|  |
| --- |
| **Subject** |
| Belgian report on the cooperation between Internet service/access providers and law enforcement authorities |

|  |
| --- |
| **Authors** |
| Professor Dr. Paul De Hert, Vrije Universiteit Brussel (Free University Brussels, Belgium) & TilburgUniversity(the Netherlands)Gertjan Boulet, Vrije Universiteit Brussel (Free University Brussels, Belgium) |

|  |
| --- |
| **Awarding Entity** |
| Nicolaus Copernicus University, The Cybercrime Research Centre (Poland) |

|  |
| --- |
| **Project title**  |
| Towards a Polish Cybercrime Centre of Excellence |

|  |
| --- |
| **Funding**  |
| Prevention of and Fight against Crime Programme of the European Union, ISEC Programme |

|  |
| --- |
| **Publication date**  |
| February 2015 |



Co-funded by the Prevention of and Fight against Crime Programme of the European Union

**Contents**

1 Introduction 3

2 Classifications of electronic communications networks 3

2.1 Electronic Communications Act of 13 June 2005 3

2.1.1 Operator: provider of a (public) electronic communications network 4

2.1.2 Closed user communities 5

2.2 Mere conduit, caching and hosting 5

2.3 Autonomous interpretation of criminal law 5

3 Data retention 6

3.1 Publicly available operators 6

3.2 Royal Decree of 19 September 2013: data to be retained 8

3.3 No data retention obligations for closed user communities and ISPs acting as mere conduit, catching and hosting 11

4 Law enforcement access to data 11

4.1 Operators and closed user communities 12

4.2 Sui generis cooperation duties for ISPs acting as mere conduit, catching and hosting 13

4.3 Identification data 14

4.3.1 Cooperation with law enforcement agencies 14

4.3.2 Cooperation with intelligence and security services 15

4.4 Traffic data 15

4.4.1 Cooperation with law enforcement agencies 15

4.4.2 Cooperation with intelligence and security services 16

4.5 Content data 17

4.5.1 Cooperation with law enforcement agencies 17

4.5.2 Cooperation with intelligence and security services 18

4.6 Remuneration of costs for cooperation with LEAs 18

5 Taking down and blocking illegal content on the Internet 20

5.1 Code of Criminal Procedure 20

5.2 New Commercial Code 20

5.3 Act on gambling 21

5.4 Challenges for investigating and taking down child abuse images on the Internet 21

6 Research projects 22

7 Case law 22

7.1 Data retention 22

7.2 Extraterritorial judicial cooperation requests for identification data 23

7.2.1 Taking down and blocking 23

8 New legislation 24

Annex 1 Bibliography 25

Doctrine 25

EU legislation 25

EU case law 25

Belgian Acts 25

Belgian Royal Decrees 26

Belgian case law 26

Other materials 27

Annex 2 List of abbreviations 28

Annex 3 Questionnaire: cooperation of ISP with law enforcement 29

# Introduction

This report replies to the questionnaire provided by the awarding entity, on the subject ‘cooperation of ISP with law enforcement’. A table at the beginning of each section shows the questions addressed in the section. The first section discusses classifications of electronic communications networks under Belgian law. The next sections cover the themes data retention, law enforcement access to data, and taking down and blocking illegal content on the Internet. With regard to these topics, the final three sections discuss research projects, case law and new legislation. The annexes include a bibliography, a list of abbreviations and a copy of the questionnaire.

As the questionnaire focuses on cooperation between law enforcement and ISPs, law cooperation with other actors such as notaries, bailiffs, accountants and lawyers falls outside the scope of this report.[[1]](#footnote-1) On the other hand, the authors give a broad interpretation to law enforcement, and therefore also included an overview of the legal bases for cooperation between ISPs and intelligence and security agencies. On the other hand, the report does not address the cooperation between ISPs and states under emergency situations.[[2]](#footnote-2)

# Classifications of electronic communications networks

|  |
| --- |
| **Question 1** |
| How providers of publicly available telecommunication technologies are classified in the legal system of your country? |

## Electronic Communications Act of 13 June 2005

The definitions in the Electronic Communications Act of 13 June 2005[[3]](#footnote-3) partially reflect the definitions in the Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).[[4]](#footnote-4)

### Operator: provider of a (public) electronic communications network

Article 2, 11° of the Electronic Communications Act of 13 June 2005 defines an operator as a person subject to a notification duty under article 9 of the same Act. Article 9§1 of the Act lays down a duty of notification to the Belgian Institute for Postal Services and Telecommunications (BIPT) for providers or resellers, for their own account, of electronic communications networks or electronic communications services.

Article 2, 4° of the Electronic Communications Act of 13 June 2005 gives the following definition of a ‘provider of an electronic communications network’: "the establishment, operation, control or making available of an electronic communications network;”

#### Electronic communications network

Article 2, 3° of the Electronic Communications Act of 13 June 2005 gives the following definition of an ‘electronic communications network’: “the transmission 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, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, to the extent that they are used for the purpose of transmitting signals other than radio broadcasting and television.”[[5]](#footnote-5)

#### Public electronic communications network

Article 2, 10° of the Electronic Communications Act of 13 June 2005 gives the following definition of a ‘public electronic communications network’: “an electronic communications networks used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points.”[[6]](#footnote-6)

Article 2, 5° of the Electronic Communications Act of 13 June 2005 gives the following definition of an ‘electronic communications service’: “a service normally provided for remuneration which consists wholly or mainly in the conveyance, including switching and routing operations, of signals on electronic communication networks, except for (a) services using electronic communications networks and services to provide or exercise editorial control over content transmitted, (b) information society services as defined in article 2 of the Law of 11 March 2003 on certain legal aspects of information society services, which do not wholly or mainly consist of the conveyance of signals on electronic communications network and excluding (c) radio broadcasting and television;”[[7]](#footnote-7)

### Closed user communities

Article 9§5-6 of the Electronic Communications Act of 13 June 2005 refers to two categories of persons that are exempted from the notification duty under article 9§1 of the same Act: the providers and resellers of electronic communications networks or services which do not exceed the public domain (§5), and the provision or resale of electronic communications networks or services exclusively to a legal entity in which the provider or seller has a controlling interest, or to natural or legal persons in the framework of an agreement involving the provision of electronic communications networks or services as mere support and accessory (§6).

