CENTRE FOR
CYBER SECURITY
BELGIUM

GUIDE TO COORDINATED VULNERABILITY DISCLOSURE POLICIES

PART I: GOOD PRACTICES

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

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de Loi,16
1000 Brussels

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

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

A. TABLE OF CONTENTS

CENTRE FOR
CYBER SECURITY
BELGIUM

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.

** Shutterstock - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

B. INTRODUCTION

I. Background

The increasing importance of information systems in our society significantly increases the risk of incidents related to the security of these systems. These incidents can, for example, compromise the availability of a particular service or the integrity, authenticity or confidentiality of data. As more and more devices are being used that are connected to the Internet, any incident will have even greater consequences.

As far as the causes of these incidents are concerned, vulnerabilities pose a major risk. However, this risk is inherent in the development, use and update process of these systems. Taking into account the extent and technicality of this problem, it seems an illusion to believe that all device manufacturers or those responsible for IT systems will be able to solve it on their own.

An organisation may choose to rely on a particular company to verify the security of its information systems (e.g. through a security audit), or, publicly, on persons with good intentions ("*ethical hackers*") who wish to contribute to improving the security of these technologies by identifying existing vulnerabilities and helping to resolve them.

II. Concepts

A. *A coordinated vulnerability disclosure policy*[1]*(CVDP)* is a set of rules pre-determined by an organisation responsible for IT systems that allows participants[2] (or "*ethical hackers*"), with good intentions, to identify possible vulnerabilities in its systems, or to provide it with all relevant information about them. These rules, usually published on a website, make it possible to define a legal

[1] Also called "responsible disclosure policy": we prefer the term "coordinated" rather than "responsible" as it avoids any confusion with the concepts of civil liability and emphasizes the reciprocal nature of the process.
[2] These could be, for example, cyber security researchers or users. Participants may be subject to selection by a third party who acts as a confidential adviser ("coordinator").

framework for the cooperation between the responsible organisation and participants under the policy. These rules should ensure, inter alia, the confidentiality of the information exchanged and provide a responsible and coordinated framework for any disclosure of discovered vulnerabilities.

Thus, the term 'disclosure' does not necessarily mean that the vulnerability is made public, but rather that the participant communicates it to the responsible organisation. The participant is obliged to communicate the vulnerability to the responsible organisation, but the public disclosure of the vulnerability (by the participant or the organisation concerned) is optional in the context of a CVDP.

B. ***A vulnerability***[3] is a flaw or a weakness, a design[4] or execution error[5] the lack of updates in light of existing technical knowledge, which may affect IT security.[6] A vulnerability can lead to an unexpected or unwanted event and be exploited by malicious third parties to harm the integrity, authenticity, confidentiality or availability of a system[7]or to damage a system.

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

[4] For example, an error or omission in the design of a system or protocol that makes it intrinsically vulnerable.

[5] For example, an error during implementation, configuration or use.

[6] For example, a system, network, process, program, application, service, protocol or component.

[7] Or the information it contains.

C. ***A responsible organisation*** is a natural person or legal entity who manages, owns, sells or manufactures systems or products related to IT and is responsible for their security and proper functioning.

D. ***CVDP participant*** [8] ***(or "ethical hacker***") is a person with good intentions who, with the consent of the responsible organisation, wishes to contribute to improving the security of IT systems. They may, for example, carry out pentests or use other methods to check the security of information systems. This is completely different from *hackers* who use their skills to illegally break into systems with bad intentions[9]. Participants want to inform the IT manager or coordinator of any vulnerabilities discovered, so that they can be eliminated.

E. ***A coordinator*** is a natural person or legal entity who acts as an intermediary between the participants and the organisation in charge of an IT system by providing logistical, technical and legal assistance or other functions[10] to facilitate cooperation. If no CVDP coordinator is appointed, the Centre for Cybersecurity Belgium (vulnerabilityreport@cert.be) can fulfil this role.

F. ***A Vulnerability Rewards Program (or bug bounty program)***[11] relates to all rules set by a responsible organisation to give rewards to participants who identify vulnerabilities in the technologies it uses. This reward can be a sum of money, but also a gift or simply public recognition (ranking among the best participants, publication, conference, etc.). This is a coordinated vulnerability disclosure policy that provides for a reward to be paid to the participant according to the amount, importance or quality of the information transmitted.

[8] Sometimes called "white hats", as a reference to the fact that heroes in American westerns usually wore white hats.
[9] Sometimes called "black hats", as a reference to the fact that bad guys in American westerns usually wore black hats.
[10] For example, to review the vulnerability reports or as mediator.
[11]« Program de récompense pour la découverte de vulnérabilités » in French or « beloningsprogramma voor het opsporen van kwetsbaarheden » in Dutch.

This policy is more attractive to potential participants and often leads to better results for the organisation. The organisation may, for example, use a *bug bounty platform* that provides technical and administrative assistance to manage of its vulnerability detection reward program (coordinator role).

III. Goals

a. To provide a legal framework for useful, fair, effective, legal and budget-friendly cooperation

When an organisation uses a particular external service provider to check the security of its IT systems, it enters into a security audit agreement which may include pentests (or "penetration tests"), simulating an attack by persons with malicious intentions, to demonstrate existing vulnerabilities. In that case, the mutual legal obligations of the parties are, in principle, described in a specific agreement or general terms and conditions[12].

However, this is not always the case when an organisation wants to co-operate with unspecified individuals *(*participants or ethical hackers) who can identify vulnerabilities in its IT systems. In that case, there is no clear contractual framework between the parties. It is then necessary for the organisation to define its expectations and the legal obligations of the participants prior to each cooperation.

In this respect, the coordinated vulnerability disclosure policy is a type of accession agreement outlining all contractual provisions for the responsible organisation and subsequently accepted by the participant when it freely decides to participate in the program.

[12]The responsible organization can also entrust these tasks to certain employees. The respective obligations of the parties will then be described in specific internal regulations or in general employment contract.

The adoption of such a policy clarifies the participants' legal position. After all, they can demonstrate that they have prior authorization to access the IT systems concerned and therefore do not intrude into those systems unlawfully, provided that the conditions set out in the policy are met *(see Coordinated Vulnerability Disclosure Policies Guide. Part II: Legal aspects*).

This cooperation can provide the responsible organisation with fair and lawful information about vulnerabilities in its systems and enable it to take adequate and timely action. In this way, potential risks and harm that these vulnerabilities may cause can be prevented or mitigated as effectively as possible.

The coordinated vulnerability disclosure policy provides an opportunity for continuous and effective monitoring of the security of systems or equipment. Obviously, the policy is more attractive and effective when the responsible organisation decides to give rewards to participants, depending on the importance and quality of the information provided (as part of a Vulnerability Rewards Program or bug bounty program[13]).

