LEGISLATION TRANSLATION

BELGIAN CYBERCRIME PROVISIONS

UNOFFICIAL ENGLISH TRANSLATION – CONSOLIDATED VERSION[1]

By **Johan Vandendriessche**[2]

The Act of 28 November 2000 on cybercrime inserted several new substantive and procedural cybercrime provisions in the Belgian Criminal Code and the Belgian Code of Criminal Proceedings. In addition to these new provisions, some other provisions that indirectly relate to cybercrime were amended. As a result of the ratification of the Council of Europe Convention on Cybercrime (Treaty No. 185) by Belgium, some of these provisions were amended.

In order to provide a translation of the current provisions, it is necessary to extract these provisions from the Belgian Criminal Code and the Belgian Code of Criminal Proceedings, and translate them "as such", rather than translating the original acts by which these provisions were inserted or amended.

This translation contains the following cybercrime provisions:

Substantive provisions (Belgian Criminal Code):

Article 210*bis* (Computer-related Forgery)

Article 504*quater* (Computer-related Fraud)

Article 550*bis* (Illegal Access / "Hacking")

Article 550*ter* (Data and System Interference)

Procedural provisions (Belgian Code of Criminal Proceedings)

Article 39*bis* (Expedited Preservation of Stored Computer Data / Data Seizure)

Article 88*ter* (Computer and Network Search)

Article 88*quater* (Duty to Cooperate – Computer and Network)

Article 90*quater* (Duty to Cooperate – Telecommunications)

*

* *

I. Provision in the Belgian Criminal Code

Article 210*bis*. (Computer-related Forgery)

§1. He who commits forgery by inputting, altering or deleting any data that is stored, processed or transmitted by a computer system, or by changing by any other technological means the use of any data in a computer system, resulting in the modification of the legal effect of such data, shall be punished with a term of imprisonment between six months and five years and with a fine between 26 euro and 100.000 euro or with one of these sanctions.[3]

§2. He who knows that the data obtained are inauthentic and uses such data, shall be punished with the same sanctions as a perpetrator of forgery.

§3. An attempt to commit the criminal offence established in §1 shall be punished with a term of imprisonment between six months and three years and with a fine between 26 euro and 50.000 euro or with one of these sanctions.

[1] This version is consolidated to 1 July 2012. Bibliographical information can be found at the end of this document.

[2] The translator will appreciate receiving comments or remarks in view of improving this translation at the following address: johan@adv-vandendriessche.be. The translator would like to express his thanks to Stephen Mason for the assistance in this translation.

[3] The fines are represented in euro prior to 'revaluation'. In order to obtain the current amount of the fine, the amount must be multiplied by 6. For instance, a fine of 100 euro should be read as a fine of 600 euro.

§4. The sanctions established in §§1 to 3 are doubled if a violation of one of those provisions has been committed within a period of five years after a conviction for one of those criminal offences or for one of the criminal offences established in the articles 259*bis*, 314*bis*, 504*quater* or in Title IX*bis*.[4]

Article 504*quater*. (Computer-related Fraud)

§1. He who aims to procure without right, with intent to defraud, an economic advantage for himself or for another by inputting, altering or deleting any data that is stored, processed or transmitted by a computer system, or by changing by any other technological means the normal use of data in a computer system, shall be punished with a term of imprisonment between six months and five years and with a fine between 26 euro and 100.000 euro or with one of these sanctions.

§2. An attempt to commit the criminal offence established in §1 shall be punished with a term of imprisonment between six months and three years and with a fine between 26 euro and 50.000 euro or with one of these sanctions.

§3. The sanctions established in §§1 and 2 are doubled if a violation of one of those provisions has been committed within a period of five years after a conviction for one of those criminal offences or for one of the criminal offences described in the articles 210*bis*, 259*bis*, 314*bis* or in Title IX*bis*.

Article 550*bis*. (Illegal access/'Hacking')

§1. He who obtains access to a computer system or maintains access to a computer system, while knowing that he is not entitled thereto, shall be punished with a term of imprisonment between three months and one year and with a fine between 26 euro and 25.000 euro or with one of these sanctions.

When the criminal offence established in the first paragraph is committed with intent to defraud, the term of imprisonment shall be between six months and two years.

