



CENTRE FOR  
**CYBER SECURITY**  
BELGIUM

# GUIDE TO COORDINATED VULNERABILITY DISCLOSURE POLICIES

## PART II: LEGAL ASPECTS

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

CENTRE FOR  
CYBER SECURITY BELGIUM  
Rue de la Loi, 18  
1000 Brussels

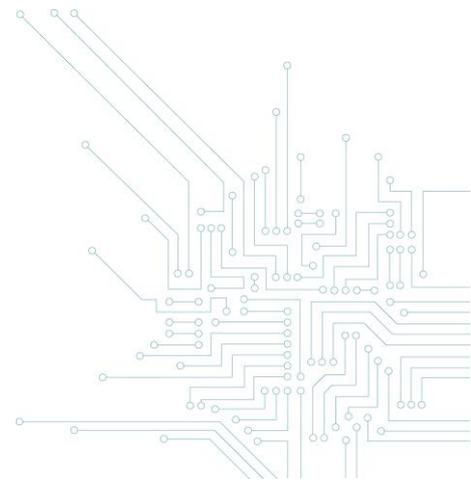
[info@ccb.belgium.be](mailto:info@ccb.belgium.be)  
[www.ccb.belgium.be](http://www.ccb.belgium.be)



.be

UNDER THE AUTHORITY  
OF THE PRIME MINISTER

<b>A.</b>	<b>Application of Belgian criminal law .....</b>	<b>4</b>
<b>B.</b>	<b>Intrusion into an IT system .....</b>	<b>4</b>
	<i>Section 1. External intrusion.....</i>	<i>4</i>
	<i>Section 2. Internal intrusion .....</i>	<i>10</i>
	<i>Section 3. Aggravating circumstances of the intrusion.....</i>	<i>12</i>
	<i>Section 4. The coordinated vulnerability disclosure policy and intrusions.....</i>	<i>13</i>
<b>C.</b>	<b>Manipulation of IT data .....</b>	<b>16</b>
	<i>Section 1. Material constitutive elements.....</i>	<i>16</i>
	<i>Section 2. Moral element .....</i>	<i>16</i>
	<i>Section 3. Aggravating circumstances .....</i>	<i>17</i>
	<i>Section 4. Providing means to facilitate the infringement related to data to take place .....</i>	<i>17</i>
	<i>Section 5. Attempt.....</i>	<i>18</i>
	<i>Section 6. The coordinated vulnerability disclosure policy and infringements related to IT data ....</i>	<i>18</i>
<b>D.</b>	<b>IT forgery and IT fraud .....</b>	<b>19</b>
	<i>Section 1. IT forgery and the use of false instruments in IT .....</i>	<i>19</i>
	<i>Section 2. IT fraud .....</i>	<i>20</i>
	<i>Section 3. Coordinated vulnerability disclosure policy, IT forgery and IT fraud.....</i>	<i>21</i>
<b>E.</b>	<b>Crimes concerning the secrecy of communications.....</b>	<b>22</b>
	<i>Section 1. Crimes concerning the secrecy of non-public communications and data from an IT system .....</i>	<i>22</i>
	<i>Section 2. Preparatory actions .....</i>	<i>24</i>
	<i>Section 3. Receiving and handling illegally obtained communication .....</i>	<i>25</i>
	<i>Section 4. Attempt.....</i>	<i>26</i>
	<i>Section 5. Secrecy of electronic communications.....</i>	<i>26</i>
	<i>Section 6. Coordinated vulnerability disclosure policy and Communication.....</i>	<i>30</i>
<b>F.</b>	<b>Compliance with other legal provisions .....</b>	<b>31</b>
	<i>Section 1. Concepts relating to personal data .....</i>	<i>32</i>
	<i>Section 2. Legal interpretation of the role of participant.....</i>	<i>34</i>
	<i>Section 3. Consequences for the content of the CVDP .....</i>	<i>35</i>
<b>G.</b>	<b>Legal references .....</b>	<b>37</b>



**Warning:**

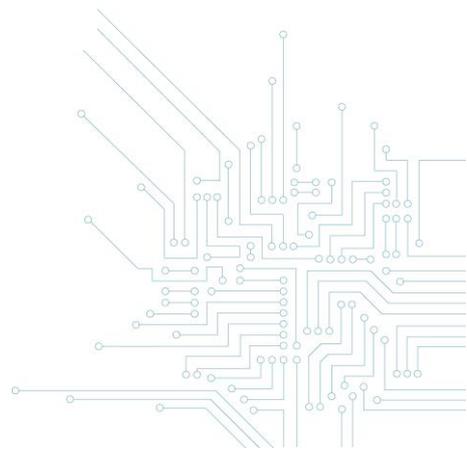
***This guide provides an overview of the concepts, objectives, legal issues and good practices surrounding the adoption of coordinated vulnerability disclosure policies ("CVDP") in the current state of Belgian legislation - see the examples on the CCB website.***

***We would like to point out that the documents drawn up by the CCB in no way change the existing legal rules. Unauthorized intrusion into a third party's computer system, even with good intentions, is a criminal offence.***

***Participants in a CVDP must be aware that they cannot invoke a general exclusion of liability when participating in that policy: they must act prudently and scrupulously comply with all the conditions of the policy as well as the applicable legal provisions.***



*Designed by CCB and Intigrity (2020)*



## A. Application of Belgian criminal law

The application of Belgian criminal law depends mainly on the location of the crime. According to the objective ubiquity theory, a crime is located in the place where the act took place and in the place(s) where its result appears<sup>1</sup>

For the Belgian criminal law to be applicable, it is sufficient that one of the material constitutive or material aggravating elements<sup>2</sup> of a crime took place on Belgian territory, without the entire crime having to have been committed in Belgium. For example, Belgian criminal law may apply if the perpetrator has committed material acts in Belgium, if the IT system or the data are located in Belgium, or if any damage has been caused in Belgium.

In this context, the rules described in this guide may be applied if the perpetrator is in Belgium during their participation in the coordinated disclosure policy or if the IT system that is intruded is located in Belgium.

In view of the common rules of the Budapest Cybercrime Convention<sup>3</sup> and the European legislation<sup>4</sup>, some elements of this legal analysis in Belgium are also applicable to other countries, particularly in Europe. Nonetheless, the competent national authorities must verify, every time, that this is the case.

## B. Intrusion into an IT system<sup>5</sup>

### Section 1. External intrusion

Article 550 *bis*(1) of the Criminal Code punishes a person who, knowing that he is not entitled to do so, accesses or maintains access to an IT system.

---

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

<sup>2</sup> And not just intentional elements.

<sup>3</sup> Council of Europe Convention on Cybercrime, drawn up in Budapest on 23 November 2001, entered into force on 1 July 2004.

<sup>4</sup> Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against IT systems and replacing Council Framework Decision 2005/222/JHA, pb. August 14, 2013.

<sup>5</sup> We prefer the term "intrusion" to "hacking" here because in IT, "hacking" does not fully correspond to the term "illegal computer piracy" and may also refer to activities carried out with the consent of the person in charge of the IT system. The term 'intrusion' does indeed mean intruding (part of) an IT system, without being authorised to do so.

## 1. Material constitutive elements

### 1.1. Access to or maintaining access to an IT system

#### a) IT system

The Act of 28 November 2000 on IT-related crime, which introduced Article 550 *bis* into the Criminal Code, did not define what was to be understood by "IT system".<sup>6</sup> Nevertheless, the parliamentary records of the act describe, on the one hand, the term "IT system" as any system that permits the storage, processing or transmission of data and, on the other hand, the term "data" as representations of information, whatever their material form (electromagnetic, optical or other), which are suitable for storage, processing and transmission via an IT system.<sup>7</sup>

We can also refer to the European Directive 2013/40/EU of 12 August 2013 on attacks against IT systems<sup>8</sup>, which defines these two concepts:

- an "IT system" is a device or group of inter-connected or related devices, one or more of which, on pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance<sup>9</sup>;
- "computer data" means a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function.

The notion of 'IT system' thus goes beyond that of the ordinary personal computer and covers, in a broad sense, all forms of data-processing systems: electronic tablets, GPS systems, smartphones, electronic watches, networks, servers, routers, decoders, Internet TVs, on-board computers of a vehicle, electronic payment terminals, smart cards, etc.

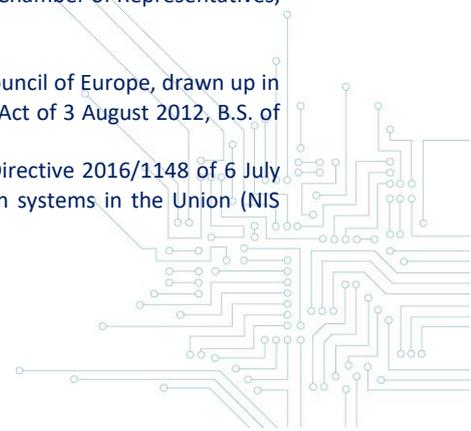
---

<sup>6</sup> In this regard, the legislator seems to have deliberately remained vague in order to avoid the concepts being overtaken by the evolution of IT technologies: cf. in this respect, *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 12. The Belgian legislator took account of the rapid evolution of technology when drafting the Act of 28 November 2000 on IT-related crime, so that the terminology of the Act is technologically neutral: *Parl. Records*, Chamber of Representatives, 2003-2004, No 1284/001, p. 5.

<sup>7</sup> *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 12.

<sup>8</sup> Pb., August 14, 2013. Also see the definitions in art. 1 of the Cybercrime Convention of the Council of Europe, drawn up in Budapest on 23 November 2001, entered into force on 1 July 2004 and approved by Belgium (Act of 3 August 2012, B.S. of 21 November 2012, p. 69092).

<sup>9</sup> These elements are also included in the definition of 'network and information system' of Directive 2016/1148 of 6 July 2016 laying down measures for a high common level of security of network and information systems in the Union (NIS Directive).



## b) Access or maintaining access

Since the terms "access" or "maintaining access" are not defined by the Criminal Code or parliamentary records, they must be understood in the sense of colloquial language, without requiring the use of any particular technology.

The term "access" implies a positive act of intrusion that expresses with certainty the will to intrude into the IT system<sup>10</sup>, without necessarily requiring complex computer manipulations<sup>11</sup>: it suffices, for example, to execute a command that makes it possible to start a system, open a program, look up a file or scroll through a text.

In the event of an intrusion, the perpetrator of the crime usually acts from outside the system via telecommunications infrastructure, bypassing security measures.

However, the concept of access does not require data to be entered, modified or deleted in the IT system.

Maintaining access concerns in particular the case where a person negligently (without realising it) accesses an IT system without authorisation and maintains it after having realised it. It may also be the case when a person retains access to the system even though their authorisation to do so has expired (due to the expiry of a certain period of time or because their post has ended).<sup>12</sup>

## c) Computer system security

The crime does not require that access to or maintaining access to an IT system took place as a result of breaching the system or circumventing security measures (password, firewall, identification, encryption, etc.). The absence of security measures in the IT system does not therefore rule out the existence of an external intrusion.