Even when the organisation grants rewards and calls on an external coordinator (ethical hacking platform), setting up costs of a coordinated vulnerability disclosure policy are more budget-friendly than having external companies perform audits.[14] After all, the reward for a bug bounty program is the result of a commitment on the part of the participant to achieve a certain result, whereas an external auditor is usually only bound by a commitment of means. The latter must therefore be compensated for all their activities, even if they have not found any vulnerabilities or only minor vulnerabilities at the end of their investigation.

[13] In addition to a vulnerability rewards program, the responsible organization may still decide to give a reward to participants following the procedure.
[14] Some costs need to be budgeted for, such as the costs for the technical team needed to analyze the information provided by the participants.

b. Improving the security of IT systems and driving research

Introducing such a policy provides the responsible organisation with the opportunity to obtain information about the security of its IT systems from various sources. Taking into account the current complexity and technically advanced nature of these systems, it is very useful to involve a large number of potential experts instead of using a few external service providers who cannot be experts in all the technologies used by the organisation.

In addition to other technical and organisational measures, setting up such a cooperation may be an appropriate measure to prevent incidents that would compromise the security of its network and information systems. It has the undeniable advantage of identifying and resolving vulnerabilities before a security incident occurs.

Improved security can be achieved by addressing vulnerabilities, minimising the risks associated with certain vulnerabilities and continually evaluating these risks to the responsible organisation's IT systems.

The introduction of a CVDP obviously implies that the organisation has security measures that can be tested and an internal (or external) team that can follow up the information provided by the participants.

In addition to increasing security, this type of policy can also improve knowledge about cyber security and drive research in this field. The work of researchers makes it possible to identify new vulnerabilities, as well as the circumstances in which they occur, methods for avoiding them and the means of remedying them.

c. Ensuring users have confidence in IT technologies

Implementing a CVDP demonstrates to the public and users that the responsible organisation attaches great importance to the security of its IT technologies.

After all, this approach implies a commitment by the organisation to process the information provided by the participants and to try to remedy the vulnerabilities identified, or at least to inform the users of the risks.

This commitment can also be a marketing tool. The organisation can refer to this in its communication. Trust in IT systems is certainly an important bonus for users or consumers.

d. Guaranteeing confidentiality

The confidentiality of information concerning a vulnerability in an IT system must be guaranteed as far as possible.

Full disclosure of a vulnerability[15], while it still exists among many users, poses a major IT security risk. Indeed, third parties with bad intentions can develop and disseminate specific tools to exploit this vulnerability.

[15] A disclosure to the general public.

It is therefore not desirable to make a security problem public before it has been resolved by the responsible organisation, which should be given the necessary time to do so, or before the responsible organisation has been able to inform the authorities responsible for the security of network and IT systems[16] about it.

Full disclosure may also delay the effective application of a solution for the vulnerability, as the responsible organisation is forced to respond in a crisis situation.

Disclosing security problems may also harm the reputation of the responsible organisation and undermine user confidence in the technologies concerned.

In addition, the dissemination or making available to the public of IT data, such as software or instructions, that make it possible to penetrate the security of IT systems may be a criminal offence[17] or may involve the civil liability for the person who published the information[18] *(see Guide - Part II Legal Aspects*).

Consequently, public disclosure of information about a vulnerability must be made with the utmost care and in coordination with the responsible organisation.

[16] In Belgium, this role is played mostly by the Centre for Cyber Security Belgium (CCB). Where appropriate, the CCB may inform organizations of vital interest (public authorities, providers of essentials services, digital service providers, critical infrastructures, etc).
[17] Art. *550 bis)* § 5 of the Belgian Criminal Code.
[18] Art. 1382 of the Belgian Civil Code.

The responsible organisation must respond within a reasonable period of time: it will implement a solution or at least inform the IT systems' users affected by the vulnerability. After all, the organisation may, for example, be held liable for leaving its customers in the dark about the vulnerability (see item e below).

It may also prove very useful, once the main security risks have been eliminated, to publish information on the vulnerabilities detected and their resolution, in an appropriate framework[19], in order to advance research on IT security.

The interest of a CVDP therefore lies in the establishment of a legal framework that reinforces confidentiality and provides the best possible framework for a possible public disclosure.

e. Ensuring better compliance with legal obligations in the area of IT security

By implementing a coordinated disclosure policy, the organisation demonstrates its commitment to comply with its legal obligations to ensure the security of its network and IT systems: General Data Protection Regulation EU No 2016/679 ("GDPR"), Act of 7 April 2019 establishing a framework for the security of network and IT systems of general interest for public security ("NIS Act"), Civil Liability Regulation, Economic Law Code, etc.

Article 32 of the GDPR provides that the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented, taking into account the state of the art and the cost of their implementation, as well as the nature, scale, context and purposes of the processing operations and the risks to the rights and freedoms of natural persons (which vary in their likelihood and seriousness).

[19] For example, in scientific publications or technical reports distributed to researchers in the area of IT security.

The provision clarifies that the controller and the processor may use:

(a) pseudonymisation and encryption of personal data;
(b) the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on a permanent basis;
(c) the ability to restore timely availability of and access to personal data in the event of a physical or technical incident;
(d) a procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure the security of processing.

In its Recommendation on security measures to prevent data breaches (No 01-2013), the Belgian Commission for the Protection of Privacy (now Data Protection Authority) recalls the importance of documenting, monitoring and improving IT security measures as often as necessary[20].

The guidelines on information security for personal data issued by the former Belgian Commission for the Protection of Privacy also point out that the controller should regularly organise a proper information security audit of personal data and take management measures to ensure the confidentiality and integrity of the data.[21]

[20] Commission for the Protection of Privacy, Recommendation on security measures to be observed to prevent data breaches (No 01-2013), www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2013.pdf, p. 3, point 6.
[21] Commission for the Protection of Privacy, *Guidelines on information security of personal data*, (version 2.0 Dec. 2014), p. 20 and 27, www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Richtsnoeren_CBPL_V%202%200%20FR_TRA.pdf.

The implementation of a CVDP is an appropriate technical and organisational measure to demonstrate, among other measures, the controller's commitment to ensuring the confidentiality, integrity, availability and resilience of his processing systems on a permanent basis[22] and to regularly test, assess and evaluate the effectiveness of the processing security measures[23]. Moreover, the international technical standards on IT security explicitly recommend the implementation of a CVDP (see, for example, international ISO/IEC standards 29147[24] and 30111[25]).

The responsible organisation can then rely on its CVDP to demonstrate to the personal data supervisory authorities that it is making efforts to assess and manage the risks associated with vulnerabilities in its IT systems.

In the same vein, a CVDP allows the controller to be better informed of possible personal data breaches and to assess which breaches should be reported as soon as possible to a supervisory authority[26] or a natural person[27].