§2. He who exceeds his rights of access to a computer system with intent to defraud or with intent to cause damage, shall be punished with a term of imprisonment between six months and two years and with a fine between 26 euro and 25.000 euro or with one of these sanctions.[5]

§3. He who finds himself in one of the situations established in §§ 1 and 2, and either:

1° copies in any manner the data that are stored, processed or transmitted by means of the computer system; or

2° makes any use of the computer system of a third party or uses the computer system to obtain access to the computer system of a third party; or

3° causes, even unintentionally, any damage to the computer system or to the data that are stored, processed or transmitted by that computer system or to a computer system of a third party or to the data that are stored, processed or transmitted by the aforementioned computer system, shall be punished with a term of imprisonment between one year and three years and with a fine between 26 euro and 50.000 euro or with one of these sanctions.

§4. An attempt to commit one of the criminal offences established in §§ 1 and 2 shall be punished with the same sanctions.

§5. He who illegitemately posesses, produces, sells, procures for use, imports, distributes, disseminates or otherwise makes available any instrument, including computer data, designed or adapted primarily to enable one the criminal offences established in §§ 1 to 4, shall be punished with a term of imprisonment between six months and three year and with a fine between 26 euro and 100.000 euro, or with one of these sanctions.

§6. He who instructs or incites the commission of one of the criminal offences established in §§ 1 to 5, shall be punished with a term of imprisonment between 6 months and 5 years and with a fine between 100 euro and 200.000 euro or with one of these sanctions.

§7. He who keeps, divulges to another person or disseminates data, or makes any use thereof, whilst knowing that these data have been obtained by the commission of one of the criminal offences established in §§ 1 to 3, shall be punished with a term of imprisonment between six months and three years and with a fine between 26 euro and 100.000 euro or with one of these

[4] *The articles 259bis and 314bis of the Belgian Criminal Code relate to the interception of electronic communication. Chapter IXbis of the Belgian Criminal Code covers the articles 550bis and 550ter.*

[5] *Article 550bis, §1 relates to ' external hacking' , whereas article 550bis, §2 relates to ' internal hacking' . External hacking is performed by someone who has no rights of access to a computer system, whereas internal hacking is performed by someone who has rights to obtain access a computer system, but exceeds those rights. The distinction in the punishment has been challenged before the Belgian Constitutional Court, but the provisions were upheld (Constitutional Court, decision 51/2004 of 24 March 2004).*

sanctions.

§8. The sanctions established in §§ 1 to 7 are doubled if a violation of one of those provisions has been committed within a period of five years after a conviction for one of those criminal offences or for one of the criminal offences described in the articles 210*bis*, 259bis, 314*bis*, 504*quater* or 550*ter*.

Article 550ter. (Data and System Interference)

§1. He who directly or indirectly introduces, alters, deletes or changes by any other technological means the normal use of any data in a computer system, whilst knowing that he is not entitled to do so, shall be punished with a term of imprisonment between six months and three years and with a fine between 26 euro and 25.000 euro or with one of these sanctions.

If the criminal offence established in the first paragraph is committed with intent to defraud or with the intent to cause damage, the term of imprisonment shall be between six months and five years.

§2. He who damages computer data in the computer system or in any other computer system as a result of committing a criminal offence established in §1, shall be punished with a term of imprisonment between six months and 5 years and with a fine between 26 euro and 75.000 euro or with one of these sanctions.

§3. He, who partially or completely hinders the correct functioning of the computer system or any other computer system as a result of committing one of the criminal offences established in §1, shall be punished with a term of imprisonment between one year and 5 years and with a fine between 26 euro and 100.000 euro or with one of these sanctions.

§4. He who illegitemately posesses, produces, sells, procures for use, imports, distributes, disseminates or otherwise makes available any instrument, including computer data, designed or adapted to enable one the criminal offences established in §§ 1 to 3, shall be punished with a term of imprisonment between six months and three years and with a fine between 26 euro and 100.000 euro, or with one of these sanctions.

§ 5. The sanctions established in §§ 1 to 4 are doubled if a violation of one of those provisions has been committed within a period of five years after a conviction for one of those criminal offences or for one of the criminal offences established in the articles 210*bis*, 259bis, 314*bis*, 504*quater* or 550*bis*.