In the course of parliamentary works, this choice was justified by the fact that, on the one hand, the concept of 'breaking into' the system would entail a number of practical complications (determining a certain level of security that is required and the need to make security systems publicly available in the

---

<sup>10</sup> The computerised terminal of a banking transaction system is, for the purposes of this provision, an IT system: Corr. Court of Dendermonde, 14 May 2007, *T. Strafr.*, 2007, p. 403.

<sup>11</sup> Corr. Court of Antwerp, 10 November 2014, *T. Strafr.*, 2015, p. 94.

<sup>12</sup> For example, a former employee maintain their access to their company's IT system.

context of evidence) and, on the other hand, it might not make sense because of the increasing standardisation of system security.<sup>13</sup>

An external intrusion can therefore consist of the mere use of an unsecured wireless network to connect to the Internet without the authorisation from the administrator of that network.<sup>14</sup>

#### d) Harm caused to the IT system

It is not required that the intrusion or maintaining access has caused harm to the IT system. A mere risk is sufficient, even if it does not materialise.<sup>15</sup> After all, the legislator considers external intrusion to be "an offence that creates a risk and is punishable as such, regardless of the particular malicious intent or the effects achieved".

The legislator wanted to penalise unauthorised access to an IT system as such. In this way, merely acquiring knowledge of the content or of the operating or security parameters of a third party's IT system, even without altering or damaging them, can constitute a crime.

### 1.2. Total lack of authorisation

The concept of "authorisation" is not clarified in the Criminal Code and must therefore, in accordance with the principles of interpretation in criminal matters, be understood in the sense of colloquial language. In this case, this is the authorisation given, by one authorised person to another person, to gain or to maintain access to the IT system concerned.

In concrete terms, two situations may arise: either a person deliberately intrudes into an IT system even though he does not have authorisation to do so, even in part, or a person negligently gains access to an IT system, or deliberately after his authorisation has expired, and unlawfully continues to do so.

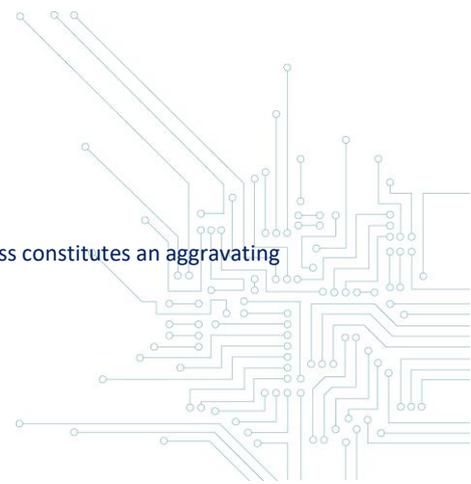
The external intrusion is an instantaneous crime and therefore exists from the moment the individual accesses or maintains access in the IT system without authorisation. Therefore, any authorisation granted after the facts does not cause the crime to disappear.

---

<sup>13</sup> *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 17.

<sup>14</sup> *Corr. Court of Dendermonde*, 14 November 2008, *T. Criminal Law*, 2009, p. 114.

<sup>15</sup> In accordance with art. 550(2), § 3, 3°, of the Criminal Code, the existence of harm nevertheless constitutes an aggravating circumstance of the crime.



In order to be valid, authorisation to access or maintain access to an IT system must necessarily come from a person authorised to do so by the holder of the rights to the system, i.e. the person in charge of that system.<sup>16</sup> After all, it is the person in charge of the system and their delegates who are responsible for granting, withdrawing and determining the conditions of such authorisation. This authorisation may be express or tacit, provided that it exists with certainty.

#### **a) Express authorisation**

Express authorisation consists in the express approval of the manager of the IT system to allow a given natural or legal person to gain access to his IT system, for example in order to carry out maintenance work, security tests or programme updates there. This explicit authorisation is usually included in contractual provisions or internal documents of the organisation.

If an organisation enters into a security audit agreement that includes the performance of intrusion tests<sup>17</sup>, it explicitly authorises access to - at least part of - its IT system. In that case, the service provider, an information security specialist, has access authorisation and should not fear criminal prosecution for external hacking.

#### **b) Tacit authorisation**

Tacit authorisation arises from the particular circumstances of the case. For example, the performance of a function on behalf of a company which necessarily involves access to its IT resources in order to carry out its tasks, even without express authorisation<sup>18</sup>

In the same sense, tacit authorisation may also result from the existence of an IT system clearly made available to the public.<sup>19</sup>

It goes without saying that the owner of the IT system and his or her legal representatives have an authorisation - at least a tacit one - to access the computer system concerned, as long as they can validly invoke these capacities.

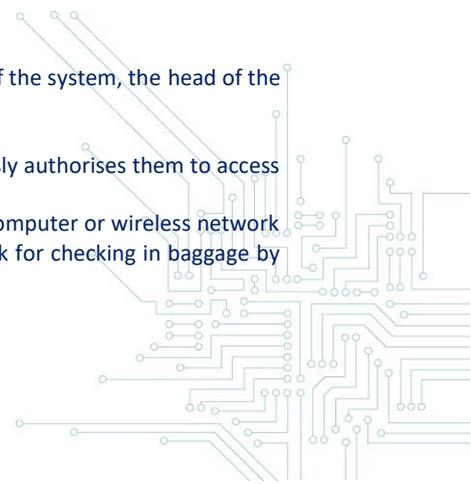
---

<sup>16</sup> Depending on the structure of the organisation, this person may for example be the owner of the system, the head of the organisation, the IT manager or the information security adviser.

<sup>17</sup> "Pentesting" agreement.

<sup>18</sup> Employees, however, often receive a login and password from their employer, which expressly authorises them to access the IT system.

<sup>19</sup> For example, a wireless network in a public area without a password (hotspots), a wireless computer or wireless network from an institution that is made available to customers, an automatic checkout system, a kiosk for checking in baggage by passengers at an airport, etc.



However, the tacit authorisation shall cease to apply from the moment when the professional activity conducted on behalf of the company, the public nature of the access, the making available to customers or the right of ownership expires. If the person concerned subsequently maintains access or accesses the IT system, this is therefore regarded as an intrusion.

## 2. Moral element

### 2.1 Intent to access the system and knowledge of the lack of authorisation

The crime simply requires the deliberate and free will to access or maintain access to an IT system even though one knows that one is not entitled to do so. Article 550 *bis* of the Criminal Code does not require special intent, such as, for example, fraudulent intent or intent to harm. The intentional and unauthorised intrusion or maintenance of access to an IT system is sufficient to commit the crime. On the other hand, intrusion resulting from negligence, absent-mindedness, a manipulation error or insufficient mastery of the IT tool (where the person has acted in good faith) is not punishable (if the person does not subsequently knowingly maintains access to the IT system).

Intentional (unauthorised) intrusion with honourable motives, such as detecting computer security flaws in a third party's IT system, is punishable.<sup>20</sup> The legislator wanted to punish any intrusion - except unintentional intrusion - into an IT system without taking into account the intruder's intention.<sup>21</sup> The aim is to protect as far as possible the confidentiality, integrity and availability of computer systems and of the data stored, processed or transmitted in them.

Therefore, the fact that the intruder had good intentions or, after the event, obtained authorisation from the person responsible for the IT system does not constitute a ground of justification excluding a possible criminal conviction for external intrusion. Indeed, it would be easy for intruders to invoke so-called good intentions after the beginning of their persecution and it would be difficult to verify this after the facts.

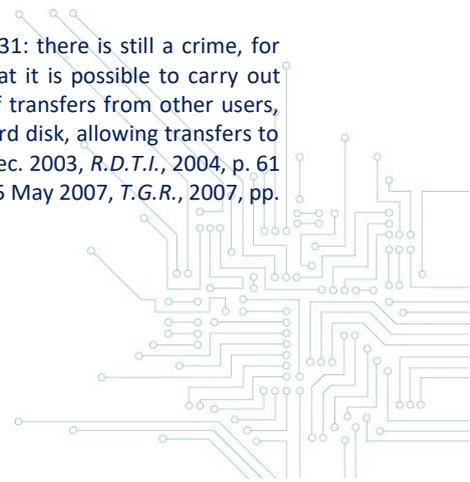
Case law has thus confirmed that external intrusion for the sole purpose of verifying whether a competitor's IT security measures are as unreliable for its data protection as its own is indeed a crime.<sup>22</sup>

---

<sup>20</sup> Corr. Hasselt, 21 January 2004, *Lim. Rechtsl.*, 2005, p. 133; *Computerr.*, 2004, book 3, p. 131: there is still a crime, for example, when a user who checks the security of his bank's PC banking system discovers that it is possible to carry out operations that could harm users of the system (such as downloading lists of beneficiaries of transfers from other users, changing bank account numbers from these lists and putting that changed list back on their hard disk, allowing transfers to account numbers other than those of the beneficiaries) and notifies his bank; Corr. Eupen, 15 Dec. 2003, *R.D.T.I.*, 2004, p. 61 and note O. LEROUX; Corr. Leuven, 15 June 2010, *T. Strafr.*, 2011, p. 270; Corr. Dendermonde, 25 May 2007, *T.G.R.*, 2007, pp. 351 et seq.

<sup>21</sup> Corr. Brussels, Jan 8, 2008, *J.T.*, 2008, p. 337.

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



Nevertheless, the fraudulent intent of the perpetrator is considered an aggravating circumstance of the crime, which will aggravate the penalty imposed.<sup>23</sup>

## Section 2. Internal intrusion

Article 550 *bis*(2) of the Criminal Code concerns those who, with fraudulent intent or with the intent to cause harm, exceed their access authorisation to an IT system.

### 1. Material constitutive elements

#### 1.1. Existence of a partial authorisation

Internal intrusion presupposes the existence, prior to the commission of the crime, of partial authorisation to access the IT system concerned.<sup>24</sup> In the absence of further explanation in the Criminal Code, authorisation must be understood in the usual sense, as in the case of external intrusion (*see above*).

In principle, the nature and extent of access to an IT system are not determined by the legislator, but are left to the discretion of the system's owner, who is best placed to determine who is granted access and within what limits.<sup>25</sup>

For example, the limits imposed on access authorisation may be "spatial", i.e. linked to certain prohibited parts of the IT system, or "functional", i.e. linked to certain prohibited operations or certain categories of prohibited data for the whole system. The limitation is clear if, for example, the system is equipped with a prior identification process to access certain data or programs.<sup>26</sup>

The purpose for which a person is authorised to access an IT system does not limit this right of access, unless expressly stated otherwise by the person in charge of the system. It cannot be said that a person has exceeded their right of access within the meaning of Article 550 *bis*(2) of the Criminal Code simply because he would have diverted this authorisation from its purpose.<sup>27</sup> Consequently, a person who uses his right of access to an IT system for personal purposes, even though he has been authorised to access it for specific professional purposes, does not commit any internal intrusion.

---

<sup>23</sup> Art. 550 *bis*(1) al. 2, of the Criminal Code.

<sup>24</sup> Corr. Leuven, 15 June 2010, *T. Strafr.*, 2011, p. 270: the court ruled that the fact of being a customer of a bank and having authorisation to access the PC banking system does not grant that person authorisation to access the bank's IT system.