Also, article 20 of the Belgian NIS Act states that the operator of essential services ("OES") must "take appropriate and proportionate technical and organisational measures to manage the risks to the security of the network and information systems on which its essential services depend. These

[22] Art. 32 (1) (b) of the GDPR.
[23] Art. 32 (1) (d) of the GDPR.
[24] ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (https://www.iso.org/standard/72311.html).
[25] ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html).
[26] Art. 33 of the GDPR provides that the controller must notify personal data breaches to the competent supervisory authority without undue delay and, if possible, no later than 72 hours after becoming aware of them, unless such breaches are not likely to jeopardize the rights and freedoms of natural persons. The processor should also inform the controller without delay as soon as they become aware of a personal data breach.
[27] Art. 34 of the GDPR requires the controller to notify the data subject without delay of a personal data breach where the breach is likely to pose a great risk to the rights and freedoms of a natural person.

measures shall ensure a level of physical and logical security of network and information systems appropriate to the risks presented, taking into account the state of technical knowledge".

The OES must also "take appropriate measures that are appropriate to prevent or minimise incidents affecting the security of the network and information systems used for the provision of essential services in order to ensure the continuity of these services"[28].

Security measures are defined in the NIS Act as measures that enable a system, with a certain degree of reliability, to withstand actions that compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or the related services offered by or accessible via those network and information systems[29]. In order to take appropriate measures commensurate with the risks involved, [30]the risks associated with incidents should be identified and their impact on the security of network and information systems must be minimised.

In this case, the implementation of a CVDP enables the AED or digital service provider to have a better understanding of possible vulnerabilities and threats to its network and information systems in order to provide an adequate response to the requirements of the NIS Act.

[28] Art. 20 of the NIS Act; see also art. 33 of the NIS Act for the security measures of digital service providers (DSPs) - e.g. providers of cloud computing services.
[29] Art. 6, 9°, of the NIS Act.
[30] Art. 6, 15°, of the NIS Act defines the risk as 'any reasonably foreseeable circumstance or event with a potential negative impact on the security of network and information systems'.

In addition, the Cyber Security Act[31] provides that a European cybersecurity certification scheme should at least include rules concerning how previously undetected cybersecurity vulnerabilities in ICT products[32], ICT services[33] and ICT processes[34] are to be reported and dealt with.[35]

The Regulation requires thus manufacturers or providers of certified ICT products, ICT services and ICT processes to make publicly available information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers.[36]

In addition, the responsible organisation may be held civilly liable (contractually or extra-contractually) if a security flaw in its technologies has caused harm to a third party.[37]

Finally, the responsible organisation selling ICT systems must guarantee its customers against hidden defects or non-conformity of the goods sold.[38] As a manufacture of a product (physical object) or provider of a service, it may also only market safe products and provide safe services.[39]Compliance with that general safety obligation may be assessed taking into account national or international standards, the codes of conduct in force in the industry concerned, the current state of knowledge and the state of the art and the security which users may reasonably expect.[40]

---

[31] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Cybersecurity Agency), and on the certification of cybersecurity of information and communication technologies and repealing Regulation (EU) No 526/2013.
[32] An element or group of elements of a network or information system (art. 2, 12 of the Cyber Security Act).
[33] A service which consists wholly or mainly in the transmission, storage, retrieval or processing of data by means of network and information systems (Art. 2, 13 of the Cyber Security Act).
[34] A series of activities carried out to design, develop, deliver or maintain an IT product or service (art. 2, 14 of the Cyber Security Act).
[35] Art. 54, 1, m, of the Cyber Security Act.
[36] Art. 55, 1, c, of the Cyber Security Act.
[37] Art. 1382 of the Civil Code.
[38] See art. 1641 and 1625 of the Civil Code on the indemnity for hidden defects or art. 1649 *bis et* seq. of the Civil Code on the indemnity for lack of conformity for sales to consumers.
[39] See Article IX.2 et seq. of the Code of Economic Law.
[40] In the absence of harmonized European standards.

C. GOOD PRACTICES

Currently, many companies in Belgium already apply a coordinated vulnerability disclosure policy and use bug bounty platforms.

There are two international ISO/IEC standards on CVDP: ISO/IEC 29147[41] and ISO/IEC 30111[42]. The first describes the procedure for disclosing a vulnerability, while the second deals with the processing procedures for the reported vulnerability. These two standards describe a complete model with the different aspects of a CVDP.

ENISA (European Union Cybersecurity Agency) has also published recommendations on good practices regarding the introduction of a CVDP.[43]

[41] ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (https://www.iso.org/standard/72311.html).

[42] ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html).

[43] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, 2015, www.enisa.europa.eu/publications/vulnerability-disclosure. Art. 6 (1) (b) of Regulation (EU) 2019/881, tasks ENISA with assisting the Member States of the Union and the European institutions in drawing up and implementing a voluntary disclosure policy on vulnerabilities.

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

I. Content of a CVDP

a. Authorized persons

The policy must be implemented by persons or bodies that can validly represent the responsible organisation and not, for example, by a member of the IT team who is not legally authorized to do so[44].

[44]Subject to the doctrine of sham representation or to the general legal principle of respect for the legitimate expectations of the other.

Indeed, the authorizations provided under the coordinated disclosure policy must necessarily come from a person authorized to do so by the holder of the rights to the system or equipment concerned[45].

b. Publicity

The publicity given to the responsible disclosure policy is an important element for its success[46]. Its content should therefore be easily accessible to potential participants and should preferably be accessible from the website of the responsible organisation. The existence of the CVDP must therefore be clearly and visibly stated on the website of the responsible organisation (e.g. with a specific tab or a section with the full content of the policy)[47]. For this purpose, there are standardisation proposals where an organisation's CVDP is included in a "security.txt" file in a known location of the tree structure of each website[48] or extensions for web browsers to track down websites that have a CVDP[49].

If a Vulnerability Rewards Program is introduced via a bug bounty platform, the full content of the CVDP must also be included on that platform[50].

The CVDP must be written in all languages of the website and, to the extent possible, also in English. It may also be useful to place a link to the CVDP page in other locations (for example, in the help section of the program, in the user manual, in the user licence, etc.).

[45] By default, this is the system's owner.
[46] In order to prevent a crime from being committed (unauthorized intrusion into an IT system), the coordinated disclosure policy must be in place before participants take steps. The best way to avoid doubts about the existence or not of a coordinated vulnerability disclosure policy is to make it public. (See Part II. Legal aspects). However, organizations may have a non-public CVDP limited to a few pre-selected participants (see in particular some private bug bounty programs).
[47] For example: https://www.[organisatie].be/security or /disclosurepolicy or /vulnerability-policy.
[48] See the project https://securitytxt.org/
[49] See for example the YesWeHack VDP Finder extension for Chrome and Firefox.
[50] For example, www.intigriti.be; www.yeswehack.com; www.bugcrowd.com; www.hackerone.com.