As we will see below, both the data retention duties and the duties to cooperate with law enforcement of persons with no notification duty are still to be determined in two Royal Decrees. Belgian Federal Magistrate Jan Kerkhofs and Investigative Judge Philippe Van Linthout state that, although it could be said that Belgian persons with no notification duty are currently released from data retention obligations (considering the lack of a specific Royal Decree), they would not be freed from their legal duty to cooperate with law enforcement.[[8]](#footnote-8)

## Mere conduit, caching and hosting

The Law of 11 December 2013[[9]](#footnote-9) and the Law of 26 December 2013[[10]](#footnote-10) repealed the two e-Commerce Acts of 11 March 2003[[11]](#footnote-11), which implemented the e-commerce Directive.[[12]](#footnote-12) Article 2, 1° of the Law of 11 December 2013 does not change the definition of an ‘information society service’ in article 2,1° of the first e-Commerce Act: “any service normally provided for remuneration by electronic means, at a distance and at the individual request of a recipient of services.” The provisions on liability state that an ISP is not held liable, when it merely acts as conduit or provides caching and hosting activities. As we will see below, the ISP that acts as mere conduit or provides caching and hosting activities is released from data retention obligations. Moreover, under certain conditions they can be freed from their legal duty to cooperate with law enforcement.

## Autonomous interpretation of criminal law

On 18 January 2011, the Supreme Court gave an autonomous interpretation to the term ‘electronic communications provider’ in article 46*bis* of the Code of Criminal Procedure (CCP, see below). The Court held that “the obligation to cooperate under article 46*bis* of the Code of Criminal Procedure is not restricted to operators of an electronic communications network or to providers of an electronic communications service that are also operators within the meaning of the Electronic Communications Act of 13 June 2005, or that only provide their electronic communications services through their own infrastructure. This obligation also applies to anyone who provides a service, which consists wholly, or mainly in the conveyance of signals on electronic communications networks. The person who provides a service which consists of enabling its customers to obtain, or to receive or distribute information through an electronic network, can also be a provider of an electronic communications service.”[[13]](#footnote-13)

# Data retention

|  |
| --- |
| **Question 2** |
| What are the regulations concerning data retention by IAPs (i.e. providers of publicly available electronic communications services or of public communications networks) and ISPs (i.e. providers of information society services)? |

|  |
| --- |
| **Question 3** |
| Are there traffic data related to technologies such as Facebook, blogs or other information society services covered by your national legislation? |

|  |
| --- |
| **Question 4** |
| What data are kept by ISP, IAP? |

## Publicly available operators

The Belgian Communication Act of 30 July 2013[[14]](#footnote-14) transposes the invalidly declared EU Data Retention Directive,[[15]](#footnote-15) and changed the genera data retention provision, Article 126 of the Electronic Communications Act of 13 June 2005. Article 126 of the Electronic Communications Act of 13 June 2005 is further elaborated in a Royal Decree of 19 September 2013, which provides the type of data to be retained.[[16]](#footnote-16)

Article 126§1 of the Electronic Communications Act of 13 June 2005 provides that the following providers of *publicly available* services are subject to data retention obligations:

* Fixed telephony services;
* Mobile telephony services;
* Internet access services;
* Internet email services;
* Internet telephony services.

Article 126 of the Electronic Communications Act of 13 June 2005 also applies to

* Providers of underlying public electronic communication networks;
* Resellers in own name and on own behalf.

Article 126§2 of the Electronic Communications Act of 13 June 2005 distinguishes following purposes of data retention:

* The investigation, detection, and prosecution of criminal activities as defined in article 46bis and article 88bis CCP;
* To curb fraudulent calls to emergency services;
* The detection by the Telecom Mediation Service of the identities of users that made fraudulent use of an electronic communications network or an electronic communications service as defined in Article 43bis, § 3, 7° the Act of 21 March 1991 on the reform of certain economic public enterprises;[[17]](#footnote-17)
* The special investigative methods for intelligence services, as defined in Articles 18/7[[18]](#footnote-18) and 18/8[[19]](#footnote-19) of the Law of 30 November 1998 Law on the Intelligence and Security Services.[[20]](#footnote-20)

Article 126§2 of the Electronic Communications Act of 13 June 2005 also provides that the network and service providers ensure that the data are accessible from Belgium without any restrictions, and can be communicated upon simple request and without undue delay to the authorities charged with the aforementioned purposes. Of note here is the uncertainty regarding the application of Article 126 of the Electronic Communications Act of 13 June 2005 to foreign based companies. For Belgian Federal Magistrate Jan Kerkhofs and Investigative Judge Philippe Van Linthout, the provision “to ensure that the data are accessible from Belgium without any restrictions” in article 126§2 shows that the Belgian legislator took account of the possibility that providers which offer their services in Belgium do not necessarily store their data on Belgian territory.[[21]](#footnote-21) Partners at the law firm Lorenz, on the other hand, add that *“[n]either the Act nor the Royal Decree clearly determine to what extent the data retention requirements apply to companies established abroad. We assume that the obligation is triggered when companies established abroad offer services on the Belgian territory. However, it remains unclear when a company, established abroad, is considered to provide services on the Belgian territory.*”[[22]](#footnote-22)

Article 126§3 of the Electronic Communications Act of 13 June 2005 installs a data retention period of 12 months. The start date of the retention period is different for identification data on the one hand, and for traffic and localisation data on the other.