§ 6. An attempt to commit one of the criminal offences established in §1 shall be punished with the same sanctions.

II. Provisions in the Belgian Code of Criminal Proceedings

Article 39*bis*. (Expedited Preservation of Stored Computer Data/Data Seizure)

§ 1. Without prejudice to the specific provisions of this article, the provision of this Code in relation to seizure, including the article 28sexies, apply to the copying, the rendering inaccessible and the deleting of data that are stored in a computer system.

§ 2. When a public prosecutor or a public prosecutor before a social court discovers data that are stored in a computer system that are useful for the same purposes as the seizure, but the seizure is not desirable, these data shall be copied on storage media belonging to the government, together with the data that are necessary to render these data intellegible. In case of urgency or due to technical reasons, use can be made of the storage media available to the persons entitled to use the computer system.

§ 3. He also applies adequate technical means to prevent access to these data in the computer system, as well as to the copies thereof that are at the disposal of the persons that are entitled to use the computer system, and to ensure the integrity of these data.[6]

If the data are the object of a criminal offence or if they are the result of a criminal offence and if these data are contrary to the public order or the accepted principles of morality, or if they represent a danger to the integrity of computer systems or the data that are being stored therein or processed or communicated therewith, the public prosecutor or the public prosecutor before a social court shall apply all adequate technical means to render these data inaccessible.

He may however, except in the case referred to in the previous paragraph, allow the further use of all or part of these data, when this does not present a danger to the prosecution.[7]

§ 4. When the measure mentioned in §2 is not possible

[6] *The word ' he' refers to the public prosecutor or the public prosecutor before a social court mentioned in §2.*

[7] *The word ' he' refers to the public prosecutor or the public prosecutor before a social court mentioned in §2.*

due to technical reasons or due to the extent of the data, he shall apply adequate technical means to prevent access to these data in the computer system, as well as to the copies thereof that are at the disposal of the persons that are entitled to use the computer system, and to ensure the integrity of these data.[8]

§ 5. The public prosecutor or the public prosecutor before a social court informs the person responsible for the computer system about the search in the computer system and communicates a summary of the data that have been copied, rendered inaccessible or deleted.

§ 6. The public prosecutor or the public prosecutor before a social court applies adequate technical means to provide for the integrity and confidentiality of these data.

Adequate technical means are applied for the storage of these data at the court registry.

The same applies when data that are being stored in, or processed or communicated with a computer system are being seized, in accordance with the previous articles, together with their storage media.

Article 88*ter*. (Computer and Network Search)

§ 1. When an investigating judge orders a search in a computer system or in a part thereof, this search can be extended to a computer system or a part thereof that is located at another place other than the place where the search takes place:

- if this extension is necessary to bring the truth to light concerning the criminal offence that is the object of the search; and
- if other measures would be disproportional, or if there is a risk that evidence would be lost without this extension.

§ 2. The extension of the search in a computer system may not be expanded beyond the computer systems or parts thereof to which the persons that are entitled to use the computer system that is being searched, have access in particular.

§ 3. In relation to the data that have been discovered as a result of the extension of the search in a computer system and that are usefull for the same purposes as the seizure, the provisions of article 39*bis* are applied. The investigating judge informs the person responsible for this computer system, unless his identity or domicile cannot reasonably be discovered.

When it appears that these data are not located on the territory of the Kingdom, they shall only be copied. In that case, the investigating judge shall immediately inform, through the public prosecutor, the Ministry of Justice, which will inform the competent authority of the concerned State, if this can reasonably be established.

§ 4. Article 89*bis* applies to the extension of a search in a computer system.

Article 88quater. (Duty to Cooperate – Computer and Network)

§ 1. The investigating judge or, acting under his authority, a judicial police officer, support officer of the public prosecutor or public prosecutor before a social court may order persons, whom he suspects to have particular knowledge about the computer system that is the object of the warrant or about services that are being used to secure of encrypt data that are being stored in or processed or communicated with a computer system, to provide information about the functioning thereof or about the manner to obtain access thereto, or to obtain access to the data that are being stored therein or processed or communicated therewith in an intelligible manner. The investigating judge shall mention the circumstances proper to the case, which justify the measure, in a reasoned order that he communicates to the public prosecutor or the public prosecutor before a social court.