<sup>25</sup> Court of Arbitration, 24 March 2004, No 51/2004, B.4.3, p. 7.

<sup>26</sup> Corr. Brussels, 8 January 2008, *J.T.*, 2008, p. 337.

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

The term covers both persons with a permanent partial authorisation, such as that granted to the staff of a company, and persons with a partial authorisation limited in time, such as that granted temporarily to a consultant of an external company specialised in IT security.

Although the concept of prior partial authorisation is often used in the context of a contractual obligation, it does not necessarily imply a subordinate, hierarchical or contractual relationship between the grantor of the authorisation and the beneficiary.

## 1.2. Exceeding the authorisation

The crime exists as soon as the offender exceeds their access rights to enter or maintain access to part of the IT system for which they do not (or no longer) have authorisation to access at the time of the offence.<sup>28</sup>

This case concerns, *inter alia*, the situation of an employee who has been granted partial access to his company's server in order to perform his duties, but exceeds the limits imposed.

As with the external intrusion, the internal intrusion must not necessarily have caused damage to the visited system in order to be penalised.

## 2. Moral element

### 2.1 Intent to exceed the authorisation granted

The crime requires the intent to intentionally and knowingly gain access to, or retain access to, part of the IT system, even though the person knows that they are exceeding their authorisation to access the computer system.

### 2.2. Special intent: fraudulent intent or intent to harm

The mere fact of intruding into certain parts of the IT system without authorisation, for example out of sheer curiosity, is not punished. The intrusion must be motivated by a special intent, i.e. unlawful profit (fraud) or malicious intent (intent to harm), to be a crime. This may be the case, for example,

---

<sup>28</sup> See Cass., 5 January 2011, P.10.1094.F., [www.cass.be](http://www.cass.be): the finding that the persons prosecuted had a right of access to the data at issue when they requested and were given the copy of the data excludes the exceeding of the right of access that is punishable under article 550 *bis*(2), Criminal Code.

when an employee who has access to part of the company network exceeds this authorisation to access the accounting software and carry out unauthorised banking transactions there, or even to commercialise certain data for his own benefit.<sup>29</sup>

The legislator justified this distinction with the crime of external intrusion by the fact that third parties who do not have authorisation to access the system would endanger the security of the IT system more than a person who has a partial authorisation.<sup>30</sup> In addition, parliamentary records have pointed out that the person in charge of the system has other sanctions at his disposal (civil or contractual sanctions, or disciplinary sanctions) against the beneficiary of a partial authorisation which would have been exceeded without fraudulent or malicious intent.<sup>31</sup>

### Section 3. Aggravating circumstances of the intrusion

Article 550 *bis*(3) of the Criminal Code provides for a number of aggravating circumstances which apply to both intrusion crimes.

#### 1. Acquisition of data

The first aggravating circumstance is the acquisition, by any means, of data stored, processed or transmitted by means of the IT system visited.<sup>32</sup> This involves acquiring IT data (original or copy) from the system visited so that it can be reused if necessary.<sup>33</sup> The wording "by any means" is very broad and can therefore refer to printing, sending by mail, copying onto a carrier, storing in a cloud system, taking a screenshot, etc.<sup>34</sup> One of the legislator's objectives here was to combat the theft of industrial secrets in the context of industrial espionage.<sup>35</sup>

Finally, the concept of 'acquisition' of data seems to require a moral element since it derives from the fact that the offender himself takes the initiative to retrieve these data and not from the mere automatic storage of data by the computer system used for the intrusion.

---

<sup>29</sup> *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/004, p. 6.

<sup>30</sup> *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 16.

<sup>31</sup> *Parl. Records*, Senate, 1999-2000, 2-392/3, p. 6; *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 16.

<sup>32</sup> *Corr. Dendermonde*, 14 May 2007, *T. Strafr.*, 2007, p. 403.

<sup>33</sup> This is sometimes called "bitnapping", a reference to the kidnapping of data.

<sup>34</sup> However, it should be made clear that this provision does not refer to the physical removal of the medium on which IT data were printed or stored (e.g. stealing printed data, a hard disk or a USB stick) which is another crime, stealing the carrier itself.

<sup>35</sup> *Parl. Records*, Chamber of Representatives, 1999-2000, no. 50, 0213/001, p.17: an employee who attempts to steal corporate secrets from their employer may also be prosecuted for the offence of communicating trade secrets, as referred to in art. 309 of the Criminal Code.

## 2. Use of the system visited

The second aggravating circumstance is any use of a third party's computer system or the use of the computer system to gain access to a third party's computer system. On the one hand, the provision concerns the use of the capacity of the computer system visited, which temporarily limits the possibilities of use of other users (e.g. time theft or bandwidth theft).<sup>36</sup> On the other hand, it concerns the fact of accessing another computer system via the system visited, which is used as an intermediary for a computer attack that gives the impression that the attack comes from an intermediary system<sup>37</sup>

The two cases in question do indeed presuppose a moral element, i.e. that the offender knowingly and intentionally intended to use the computer system for these purposes. This element excludes, for example, cases where the reduction in IT system's capacity would unexpectedly result from the intrusion.

## 3. Harm to the computer system or data

The third aggravating circumstance is to cause any harm, even accidental, to the computer system or to the data stored, processed or transmitted in it, or to the IT system or the IT data of a third party.

This includes any type of harm, whether material (physical damage to the system, cables or peripherals) or immaterial (saturation of the system, unavailability), to the computer system visited or to its data.

In this case, the harm may have been caused intentionally or unintentionally, so that no moral element is required on the part of the perpetrator.<sup>38</sup>

## Section 4. The coordinated vulnerability disclosure policy and intrusions

As explained above, the crime of external intrusion into an IT system exists even if the perpetrator has no malicious intent, does not circumvent security measures, does not use the visited system, does not

---

<sup>36</sup> *Parl. Records*, Chamber of Representatives, 1999-2000, No 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", *quoted*, p. 639; For example, it may involve using the IT system as part of a "botnet" network, i.e. a group of infected computers ("zombies") controlled remotely by a hacker to attack other computer systems, hiding the real origin of the attack.

<sup>38</sup> Nevertheless, the occurrence of this circumstance must be foreseeable for the perpetrator and there must be a causal link between this circumstance and the commission of the principal offence. Intentionally caused harm resulting from the input, modification or deletion of data will give rise, where appropriate, to another crime, i.e. infringement relating to IT data referred to in art. 550 *ter* of the Criminal Code.

take over data and does not cause harm to the system or to the data. The good intentions of the participant in a CVDP are therefore not sufficient to avoid the existence of this criminal offence.

However, external intrusion will only occur if the participant does not have an authorisation from the responsible organisation to access its computer system. If the participant has authorisation, there is no external intrusion.

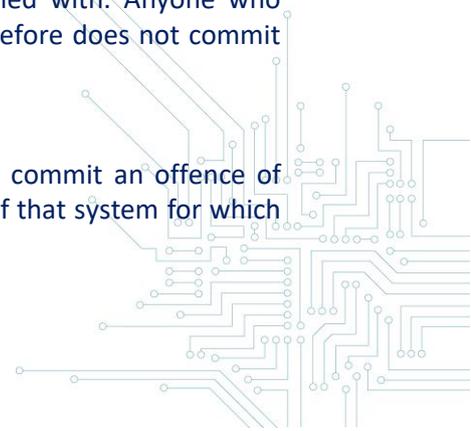
In the context of a coordinated vulnerability disclosure policy or a vulnerability rewards program, there is such authorisation - either explicit or tacit.

When introducing a coordinated vulnerability disclosure policy, including a reward programme, a de facto and at least tacit and clear authorisation is granted. Indeed, this policy clarifies the modalities of cooperation between an organisation responsible for the IT system concerned and participants willing to inform it of vulnerabilities in its IT system. Such cooperation shall necessarily involve authorisation to access or maintain access to the IT system concerned with a view to improving its security and in compliance with the conditions laid down in advance. Even if the beneficiary of the authorisation is not precisely known at the time when the coordinated disclosure policy is introduced, it is in fact an authorisation granted unilaterally by the person in charge of the IT system to persons wishing to take part in its coordinated disclosure programme.

In view of the principle of legality, criminal law must be interpreted restrictively. In case of doubt regarding the scope of the repressive terms used, the judge is therefore obliged to limit their scope. Consequently, the lack of authorisation, within the meaning of Article 550 *bis* of the Criminal Code, must be interpreted strictly, i.e. in the event that no action can justifiably lead third parties to believe that the responsible organisation is allowing access to its IT system. If the responsible organisation has deliberately and consciously implemented a coordinated disclosure policy, it is clearly willing, in advance, to allow access to its IT system, provided that the conditions set are respected. It should also be noted that part of the case law gives an extensive interpretation of the provisions favourable to the accused, which may also be the case for the concept of "authorisation". Since the authorisation is favourable to the perpetrator and excludes the existence of a crime, it must be interpreted as being inherent to the introduction of a coordinated disclosure policy.

The importance of a coordinated disclosure policy therefore consists in excluding one of the material constitutive conditions for the crime of external intrusion, i.e. the total lack of authorisation, provided that the conditions formulated by the responsible organisation are complied with. Anyone who participates in such a policy and complies with its terms and conditions therefore does not commit external intrusion.

Any participant with partial access authorisation for an IT system shall not commit an offence of internal intrusion if, with good intent, he detects security breaches in parts of that system for which



he does not have access authorisation. As long as the participant exceeds their access authorisation without fraudulent intent or intent to harm, there will be no internal intrusion, which would be punishable by criminal law.

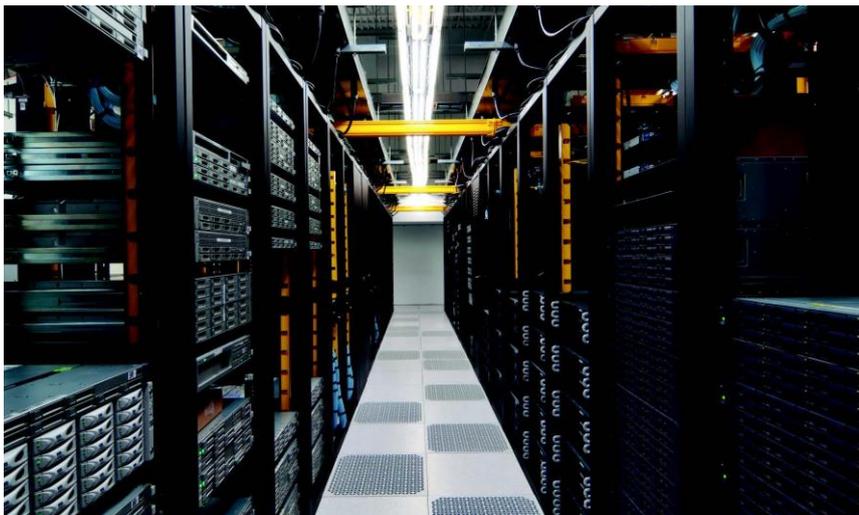
Although it is intended that a coordinated vulnerability disclosure policy applies primarily to persons outside the responsible organisation who do not have any authorisation to access the IT system, this policy may also provide a framework, where appropriate, for the conduct of participants with good intentions within the organisation. Indeed, in the absence of contractual rules for these cases, or in case these rules are lacking, a coordinated disclosure policy of the responsible organisation can be effectively applied by the parties. Therefore, such a policy is not only relevant for persons who have no legal ties with the responsible organisation.

