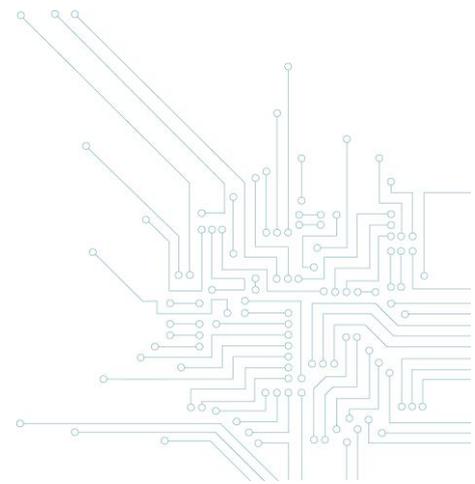
Dans le même ordre d'idée, une habilitation tacite peut résulter de l'existence d'un système informatique mis sans ambiguïté à la disposition du public<sup>19</sup>.

---

<sup>17</sup> Contrat de « pentesting ».

<sup>18</sup> Toutefois, l'employé recevra souvent de son employeur un identifiant et un mot de passe autorisant explicitement l'accès au système informatique.

<sup>19</sup> 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. Élément moral

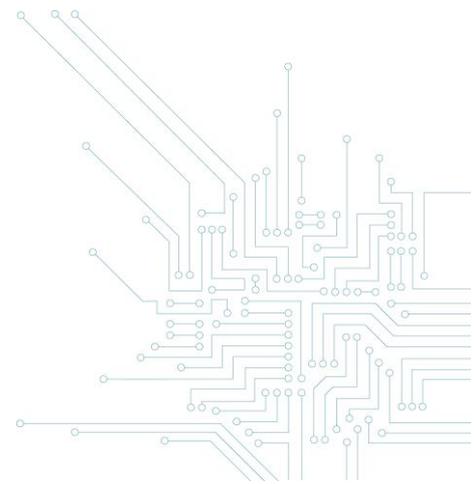
### 2.1. La volonté d'accès au système et la connaissance de l'absence d'autorisation

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<sup>20</sup>. En effet, le législateur a entendu sanctionner toute intrusion, sauf

---

<sup>20</sup> 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<sup>21</sup>. 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<sup>22</sup>.

L'intention frauduleuse de l'auteur intervient néanmoins comme une circonstance aggravante de l'infraction, laquelle va alourdir la peine infligée<sup>23</sup>.

## 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, outrepassa son pouvoir d'accès à un système informatique.

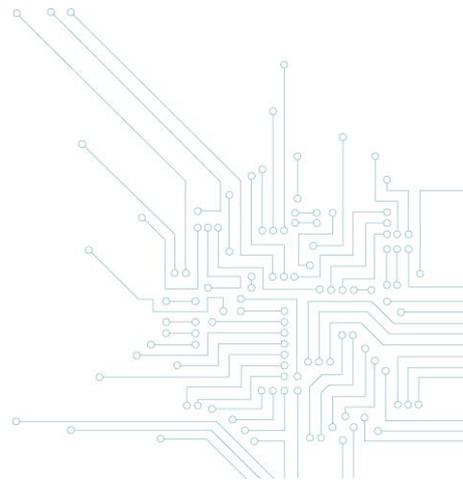
---

disque dur, en permettant des virements vers d'autres numéros de comptes que ceux des bénéficiaires) et d'en avvertir sa banque, n'est pas une situation évasive 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.

<sup>21</sup> Corr. Bruxelles, 8 janv. 2008, *J.T.*, 2008, p. 337.

<sup>22</sup> Corr. Eupen, 15 déc. 2003, *R.D.T.I.*, 2004, p. 61.

<sup>23</sup> Art. 550 *bis*, § 1<sup>er</sup>, 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<sup>24</sup>. 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<sup>25</sup>.

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<sup>26</sup>.

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<sup>27</sup>. Par voie de conséquence, l'auteur qui utilise son droit d'accès à un système informatique pour des fins

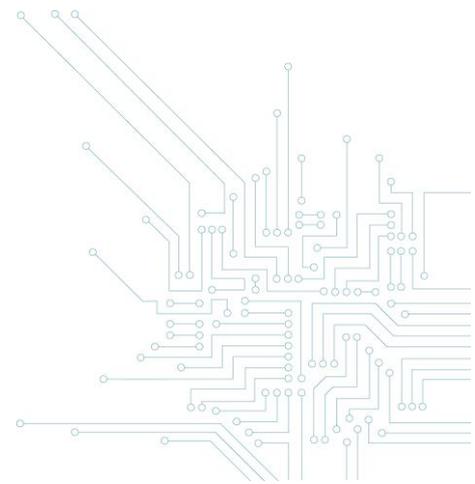
---

<sup>24</sup> 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.

<sup>25</sup> C.A., 24 mars 2004, n°51/2004, B.4.3, p. 7.

<sup>26</sup> Corr. Bruxelles, 8 janv. 2008, *J.T.*, 2008, p. 337.

<sup>27</sup> Cass., 24 janvier 2017, P.16.0048.N, [www.cass.be](http://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

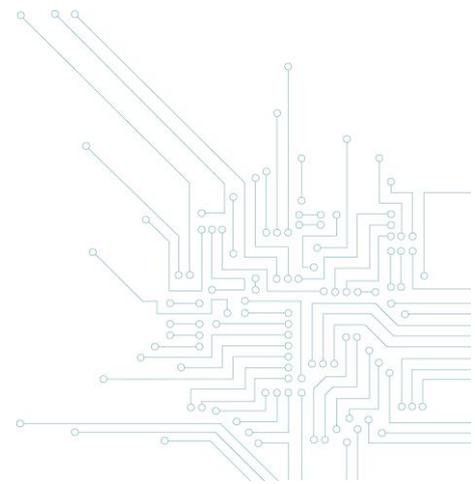
L'infraction existe dès l'instant où l'auteur outrepassé ses droits d'accès pour pénétrer ou se maintenir dans une partie du système informatique à laquelle il n'était pas ou plus autorisé à accéder au moment de l'infraction<sup>28</sup>.

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 outrepassé 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.

---

<sup>28</sup> Voy. Cass., 5 janvier 2011, P.10.1094.F., [www.cass.be](http://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. Élément 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 outrepassé 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<sup>29</sup>.

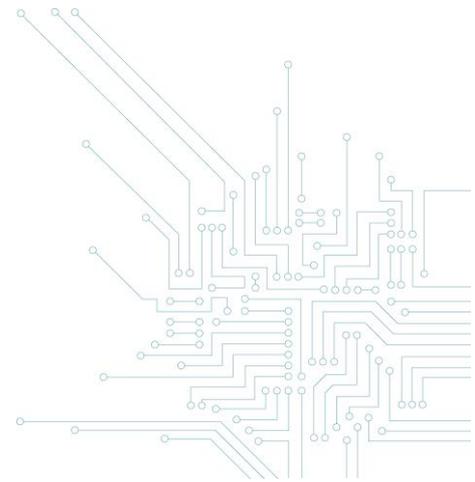
Le législateur a justifié cette différence, avec l'infraction d'intrusion externe, par le fait que les tiers qui ne disposent d'aucune autorisation d'accès mettraient plus en danger la sécurité du système informatique qu'une personne bénéficiant d'une autorisation partielle<sup>30</sup>. De plus, les 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<sup>31</sup>.