Finally, it is important for the responsible organisation to inform any subcontractors about the content of its CVDP and to adapts its subcontracting contracts if necessary.

c. Point of contact

The responsible organisation must include a contact point in its policy, to which any information on vulnerabilities can be sent. A specific e-mail address can be used for this purpose[51]. The responsible organisation must also ensure that e-mails received at other e-mail addresses[52] are forwarded internally to this contact point.

The use of an online form is also interesting to receive information about discovered vulnerabilities. This method has the advantage that the input and processing of data and the sending of an acknowledgement of receipt can be done automatically.

In addition, it may be useful to mention the telephone details of the service or person authorized to deal with notifications about IT vulnerabilities.

Lastly, the information to be provided by the participant should be clarified (see Section II Procedure below).

[51] For example: vulnerabilitypolicy@organisation.com; security@organisation.com; csirt@organisation.com; support@organisation.com; security-alert@organisation.com, etc.
[52] For example: info@organisation.com or contact@organisation.com.

d. Security and confidentiality of communications

This is crucial as risks of information leakage on vulnerabilities should be avoided as much as possible by ensuring the confidentiality and integrity of communications.

It is therefore strongly recommended to use a secure method of communication. This can include the use of a data encryption tool[53] creating a secure internet portal[54]or at least password-protecting the documents[55]. When developing the communication methods recommended to participants, the responsible organisation must therefore pay particular attention to their security[56].

e. Description of mutual obligations

1. Policy scope

The responsible organisation must explicitly define the scope of its coordinated disclosure policy: which sites, products, devices, services, systems or networks are in scope for the policy?

Ideally, the responsible organisation should apply the rules of its CVDP to its various IT systems and to its contractual commitments (suppliers, clients, subcontractors, staff, etc.).

If this is not the case, the CVDP must explicitly list IT systems of third parties that are excluded from the scope of the policy (in the absence of the consent of these third parties). In case of doubt about the scope of the CVDP, participants should seek the approval of the responsible organisation before continuing their analysis.

---

[53] For example: Transport Layer Security (TLS) or its predecessor Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP).
[54] in HTTPS or via encryption in the web browser.
[55] Ideally, the participant should then provide the password to the responsible organization via another means of communication (telephone, SMS, message application, other e-mail address, etc.).
[56] For example, provide the public key and fingerprint of its contact point to send information in an encrypted manner, or secure its online form in HTTPS.

Also, the CVDP should clearly state that the participant's research on information systems not explicitly included as part of the policy could lead to legal action against the participant (by the public prosecutor, the responsible organisation or third parties to the CVDP).

2. Policy conditions

The very existence of a coordinated vulnerability disclosure policy or a bug bounty program necessarily implies that - at least tacitly - authorization to access the computer system has been granted to the participant[57]. In principle, the participant also has an authorization to enter data into the system concerned or to attempt to do so (see *Guide - Part II Legal Aspects*).

The responsible organisation must, however, clearly state in its coordinated disclosure policy the conditions under which participants may access the computer system and attempt to enter or modify data. The actions that may or may not be authorized must be clearly defined, based on the intended purposes.

The authorization to modify or delete IT data[58] depends on the way in which the coordinated vulnerability disclosure policy has been drawn up. In drawing up this policy, the responsible organisation must assess the benefits, the specific conditions imposed, and the risks involved in order to decide whether or not to allow these actions. It should be noted that participants have to strictly adhere to the terms of the policy on changing and deleting IT data. If not, they are guilty of a crime, i.e. an offence relating to IT data.

[57] The coordinated vulnerability disclosure policy will include provisions which, depending on their exact wording, may be considered as explicit or tacit authorizations.
[58] Or to try such actions.

For example, it is good practice to prohibit participants from using Distributed Denial of Service (DDoS) attacks or social engineering attacks, installing malware or viruses, stealing passwords, sending phishing or spam mails, removing or altering data/parameters from the system, etc.

The CVDP must expressly exclude any deliberate attempt[59] to intercept, record or become aware of communications that are not accessible to the public or electronic communications.[60] Nevertheless, it may be permitted for the content of communications to be disclosed to participants, in a strictly accidental manner, for the purposes of vulnerability detection[61]

It should also be stated that the participant may not use, retain, divulge or disclose any communication that is not accessible to the public, nor any data from an IT system which it has reasonable grounds to believe has been obtained illegally.

It should also be prohibited for participants to install or have installed a device enabling the interception, knowledge or recording of communications not accessible to the public, unless they can prove that they have no intention of using the device in question for the aforementioned purposes, either with the consent of all participants in the communication or by participating in the communication himself.

3. Reporting

The CVDP must clearly state what information the participant must provide when reporting a vulnerability: type of vulnerability, configuration details, actions taken, tools used, test data, evidence, IP address or URL of the affected system, screenshot, contact details, etc.

[59] Which is different from accidental interception (see Guide Part II Legal Aspects).
[60] Except in the rather exceptional case where the participant has the consent of all participants or participates in the electronic communication himself.
[61] See the confidentiality of electronic communications (Act of 13 June 2005).

4. Proportionality

In general, the participant must commit to complying with the principle of proportionality, i.e. not to disrupt the availability of the services provided by the system and not to exploit vulnerabilities beyond what is strictly necessary to demonstrate the security problem. Their approach must remain proportionate: if the problem has been demonstrated on a small scale, no further action should be taken.

If the use of personal data by the participant is not necessary to demonstrate IT vulnerability, it must be expressly excluded.

In addition, the Coordinated Disclosure Policy should clearly state that the participant may not keep the data of the responsible organisation, including any personal data, longer than necessary. All personal data collected by the participant must be deleted immediately. If it proves necessary to retain these data for a certain period of time, the participant must ensure that these data are kept secure during this period.

5. Confidentiality

One of the essential elements of a coordinated disclosure policy must be respect for confidentiality: participants may not share the information collected with third parties or disseminate it to third parties without the express consent of the responsible organisation[62].

[62] Again, subject to limited disclosure to the authorities competent in cyber security.

Also, any disclosure of IT, communication or personal data to persons outside the responsible organisation or dissemination of such data to persons outside the responsible organisation by the participant must be expressly excluded, subject to the prior consent of the responsible organisation.

The text of the coordinated disclosure policy should state that the purpose of the policy is not to permit the deliberate access to the content of IT, communication or personal data and that such access can only occur accidentally and occasionally in the context of the detection of vulnerabilities in the technologies concerned.

6. Act in good faith

The organisation responsible for the IT system must undertake to carry out its coordinated disclosure policy in good faith and don't pursue civil or criminal action against the participant complying with its terms.