§ 2. The investigating Judge or a judicial police officer, support officer of the public prosecutor or public prosecutor before a social court designated by him, may order any suitable person to operate himself the computer system or to copy, render inaccessible or delete the relevant data that are being stored therein or processed or communicated therewith, in the form ordered by him. These persons are obliged to cooperate, to the extent of their possibilities.

The order referred to in the First paragraph may not be given to the suspect and to the persons referred to in article 156.

§ 3. He who refuses to provide the cooperation ordered in paragraphs 1 and 2 or who hinders the search in the computer system, shall be punished with a prison term

[8] *The word ' he' refers to the public prosecutor or the public prosecutor before a social court mentioned in §2.*

between 6 months and 1 year and with a fine between 26 euros and 20.000 euro or with any of these sanctions.[9]

§ 4. Any person that obtains knowledge about this order as a result of his cooperation or that cooperates therewith, is held to secrecy. Every violation of this secrecy shall be punished in accordance with article 458 of the Criminal Code.

§ 5. The State is liable for the damages that have been caused unintentionally by the requisitioned persons to a computer system or to the data that are being stored therein or processed or communicated therewith.

Article 90quater. (Duty to Cooperate – Telecommunications)

§ 4. The investigating judge may order persons, whom he suspects to have particular knowledge about the communications service that is the object of the surveillance measure or about services used to secure of encrypt data that are being stored in or processed or communicated with a computer system, to provide information about the functioning thereof and about the manner to obtain access in an intelligible manner to contents of the telecommunication that is being or has been transmitted.

He may order persons to render the contents of the telecommunication accessible in the form ordered by him. These persons are obliged to cooperate therewith, to the extent of their possibilities.

He who refuses to provide the cooperation ordered in accordance with the previous paragraphs, shall be punished with a prison term between 6 months and 1 year and with a fine between 26 euros and 20.000 euro or with any of these sanctions.[10]

Any person that obtains knowledge about this order as a result of his cooperation or that is required to provide his technical cooperation, is held to the secrecy of the criminal investigation. Every violation of this secrecy shall be punished in accordance with article 458 of the Criminal Code.

Bibliographical information[11]

Act of 28 November 2000 on cybercrime (Belgian State Gazette of 3 February 2001).

Act of 15 May 2006 modifying articles 259bis, 314bis, 504quater, 550bis and 550ter of the Belgian Criminal Code (Belgian State Gazette of 12 September 2006).

Act of 6 June 2010 introducing a Social Criminal Code (Belgian State Gazette of 1 July 2010).

*

* *

An unofficial, consolidated German translation of the Belgian Criminal Code has been partially realized and published in the Belgian State Gazette:

> Articles 1 up to 100*ter*: Belgian State Gazette of 9 February 2007;
>
> Articles 101 up to 232: Belgian State Gazette of 27 April 2010;
>
> Articles 233 up to 321: Belgian State Gazette of 13 December 2010;
>
> Articles 322 up to 391*sexies*: Belgian State Gazette of 9 September 2011.

This text can be also consulted on the web site of the Central Service for German Translation – Commission for German legal terminology (Ministry of Internal Affairs) (http://www.scta.be/MalmedyUebersetzungen/downloads/18670608_CodeP%C3%A9nal.doc). The published text is an unofficial, consolidated version.

*

* *

On the web site of the Belgian Constitutional Court:

Dutch version: http://www.const-court.be/public/n/2004/2004-051n.pdf

French version: http://www.const-court.be/public/f/2004/2004-051f.pdf

Johan Vandendriessche is a member of the editorial board and a lawyer at the Bar of Leuven.

http://www.adv-vandendriessche.be/

[9] *The original text still mentions the amount in Belgian Francs. In order to avoid confusion, this has been changed in this translation.*

[10] *The original text still mentions the amount in Belgian Francs. In order to avoid confusion, this has been changed in this translation.*

[11] *This chapter provides an overview of the acts that are incorporated in this consolidated version. Reference is made to the official title of the act and its publication date.*