---

<sup>29</sup> *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/004, p. 6.

<sup>30</sup> *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 16.

<sup>31</sup> *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<sup>32</sup>. 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<sup>33</sup>. 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<sup>34</sup>. Le législateur visait ici notamment à lutter contre le vol de secrets d'entreprise dans le cadre d'espionnage industriel<sup>35</sup>.

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.

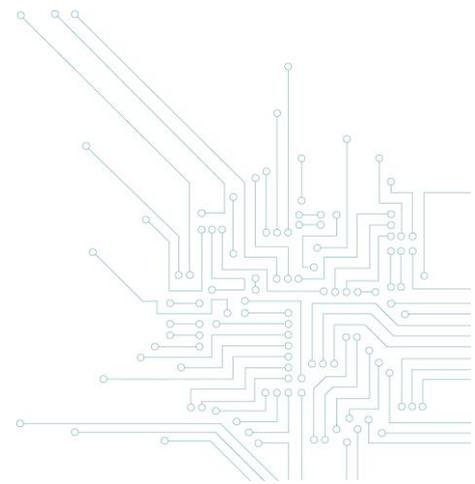
---

<sup>32</sup> Corr. Termonde, 14 mai 2007, *T. Strafr.*, 2007, p. 403.

<sup>33</sup> Ce comportement est parfois qualifié de « bitnapping », en référence au kidnapping de données.

<sup>34</sup> 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.

<sup>35</sup> *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)<sup>36</sup>. 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<sup>37</sup>.

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

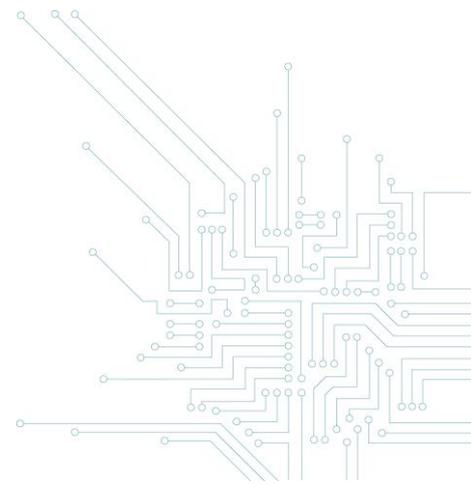
La troisième circonstance aggravante consiste à causer un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui y sont stockées, traitées ou transmises, ou au système ou aux données informatiques d'un tiers.

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.

---

<sup>36</sup> *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 17.

<sup>37</sup> 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<sup>38</sup>.

#### 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 suffisent donc pas pour éviter l'existence de cette infraction pénale.

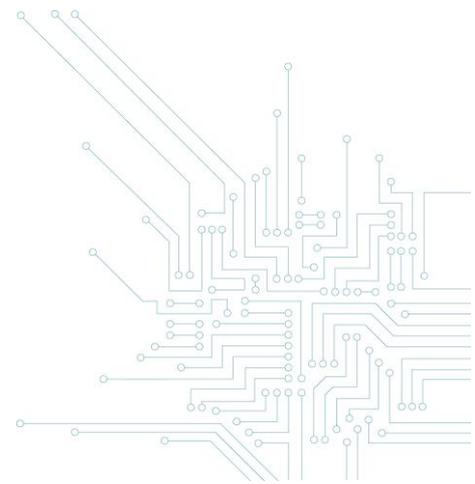
Toutefois, l'intrusion externe n'existe que lorsque le participant ne dispose pas d'une autorisation de l'organisation responsable d'accéder à son système informatique. Dès lors que le participant agit dans le cadre d'une autorisation, il n'y a pas d'intrusion externe.

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

---

<sup>38</sup> 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.



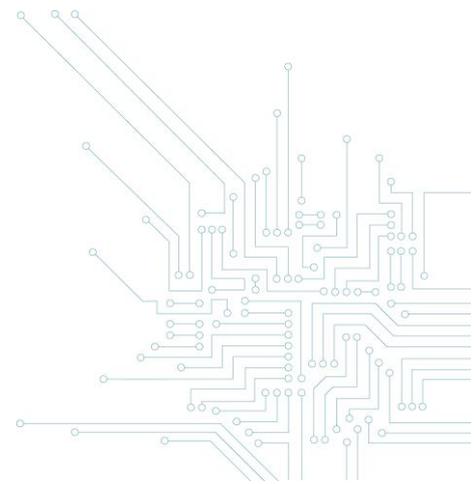
préalablement définies. Même si le destinataire précis de l'habilitation n'est pas connu au moment de l'adoption de la politique de divulgation coordonnée, il s'agit là bien d'une autorisation, accordée unilatéralement par le responsable du système informatique, aux personnes souhaitant participer à 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 outrepassé 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<sup>39</sup> 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<sup>40</sup>.

**Avertissement :**

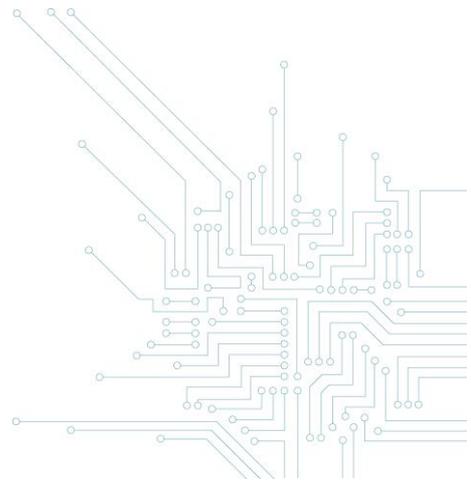
***Le participant doit être attentifs également à ne pas poser des actes, sans une autorisation complémentaire, sur des systèmes informatiques ou aux données gérés par des tiers à la politique de divulgation coordonnée de l'organisation responsable.***