On the part of the Participant, there can be no fraudulent intent, intent to harm, or desire to use or cause harm to the visited system or its data. This also applies to third party systems located in Belgium or abroad.

With respect to devices enabling a computer data breach to be committed, the participant may develop, possess or make available such devices as part of participation in a vulnerability disclosure policy. Such actions are not unlawful as long as they are justified by legitimate purposes relating to the detection of vulnerabilities with the consent of the organisation responsible for the IT system concerned.

7. Processing of personal data

The purpose of a CVDP is not to intentionally process personal data. However, it is possible that the participant may, even by accident, have to process personal data in the context of its vulnerability researches.

The processing of personal data has a broad meaning and includes in particular the storage, alteration, retrieval, consultation, use or disclosure of any data relating to an identified or identifiable natural person. 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 still, location data).

The controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing.[63]

Since the GDPR constitutes a form of accession agreement that binds the ethical hacker to the responsible organisation, it is necessary to specify the obligations of the parties with regard to the processing of personal data, in particular the purpose of and the essential resources for any processing carried out under this policy *(see Guide - Part II Legal Aspects).*

8. Procedural deadlines

It is recommended that clear deadlines be set for each stage of the procedure, in particular for sending an acknowledgement of receipt to the participant, communicating additional information, studies, developing a solution, replying to the participant, awarding a reward or any publication. However, deadlines should remain flexible to a certain extent, depending on the complexity of the vulnerability, the number of systems affected, the urgency or the seriousness of the situation.

[63] Art. 4, 7), of the GDPR.

9. Continuous communication

Good cooperation requires continuous and efficient communication. The information provided by the participant can be very useful in identifying the vulnerability and resolving it. It is therefore important to send acknowledgements of receipt, to keep participants informed of the follow-up given to their notification, to remind them of their obligations and to specify the next steps in the procedure.

In addition, the intervention of a coordinator (preferably designated in the CVDP) or of a bug bounty platform can help to establish and maintain a constructive relationship between the parties, or possibly guarantee the anonymity of participants.

If one of the parties or the designated coordinator does not respond, the parties can always call upon the Centre for Cyber Security Belgium (vulnerabilityreport@cert.be).

10. Giving a reward

Rewards or a public recognition[64] given by the responsible organisation makes the CVDP more attractive for the participants and often leads to better results for the organisation. It may even be a purely symbolic gift: for example, a t-shirt, a sticker or a special mug.

In a bug bounty program, the reward depends on the quantity, importance or quality of the information transmitted.

[64] Ranking among the best participants, publication, conference, etc.

It is essential that the responsible organisation clearly states the nature of this reward in advance in its policy. Any request for a reward outside the conditions set by the CVDP can then be equated with an illegal attempt at extortion.

The organisation can use a bug bounty platform[65], which will coordinate the technical and administrative aspects of its reward program together with the organisation.

11. Possible public disclosure

Any disclosure of a vulnerability should be coordinated and synchronised between the parties to allow sufficient time for the responsible organisation to resolve the issue and to inform affected critical operators in advance.

Where a vulnerability is identified in a program, component, protocol or format provided by a third-party vendor, the responsible organisation will notify them directly before any public disclosure is made.

The same applies where the identified vulnerability threatens to affect other organisations using similar technology more widely, or where the affected IT component is provided by the responsible organisation to other organisations (e.g. through user licences). In these cases, it is essential that a report on the vulnerability and its resolution be provided to the parties concerned so that they can protect themselves.

In case of public disclosure, the vulnerability report and the solution should ideally be published at the same time.

[65] For example: www.intigriti.com (platform based in Belgium); www.yeswehack.com (platform based in France); www.yogosha.com; www.hackerone.com (platform based in the US).

The responsible organisation must offer various means to inform and protect its users: for example, automatic system updates, publication of security notices on its website, mailings with a link to a specific internet page, distribution of this information to its network of vendors etc.

If a vulnerability is not yet known and threatens to have a direct or indirect impact elsewhere, the organisation responsible must inform the Centre for Cyber Security Belgium (vulnerabilityreport@cert.be) and the other organisations potentially concerned in advance, even if it does not want the vulnerability to be made public.

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

CENTRE FOR CYBER SECURITY BELGIUM

II. Procedure

a. Discovery

Where a participant discovers information about a potential vulnerability, he should to the extent possible, conduct prior checks to confirm the existence of the vulnerability and identify any risks involved.

Then, he must provide the responsible organisation with at least sufficient technical information to confirm the existence of this problem and provide their contact details. These elements may be supplemented according to the specifications of the coordinated publication policy or the content of the responsible organisation's online form.

b. Reporting

Participant must provide as soon as possible the technical information to the contact point or to the coordinator designated by the responsible organisation by secure means of communication.

When the responsible organisation receives a notification, it must send an acknowledgement of receipt to the participant as soon as possible, indicating the internal reference and the next stage of the procedure.

Together with this acknowledgement of receipt, the responsible organisation may indicate the content of its coordinated publication policy, or at least provide a link to it, and request any additional information.

It is particularly interesting to ask whether the participant has already reported this problem to other responsible organisations.

c. Investigation

During the investigation phase, the responsible organisation can reproduce the environment and the identified behaviour, in order to check the information provided.

Participant must be regularly informed of the results of the investigation and of the action taken on the report.

During this process, parties should ensure to link to similar or related reports, to assess the risk and severity of the vulnerability and to identify any other affected products or systems.

d. Deployment of a solution

The objective of the disclosure policy is to enable the development and deployment of a solution to remove the vulnerability from the IT system.

Unless legally or contractually obliged to do so, the responsible organisation remains free to choose to develop and implement a solution or not.

Of course, the choice not to resolve a proven security flaw could, if necessary, engage the civil liability of the organisation responsible if a third party suffers damage as a result[66].

To the extent possible, the solution should be developed within 90 calendar days at the latest.

[66] This is independent of the existence of a responsible disclosure policy.

These deadlines should be kept to the strict minimum if users of the affected systems are at risk or if there are risks to the protection of personal data. If the organisation is unable to solve the problem immediately, the IT system concerned should be taken completely out of service temporarily.

However, the supply chain and the multiple interdependencies between information systems can complicate the time needed to develop a solution and deploy it.

During this phase, the responsible organisation (or its service provider) must, on one hand, perform positive tests to verify that the solution is working properly and, on the other hand, negative tests to ensure that the solution does not disrupt the proper functioning of other existing functionalities.

If the solution is ready and the vulnerability would affect other organisations as well, it should be communicated to the CCB as a matter of priority and before any public disclosure (vulnerabilityreport@cert.be).