As regards identification data: end-user identification data, as well as identification data regarding the used electronic communications service and the presumably used end-equipment, should be retained from the moment of subscription to the service, until twelve months after the last inbound or outbound communication effected via this service.

As regards traffic and localisation data: these data should be retained for twelve months after the date of the communication.

Article 126§4 of the Electronic Communications Act of 13 June 2005 provides that the Kind can extend the data retention periods for certain categories of data, without exceeding 18 months, as well as install a temporary data retention period of more than 12 months. If the data retention period in the latter case exceeds 24 months, than the minister informs the other EU Member States and the European Commission.

Article 126§5 of the Electronic Communications Act of 13 June 2005 provides that the network providers and providers of an electronic communications service shall ensure

* 1° the same quality and the same security and protection measures for retained data and network data;
* 2° adequate technical and organizational measures to ensure the security of the retained data;
* 3° exclusive competence for the members of, or the persons appointed by, the Coordination Cell Justice, which is responsible for handling the information requests by Belgian legal authorities[[23]](#footnote-23), to allow access to the retained data;
* 4° deletion of the retained data after expiration of the retention period.

Article 126§5 of the Electronic Communications Act of 13 June 2005 provides an annual reporting obligation towards the European Commission and the Belgian Chamber of Representatives.

As said, Article 126 of the Electronic Communications Act of 13 June 2005 is further elaborated in a Royal Decree of 19 September 2013, which distinguishes the type of data to be retained.

## Royal Decree of 19 September 2013: data to be retained

Article 3§1 of the Royal Decree of 19 September 2013 provides that **fixed telephony services** retain the following identification data:

* 1° the number allocated to the user;
* 2° the user’s personal data;
* 3° the subscription’s starting date or the registration data;
* 4° the type of fixed telephony service used and the types of other services to which the user is registered;
* 5° in case of number transfer, the identity of the transferring provider and of the receiving provider;
* 6° the data relating to the payment method, the identification of the payment instrument and the time of payment for the subscription or for the use of the service.

Article 3§2 of the Royal Decree of 19 September 2013 provides that **fixed telephony services** retain the following traffic and localisation data:

* 1° the identification of the calling number and the number called;
* 2° the location of the network connection point of the calling party and of the called party;
* 3° the identification of all lines in case of group calls, call forwarding or call transfer;
* 4° data and time of the start and end of the call;
* 5° description of the telephony service used.

Article 4§1 of the Royal Decree of 19 September 2013 provides that **mobile telephony services** retain the following identification data:

* 1° the number allocated to the user and his International Mobile Subscriber Identity (IMSI);
* 2° the user’s personal data;
* 3° the date and location of the user’s registration or subscription;
* 4° the date and time of the first activation of the service and the cell ID from which the service is activated;
* 5° the additional services to which the user has subscribed;
* 6° in case of number transfer, the identity of the transferring provider;
* 7° the data relating to the payment method, the identification of the payment instrument and the time of payment for the subscription or for the use of the service;
* 8° the ID number of the user’s mobile equipment (IMEI).

Article 4§2 of the Royal Decree of 19 September 2013 provides that **mobile telephony services** retain the following traffic and localisation data:

* 1° the identification of the telephone number of the calling party and of the called party;
* 2° the identification of all lines in case of group calls, call forwarding or call transfer;
* 3° the IMSI of the calling and called participants;
* 4° the IMEI of the mobile equipment of the calling and called participants;
* 5° the data and time of the start and end of the call;
* 6° the location of the network connection point at the start and the end of each connection;
* 7° the identification of the geographic location of cells, via reference to the cell ID, at the time of connection;
* 8° the technical characteristics of the telephony service used.

Article 5§1 of the Royal Decree of 19 September 2013 provides that **Internet access services** retain the following identification data:

* 1° the user ID allocated;
* 2° the user’s personal data;
* 3° the data and time of the user’s registration or subscription;
* 4° the IP-address, source port of the connection used for subscribing or registering the user;
* 5° the identification of the network connection point used for subscribing or registering the user;
* 6° the additional services to which the user has subscribed with the provider concerned;
* 7° the data relating to the payment method, identification of the payment instrument and the time of payment of the subscription fee or for the use of the service.

Article 5§2 of the Royal Decree of 19 September 2013 provides that **Internet access services** retain the following traffic and localisation data:

* 1° the user’s ID;
* 2° a) the IP-address;
* 2° b) in case of shared use of an IP-address, the ports allocated to the IP-address and the data and time of allocation;
* 3° the identification and location of the network connection point used when logging-in and logging-off;
* 4° data and time of an Internet access service session’s log-in and log-off;
* 5° the data volume up- and downloaded during a session;
* 6° data necessary to identify the geographic location of cells, via reference to the cell ID, at the time of the connection.

Article 6§1 of the Royal Decree of 19 September 2013 provides **that Internet email services and Internet telephony services** retain the following identification data:

* 1° the user ID;
* 2° the user’s personal data;
* 3° the data and time of creation of the email or Internet telephony account;
* 4° the IP-address and source port used for the creation of the email or Internet telephony account;
* 5° the data relating to the payment method, the identification of the payment instrument and the time of payment of the subscription fee or for the use of the service.