Of course, the circumstances in which such a "benevolent" breach may occur and the rules to be followed in that case must be strictly limited in contractual documents<sup>39</sup> or in the coordinated vulnerability disclosure policy<sup>40</sup>.

**Caution:**

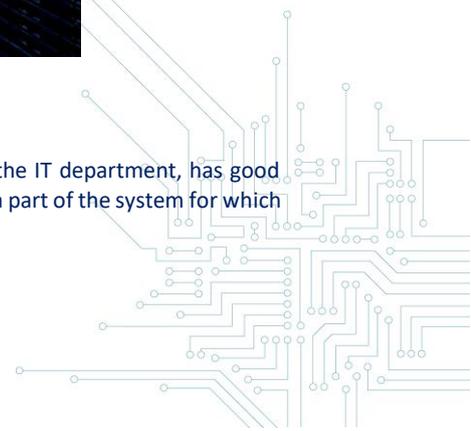
***Participants must also ensure that they do not take any action, without additional authorisation, with respect to any IT systems or data managed by third parties not covered by the responsible organisation's coordinated disclosure policy.***

***After all, third parties are not subject to the content of the disclosure policy and may take legal action because of the participant's conduct.***



<sup>39</sup> For example, an employment contract, a statutory relationship or a service contract.

<sup>40</sup> This may be the case where the beneficiary of a partial authorisation, e.g. an employee of the IT department, has good reason to suspect that there is a vulnerability, a virus, a worm, a Trojan horse or ransomware in a part of the system for which he does not, in principle, have authorisation to access.



## C. Manipulation of IT data<sup>41</sup>

Article 550 *ter* of the Criminal Code punishes those who, despite knowing that they are not entitled to do so, directly or indirectly, engage in introducing, modifying or deleting data in an IT system, or changing the normal use of data in an IT system by any technological means.

### Section 1. Material constitutive elements

#### 1.1. Entering, modifying or deleting IT data by any technological means

The purpose of the offence is to enter, modify, delete data or change the normal use of data by any technological means in an IT system. The main purpose of this provision is to protect the integrity of an IT system or of the data it contains, stores and transmits against computer manipulation in the broad sense. Intervention in the system may be direct, i.e. via the use of a computer directly connected to the network, or indirect, i.e. via a remote connection using a telecommunications network or an intermediary computer.

In practice, this can involve entering a virus, a logical bomb, a worm, a Trojan horse, deleting or creating a file, disrupting an operating system, encrypting files, rendering a hard disk unusable or simply changing a user's password.

Contrary to what one might think, harm is not a constitutive element of the crime, but only an aggravating circumstance. Simply leaving behind an entry in the system, such as 'X was here', is an infringement relating to IT data. However, there is a crime even if the deliberate input of data into a computer has not achieved its purpose, e.g. due to a technical malfunction.

#### 1.2. Lack of authorisation

The intention is to penalise any manipulation of IT data<sup>42</sup> that has not been authorised in advance by the person in charge of the IT system concerned. The authorisation should cover the modification of data in the IT system, irrespective of whether or not access to the computer system has been authorised.

### Section 2. Moral element

The perpetrator must have been aware that he was performing an unauthorized act. The unintentional and unconscious transmission of a virus as an attachment to an e-mail is therefore not a crime on the part of the sender.

---

<sup>41</sup> The choice of the term "IT sabotage" is not ideal, as it could be wrongly inferred that there is harm, which is not a constitutive element of the crime. In a broader sense, the offence is a breach of the integrity and authenticity of IT data.

<sup>42</sup> *Parl. Records*, Chamber of Representatives, 1999-2000, N°50, 0213/001, p. 19.

## Section 3. Aggravating circumstances

### 1. Fraudulent intent or intent to harm

Although the existence of a special intent on the part of the offender is not required for the crime, it is nevertheless an aggravating circumstance.<sup>43</sup>

### 2. Harm to data

Harm to data in the IT system concerned or in any other IT system is an aggravating circumstance of the crime.<sup>44</sup> This concerns the alteration of data stored, transmitted or processed by the IT system, as opposed to harm to the system itself.

### 3. Obstructing the operation of the system

This aggravating circumstance consists of the infringement relating to IT data which has the effect of obstructing, in whole or in part, the proper functioning of the IT system in question or of any other IT system.<sup>45</sup> This includes the destruction of content, total or partial crippling of the computer system or a delay in its operation, for example through the massive sending of queries to overload the server or even the infliction, remotely, of physical damage to the computer system. Since this provision also refers to 'any other IT system', it also covers the development or distribution of computer worms, which can automatically multiply and copy themselves via communication networks. However, there must be a causal link between the main crime and the foreseeable harm caused.

## Section 4. Providing means to facilitate the infringement related to data to take place

Independently of the crime of infringement relating to IT data, the Criminal Code also punishes any person who unlawfully possesses, produces, sells, acquires with a view to its use, import, distributes or makes available in some other form any device, including IT data, designed or adapted primarily to enable the offences of infringement relating to computer data, knowing that such data may be used to cause damage to data or, in whole or in part, to impede the proper functioning of an IT system.<sup>46</sup>

### 1. Material constitutive elements

The offence consists of the creation, possession or making available of tools or IT data primarily designed or adapted to commit an offence relating to computer data. The concept of "device" here corresponds to the means facilitating intrusion.

---

<sup>43</sup> See the considerations on the special intent required for the offence of internal unauthorised intrusion; art. 550 *ter* (1) of the Criminal Code.

<sup>44</sup> Art. 550 *ter*(2) of the Criminal Code.

<sup>45</sup> Art. 550 *ter*(3) of the Criminal Code provides for one year to five years imprisonment and a fine of €26 to €100,000 or one of those penalties. Moreover, given the importance of IT systems in our society, obstructing the proper functioning of an IT system is punished more severely than simply causing harm to data.

<sup>46</sup> Art. 550 *ter*(4) of the Criminal Code.

## 2. Moral element

The crime requires an intentional element, i.e. that the perpetrator knows that the tools or data can be used to cause harm to data or impede the proper functioning of an IT system in whole or in part. The perpetrator must therefore act in full knowledge of the facts and with the intent to draw up, possess or make available such devices.<sup>47</sup> Consequently, the unintentional and unconscious possession of such devices is not a constitutive element of the crime. Similarly, merely owning a program that allows both lawful and unlawful use is not necessarily a crime.

As with the crime involving hacker tools, the term "wrongful" means that the intentional possession or deliberate provision justified by an academic<sup>48</sup>, scientific or professional use, is not punishable by criminal law.

## Section 5. Attempt

The attempt is punishable by the same penalties as the infringement relating to IT data itself.<sup>49</sup>

However, the attempt is only realised if the perpetrator has not only performed preparatory acts but also unambiguous executive acts.<sup>50</sup>

## Section 6. The coordinated vulnerability disclosure policy and infringements related to IT data

By participating in a coordinated vulnerability disclosure policy, the participant has, in principle, an authorisation to enter IT data into the system concerned or to attempt to do so. It is indeed difficult to detect security flaws without at least trying to enter data or execute orders containing such data.

However, the authorisation to modify or delete IT data (or to try to do so) depends on the way in which the coordinated vulnerability disclosure policy has been drawn up. In order to avoid an infringement related to IT data, participants must strictly comply with the terms of the policy on the modification and deletion of IT data.

Depending on the content of the coordinated vulnerability disclosure policy and the participant's compliance with these conditions, there will or will not be an offence relating to an IT data breach.<sup>51</sup>

With regard to the tools enabling an IT data breach, the participant may develop, own or make available such tools as part of participation in a vulnerability disclosure policy. Such actions are not

---

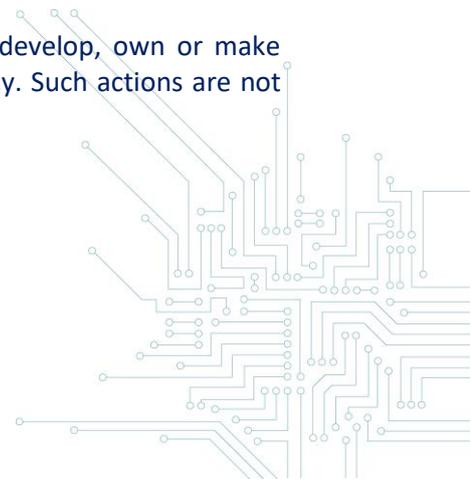
<sup>47</sup> O. LEROUX, "La Criminalité informatique", quoted , p. 437.

<sup>48</sup> For example, IT security training.

<sup>49</sup> Art. 550 *ter*(6) of the Criminal Code.

<sup>50</sup> See the explanation of the attempted intrusion into an IT system.

<sup>51</sup> And this crime may, where appropriate, be linked to aggravating circumstances.



unlawful as long as they are justified by legitimate purposes relating to the detection of vulnerabilities with the consent of the organisation of the person in charge of the IT system concerned.

Nevertheless and once again, the participant will have to prove that he or she is a concrete participant in an existing vulnerability disclosure policy and that that policy is clearly identifiable. The mere intention to hypothetically participate, in a general manner, in such a policy is not enough.

## D. IT forgery and IT fraud

### Section 1. IT forgery<sup>52</sup> and the use of false instruments in IT<sup>53</sup>

Article 210 *bis* of the Criminal Code punishes forgery which consists in introducing into an IT system, changing or deleting data that are stored, processed or transmitted by means of an IT system, or altering, by any technological means, the possible use of data in an IT system, thereby altering the legal scope of such data.<sup>54</sup>

This provision also punishes, on the one hand, the use of data obtained from IT forgery, when it is known that these data are falsified,<sup>55</sup> and, on the other hand, the attempt to commit IT falsification.<sup>56</sup>

#### 1. Material constitutive elements

##### 1.1 Twisting the truth in one of the ways provided by law (introducing, changing or deleting data)

Forgery has not been legally defined but case law has clarified that forgery is a distortion of the truth that may create rights vis-à-vis third parties who cannot in practice verify the accuracy thereof. For example, it could be the creation and use of a fake email address in the name of a third person, a fake online sale ad or a fake profile on a social network. Data that can be falsified must therefore have a legal scope and be subject to public faith.<sup>57</sup>

These may be IT files stored on the hard drive of a terminal or on an optical or digital medium (provided it is carried out on a system) or data transmitted in a network. The forgery of a paper document on which computer data is printed, on the other hand, is an example of “classic” forgery (forgery in writing).<sup>58</sup>

---

<sup>52</sup> Art. 210 *bis*(1) of the Criminal Code.

<sup>53</sup> Art. 550 *bis*(4) of the Criminal Code.