The responsible organisation should respect a reasonable period of time from this transmission before a possible general disclosure to users, in order to allow operators of vital interest (operators of essential services NIS, critical infrastructures, public administrations, etc.) to implement the solution as a priority.

e. Possible public disclosure

Unless there is a specific legal requirement, the public disclosure of a vulnerability is not a mandatory step in a CVDP. Indeed, the participant and the responsible organisation can agree not to disclose the existence of the vulnerability. This could be the case if the vulnerability proves too difficult or impossible to resolve, or if resolving it would involve disproportionate costs compared to the potential risks involved.

However, this should remain the exception, as the purpose of a CVDP is to improve security and transparency vis-à-vis users. In addition, certain legal provisions require the responsible organisation to inform the users of the IT systems[67] or the natural persons involved in a personal data breach[68].

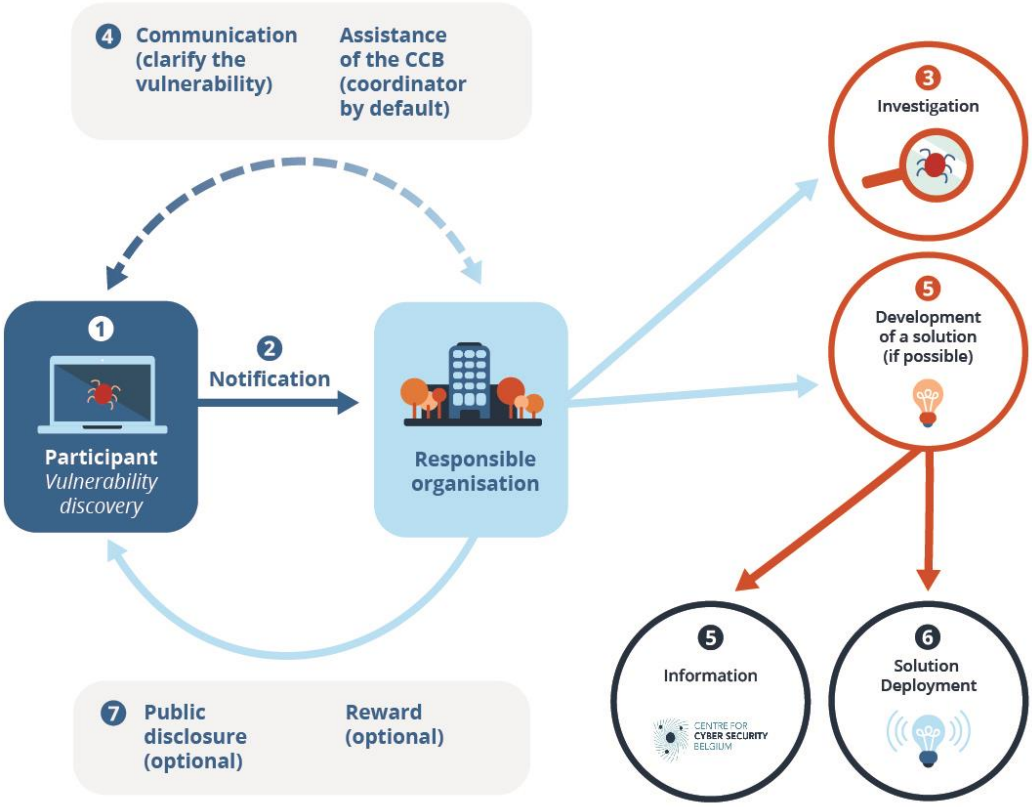
In any case, information relating to a vulnerability that would also affect other organisations will at least be submitted to the CCB (vulnerabilityreport@cert.be**).**

If the vulnerability is made public, the responsible organisation will, in consultation with the participant, lay down the terms and conditions for the disclosure. Ideally, information about the vulnerability should be disclosed at the same time as the solution. The responsible organisation is recommended to inform its customers by posting a security notice on its website or by other means of communication (e-mail, information letter, system update, etc.).

The responsible organisation should also inform other organisations likely to be involved in the same vulnerability. The possible interdependence of IT systems or the supply chain may lead to wider coordination of possible disclosure.

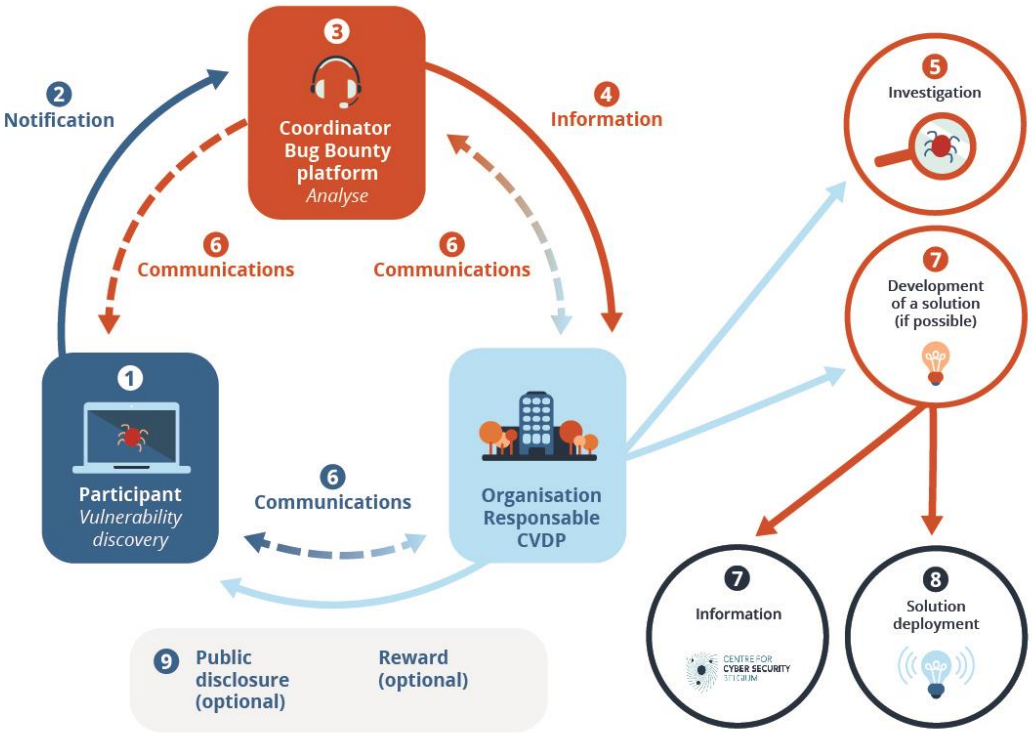
It is also important to collect users' comments on the application of the solution and to take the necessary corrective action to resolve any problems caused by the solution, including those relating to compatibility with other products or services.

[67] See in particular the rules on contractual and non-contractual liability.
[68] Art. 34 of the GDPR.