Article 6§2 of the Royal Decree of 19 September 2013 provides **that Internet email services and Internet telephony services** retain the following traffic and localisation data:

* 1° the user’s ID relating to the e-mail or Internet telephony account, including the number of ID code of the intended recipient of the communication;
* 2° the telephony number allocated to each communication entering the telephony network in the framework of an Internet telephony service;
* 3° a) the IP-address and the source port used by the user;
* 3° b) the IP-address and the source port used by the addressee;
* 4° the data and time of the log-in and log-off of a session of the email service or Internet telephony service;
* 5° the data and time of a connection made by means of the Internet telephony account;
* 6° the technical characteristics of the service used.

Article 7§1 of the Royal Decree of 19 September 2013 provides that network or service providers of multiple services, shall retain all data in relation to the different services. The article further explains that the combination of the registered data should allow identification of the link between the source and the recipient of the communication.

## No data retention obligations for closed user communities and ISPs acting as mere conduit, catching and hosting

Article 9§7 of the Electronic Communications Act of 13 June 2005 provides that a specific Royal Decree shall address the matter of the data retention by the Belgian Persons with no notification duty under Article 9§1 of the same Act. Federal Magistrate Jan Kerkhofs and Investigative Judge Philippe Van Linthout state that it could be said that Belgian persons with no notification duty are currently released from data retention obligations, considering the lack of a specific Royal Decree.

The ISP that acts as mere conduit or provides caching and hosting activities under the New Commercial Code is released from data retention obligations. However, it can be ordered a temporary surveillance period in specific cases (see below).

# Law enforcement access to data

|  |
| --- |
| **Question 3** |
| Are there traffic data related to technologies such as Facebook, blogs or other information society services covered by your national legislation? |

|  |
| --- |
| **Question 5** |
| What are the legal regulations enabling law enforcement and judicial authorities to obtain data from IAP, ISP with particular stress on social networking sites? |

|  |
| --- |
| **Question 6** |
| What are the legal requirements for an access of traffic data, stored content (eg. e-mail message) and subscriber’s data by LE/judicial authorities from ISPs? |

## Operators and closed user communities

The Electronic Communications Act of 13 June 2005 recognizes the possibility of cooperation between ISPs and law enforcement agencies and intelligence services.

Article 122, §1 of the Electronic Communications Act of  13 June 2005 provides that operators shall remove or anonymise traffic data relating to subscribers or end users, when these data are not longer necessary for the transmission of communication. However, Article 122, §1 continues providing that the previous provision is without prejudice to the duties of legal cooperation with law enforcement authorities, the Telecom Mediation Service and intelligence and security agencies.

Article 122, §4 of the Electronic Communications Act of  13 June 2005 adds that, in derogation from §1, data can be processed to detect fraud, and that in case of a criminal offence the data are communicated to the competent authorities.

Article 125, §1 of the Electronic Communications Act of  13 June 2005 confirms that Article 122 of the same Act is not applicable when the Belgian Institute for Postal services and Telecommunications (BIPT) acts by order of the investigative judge, the Director-General of the intelligence and security services, the Telecom Mediation Service (except for interceptions), and the civil servants of the Federal Public Service of Economy (except for interceptions).

Article 125, §2 of the Electronic Communications Act of  13 June 2005 provides that the King determines the modalities and the means to be put in place with a view to enable identification, detection, localisation, interception, taking cognizance and recording of electronic communications.

Article 127, §2, 1° of the Electronic Communications Act of  13 June 2005 provides that the King determines the technical and administrative measures that operators or end users need to take with a view to enable identification, detection, localisation, interception, taking cognizance and recording of private communications under the conditions provided in Articles 46bis, 88bis and 90ter to 90decies CPP and the law of 30 November 1998 Law on the Intelligence and Security Services. The modalities for these measures have been determined in the Royal Decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communication,[[24]](#footnote-24) and in the Royal Decree of 12 October 2010 determining the conditions of the legal collaboration obligation in case of judicial requests on electronic communications by the intelligence and security services.[[25]](#footnote-25) Both Royal Decrees install a Coordination Cell Justice responsible for handling the information requests by Belgian legal authorities.

As said, Belgian Federal Magistrate Jan Kerkhofs and Investigative Judge Philippe Van Linthout underline that although the Belgian Persons with no notification duty under Article 9§1 of the Electronic Communications Act of  13 June 2005 may currently be released from data retention obligations, they would be not freed from their legal duty to cooperate with law enforcement.[[26]](#footnote-26) Article 9§7 of the Electronic Communications Act of 13 June 2005 provides that a specific Royal Decree shall address the matter of the cooperation between law enforcement agencies and the persons with no notification duty.

## Sui generis cooperation duties for ISPs acting as mere conduit, catching and hosting

The ISP that acts as mere conduit or provides caching and hosting activities is released from data retention obligations, *and* under certain conditions can be freed from its legal duty to cooperate with law enforcement.

As said, the two e-Commerce Acts of 11 March 2003 were repealed by the Law of 11 December 2013 and the Law of 26 December 2013, which however did not change the provisions on liability of Internet service providers but moved them in their original versions to the New Commercial Code. The provisions on liability state that an ISP is not held liable, when it merely acts as conduit or provides caching and hosting activities.

First,mere conduit: Article XII.17 of the New Commercial Code (former Article 18 of the e-commerce Act) states that an ISP cannot be held liable for any such activities (e.g., transmitting information or providing access to a communications network), as long as the ISP does not initiate the transmission; select the recipient of the transmission; or select or modify the transmitted information. Provided that the information is stored for no longer than is reasonably necessary to do so, this exception will encapsulate the automatic, intermediate and temporary storage of information for the sole purpose of carrying out a transmission.