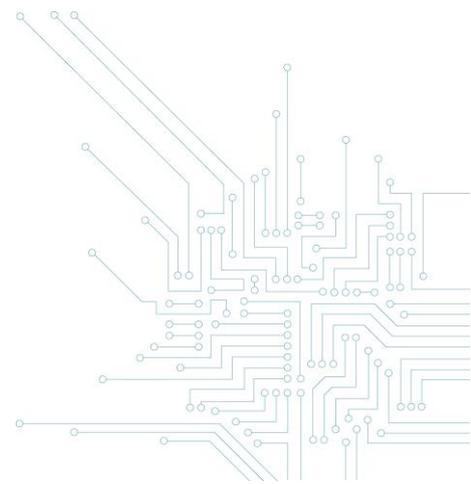
<sup>54</sup> Art. 210 *bis*(1) of the Criminal Code.

<sup>55</sup> Art. 210 *bis*(2) of the Criminal Code.

<sup>56</sup> Art. 210 *bis*(3) of the Criminal Code.

<sup>57</sup> *Parl. Records*, Chamber of Representatives, 1999-2000, No 0213/001, p. 10.

<sup>58</sup> Art. 194 et seq. of the Criminal Code.



## 1.2. Changing the legal scope of the data

For the crime to have been committed, the manipulation of the data must have led to a change in its legal scope. The legal scope corresponds to the amended data as a whole and not to a unit. The change may relate to the computer data themselves or to the idea they express.

Parliamentary records mentions, for example, the counterfeiting or falsification of credit cards<sup>59</sup> and digital contracts or the introduction of a counterfeit credit card number in an IT system.

## 2. Moral element

The crime requires a fraudulent intent or intent to harm.<sup>60</sup> This particular intent is justified by the fact that computer (or IT) forgery is equated with the other categories of forgery. The fraudulent intent consists of the desire to provide oneself or someone else with an undue gain or advantage. The intent to harm concerns the will to harm a natural or legal person.

Mistakes, negligence or carelessness alone are therefore not sufficient to constitute a crime of computer forgery.

Similarly, the creation or use of a false instrument for IT purposes is not punishable under criminal law if the perpetrator acts for scientific, professional or educational purposes.

## 3. Attempt

Attempting to commit forgery of information is also punishable, without any harm having to actually arise.

Nevertheless, the attempt involves both preparatory and executive acts that leave no doubt as to the criminal intent of the offender.<sup>61</sup>

## Section 2. IT fraud

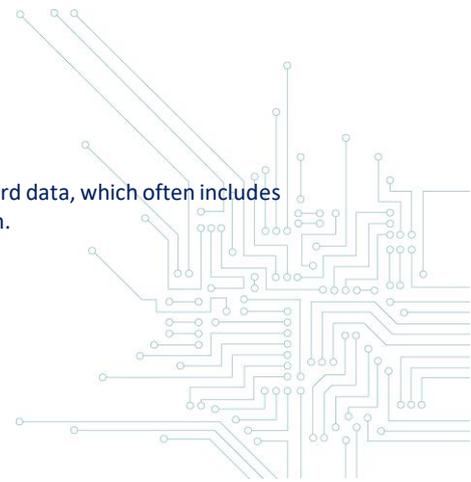
Article 504 *quater* of the Criminal Code criminalises any person who, with fraudulent intent, seeks to obtain an undue economic advantage for himself or for another person by introducing in an IT system, altering or erasing data stored, processed or transmitted by a computer system, or by altering the normal use of data in a computer system by any technological means.

---

<sup>59</sup> This concerns in particular the penalisation of "skimming", i.e. the illegal copying of payment card data, which often includes offences relating to IT forgery, computer fraud and unauthorised intrusion into a third IT system.

<sup>60</sup> See Article 193 of the Criminal Code.

<sup>61</sup> See the attempted intrusion into an IT system.



## 1. Material constitutive elements

### 1.1 Manipulating data

The crime involves introducing, modifying<sup>62</sup> or deleting data in an IT system or the use of any technology to alter the normal use of data stored, processed or transmitted by means of an IT system (see *above* IT forgery).

### 1.2. Pursuit of an undue economic advantage

The offence does not require that the intended unlawful economic advantage be acquired in practice, but merely the pursuit of such an objective, even if that objective has ultimately not been achieved. IT fraud is a crime where a mere risk is sufficient or a "formal" crime, where it is only necessary to prove that the data processing is causally linked to the pursuit of an undue economic advantage. The economic advantage<sup>63</sup> can be direct or indirect and take different forms: tangible goods, intangible goods, services. It may be for the benefit of the perpetrator or another person.

## 2. Moral element

IT fraud presupposes not only that the offender knowingly and willfully committed the crime, but also that he was pursuing a particular intention, i.e. a fraudulent intent to gain an undue economic advantage for himself or for someone else.

## 3. Attempt

Attempts at IT fraud are also punishable.<sup>64</sup>

Here, too, the attempt will only have been proven if the Public Prosecution Service demonstrates that the perpetrator not only performed preparatory acts but also unambiguous executive acts.

## Section 3. Coordinated vulnerability disclosure policy, IT forgery and IT fraud

Since IT forgery requires a fraudulent intent or an intent to harm, participation in a coordinated vulnerability disclosure policy excludes this offence on the part of the participant. In the same sense, the participant in a CVDP or a vulnerability reward programme does not, in principle, run the risk of being criminally prosecuted for IT fraud, as there is no fraudulent intent on the part of the participant.

---

<sup>62</sup> For example, changing the balance on a bank account.

<sup>63</sup> Article 504 *quater* previously required the offender to obtain a fraudulent financial advantage for himself or for another person, which was not fully in line with Article 8 of the Council of Europe Convention on Cybercrime: *Parl. Records, Chamber of Representatives, 2003-2004, No 1284/001, p. 6 and 8.*

<sup>64</sup> See the considerations relating to attempted unauthorised intrusion.



## E. Crimes concerning the secrecy of communications

### Section 1. Crimes concerning the secrecy of non-public communications and data from an IT system

Article 314 *bis* of the Criminal Code punishes anyone who, intentionally and by means of any device, intercepts or causes to be intercepted, takes cognisance of, or causes to be taken cognisance of, records or causes to be recorded communications that are not accessible to the public without the consent of all the participants in these communications.<sup>65</sup>

#### 1. Material element

##### 1.1 Intercepting, taking cognisance or recording by means of a device

In the absence of a legal definition, the interception, taking cognisance or recording of communication must be understood in the sense of colloquial language. First and foremost, the interception consists of hijacking communications that are addressed to someone else, sent to someone else or intended for someone else, along the way, by surprise. Subsequently, taking cognisance of a communication means being aware of the existence and content of a communication between persons although not being the recipient of this communication. The latter concept has a broad meaning and is also applicable to technical forms of communication, such as electronic data transmission. Finally, the recording concerns the act of fixing data on a local or remote physical carrier<sup>66</sup>, for later use.

The offence of intercepting communications is intended to punish not only the perpetrator of the crime but also the person who ordered it.<sup>67</sup>

The provision further clarifies that intercepting<sup>68</sup>, taking cognisance of or recording must be done with the help of any device.<sup>69</sup> This is a broad formulation, but it necessarily involves the use of a technical aid. If not, the facts are not punishable. This requirement seems to be met as soon as a computer manipulation is carried out or a programme is used.<sup>70</sup>

---

<sup>65</sup> Art. 314 *bis*(1) 1°, of the Criminal Code.

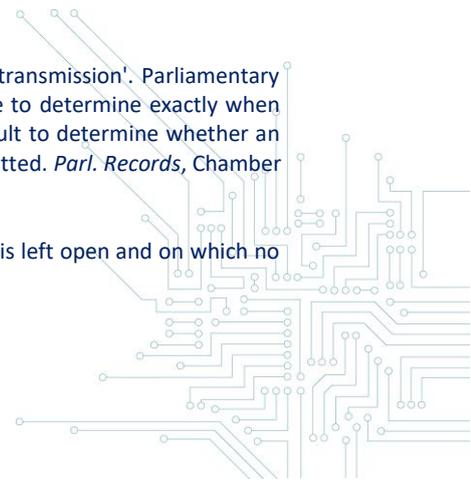
<sup>66</sup> For example, via a cloud storage service.

<sup>67</sup> *Parl. Records*, Senate, 1992-1993, No 843/1, pp. 8-9.

<sup>68</sup> From now on, the provision no longer requires communications to be intercepted 'during transmission'. Parliamentary records explain this change by the fact that new developments in IT often make it impossible to determine exactly when communications are still in "transmission" or have already been delivered. After all, it is difficult to determine whether an unread e-mail should be regarded as a communication delivered or as a communication transmitted. *Parl. Records*, Chamber of Representatives, 2015-2016, no. 1966/001, p. 54.

<sup>69</sup> *Parl. Records*, Senate, 1992-1993, No 843/1, p. 6.

<sup>70</sup> Conversely, merely displaying an e-mail or a web page directly on a computer screen, which is left open and on which no manipulation is carried out, does not fall within the scope of the offence.



## 1.2. Non-public communication in which one does not participate

Article 314 *bis* of the Criminal Code henceforth clarifies that the communication in question is 'not publicly accessible' and no longer 'private communication or private telecommunication'.<sup>71</sup> As before, this concept can be interpreted depending on the context and intentions of the participants in the communication.<sup>72</sup> Non-public access means that the communication is not intended to be heard by persons other than the correspondents of the communication.<sup>73</sup> In principle, the professional or non-professional nature of a communication has no impact on the assessment of its non-public nature.<sup>74</sup>

The communication concerns in particular electronic data transmission in computers and computer networks.<sup>75</sup> This refers in particular to e-mails.

The provision criminalises only those persons who do not participate in the communication. Conversely, any person who participates in a communication that is not accessible to the public and who records this communication, even without the other participants being aware of it, does not commit an offence within the meaning of Article 314 *bis* of the Criminal Code.

## 1.3 Lack of consent of the participants

In order for it not to be a crime, one must have obtained the prior consent of all participants in the electronic communication and not just some of them. The consent of the participants, arising from a set of circumstances, can be express or tacit, as long as it is clear. Some authors add that this consent must necessarily have been given in a specific and individual manner, and must not have been derived from a prior agreement, for example, in a clause of an employment contract or of an internal regulation. Consent should also have been obtained fairly and with due regard for any purpose communicated to the participants.

---

<sup>71</sup> Article 32 of the Act of 25 December 2016 on various amendments to the Code of Criminal Procedure and the Criminal Code with a view to improving the special investigation methods and certain investigation methods relating to the Internet and electronic and telecommunications and creating a voice print database, Official Gazette of 17 January 2017, p. 2738; Parliamentary works justify this change as a terminological adaptation, taking into account the amendments to articles 90 *ter* et seq. of the Code of Criminal Procedure.

<sup>72</sup> *Parl. Records*, Senate, 1992-1993, No 843/1, p. 6. Parliamentary records also explain that the concept of 'non-public communication' refers to communication or electronic communication that takes place in the private sphere. It is therefore an overarching concept that also includes the former terms "private communication or telecommunication": *Parl. Records*, Chamber of Representatives, 2015-2015, no. 1966/001, p. 53.

<sup>73</sup> *Parl. Records*, Senate, 1992-1993, no. 843/1, p. 7. Commission for the Protection of Privacy, Recommendation No 08/2012 of 2 May 2012 on employer monitoring of the use of electronic communication tools in the workplace, [www.privacycommission.be](http://www.privacycommission.be).