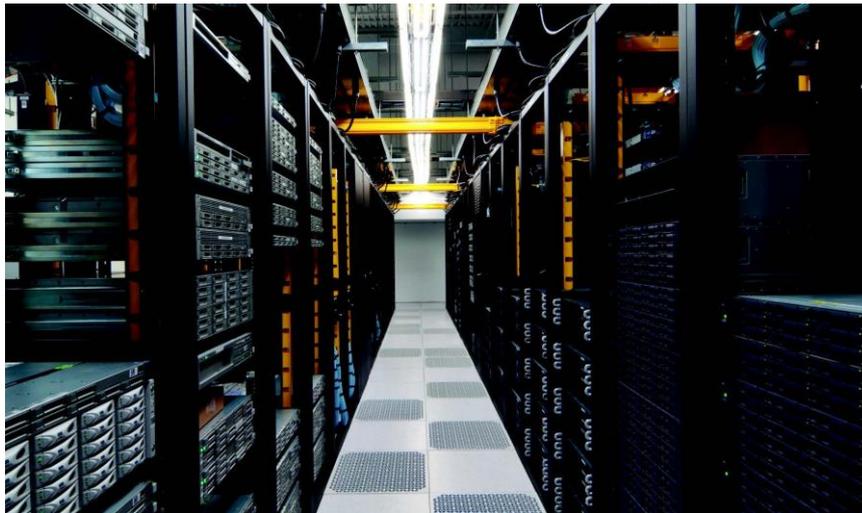
***Les tiers ne sont pas tenus au contenu de la politique de divulgation responsable et pourraient, en effet, entreprendre des actions judiciaires en raison du comportement du participant.***

---

<sup>39</sup> Par exemple, un contrat de travail, une relation statutaire ou un contrat de service.

<sup>40</sup> 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.



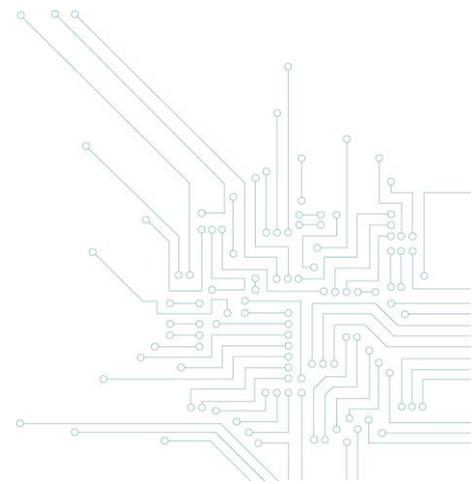


#### D. La violation de données informatiques<sup>41</sup>

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.

---

<sup>41</sup> 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.

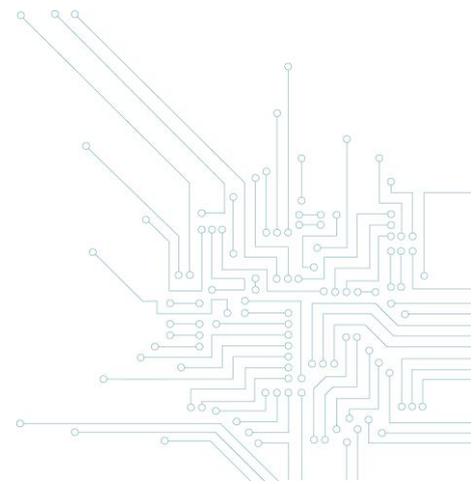
Contrairement à ce que l'on pourrait croire, le dommage n'est pas un élément constitutif de l'infraction, mais seulement une circonstance aggravante. Le simple fait de laisser une mention dans le système, tel que « x était ici », constitue une violation de données informatiques. Par contre, l'infraction 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<sup>42</sup> 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.

---

<sup>42</sup> *Doc. parl.*, Ch. Repr., 1999-2000, n°50, 0213/001, p. 19.



## Section 2. Élément 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<sup>43</sup>.

### 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<sup>44</sup>. 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

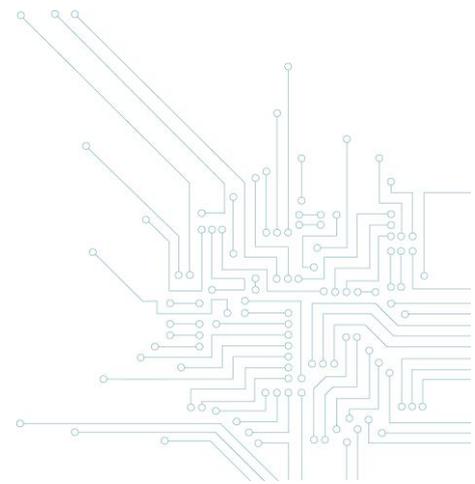
Cette circonstance aggravante vise la violation de données informatiques qui a pour conséquence d'empêcher, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique<sup>45</sup>. On vise ici la destruction du contenu, une paralysie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

---

<sup>43</sup> Voy. les considérations émises sur l'intention spéciale requise pour l'infraction d'intrusion non autorisée interne ; Art. 550 *ter*, § 1 du Code pénal.

<sup>44</sup> Art. 550 *ter*, § 2 du Code pénal.

<sup>45</sup> 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<sup>46</sup>.

##### **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.

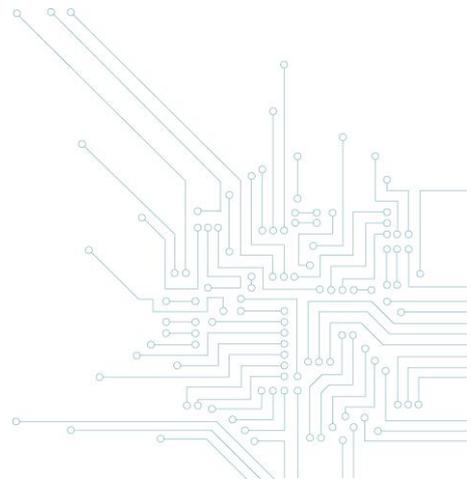
##### **2. Élément moral**

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<sup>47</sup>. La possession involontaire et ignorée de tels dispositifs n'est, par voie de conséquence, pas constitutive de

---

<sup>46</sup> Art. 550 *ter*, § 4 du Code pénal.

<sup>47</sup> 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<sup>48</sup>, 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<sup>49</sup>.

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<sup>50</sup>.

### **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.

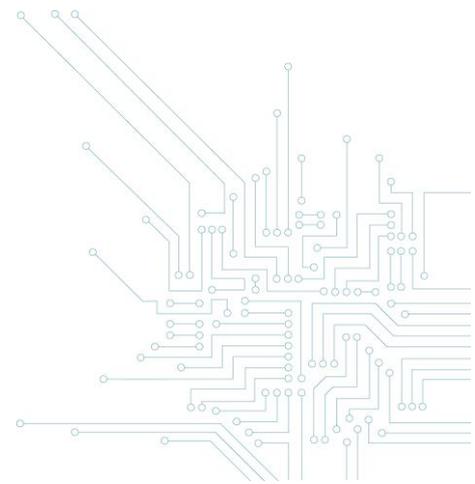
Par contre, l'autorisation de modifier ou de supprimer (ou de tenter de telles actions) des données informatiques dépend de la manière dont la politique de divulgation coordonnée des vulnérabilités est rédigée. Pour éviter de commettre une violation de données informatiques, le participant devra

---

<sup>48</sup> Par exemple, l'enseignement de la sécurité informatique.

<sup>49</sup> Art. 550 *ter*, § 6 du Code pénal.

<sup>50</sup> 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<sup>51</sup>.