Second,catching: Article XII.18 of the New Commercial Code (former Article 19 of the e-commerce Act) releases the provider from any liability in catching activities for the automatic, intermediate and temporary storage of information for the sole purpose of making the transmission of that information more efficient provided certain conditions. In this respect, the ISP may not modify the information, it must comply with the conditions on access to the information, comply with the rules regarding the updating of the information specified in a manner recognized and used by industry; not interfere with the lawful use of technology, widely recognized and used by industry to obtain data on the use of the information; and act expeditiously to remove or disable access to the information upon obtaining actual knowledge that the initial source of the information has been removed or access to it has been disabled, possibly by order of a court or an administrative authority.

Third,hosting activities: Article XII.19 of the New Commercial Code (former Article 20 of the e-commerce Act) provides that ISPs are not held responsible provided that they: (i) do not possess actual knowledge of any illegal activity or information and, as regards claims for damages, are unaware of any facts or circumstances from which illegal activity or information is apparent; and (ii) act expeditiously to remove or disable access to the information, upon obtaining such knowledge or becoming aware of such activity. As with caching activities, the act obliges the ISP to notify and collaborate with the public prosecutor.

Article XII.20§1 of the New Commercial Code (former Article 21§1 of the e-commerce Act) confirms that ISPs do not have a general duty to monitor the information they transmit or store, nor actively to investigate facts or circumstances indicating illegal activity. However, Article XII.20§1 of the New Commercial Code allows the judicial authorities to order a temporary surveillance period in specific cases, given this is expressly allowed by statute. The relevant statutory provisions are articles 39bis, 89 and 90ter CCP.

Article XII.20§2 of the New Commercial Code (former Article 21§2 of the e-commerce Act) provides that ISPs have the obligation to promptly notify the competent judicial or administrative authorities of any alleged illegal activities committed or illegal information provided by their customers. In the original wording, ISPs also had to communicate to the authorities information enabling the identification of these customers. Article 59 of the Programme Act of 20 July 2005 altered article 21 of the e-commerce Act:[[27]](#footnote-27) under the new version, ISPs have to supply the judicial or administrative authorities, *at their request*, with all information about their users that they have at their disposal and that helps the search for unlawful acts committed by the users' intervention.

Article XV.118 of the New Commercial Code provides sanctions for failure to cooperate under Article XII.20§§1 and 2 of the New Commercial Code.

## Identification data

### Cooperation with law enforcement agencies

Article 46*bis* CPP obliges operators of an electronic communications network and providers of an electronic communications service to provide identification data upon request of the public prosecutor. Article 46*bis* CCP reads as follows:

“§ 1. In detecting crimes and misdemeanors, the public prosecutor may, by a reasoned and written decision, if necessary by requiring the cooperation of the operator of an electronic communications network or of the provider of an electronic communications service or of a police service designated by the King, proceed or cause to proceed, on the basis of any information in his possession or through access to the customer files of the operator or of the service provider, to:

1° the identification of the subscriber or the habitual user of an electronic communications service or of the used electronic communication means;

2° the identification of electronic communications services to which a particular person is a subscriber or that are habitually used by a particular person. The reasoning reflects the proportionality in relation to the privacy and the subsidiarity in relation to any other investigatory act.

In cases of extreme urgency, any judicial police officer can, after verbal and prior consent of the public prosecutor, in a reasoned and written decision order the production of these data. The judicial police officer shall communicate this reasoned and written decision and the information obtained within twenty-four hours to the public prosecutor and shall also motivate the extreme urgency.

§ 2. Any operator of an electronic communications network and any provider of an electronic communications service that is required to communicate information referred to in paragraph 1, provides the public prosecutor or judicial police officer the data that were requested within a period to be determined by the King, on the proposal of the Minister of Justice and the Minister responsible for Telecommunications.

The King determines, upon advice of the Privacy Commission and based on the proposal of the Minister of Justice and the Minister responsible for Telecommunications, the technical conditions for the access to the information referred to in § 1, which is available to the public prosecutor and to the police services designated in the same paragraph.

Any person, who by virtue of his office is informed of the action or cooperates thereto, is bound to secrecy. Any breach of secrecy is punishable in accordance with Article 458 of the Criminal Code.

Refusal to disclose the information is punishable with a fine of twenty-six euro to ten thousand euros.”[[28]](#footnote-28)

### Cooperation with intelligence and security services

The ‘Law of 30 November 1998 Law on the Intelligence and Security Services’ distinguishes normal, specific and exceptional methods of investigation. Special and exceptional methods of investigation need to be notified to the ‘Administrative Commission supervising the specific and exceptional methods for collecting data by the intelligence and security agencies’, the so-called BIM-Commission. Exceptional methods of investigation also require the prior authorization of the BIM-Commission. Both the special and exceptional methods of investigation are subject to the requirement of proportionality and subsidiarity.

The Law of 30 November 1998 classifies the collection of identification data as a specific method of investigation. Article 18/7 of the ‘Law of 30 November 1998 Law on the Intelligence and Security Services’ obliges operators of an electronic communications network and providers of an electronic communications service to cooperate upon request of the public prosecutor in order to:

- Identify the subscriber or user of an electronic communications service or of the used electronic communications method/

- Identify electronic communications services on which a specified person has been a subscriber or user.

- Produce invoices related to the identified subscriptions.