<sup>74</sup> *Parl. Records*, Senate, 1992-1993, No 843/1, p. 8 and No 843/2, pp. 10 and 36.

<sup>75</sup> In that sense: *Parl. Records*, Senate, 1992-1993, No 843/1, p. 7.

## 2. Moral element

The crime expressly requires that the perpetrator acts intentionally, i.e. knowingly and willfully. Parliamentary records clearly stated that mere chance or immodesty is not enough to constitute a crime.<sup>76</sup> Consequently, the mere accidental discovery of communications that are not accessible to the public is not punishable by law. However, anyone who acts intentionally but merely out of curiosity commits a crime.<sup>77</sup> For example, accidentally learning of the content of a communication by a technician while checking the proper functioning of an IT system is not punishable, except if he acted deliberately out of curiosity.

### Section 2. Preparatory actions

#### 1. Setting up a device

##### 1.1 Material element

The Criminal Code punishes anyone who installs or causes to be installed any device enabling the unauthorised interception, cognisance-taking or recording of communications.<sup>78</sup> After all, the device is not necessarily placed and used by or on behalf of the same people.<sup>79</sup>

##### 1.2. Moral element

The crime requires the offender to act with the intent to commit an unauthorised interception, cognisance-taking or recording.

#### 2. Making available of a device

##### 2.1 Material constitutive elements

The legislator punishes whoever wrongfully possesses, produces, sells, obtains with a view to its use, imports, distributes or makes available in any other way, a device, including computer data, designed or adapted primarily to enable the unauthorised interception of communications.<sup>80</sup>

The term 'device' signifies the means of access or other tools designed, for example, to modify or destroy data or to penetrate the functioning of systems, such as virus software, or software designed or adapted to access computer systems.<sup>81</sup>

---

<sup>76</sup> *Parl. Records*, Senate, 1992-1993, No 843/1, p. 6.

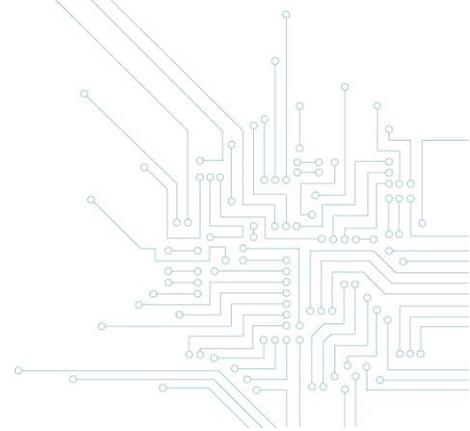
<sup>77</sup> *Parl. Records*, Senate, 1992-1993, No 843/1, p. 6.

<sup>78</sup> Art. 314 *bis*(1) 2°, of the Criminal Code.

<sup>79</sup> *Parl. Records*, Senate, 1992-1993, No 843/1, p. 9.

<sup>80</sup> Art. 314 *bis*(2*bis*) of the Criminal Code.

<sup>81</sup> *Parl. Records*, Chamber of Representatives, 2003-2004, No 1284/001, p. 6.



## 2.2. Moral element

As with the provision of means to facilitate unauthorised intrusion, the offender must have knowingly and willingly developed, possessed or made available such a device. He must therefore have been aware that the criminal device was primarily designed or adapted to allow unauthorised interception, recording and cognisance-taking of communications.

Nevertheless, the term 'wrongfully' means that possessing or making available such a device for legitimate purposes, such as scientific or professional purposes in the field of communication system security is not a criminal offence.

## Section 3. Receiving and handling illegally obtained communication

The Criminal Code punishes any person who knowingly keeps, discloses or disseminates to another person the content of communications that are not accessible to the public or data from an IT system that have been unlawfully intercepted or recorded or of which knowledge has been acquired unlawfully, or who knowingly makes any use of information obtained in this way.<sup>82</sup>

### 1. Material element

#### 1.1 Content of communications not accessible to the public or data from an IT system that have been unlawfully intercepted or recorded or of which cognisance has been taken unlawfully

Any person who, by mistake or coincidence, receives communication not intended for him does not commit a crime.

#### 1.2. Keeping, disclosing or distributing to another person, or using in any way

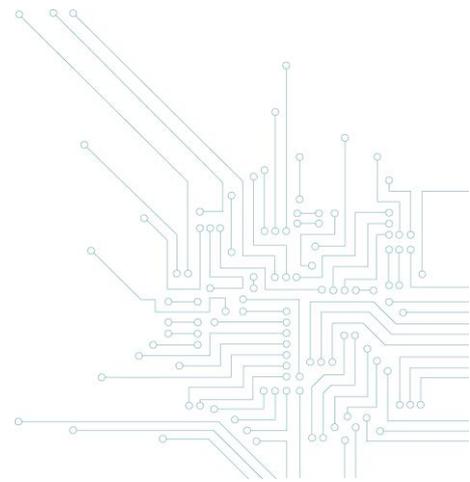
With regard to these concepts, reference is made to the explanatory note on receiving and handling unlawfully obtained IT data.

### 2. Moral element

One must have acted "knowingly", i.e. intentionally and with knowledge of the illegality of the information obtained.

---

<sup>82</sup> Art. 314 *bis*(2) of the Criminal Code.



## Section 4. Attempt

The attempted unauthorised interception of communications not accessible to the public shall also be punished.<sup>83</sup>

To this end, it must be proved that preparatory and executive acts have been taken which leave no doubt as to the criminal intent of the perpetrator.

## Section 5. Secrecy of electronic communications

Article 145 of the Law of 13 June 2005 on electronic communications provides for criminal sanctions for various actions that violate the confidentiality of electronic communications, which is protected by Article 124 of the same Act.

These different sanctions are aimed at ensuring the confidentiality of information transmitted over an electronic communications network.<sup>84</sup>

### 1. Material constitutive elements

#### 1.1 Consent of the persons directly or indirectly concerned

In spite of the broad wording of the law, which suggests that all persons directly or indirectly involved in the communication and its content should give their consent<sup>85</sup>, it nevertheless seems more reasonable to assume that only the persons to whom the communication is directly or indirectly linked, i.e. the sender and the recipient(s), should give their consent. As far as connection data or data from web pages consulted are concerned, it is sufficient to obtain the consent of the user concerned.

#### 1.2. Deliberate cognisance-taking by a person of the existence of information of any kind sent by electronic means and not intended for them personally<sup>86</sup>

##### 1.2.1. Information sent electronically

The Law of 13 June 2005 indirectly defines the concept of 'electronic communications' through the definition of electronic communications *service*, which is 'a service normally provided for remuneration and consisting wholly or mainly in the conveyance, including switching and routing, of signals on electronic communications networks (...)' and of *electronic communications network*, which are

---

<sup>83</sup> Art. 314 *bis*(3) of the Criminal Code. See Corr. Brussels, 8 January 2008, *J.T.*, 2008, p. 337, for an example of an attempt to intercept communication by means of a 'keylogger', i.e. spyware that records the activity (keystrokes) of a computer and forwards it to a third party.

<sup>84</sup> *Parl. Records*, Senate, 2004-2005, No 1425-1426/01, p. 76.

<sup>85</sup> Commission for the Protection of Privacy, Opinion No 8/2004 of 14 June 2004 on the preliminary draft law on electronic communications, p. 7, [www.privacycommission.be](http://www.privacycommission.be). The CBPL wondered whether, according to the law, a person mentioned in the message itself should be regarded as indirectly involved in the communication, which went far beyond the European text.

<sup>86</sup> Art. 124, al. 1, of the Act of 13 June 2005 on electronic communications.

'transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means' (...).<sup>87</sup> The Code of Economic Law defines "electronic mail" as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient".<sup>88</sup>

The term 'electronic communication' includes telephone communications, e-mails, text messages, messages sent over a wireless network or the exchange of cellular data, connections to a network or to an information technology system. This term therefore includes e-mails and internet connection data that make it possible to identify the websites consulted.

Cognisance-taking covers the information in its entirety, including the content of electronic mail.<sup>89</sup> Any person who has become aware of the existence of electronic mail and has made use of it, has necessarily simultaneously become aware of its contents. The knowledge and use of the content of an e-mail are related to the knowledge and use of the existence of that e-mail.<sup>90</sup> It can be assumed that article 124 of the Law of 15 June 2005 therefore constitutes an obstacle to knowledge of the content of electronic communications.

### **1.2.2. Information of any kind which is not intended for them personally**

Taking cognisance of an information of any kind intended for the person who becomes aware of it does not constitute a violation of Article 124, al. 1 of the Law of 13 June 2005.

### **1.3 Deliberately identifying the persons involved in sending the information and its content**

Article 124, al. 2 prohibits the identification of persons involved in both the sending of the information and its content. This includes the identity details of the sender, the recipient(s) of the messages and the persons involved in the content (e.g. those mentioned in the e-mail).

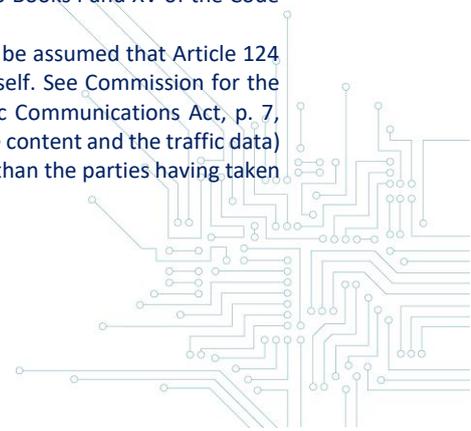
---

<sup>87</sup> Art. 2, 3° and 5° of the Act of 13 June 2005 on electronic communications, *Official Gazette* of 20 June 2005, p. 28070.

<sup>88</sup> Act of 15 December 2013 inserting Book XII, "Law of the digital economy", into the Code of Economic Law, and inserting the definitions specific to Book XII and the law enforcement provisions specific to Book XII, into Books I and XV of the Code of Economic Law.

<sup>89</sup> Cass., 1 Oct. 2009, C.08.0064.N, [www.cass.be](http://www.cass.be). The legal doctrine doubted whether it should be assumed that Article 124 related not only to the existence of information, but also to the content of the information itself. See Commission for the Protection of Privacy, Opinion No 8/2004 of 14 June 2004 on the preliminary draft Electronic Communications Act, p. 7, [www.privacycommission.be](http://www.privacycommission.be): "The purpose of this Article is to protect communications (both the content and the traffic data) in such a way that no one other person can take cognisance of them or manipulate them other than the parties having taken part in the communication".

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



#### **1.4. Deliberately taking cognisance of data relating to electronic communications and to another person<sup>91</sup>**

Electronic communication data are data transmitted over networks, such as the e-mail addresses of sender and recipient, the time of sending and receiving, routing data, message size, presence of attachments, etc.<sup>92</sup>

Taking cognisance of this information consists of being aware of the existence and content of data relating to electronic communications between persons although one is not the recipient of these communications.

#### **1.5. Altering, deleting, disclosing, storing or using in any way the information, identification or data obtained intentionally or unintentionally<sup>93</sup>**

It is forbidden to alter, delete, disclose, store or make any use of the information, identification or data obtained intentionally or unintentionally.