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<sup>52</sup> et l'usage de faux en informatique<sup>53</sup>

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<sup>54</sup>.

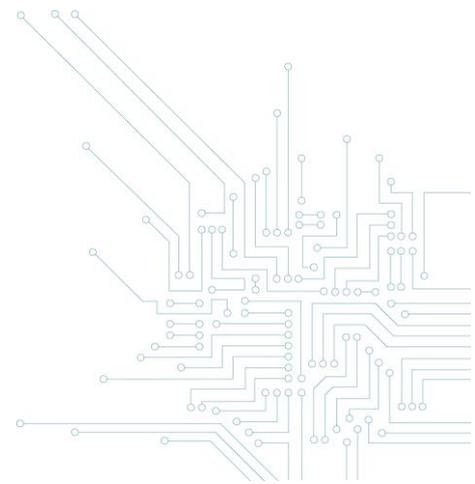
---

<sup>51</sup> Et elle pourra, le cas échéant, être accompagnée de circonstances aggravantes.

<sup>52</sup> Art. 210 *bis*, § 1<sup>er</sup>.

<sup>53</sup> Art. 210 *bis*, § 2.

<sup>54</sup> 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<sup>55</sup> et, d'autre part, la tentative de commettre un faux en informatique<sup>56</sup>.

## 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<sup>57</sup>.

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.<sup>58</sup>

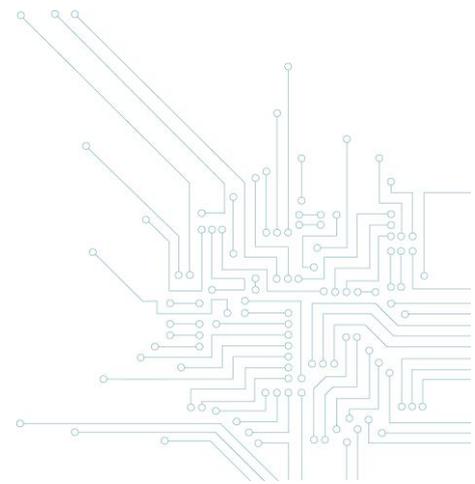
---

<sup>55</sup> Art. 210 *bis*, § 2 du Code pénal.

<sup>56</sup> Art. 210 *bis*, § 3 du Code pénal.

<sup>57</sup> *Doc. Parl.*, Ch. Repr., 1999-2000, n°0213/001, p. 10.

<sup>58</sup> 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<sup>59</sup> 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. Élément moral

L'infraction exige une intention frauduleuse ou le dessein de nuire<sup>60</sup>. 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.

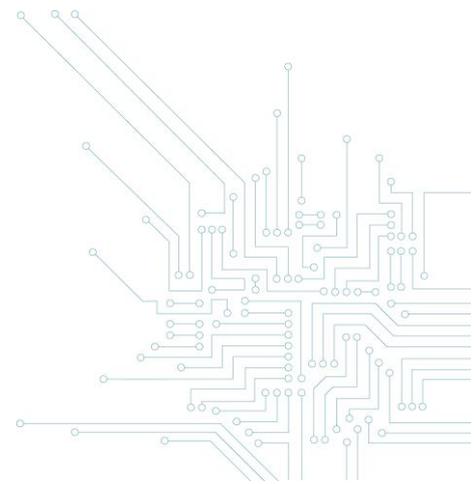
De seules erreurs, négligences ou imprudences ne sont dès lors pas suffisantes pour constituer une infraction de faux en informatique.

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.

---

<sup>59</sup> 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.

<sup>60</sup> 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<sup>61</sup>.

## 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

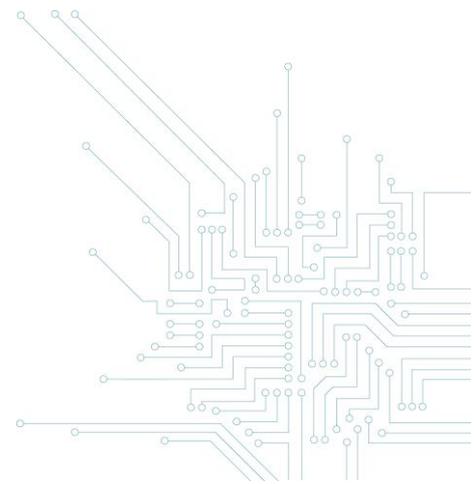
#### 1.1. La manipulation de données

L'infraction implique l'introduction, la modification<sup>62</sup> 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).

---

<sup>61</sup> Voy. la tentative d'intrusion dans un système informatique.

<sup>62</sup> 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<sup>63</sup> 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. Élément 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

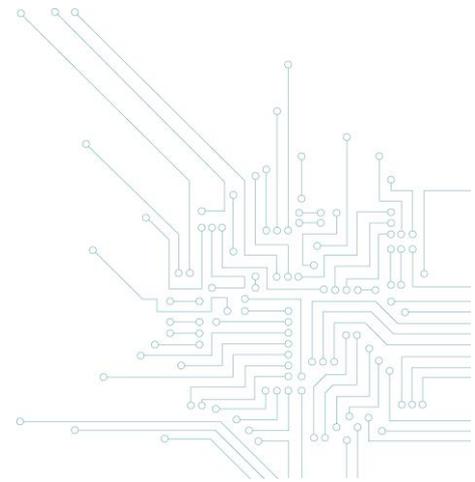
La tentative de fraude informatique est également sanctionnée<sup>64</sup>.

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.

---

<sup>63</sup> 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.

<sup>64</sup> 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<sup>65</sup>.

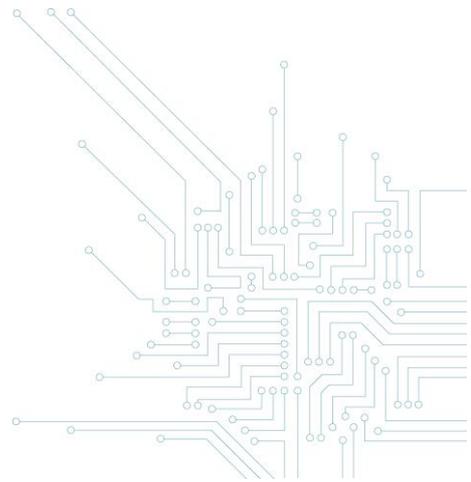
#### **1. Élément matériel**

##### **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

---

<sup>65</sup> Art. 314 *bis*, §1<sup>er</sup>, 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<sup>66</sup>, 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<sup>67</sup>.

La disposition précise encore que l'interception<sup>68</sup>, la prise de connaissance ou l'enregistrement doit intervenir à l'aide d'un appareil quelconque<sup>69</sup>. 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<sup>70</sup>.