Failure to comply is punishable by a fine of 26-10000 euros

## Traffic data

### Cooperation with law enforcement agencies

Article *88bis C*CP reads as follows:

“§ 1. The investigative judge, who finds circumstances that necessitate the detection of telecommunications or localisation of the origin or the destination of telecommunications in order to find the truth, can, if necessary by requesting the cooperation of an operator of an electronic communications network or the provider of an electronic communications service:

- trace traffic data of telecommunication means from which or to which calls are or were made.

- locate the origin or the destination of telecommunications.

In the cases provided for in the first paragraph, the day, time, duration, and, if necessary, the place of the call for each telecommunications method of which the call data are detected or of which the destination of the telecommunications is localized, shall be determined and included in an official report.

The investigating judge shall state the factual circumstances of the case that justify the measure in a substantiated warrant that he communicates to the public prosecutor.

He also mentions the duration of the measure, which shall not be longer than two months starting from the warrant, without prejudice to a renewal.

In case of flagrante delicto, the public prosecutor can order the measure for the offences provided in Article 90ter, §§ 2, 3 and 4. In that case, the investigative judge must confirm the measure within twenty-four hours. However, if it concerns an offense referred to in Article 347*bis* [taking of hostages] and 470 [extortion by force] of the Criminal Code, the public prosecutor can order the measure during the situation flagrante delicto, without requirement of confirmation by the investigating judge.

The public prosecutor can order the measure upon request of the complainant, when the measure seems essential for establishing an offense referred to in Article 145 § 3 and § 3a of the Electronic Communications Act of 13 June 2005.[[29]](#footnote-29)

§ 2. Any operator of an electronic communications network and any provider of an electronic communication service shall communicate the requested data within a period to be determined by the King, on the proposal of the Minister of Justice and the Minister responsible for Telecommunications.

Any person, who by virtue of his office is informed of the action or cooperates thereto, is bound to secrecy. Any breach of secrecy is punishable in accordance with Article 458 of the Criminal Code.

Any person who refuses technical cooperation with the request mentioned in this article, of which the King determines the modalities, shall be punished with a fine of twenty-six euro to ten thousand euros, on the proposal of the Minister of Justice and the Minister responsible for Telecommunications.”

### Cooperation with intelligence and security services

The ‘Law of 30 November 1998 Law on the Intelligence and Security Services’ classifies the collection of traffic data as a specific method of investigation. Article 18/8 of the ‘Law of 30 November 1998 Law on the Intelligence and Security Services’ obliges operators of an electronic communications network and providers of an electronic communications service to cooperate upon request of the investigating judge in order to:

- Trace traffic data of electronic communications means from which or to which calls are or were made.

- Locate the origin or the destination of electronic communications.

Failure to comply is punishable by a fine of 26-10000 euros.

## Content data

### Cooperation with law enforcement agencies

The use of encryption is free according to Article 48 of the Electronic Communications Act of 13 June 2005. Article 88*quater* CCP allows the public prosecutor to impose the obligation to certain individuals to co-operate during an investigation. These individuals are described as persons of whom the investigative judge thinks that they have special capacities/knowledge concerning the computer system that has been the object of an investigation, or of services used to store, process, encrypt or transfer data. This obligation to co-operate is two-fold: (1) an obligation to provide information concerning how the system works or how one can get access to the stored data in an understandable format; and (2) an obligation to operate the system to deliver the data or to search it and to give access, copy the data or to make them inaccessible or delete them.

This action cannot be taken against suspects (nemo tenetur principle) or their families.

Failure to comply is punishable by 6 months to 1 year of imprisonment and/or a fine from 26 to 20000 euros (+ surcharges).

Article 90*ter* CCP empowers the investigative judge to intercept private communications or telecommunications during transmission, which include, amongst others, telephone conversations, email and voicemail. The power is subjected to the fulfillment of three strict conditions. First, serious reasons need to exist to believe that the suspect committed one of the listed crimes: these are offences of a grave and serious nature and include, amongst others, murder, trafficking in human beings, taking of hostages and kidnapping. Second, the measure must be considered a subsidiary measure in relation to any other investigatory act. Third, interception is only to be used reactively, in the presumption of occurrence of one of the aforementioned offences.

If it concerns an offense referred to in Article 347*bis* [taking of hostages] and 470 [extortion by force] of the Criminal Code, the public prosecutor can order the measure during the situation flagrante delicto, without requirement of confirmation by the investigating judge.

Article 90*quater*§1 CCP states that the warrant needs to contain: 1°, the indications and the concrete facts proper to the case which justify the interception measure(s); 2°, the reasons for which the measure is necessary to reveal the truth; 3°, the person, means of communication or telecommunications or the place of interception; 4°, the period during which the interception can be executed (no longer than one month starting from the decision ordering the measure); and 5°, the name of the judicial police officer designated to execute the measure.

Article 90*quater*§2 CCP obliges operators of an electronic communications network and providers of an electronic communications service to provide technical assistance to a data tapping measure upon request of the investigating judge. Failure to comply is punishable by a fine of 26-10000 euros

Article 90*quarter*§4 CCP: similar to article 88*quarter*, but here concerning data tapping measure. This action cannot be taken against suspects (nemo tenetur principle) or their families. Failure to comply is punishable by 6 months to 1 year in jail and/or a fine from 26 to 20000 euros.

### Cooperation with intelligence and security services

The ‘Law of 30 November 1998 Law on the Intelligence and Security Services’ classifies the collection of identification data as an exceptional method of investigation. Article 18/10§2 of the Law of 30 November 1998 provides that the authorization by the Director-General needs to be written and contain: 1°, a description of the exceptional threats that justify the interception; 2°, reasons why the interception is necessary; 3°, the subjects and objects that are intercepted; 4°, the technical means used for the interception, 5°, the period of interception; and 6°, the names of the intelligence officers involved in the operation.