1. Participant finds a vulnerability in the context of a CVDP.
2. Participant informs the responsible organisation based on the CVDP details.
3. The responsible organisation analyses the vulnerablity.
4. Communication between the participant and the responsible organisation continues to clarify the vulnerability. assistance from the CCB (as coordinator by default) can be asked if there is a lack of communication in this process.
5. A solution is developed (if possible). In case the vulnerability could affect also others organisations, the responsible organisation informs the CCB.
6. The responsible organisation deploys the solution to its users or customers.
7. Approval for public disclosure can be discussed and a reward can be given based on the CVDP.

** Designed by CCB and Intigriti - 2020*



1. Participant finds a vulnerability in the context of a CVDP.
2. Participant informs the responsible organisation through a coordinator, such as a bug bounty platform, based on the CVDP details.
3. The Coordinator analyses the vulnerablity.
4. After validation the coordinator will inform the responsible organisation.
5. The responsible organisation analyses the vulnerablity.
6. 6 Communication between the participant and the responsible organisation continues to clarify the vulnerability, if desired through the coordinator.
7. 7 A solution is developed (if possible). In case the vulnerability could affect also others organisations, the responsible organisation informs the CCB.
8. The responsible organisation deploys the solution to its users or customers.
9. Approval for public disclosure can be discussed and a reward can be given based on the CVDP.

** Designed by CCB and Intigriti - 2020*

CENTRE FOR CYBER SECURITY BELGIUM

D. REFERENCES

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

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

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

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

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

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

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

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

ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure (https://www.iso.org/standard/72311.html)

ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes (https://www.iso.org/standard/53231.html)

CENTRE FOR CYBER SECURITY BELGIUM

GUIDE FOR THE COORDINATED VULNERABILITY DISCLOSURE POLICY
PART I: GOOD PRACTICES

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.

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 16
1000 Brussels

Legal deposit:
D/2020/14828/014

2020

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
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

<u>Warning</u>:

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 Intigriti (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[1]

For the Belgian criminal law to be applicable, it is sufficient that one of the material constitutive or material aggravating elements[2] 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[3] and the European legislation[4], 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[5]

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.

[1] Cass, 23 January 1979, *Pas.*, I, 1979, p. 582; Cass., 4 February 1986, *Pas.*, 1986, p. 664.
[2] And not just intentional elements.
[3] Council of Europe Convention on Cybercrime, drawn up in Budapest on 23 November 2001, entered into force on 1 July 2004.
[4] 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.
[5] 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.

CENTRE FOR CYBER SECURITY BELGIUM

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".[6] 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.[7]

We can also refer to the European Directive 2013/40/EU of 12 August 2013 on attacks against IT systems[8], 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[9];
- "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.

[6] 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.

[7] *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 12.

[8] 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).

[9] 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[10], without necessarily requiring complex computer manipulations[11]: 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).[12]

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

[10] 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.
[11] Corr. Court of Antwerp, 10 November 2014, *T. Strafr.*, 2015, p. 94.
[12] 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.[13]

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.[14]

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.[15] 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.

[13] *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 17.
[14] Corr. Court of Dendermonde, 14 November 2008, *T. Criminal Law*, 2009, p. 114.
[15] 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.[16] 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[17], 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[18]

In the same sense, tacit authorisation may also result from the existence of an IT system clearly made available to the public.[19]

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.

[16] 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.
[17] "Pentesting" agreement.
[18] Employees, however, often receive a login and password from their employer, which expressly authorises them to access the IT system.
[19] 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.[20] The legislator wanted to punish any intrusion - except unintentional intrusion - into an IT system without taking into account the intruder's intention.[21] 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.[22]

[20] 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.

[21] Corr. Brussels, Jan 8, 2008, *J.T.*, 2008, p. 337.

[22] 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.[23]

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.[24] 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.[25]

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.[26]

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.[27] 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.

[23] Art. 550 *bis*(1) al. 2, of the Criminal Code.
[24] 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.
[25] Court of Arbitration, 24 March 2004, No 51/2004, B.4.3, p. 7.
[26] Corr. Brussels, 8 January 2008, *J.T.*, 2008, p. 337.
[27] Cass., 24 January 2017, P.16.0048.N, 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.[28]

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,

[28] See Cass., 5 January 2011, P.10.1094.F., 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.[29]

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.[30] 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.[31]

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.[32] This involves acquiring IT data (original or copy) from the system visited so that it can be reused if necessary.[33] 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.[34] One of the legislator's objectives here was to combat the theft of industrial secrets in the context of industrial espionage.[35]

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.

[29] *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/004, p. 6.
[30] *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 16.
[31] *Parl. Records*, Senate, 1999-2000, 2-392/3, p. 6; *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 16.
[32] Corr. Dendermonde, 14 May 2007, *T. Strafr.*, 2007, p. 403.
[33] This is sometimes called "bitnapping", a reference to the kidnapping of data.
[34] 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.
[35] *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).[36] 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[37]

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.[38]

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

[36] *Parl. Records*, Chamber of Representatives, 1999-2000, No 50, 0213/001, p. 17.
[37] C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique", *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.
[38] 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.

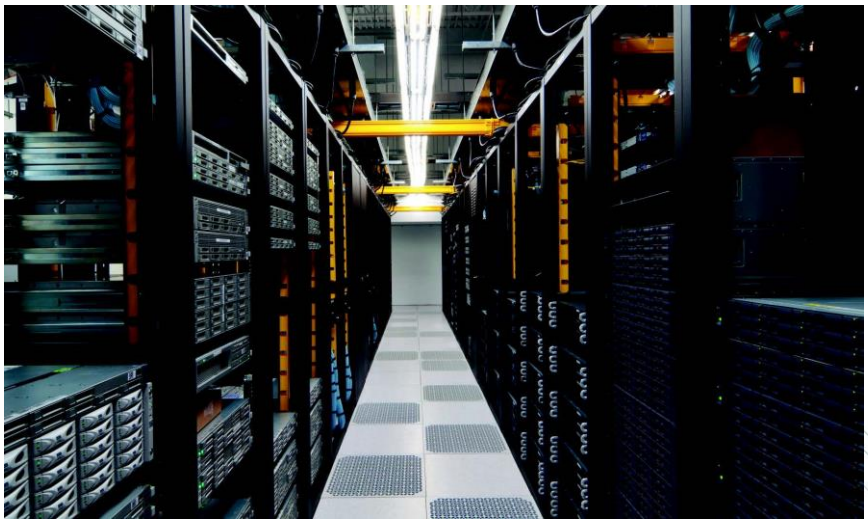
Although it is intended that a coordinated vulnerability disclosure policyapplies primarily to persons outside the responsible organisation who do not have any authorisation to access the IT system, this policy may also provide a framework, where appropriate, for the conduct of participants with good 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[39] or in the coordinated vulnerability disclosure policy[40].