## 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

---

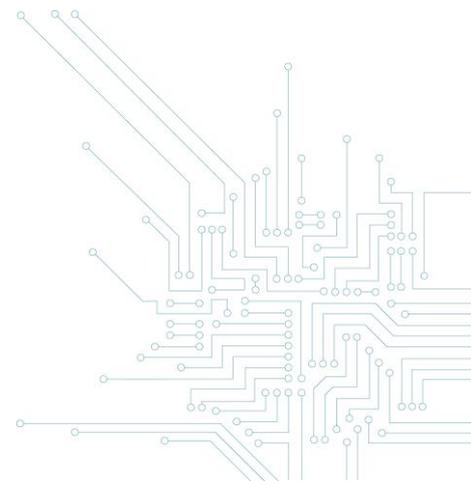
<sup>66</sup> Par exemple, via un service de sauvegarde en nuage.

<sup>67</sup> *Doc. Parl., Sén., 1992-1993, n°843/1, p. 8-9.*

<sup>68</sup> 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.*

<sup>69</sup> *Doc. Parl., Sén., 1992-1993, n°843/1, p. 6.*

<sup>70</sup> 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 »<sup>71</sup>. Il semble que l'on puisse interpréter cette notion, comme auparavant, en fonction du contexte et des intentions des participants à la communication<sup>72</sup>. 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<sup>73</sup>. Le caractère professionnel ou non d'une communication n'a, en principe, pas d'incidence pour en apprécier la nature non accessible au public<sup>74</sup>.

La communication vise notamment la transmission électronique de données dans des ordinateurs ou des réseaux d'ordinateurs<sup>75</sup>. 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

---

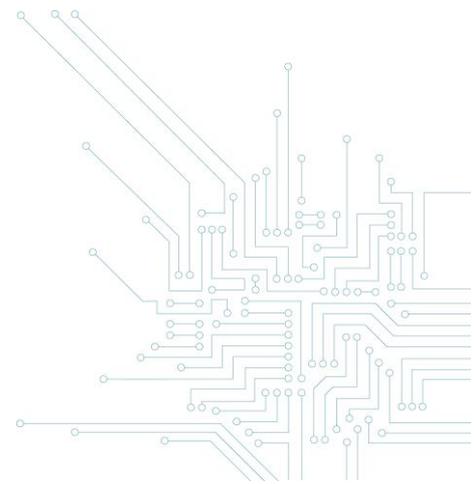
<sup>71</sup> Art. 32 de la loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications 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.

<sup>72</sup> *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.*

<sup>73</sup> *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](http://www.privacycommission.be).

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

<sup>75</sup> 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. Élément 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 indiscretion ne suffit pas pour constituer l'infraction<sup>76</sup>. 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<sup>77</sup>. 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

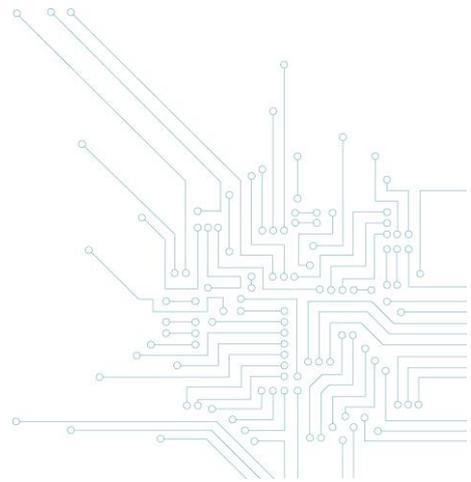
#### 1.1 Élément matériel

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

---

<sup>76</sup> *Doc. Parl., Sén., 1992-1993, n°843/1, p. 7.*

<sup>77</sup> *Doc. Parl., Sén., 1992-1993, n°843/1, p. 6.*



communications<sup>78</sup>. 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<sup>79</sup>.

## 1.2 Élément 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<sup>80</sup>.

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<sup>81</sup>.

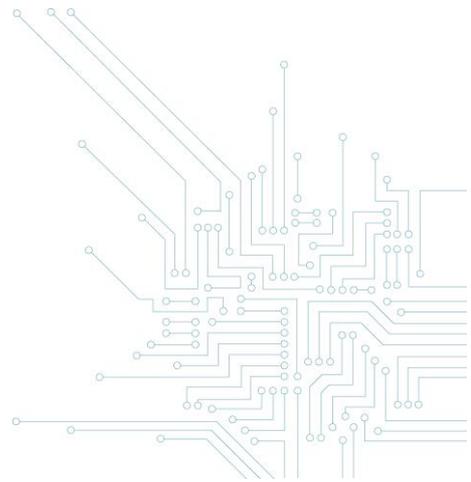
---

<sup>78</sup> Art. 314 *bis*, §1<sup>er</sup>, 2° du Code pénal.

<sup>79</sup> *Doc. Parl.*, Sén., 1992-1993, n°843/1, p. 9.

<sup>80</sup> Art. 314 *bis*, § 2 *bis* du Code pénal.

<sup>81</sup> *Doc. Parl.*, Ch. Repr., 2003-2004, n°1284/001, p. 6.



## 2.2. Élément 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<sup>82</sup>.

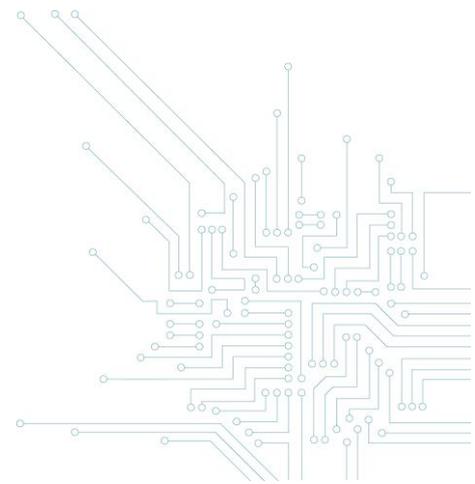
### 1. Élément matériel

#### 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.

---

<sup>82</sup> 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. Élément moral

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

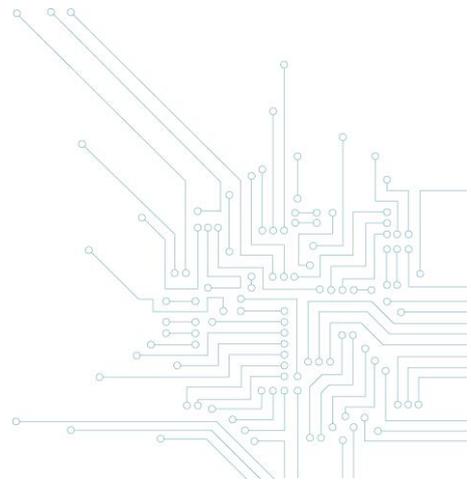
## Section 4. La tentative

La tentative d'interception illicite de communications non accessibles au public est également sanctionnée<sup>83</sup>.

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.

---

<sup>83</sup> 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<sup>84</sup>.