Article 18/17§1 of the Law of 30 November 1998 provides that the Director-General can request the technical cooperation of the operator of an electronic communications network of the provider of an electronic communications service if the interception requires an operation on an electronic communications network. Failure to comply is punishable by a fine of 26-10000 euros

## Remuneration of costs for cooperation with LEAs

|  |
| --- |
| **Question 7** |
| Are there any laws, policies or arrangements for the remuneration of costs incurred by ISPs when providing LEAs with requested data? |

Article 127 §1 of the Electronic Communications Act of 13 June 2005 empowers the King to determine the remuneration of the provider’s costs. An annex to the Royal Decree of 9 January 2003[[30]](#footnote-30) regarding the legal duty to cooperate with judicial requests regarding electronic communications provides fixed rates for listed measures, and reimbursement of actual costs for non-listed measures. The annex was amended by the Royal Decree of 8 February 2011[[31]](#footnote-31), which changed the title of the Royal Decree of 9 January 2003, and again by the Royal Decree of 31 January 2013[[32]](#footnote-32) which deleted the provisions on reimbursement for non-listed measures.

The current version of the annex to the ‘Royal Decree of 9 January 2003 reads as follows:

‘1° General costs on the basis of this Royal Decree: According to the method of delivery of results, a supplement of 1.50 may be granted if the carrier is a floppy disc or CD-ROM.

2° Claims based on article 46*bis* CCP

a. Identification according to article 3, § 1 of this Royal Decree (for operators of electronic communication networks that were not granted numbering capacity, and for providers of electronic communications services):

- 1 till 10 identifications: 3

- More than 10 identifications: 0,25 per item

- Identification of an IMEI-track: 12,50 (or 25 if outside office hours from 8 am till 6 pm)
- delivery or identification of an IP-address: 8.

b. Identification according to article 3, § 2 of this Royal Decree (for operators of electronic communication networks that were granted numbering capacity): free of charge, with the exception of:

- Identification of an IMEI-track: 12,50 (or 25 if outside office hours from 8 am till 6 pm)

- Delivery or identification of an IP-address: 8.

 3° Claims based on article 88*bis* CCP

a. Observation according to article 4, § 1, first indent, of this Royal Decree (real time):
(1) Activation: 12,50 per call number (or 25 if outside office hours from 8 am till 6 pm).
(2) Fee per call number of calendar day: 5.

b. Observation according to article 4, § 1, second indent, of this Royal Decree (retro):

(1) Activation: 12,50 per call number (or 25 if outside office hours from 8 am till 6 pm).

(2) Rates per call number of calendar day: 3,10.

c. Observation according to article 4, § 1, first indent, of this Royal Decree, on a cell tower of a mobile network:

(1) Activation: 12,50 per call number (or 25 if outside office hours from 8 am till 6 pm).

(2) Rate per call number per cell tower of hour: 5.

d. Observation according to article 4 of this Royal Decree, in case of a telephone card track: 6,90.

e. On line tracking per hour: 12,50 (or 25 if outside office hours from 8 am till 6 pm).

4° Claims according to article 90ter CCP: interception of communication according to article 5 of this Royal Decree, including IP interception:

(1) Activation: 12,50 per call number (or 25 if outside office hours from 8 am till 6 pm).
(2) Rate per call number or per e-mail address per calendar day: 25.

5° Other reimbursements

a. Copy of an invoice: 4,50;

b. Copy of a contract: 4,50;

c. Request for data regarding a reload: 12,50 per call number (or 25 if outside office hours from 8 am till 6 pm);

d. Identification of a point of sale: 3,50;

e. PUK-code or voice mail reset: 2,50;

f. SIM-analysis: 18,60 per hour;

g. Identification of the payment method for call in a telephone booth: 6,90 per quarter of an hour;

h. Operator Service Track: 6,90 per quarter of an hour;

i. Intervention of a technician: 6,90 per quarter of an hour;

j. Specific request: 6,90 per quarter of an hour;

k. Requesting a coverage card: 16;

l. Transportation costs: 16,20.’

# Taking down and blocking illegal content on the Internet

|  |
| --- |
| **Question 8** |
| What are the legal regulations concerning taking down and blocking illegal content on the Internet before start of criminal proceedings and during criminal proceedings (powers of law enforcement and powers and obligation of service providers), what problems of taking down and blocking could be indicated? |

|  |
| --- |
| **Question 11** |
| What is the effectiveness of investigation and prosecution of illegal content crimes and child abuse on the internet in your country according to available statistical data and research? |

## Code of Criminal Procedure

Article 39*bis*§ 3 CCP allows the public prosecutor to order a seizure of alleged illegal data (e.g., a computer virus). The public prosecutor can use all technical means to make data inaccessible that "are the subject of the offence or have been produced by the offence and if they infringe public order or public decency or constitute a danger to the integrity of computer systems or data stored, processed or transmitted through such system”. This power is, for example, used by prosecutors to impose an ISP to delete from their copy of Domain Name Server (DNS) the domain name of a site that violates the law, such a site distributing child pornography.

## New Commercial Code

ArticleXII.5§4, 5 and 6 of the New Commercial Code(former article 2§4, 5, 6 of the second e-commerce Act) allows the Brussels investigative judge to order certain providers to block their services. When there is a danger for public health, public safety, national security and national defence and for consumer interest, the Investigating Judge can, when he is called to do so by certain authorities[[33]](#footnote-33) turn to a Belgian provider and ask the blocking of certain services provided for by firms in other EU countries, when the Belgian providers are able to do so. The order can be given for one month. The judge may extend one or more effects of its order and must terminate it as soon as the circumstances, which justified the order, change.