## **2. Moral element**

This provision implies that the acts made punishable must be committed intentionally by the perpetrator of the offence. If it is established that the cognisance of the electronic communication was accidentally taken, the intentional nature of the discovery is lacking and article 124 of the law of 13 June 2005 does not apply.<sup>94</sup> Consequently, a distinction must be made between actively and merely accidentally learning about electronic communication.

## **3. Exceptions laid down in Article 125 of the Law**

Article 125 of the Law of 13 June 2005 on electronic communications provides for a number of exceptions to the confidentiality of communications referred to in Article 124 of the same Act and in Article 314 *bis* of the Criminal Code. This provision makes it possible, *inter alia*,<sup>95</sup> to carry out the actions that are, in principle, prohibited when they are necessary to verify the proper functioning of the network and to ensure the proper execution of an electronic communications service. Due to the general wording of the law, this provision seems to be applicable to both a public electronic communications network and a private network.

---

<sup>91</sup> Art. 124, al. 3 of the Law of 13 June 2005 on electronic communications.

<sup>92</sup> Labour Court of Brussels, 10 February 2004, R.G. 44002, [www.juridat.be](http://www.juridat.be).

<sup>93</sup> Art. 124, al. 4 of the Law of 13 June 2005 on electronic communications.

<sup>94</sup> Labour Court of Bergen, Dec. 8, 2010, *JLMB*, 2011, p. 715; *Chron. D.S.*, 2011, p. 399; Labour Court of Brussels, 4 December 2007, *J.T.T.*, 2008, p. 179; T.T. Liege, 19 March 2008, RG 360.454, [www.juridat.be](http://www.juridat.be).

<sup>95</sup> Art. 125(1) 1°, of the Law of 13 June 2005 on electronic communications also provides for the possibility of a derogation, where the law permits or imposes the performance of the otherwise illegal acts. According to the Privacy Commission, Article 16 of the Law of 3 July 1978 on employment contracts would constitute a legal basis subject to compliance with certain conditions.

In so far as this can be justified by strictly technical measures, it is therefore possible to carry out the operations referred to in Article 124. However, information on electronic communications discovered on this occasion may not be used for purposes other than checking the proper functioning of the network.

#### **4. Fraudulent electronic communication<sup>96</sup>**

##### **1. Material constitutive elements**

This is the fraudulent establishment of electronic communications by means of an electronic communications network.

##### **2. Moral element**

In addition to knowingly and intentionally acting, this crime also implies that the offender had a special intent, i.e. unlawfully giving himself or another person an advantage.

##### **3. Attempt and preparatory actions<sup>97</sup>**

The law also criminalizes any person who fraudulently attempts to establish electronic communication or sets up any device intended to establish such communication.

Like the other attempts, this attempt requires proof that the offender has performed preparatory and unambiguous executive acts.

#### **5. Unauthorised use of an electronic communications network or service<sup>98</sup>**

##### **1. Material constitutive elements**

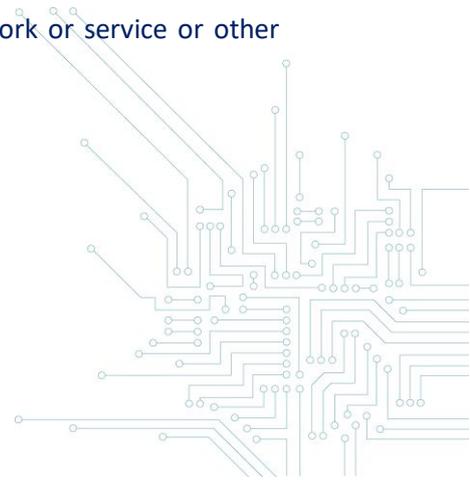
The law punishes any person who uses an electronic communications network or service or other electronic means of communication with an unauthorized purpose.

---

<sup>96</sup> Art. 145(3) 1°, of the Law of 13 June 2005 on electronic communications.

<sup>97</sup> Art. 145(3) 3°, of the Law of 13 June 2005 on electronic communications.

<sup>98</sup> Art. 145(3 *bis*) of the Act of 13 June 2005 on electronic communications.



## 2. Moral element

The crime means that the offender wants to cause nuisance or harm to his correspondent.

## 3. Attempt and preparatory acts

The law also criminalizes any person who sets up any device intended to make unauthorized use of an electronic communications network or service, as well as the attempt to do so.

The attempt must require that the offender has taken preparatory and unequivocal executive actions.

## Section 6. Coordinated vulnerability disclosure policy and Communication

Participants may not intentionally intercept, gain knowledge of or record any communication not accessible to the public using any device.<sup>99</sup> Incidentally, this is not necessary when implementing a coordinated vulnerability disclosure policy.

However, the interception, knowledge or recording by the participant of communications that are not accessible to the public does not constitute an offence if it is done either by chance or with the consent of all participants in the communication concerned<sup>100</sup>, or with the participant's own participation in the communication.

A participant may also, without committing a crime, set up or cause to be set up a device that makes it possible to intercept, take cognisance of or record communications that are not accessible to the public, provided that he is acting without the intent to use the device in question for the aforementioned purposes or with the consent of all participants, or takes part in the communication himself.

In addition, a participant may develop, own or make available to another participant a device enabling the interception, cognisance-taking or recording of non-public communications. However, this is only justified in the context of a real participation in a coordinated vulnerability disclosure policy. After all, this tool could demonstrate that vulnerabilities in the IT system can lead to unauthorised cognisance-taking of communications.

---

<sup>99</sup> Art. 314 *bis* of the Criminal Code.

<sup>100</sup> Although, in many situations, this is not self-evident, it is not excluded that, under the coordinated disclosure policy, the participant may have the consent of the participants in the communication.



Conversely, the intentional attempt to intercept, record or take cognisance of communications not accessible to the public is only justified in the context of the implementation of a coordinated disclosure policy if the participant has the consent of all participants or participates in the communication itself.

If the participant could not reasonably have known that the content of communications not accessible to the public or of data from an IT system was unlawfully obtained, he may use, maintain, disclose or distribute it. Conversely, the participant who knows that such information has been unlawfully obtained, must strictly abstain from handling it in the context of his participation in a coordinated vulnerability disclosure policy.

In view of the good intentions of the participant, he should in principle not establish a fraudulent electronic communication or use an electronic communications network or service in an unauthorized manner.

Finally, a coordinated vulnerability disclosure policy certainly does not aim at deliberately obtaining or altering information, the identity of communicating persons or data relating to electronic communications. If the participant happens to carry out these actions, it must be either fortuitously or with the consent of all the participants involved or with regard to a communication intended for him personally. The implementation of a coordinated disclosure policy, on the contrary, aims to promote the confidentiality of the electronic communications exchanged by the responsible organisation.

In our opinion, the participant in a coordinated vulnerability disclosure policy could possibly invoke the application of article 125 of the Law of 13 June 2005 on electronic communications, which makes it possible to derogate from the confidentiality of electronic communications. The actions taken by a participant in the context of a coordinated disclosure policy may be aimed at verifying the proper functioning of an electronic communications network or service, including its security.

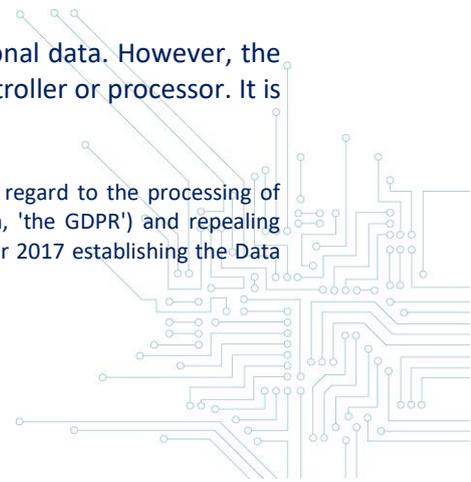
## **F. Compliance with other legal provisions**

In addition to the provisions on cybercrime, participants in a coordinated vulnerability disclosure policy should take into account other legal provisions, including legislation on the processing of personal data.<sup>101</sup>

A coordinated disclosure policy is not intended to intentionally process personal data. However, the responsible organisation will most likely have to process personal data as controller or processor. It is

---

<sup>101</sup> European Regulation No 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, 'the GDPR') and repealing Directive 95/46/EC, as well as the Belgian laws in that regard, including the Act of 3 December 2017 establishing the Data Protection Authority, Official Bulletin of 10 January 2018, p. 989.



therefore possible that the participant may, even by accident, have to process personal data stored, processed or transmitted in the IT system concerned. It may also be necessary for a participant to process personal data to demonstrate the existence of a vulnerability as part of its vulnerability analysis.

## Section 1. Concepts relating to personal data

### 1. Personal data

The GDPR defines personal data as any information about an identified or identifiable natural person. Data are identifiable if they enable a natural person to be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more elements characterising the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.<sup>102</sup> The 'identifiable' nature of the person does not depend on the mere desire to identify the data processor, but on the ability to identify the person directly or indirectly from these data (for example: an e-mail address, identification number, online identifier, IP address or location data).

### 2. Processing

The processing of personal data has a broad meaning and includes 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.'<sup>103</sup> In short, the term 'processing' includes almost all operations that may involve personal data.

For example, the mere collection or consultation of personal data is considered data processing.<sup>104</sup>

### 3. Controller

The controller is a natural person or legal person, a public authority, a service or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.<sup>105</sup>

---

<sup>102</sup> Art. 4, 1) of the GDPR.

<sup>103</sup> Art. 4, 2) of the GDPR.

<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, Brussels, published by Politeia, p. 23.

<sup>105</sup> Art. (4), 7) of the GDPR: where the purposes and means of such processing are laid down in Union or Member State law, these bodies of law may specify the controller or the criteria for its designation.

The capacity of controller thus derives from the power to determine the purposes for which personal data are processed.

### 3.1 Power of determination

For an entity, the power to determine the means that it can choose to process personal data for its own purposes<sup>106</sup>. The term 'controller' is a functional concept, intended to assign responsibilities to persons exercising an actual influence. It is therefore based on a factual rather than a formal analysis<sup>107</sup>

In practice, therefore, it is necessary to examine why processing takes place and who has actually decided to carry it out.

### 3.2 Determination of purpose and means

The purposes of the processing operations are the intended outcomes sought through the processing activities. The means are the technical and organisational methods used<sup>108</sup> to achieve the purposes of the processing. In short, the aim is to determine the 'why' and 'how' of the processing operations.<sup>109</sup>

These two elements must be in place in order to be considered as controllers.

The determination of the means must relate to the essential technical and organisational aspects of the processing (for example, the data to be processed, the duration of processing or the persons authorised to have access to the data).<sup>110</sup>

## 4. Processor

The processor is a natural or legal person, a public authority, a service or any other body that processes personal data on behalf of the controller.<sup>111</sup> The processor acts on behalf of the controller by following

---

<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, Brussels, published by Politeia, page 26.

<sup>107</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169, p. 9, ([https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf))

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

<sup>109</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169, page 13, *idem*.