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.



[39] For example, an employment contract, a statutory relationship or a service contract.

[40] 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[41]

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[42] 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.

[41] 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.
[42] *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.[43]

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.[44] 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.[45] 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.[46]

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.

[43] See the considerations on the special intent required for the offence of internal unauthorised intrusion; art. 550 *ter* (1) of the Criminal Code.
[44] Art. 550 *ter*(2) of the Criminal Code.
[45] 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.
[46] 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.[47] 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[48], 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.[49]

However, the attempt is only realised if the perpetrator has not only performed preparatory acts but also unambiguous executive acts.[50]

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.[51]

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

[47] O. LEROUX, "La Criminalité informatique", quoted , p. 437.
[48] For example, IT security training.
[49] Art. 550 *ter*(6) of the Criminal Code.
[50] See the explanation of the attempted intrusion into an IT system.
[51] 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[52] and the use of false instruments in IT[53]

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.[54]

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,[55] and, on the other hand, the attempt to commit IT falsification.[56]

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.[57]

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).[58]

[52] Art. 210 *bis*(1) of the Criminal Code.
[53] Art. 550 *bis*(4) of the Criminal Code.
[54] Art. 210 *bis*(1) of the Criminal Code.
[55] Art. 210 *bis*(2) of the Criminal Code.
[56] Art. 210 *bis*(3) of the Criminal Code.
[57] *Parl. Records*, Chamber of Representatives, 1999-2000, No 0213/001, p. 10.
[58] 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[59] 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.[60] 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.[61]

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.

[59] 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.
[60] See Article 193 of the Criminal Code.
[61] See the attempted intrusion into an IT system.

1. Material constitutive elements

1.1 Manipulating data

The crime involves introducing, modifying[62] 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[63] 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.[64]

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.

[62] For example, changing the balance on a bank account.
[63] 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.
[64] 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.[65]

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[66], 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.[67]

The provision further clarifies that intercepting[68], taking cognisance of or recording must be done with the help of any device.[69] 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.[70]

[65] Art. 314 *bis*(1) 1°, of the Criminal Code.
[66] For example, via a cloud storage service.
[67] *Parl. Records*, Senate, 1992-1993, No 843/1, pp. 8-9.
[68] 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.
[69] *Parl. Records*, Senate, 1992-1993, No 843/1, p. 6.
[70] 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".[71] As before, this concept can be interpreted depending on the context and intentions of the participants in the communication.[72] Non-public access means that the communication is not intended to be heard by persons other than the correspondents of the communication.[73] In principle, the professional or non-professional nature of a communication has no impact on the assessment of its non-public nature.[74]

The communication concerns in particular electronic data transmission in computers and computer networks.[75] 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.

---

[71] 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.

[72] *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.

[73] *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.

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

[75] 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.[76] 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.[77] 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.[78] After all, the device is not necessarily placed and used by or on behalf of the same people.[79]

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.[80]

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.[81]

[76] *Parl. Records*, Senate, 1992-1993, No 843/1, p. 6.
[77] *Parl. Records*, Senate, 1992-1993, No 843/1, p. 6.
[78] Art. 314 *bis*(1) 2°, of the Criminal Code.
[79] *Parl. Records*, Senate, 1992-1993, No 843/1, p. 9.
[80] Art. 314 *bis*(2*bis*) of the Criminal Code.
[81] *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.[82]

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.

[82] 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.[83]

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.[84]

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[85], 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[86]

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

[83] 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.
[84] *Parl. Records*, Senate, 2004-2005, No 1425-1426/01, p. 76.
[85] 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.beThe 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.
[86] 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' (...)".[87] 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".[88]

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.[89] 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.[90] 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).

[87] Art. 2, 3° and 5° of the Act of 13 June 2005 on electronic communications, *Official Gazette* of 20 June 2005, p. 28070.
[88] 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.
[89] Cass., 1 Oct. 2009, C.08.0064.N, 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: "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".
[90] *Ibidem.*

1.4. Deliberately taking cognisance of data relating to electronic communications and to another person[91]

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.[92]

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[93]

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.[94] 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*,[95] 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.

[91] Art. 124, al. 3 of the Law of 13 June 2005 on electronic communications.
[92] Labour Court of Brussels, 10 February 2004, R.G. 44002, www.juridat.be.
[93] Art. 124, al. 4 of the Law of 13 June 2005 on electronic communications.
[94] 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.
[95] 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[96]

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[97]

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[98]

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.

[96] Art. 145(3) 1°, of the Law of 13 June 2005 on electronic communications.
[97] Art. 145(3) 3°, of the Law of 13 June 2005 on electronic communications.
[98] 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.[99] 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[100], 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.

[99] Art. 314 *bis* of the Criminal Code.
[100] 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.[101]

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

[101] 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.[102] 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.[103] 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.[104]

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.[105]

[102] Art. 4, 1) of the GDPR.
[103] Art. 4, 2) of the GDPR.
[104] C. DE TERWANGNE, Vie privée et données à caractère personnel, Chap. 3.2 Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution, Brussels, published by Politeia, p. 23.
[105] 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[106]. 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[107]

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 seeked through the processing activities. The means are the technical and organisational methods used[108] to achieve the purposes of the processing. In short, the aim is to determine the 'why' and 'how' of the processing operations.[109]

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).[110]

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.[111] The processor acts on behalf of the controller by following

[106] C. DE TERWANGNE, Vie privée et données à caractère personnel, Chap. 3.2 Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution, Brussels, published by Politeia, page 26.
[107]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)
[108] C. DE TERWANGNE, *idem*, p. 28.
[109] Article 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169, page 13, *idem*.
[110] *Ibidem.*
[111] 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.[112] 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.[113]

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'.[114] 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[115] 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.

[112] Or the processor, where the responsible organisation has the status of controller.
[113] The responsible organisation can be a controller of personal data or itself a processor of a controller.
[114] Article 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169, p. 25, *idem*.
[115] 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.[116] 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[117]:

- 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;[118]

[116] Art. 28(1) of the GDPR.
[117] See in particular the conditions mentioned in Article 28 § 3 of the GDPR.
[118] 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;[119]

- 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;[120]

- upon completion of participation in the policy, delete all personal data or return them[121] 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;[122]

- 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.

[119] Art. 32(1) of the GDPR.
[120] Art. 33(2) of the GDPR.
[121] According to the choice of the controller.
[122] 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 Mémorialis. 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, I. 42/08-30.

DE HERT, P., "De wet van 28 november 2000 inzake informaticacriminaliteit en het materieel strafrecht. Een wet die te laat komt of een wet die er nooit had moeten komen?", *T. 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. 179*ff*.
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.

CENTRE FOR CYBER SECURITY BELGIUM

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.

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