### 1. Les éléments constitutifs matériels

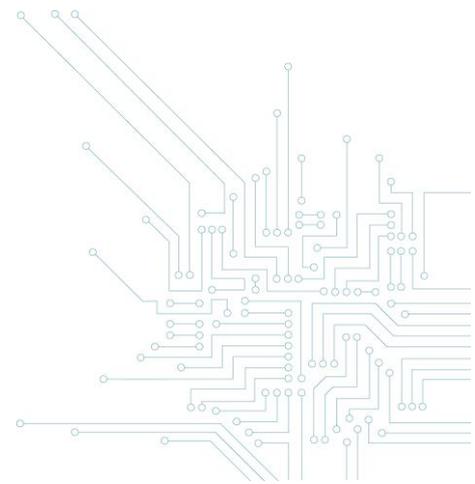
#### 1.1. L'autorisation des personnes directement ou indirectement concernées

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<sup>85</sup>, 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.

---

<sup>84</sup> *Doc. Parl.*, 2004-2005, n°1425-1426/01, p. 76.

<sup>85</sup> 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](http://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<sup>86</sup>

### 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 (...) »<sup>87</sup>. 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 »<sup>88</sup>.

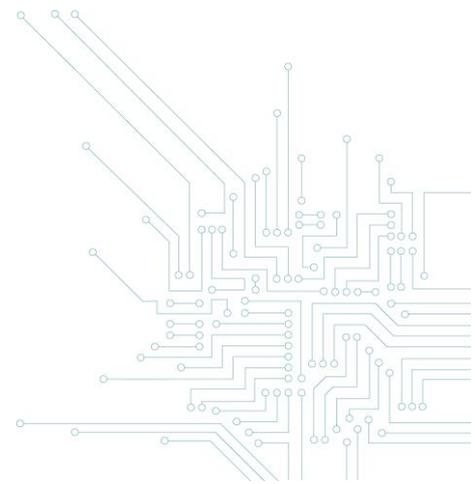
La notion de communication électronique comprend les communications téléphoniques, les courriels, les sms, les messages envoyées par réseau sans fil ou échange de données cellulaires, les connexions à un réseau ou à un système informatique. Cette notion englobe donc les courriels et les données de connexion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

---

<sup>86</sup> Art. 124, al. 1 de la loi du 13 juin 2005 relative aux communications électroniques.

<sup>87</sup> Art. 2, 3° et 5° de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.* du 20 juin 2005, p. 28070.

<sup>88</sup> 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<sup>89</sup>. 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<sup>90</sup>. 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.

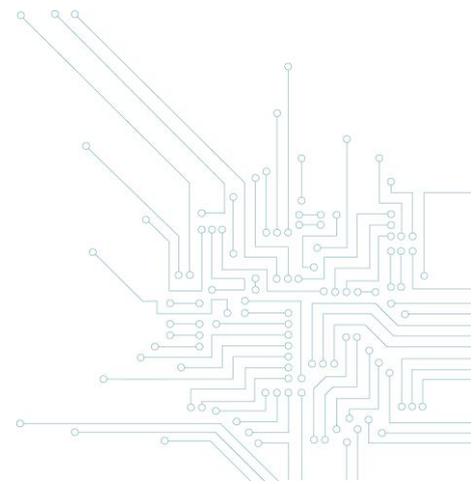
### **1.3. L'identification intentionnelle des personnes concernées par la transmission de l'information et son contenu**

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).

---

<sup>89</sup> Cass., 1 oct. 2009, C.08.0064.N, [www.cass.be](http://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](http://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 ».

<sup>90</sup> *Ibidem*.



#### **1.4. La prise de connaissance intentionnelle de données en matière de communications électroniques et relatives à une autre personne<sup>91</sup>**

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<sup>92</sup>.

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<sup>93</sup>**

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. Élément 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<sup>94</sup>. Une distinction doit dès lors

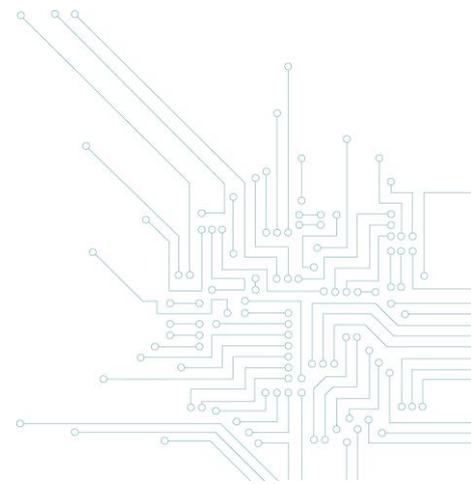
---

<sup>91</sup> Art. 124, al. 3 de la loi du 13 juin 2005 relative aux communications électroniques.

<sup>92</sup> C.T. Bruxelles, 10 février 2004, R.G. 44002, [www.juridat.be](http://www.juridat.be).

<sup>93</sup> Art. 124, al. 4 de la loi du 13 juin 2005 relative aux communications électroniques.

<sup>94</sup> 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](http://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<sup>95</sup> 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<sup>96</sup>

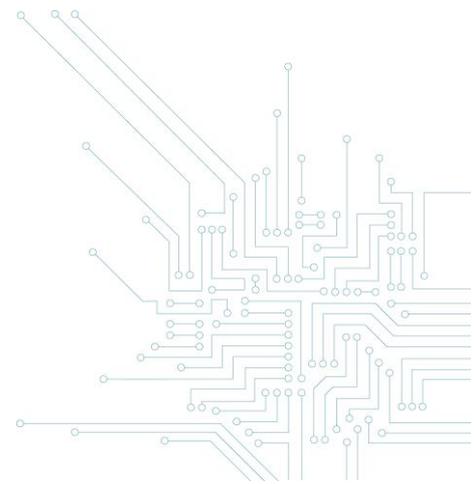
#### 1. Les éléments constitutifs matériels

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

---

<sup>95</sup> Art. 125, § 1<sup>er</sup>, 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.

<sup>96</sup> Art. 145, § 3, 1° de la loi du 13 juin 2005 relative aux communications électroniques.



## 2. Élément 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<sup>97</sup>

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<sup>98</sup>

### 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.

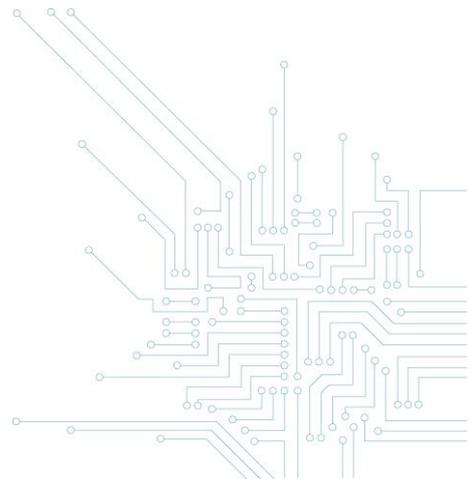
### 2. Élément moral

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

---

<sup>97</sup> Art. 145, § 3, 3° de la loi du 13 juin 2005 relative aux communications électroniques.