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

<sup>111</sup> Art. 4, 8) of the GDPR.

his instructions, at least as regards the purpose of the processing and the essential aspects of the means of processing.

## Section 2. Legal interpretation of the role of participant

The Responsible Disclosure Policy is a form of membership agreement that binds the ethical hacker vis-à-vis the data controller.<sup>112</sup> For example, the purpose and essential means of processing personal data are, in principle, determined by the responsible organization and not by the participant under a coordinated vulnerability disclosure policy. In that case, the participant must comply with the legal obligations concerning the protection of personal data in his capacity as processor of the responsible organisation.<sup>113</sup>

According to Article 28(3)(a) of the GDPR, the processor must process personal data in accordance with the instructions of the data controller. It is generally accepted that the processing entrusted to the processor may nevertheless involve 'a degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means'.<sup>114</sup> It is conceivable, for example, that the participant will have a certain freedom of choice regarding the means he uses to check the security of the information systems of the responsible organisation. The responsible organisation determines which systems and services participants are allowed to test and to which ones they do not have access.

Article 28(1) of the GDPR provides that the controller must draw up procedures for the selection of service providers in order to ensure that the latter provide "adequate safeguards with regard to the application of appropriate technical and organisational measures", particularly in terms of expertise, reliability and resources. Indeed, as part of a CVDP or a vulnerability detection reward programme, the responsible organisation may restrict participation to certain ethical hackers or require participants to have the necessary expertise and experience to test the responsible organisation's systems, including any personal data.

The controller must also be able to exercise a certain level of supervision<sup>115</sup> over the service carried out on his behalf in order to check whether this is done in accordance with the agreement concluded with the processor and with the GDPR. For example, the participant must cooperate with the responsible organisation and, at its request, be able to provide all relevant information.

---

<sup>112</sup> Or the processor, where the responsible organisation has the status of controller.

<sup>113</sup> The responsible organisation can be a controller of personal data or itself a processor of a controller.

<sup>114</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169, p. 25, *idem*.

<sup>115</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169, p. 27-28, *idem*.

However, the participant may be considered as the controller when the essential means for processing personal data are not sufficiently defined in the CVDP or when the participant does not follow the instructions of the responsible organisation. Indeed, any participant who unlawfully processes data (or processes data for purposes other than the detection of vulnerabilities) must be regarded as the controller since he himself determines a different processing purpose and/or (essential) means of processing.

### Section 3. Consequences for the content of the CVDP

It follows from the above that the CVDP must specify the obligations of the parties with regard to the processing of personal data, in particular the purpose of and the essential means for any processing. For example, the content of the policy should define the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, as well as the rights and obligations of the controller.

The responsible organisation must include rules in its CVDP that oblige the participant to provide adequate guarantees for the application of appropriate technical and organisational measures for the processing of personal data.<sup>116</sup> The participant must ensure that these data are stored with a level of security appropriate to the risks (preferably encrypted) and that they are deleted immediately after processing.

The processing of personal data for a purpose other than the detection of vulnerabilities in the responsible organisation's systems, equipment or products should be excluded.

Furthermore, participants must undertake to report any possible loss of personal data to the responsible organisation and/or to the Data Protection Authority as soon as possible after becoming aware of it.

The CVDP must contain at least the following commitments on the part of the participant<sup>117</sup>:

- process personal data only on the basis of documented instructions from the controller;
- ensure that persons authorised to process personal data have undertaken to respect confidentiality;
- ensure that natural persons acting under the authority of the processor who have access to personal data may process them only on instructions from the controller;<sup>118</sup>

---

<sup>116</sup> Art. 28(1) of the GDPR.

<sup>117</sup> See in particular the conditions mentioned in Article 28 § 3 of the GDPR.

<sup>118</sup> Art. 32(4) of the GDPR.

- take appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the cost of their implementation as well as the nature, scale, context and purposes of the processing and the varying degrees of probability and seriousness of the risks to the rights and freedoms of individuals;<sup>119</sup>
- obtain the prior consent of the controller for the employment of another processor and oblige the latter to comply with the content of the disclosure policy;
- assist, as far as possible, the controller in fulfilling his duty to reply to requests for the exercise of data subjects' rights, by means of appropriate technical and organisational measures;
- assist the controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR (security, breach notification, impact analysis, prior consultation), taking into account the nature of the processing and the information available to the participant;
- inform the controller without delay as soon as the participant becomes aware of a personal data breach;<sup>120</sup>
- upon completion of participation in the policy, delete all personal data or return them<sup>121</sup> to the data controller, and delete existing copies;
- make available to the controller all information necessary to demonstrate compliance with the obligations, including a register of all categories of processing activities carried out on behalf of the controller;<sup>122</sup>
- exclude the use of personal data for any purpose other than the detection of vulnerabilities in the system or the communication of such data to third parties.

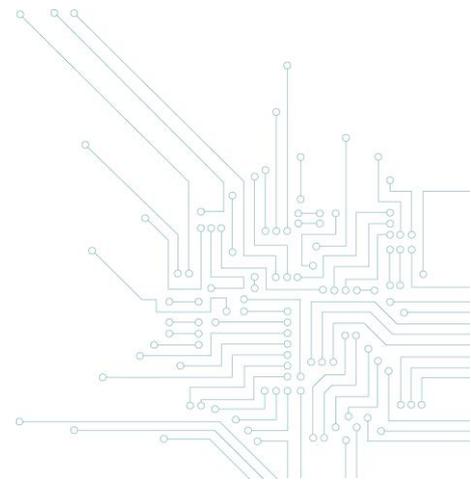
---

<sup>119</sup> Art. 32(1) of the GDPR.

<sup>120</sup> Art. 33(2) of the GDPR.

<sup>121</sup> According to the choice of the controller.

<sup>122</sup> The content of which is mentioned in art. 30(2) of the GDPR.



## G. Legal references

- DE NAUW A. and KUTY F., *Manuel de droit pénal spécial*, Waterloo, Kluwer, 2014, p. 1125-1145.
- DECHAMPS F. and LAMBILOT C., *Cybercriminalité: Etats des lieux*, Limal, Anthémis, 2016, p. 26-46.
- DEHOUSSE F., VERBIEST T., ZGAJEWSKI T., "La crité dans la société de l'information" in *Introduction au droit de la société de l'information*, Brussels, Larcier, 2007.
- DE VILLENFAGNE F. and 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, p. 287-294.
- EVRARD S., "La loi du 28 novembre 2000 relative à la criminalité informatique", *J.T.*, 2001, p. 241-245.
- HENRION T., *Mémento Droit pénal*, Brussel, Kluwer, 2016.
- KUTY F., *Principes généraux du droit pénal*, t. 1, La loi pénale, Brussels, Larcier, 2009.
- K. ROSIER, "Le traitement de données dans le cadre des communications électroniques" in X. *Vie privée et données à caractère personnel*, Brussels, Politeia.
- LEROUX O., "La Criminalité informatique", *Les infractions contre les biens*, Brussels, Larcier, 2008, p. 409-436.
- LEROUX O., in X. *Postal Mémoires. Lexique du droit pénal et des lois spéciales*, Brussels, Kluwer, 2014, p. 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, p. 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, blz. 37-160.
- OMRANI F. and 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*, Brussels, Bruylant, 2005, pp. 101-133.
- TULKENS F., VAN DE KERCHOVE M., CARTUYVELS Y. and GUILLAIN C., *Introduction au droit pénal*, 9th edition, Brussels, 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, Brussels, 2019, p. 217 et seq.
- VANDERMEERSCH D., "Eléments de droit pénal et de procédure pénale", *La Charte*, Brussels, 2012.
- BAEYENS, E., "Informatica en recht: oude griffels - nieuwe leien", *T. Criminal Law*, 2007, p. 404-407.
- DEENE J. and NERINCKX G., "Computercriminaliteit" in *Praktijkboek recht en internet*, Titel II – Hoofdstuk 10, Brugge, Vanden Broele, 2007, p. 3-43.
- DELBROUCK I., "Informaticacriminaliteit", in X., *Postal Memorialis, Lexicon strafrecht, strafvordering en bijzondere wetten*, Antwerp, Kluwer, 2007, l. 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. Criminal Law*, 2001, p. 286-334.

J. DUMORTIER, *ICT-Recht*, Acco, Leuven, 1999, p. 86 ff.

KERKHOFS J. and VAN LINTHOUT P., *Cybercrime 3.0*, Brussels, Politeia, 2019.

KERKHOFS J. and VAN LINTHOUT P., *Cybercrime*, Brussels, Politeia, 2014.

KERKHOFS J. and VAN LINTHOUT P., “Cybercriminaliteit doorgelicht”, *T. Strafr.*, 2010, pp. 179ff.

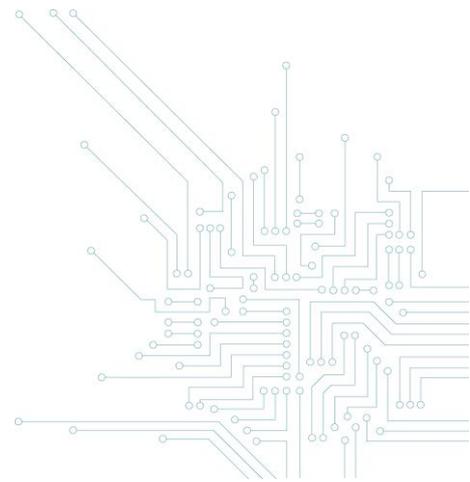
KEUSTERMANS J., F. MOLS and T. DE MAERE, “Informaticacriminaliteit” in *Strafrecht en strafvordering. Commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2010, p. 65-103.

KEUSTERMANS J. and MOLS F., “De wet van 28 november 2000 inzake informaticacriminaliteit: eerste overzicht”, *R-W*, 2001-2002, p. 721-732.

KEUSTERMANS J. and DE MAERE T., “Tien jaar wet informaticacriminaliteit”, *R-W*, 2010-2011, p. 562-568.

VAN EECKE, P., “De Wet Informaticacriminaliteit”, in X., *Elektronische handel, juridische en praktische aspecten*, Heule, UGA, 2004, p. 369-385.

VANSTEENHUYSE S. en T’JONCK P., “Cybercriminaliteit en privacy” in *Privacy en strafrecht*, Nieuwe en grensoverschrijdende verkenningen, Antwerp, Maklu, 2007.



## GUIDE FOR THE COORDINATED VULNERABILITY DISCLOSURE POLICY PART II: LEGAL ASPECTS

This document and its annexes were drawn up by the Centre for Cyber Security Belgium (CCB). This federal public service was created by the Royal Decree of 10 October 2014 and is under the authority of the Prime Minister.

All texts, layout, designs and other elements of any kind contained in this document are subject to copyright laws. Extracts from this document may only be reproduced for non-commercial purposes and if the source is mentioned.

The CCB denies any responsibility as to the content of this document.

The information provided:

- is purely general in nature and does not aim to cover all specific situations;
- is not necessarily complete, accurate or up to date in all respects.

**Responsible publisher:**  
**Centre for Cyber Security Belgium**  
M. De Bruycker, Director  
Wetstraat 18  
1000 Brussels

**Legal deposit:**

D/2020/14828/015

2020