<sup>98</sup> 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<sup>99</sup>. Cela n'est d'ailleurs pas nécessaire à la mise en œuvre d'une politique de divulgation coordonnée des vulnérabilités.

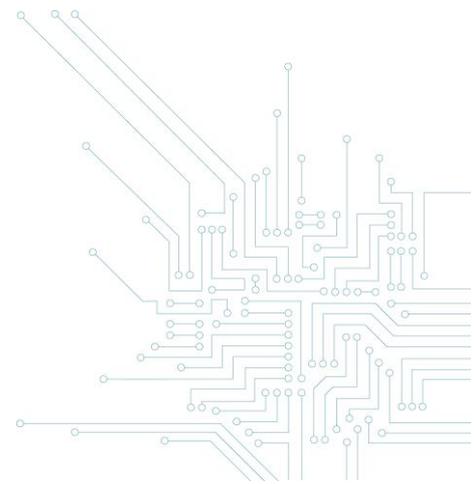
Cependant, l'interception, la prise de connaissance ou l'enregistrement d'une communication non accessible au public par le participant ne constituera pas une infraction lorsque celle-ci intervient soit de manière fortuite, soit avec le consentement de tous les participants à la communication concernée<sup>100</sup>, 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

---

<sup>99</sup> Art. 314 *bis* du Code pénal.

<sup>100</sup> 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.

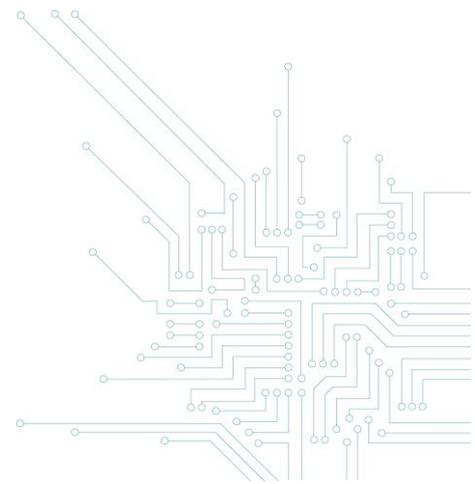
En outre, un participant pourrait élaborer, posséder ou mettre à disposition d'un autre participant un dispositif permettant l'interception, la prise de connaissance ou l'enregistrement d'une communication non accessible au public. Cela ne serait toutefois légitimement justifié que dans le cadre de la 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.

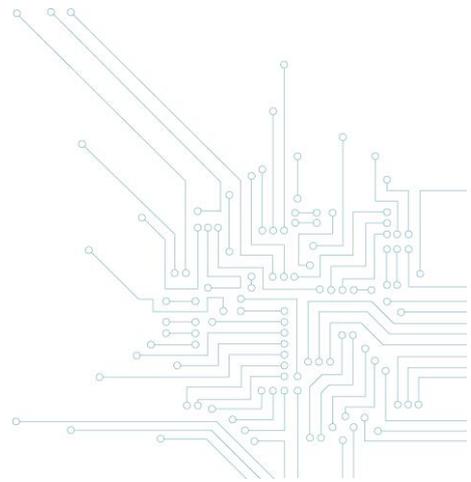
### G. Respect des autres dispositions légales

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<sup>101</sup>.

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.

---

<sup>101</sup> 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<sup>102</sup>. 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).

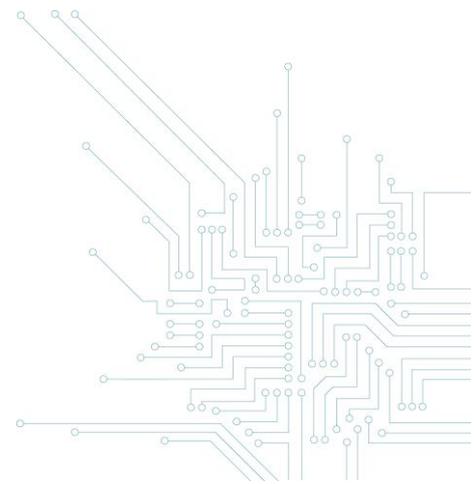
### 2. Le traitement

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 »<sup>103</sup>. En définitive, la notion de traitement vise presque toutes les opérations qui peuvent être appliquées à des données à caractère personnel.

---

<sup>102</sup> Art. 4, 1) du RGPD.

<sup>103</sup> 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<sup>104</sup>.

### 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<sup>105</sup>.

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<sup>106</sup>. 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<sup>107</sup>.

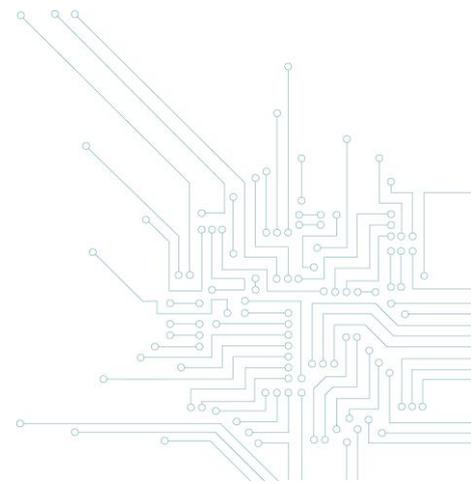
---

<sup>104</sup> 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.

<sup>105</sup> 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.

<sup>106</sup> 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.

<sup>107</sup> 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](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<sup>108</sup> appliquées pour atteindre les finalités de traitement. Il s'agit, en somme, de déterminer le « pourquoi » et le « comment » des activités de traitement<sup>109</sup>.

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)<sup>110</sup>.

## 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<sup>111</sup>. 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.

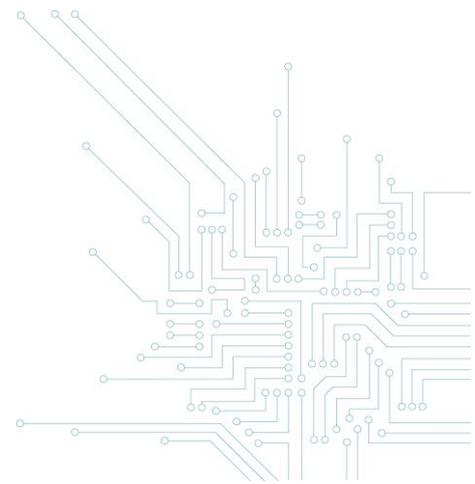
---

<sup>108</sup> C. DE TERWANGNE, *idem*, p. 28.

<sup>109</sup> Groupe de l'article 29, avis 1/2010 sur les notions de responsable du traitement et de sous-traitant, WP 169, p. 14, *idem*.

<sup>110</sup> *Ibidem*.

<sup>111</sup> 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<sup>112</sup>. 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<sup>113</sup>.

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 »<sup>114</sup>. 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.

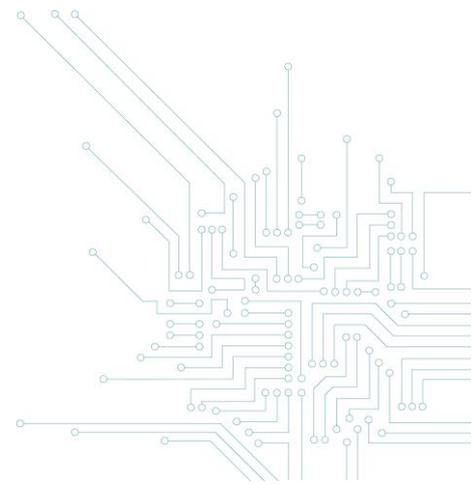
L'article 28, § 1 du RGPD impose au responsable du traitement de mettre en place des procédures de sélection des prestataires de services afin de s'assurer qu'ils présentent des « garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées », notamment en termes 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

---

<sup>112</sup> Ou du sous-traitant, si l'organisation responsable a la qualité de responsable du traitement.

<sup>113</sup> 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.

<sup>114</sup> 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<sup>115</sup> 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

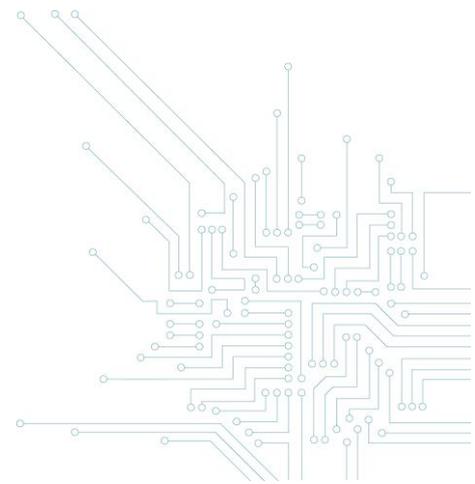
Il résulte de ce qui précède qu'il est nécessaire de préciser dans la CVDP les obligations des parties en matière de traitements de données à caractère personnel, notamment les finalités et les moyens essentiels des éventuels traitements. Le contenu de la politique devrait ainsi définir l'objet et la 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<sup>116</sup>. Le participant devrait veiller à ce

---

<sup>115</sup> Groupe de travail Article 29, Avis 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant", WP 169, p.30

<sup>116</sup> Art. 28, § 1<sup>er</sup> 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.

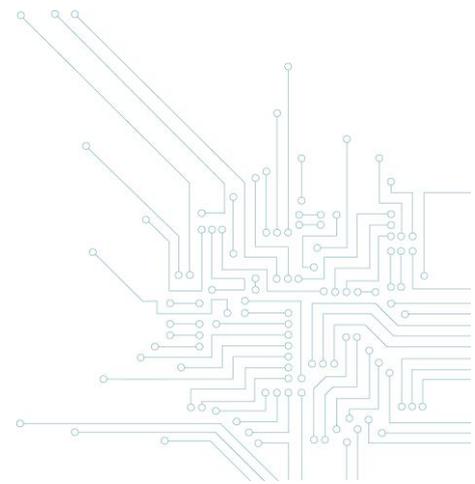
La CVDP devrait contenir au moins les engagements suivants du participant <sup>117</sup> :

- 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<sup>118</sup> ;
- 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

---

<sup>117</sup> Voy. notamment les conditions reprises à l'article 28, § 3 du RGDP.

<sup>118</sup> 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<sup>119</sup> ;

- 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<sup>120</sup> ;
- supprimer ou renvoyer<sup>121</sup> 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<sup>122</sup> ;
- 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.

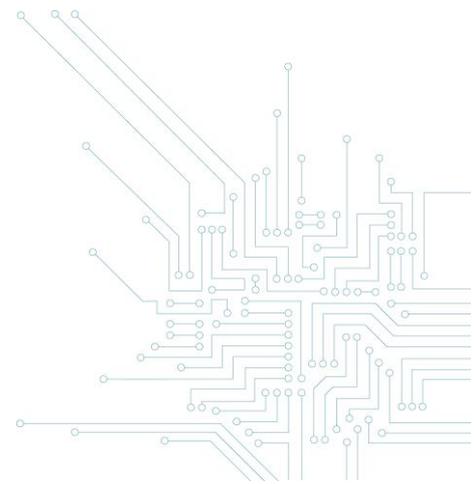
---

<sup>119</sup> Art. 32 § 1er du RGPD.

<sup>120</sup> Art. 33, § 2 du RGPD.

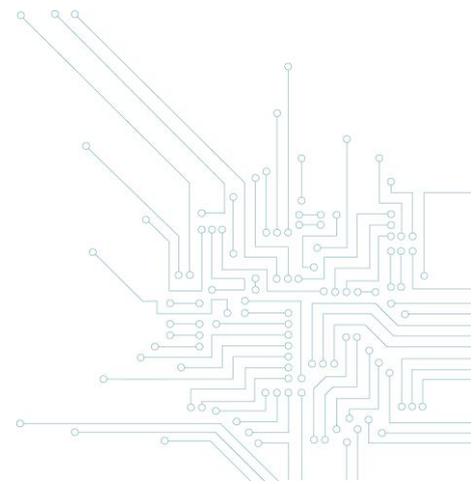
<sup>121</sup> selon le choix du responsable du traitement

<sup>122</sup> 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.
- EVARD 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 Mémoires. 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.

KERKHOF J. en VAN LINTHOUT P., *Cybercrime 3.0*, Brussel, Politeia, 2019.

KERKHOF J. en VAN LINTHOUT P., *Cybercrime*, Brussel, Politeia, 2014.

KERKHOF J. en VAN LINTHOUT P., "Cybercriminaliteit doorgelicht", *T. Strafr.*, 2010, p. 179 et s.

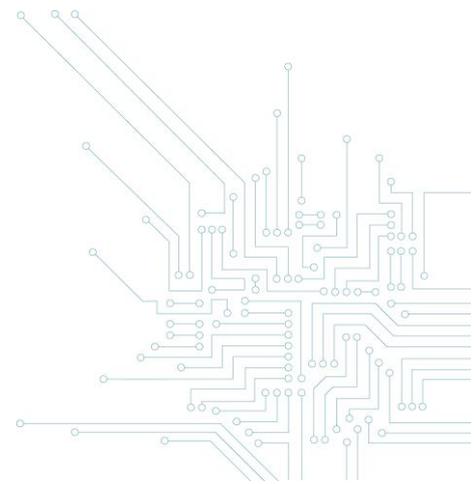
KEUSTERMANS J., F. MOLS en T. DE MAERE, "Informaticacriminaliteit" in *Strafrecht en strafvordering. Commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2010, pp. 65-103.

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.



## 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.

Tous les textes, mises en page, conceptions et autres éléments de toute nature dans ce document sont soumis à la législation sur les droits d'auteurs. La reproduction d'extraits de ce document est autorisée à des fins non commerciales exclusivement et moyennant mention de la source.

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/2020/14828/013

2020