Although Article XII.20§3 of the New Commercial Code (on hosting; former Article 21§3 of the e-commerce Act) is the only article in the same Code that explicitly refers to Article 39*bis* CCP, article XII.20§1 of the New Commercial Code (former article 21§1 the e-Commerce Act) allows its use also in other cases. Article 20§3 of the e-Commerce Act provides that the ISP may only disable access to the information, and may not destroy or delete it, as long as the public prosecutor has not reached a decision on the matter.

Furthermore, article XII.18, 5° of the New Commercial Code (on catching; former Article 19 5° of the e-commerce Act) provides that the provider acts expeditiously to remove or disable access to the information upon obtaining actual knowledge that the initial source of the information has been removed or access to it has been disabled, possibly by order of a court or an administrative authority.

## Act on gambling

The Act of 2010 on gambling provides a similar mechanism as the New Commercial Code, but requires an administrative decision of the Commission on Gambling.[[34]](#footnote-34) Only legal institutions that hold the same type of games ‘in the real world’ can hold gambling games ‘on the Internet’. The Commission on Gambling has the power to order access providers to block access to illegal sites. The law is now also applicable to ‘game media’, primarily television sets.

## Challenges for investigating and taking down child abuse images on the Internet

According to European Center for Missing and Sexually Exploited Children (Child Focus), the strict Belgian laws hinder the rapid taking down of child pornography, especially images, from the Internet.[[35]](#footnote-35) As it is an offence in Belgium it to view child pornography (article 383*bis* of the Criminal Code), Child Focus cannot analyze notifications themselves but forward notifications to the Human Trafficking Division of the Federal Police, which has to do the time-consuming check for duplicate or wrongful complaints. The 2013 annual report of Child Focus announces a more user-friendly notification form that distinguishes notifications of images from notifications of suspected social media profiles. The report mentions 1320 notifications in 2010, 1479 notifications in 2011, 1394 notification in 2013, and 1232 notification in 2013.[[36]](#footnote-36) The stagnation of notifications would be due to increased traffic of images via hidden peer-to-peer networks.

From 10 till 27 October 2014, Child Focus started a petition called “Child pornography has to disappear” which calls, amongst others, for powers to take down child pornography in less than twenty-four hours.

# Research projects

|  |
| --- |
| **Question 9** |
| Were there any research projects concerning cooperation between LEA and ISP/IAP in fighting cybercrime in your country? If yes, please specify and shortly describe the results. What are the main problems of cooperation? |

The authors are not aware of any Belgian research projects explicitly focused on the cooperation between ISP/IAP and LEA. However, the authors have participated in a EU co-funded research project on ‘Increasing Resilience in Surveillance Societies’ (IRISS)[[37]](#footnote-37) with, amongst others, a contribution on surveillance in Belgium.[[38]](#footnote-38)

Another EU project in which Belgium partners participate is the ‘Advanced Cyber Defence Centre’ (ACDC),[[39]](#footnote-39) on cyber security problems resulting from criminal activities, particularly botnets. The project also addressed the cooperation between ISP/IAP in the margins; it produced a report that verifies the compatibility of ACDC with the current EU data protection framework and the laws of the sampled Member States, providing guidance to all actors involved on the legal issues for preventing botnet attacks: CERTs, Telecom operators / ISPs, owners of websites and end users.[[40]](#footnote-40)

# Case law

|  |
| --- |
| **Question 10** |
| What problems of cooperation between LE/judicial authorities with ISP/IAP can be indicated on the base of judicial decisions/judgments? |

## Data retention

On 8 April 2014, the European Court of Justice declared the EU Data Retention Directive invalid.[[41]](#footnote-41) Furthermore, the Belgian Constitutional Court will have to rule on the validity of the Belgian Communications Act of 30 July 2013.[[42]](#footnote-42) It should be noted that the Belgian Privacy Commission positively evaluated[[43]](#footnote-43) the compatibility of the Belgian Communications Act of 30 July 2013 and the Royal Decree of 19 September 2013 with its advice of 2009 regarding the legislative proposals on data retention.[[44]](#footnote-44)

## Extraterritorial judicial cooperation requests for identification data

On 4 September 2012, the Supreme Court held that Yahoo Inc., established in the United States, must, in accordance with Article 46*bis* § 2 of the Code of Criminal Procedure, comply with requests for judicial cooperation issued by Belgian law enforcement agencies.[[45]](#footnote-45) The effective enforcement of such requests may pose future challenges.

### Taking down and blocking

In a judgment of 3 February 2004,[[46]](#footnote-46) regarding a website containing hyperlinks to other websites showing child pornography, the Supreme Court clarified the legal liability exclusion grounds for ISPs. The liability exemption for ‘conduit activities’ (article 19 of the E-commerce Act, now article XII.18 of the New Commercial Code) did not apply as the person did more than just providing an information society service that consisted of the transmission in a communication network of information provided by a recipient of the service or more than just giving access to a communication network. Nor did the liability exemption for ‘hosting’ (article 20§1 of the E-commerce Act, now Article XII.19§1 of the New Commercial Code) apply as it had been proved that the person had personally provided passwords to applicants to publish and activate explicit hyperlinks, of which he had previous knowledge of their content.

Kerkhofs and Van Linthout add that an ISP with knowledge of illegal activities on its server may even be held (co)-responsible for participating in the offence on the basis of article 66 of the Criminal Code.[[47]](#footnote-47)

On 22 October 2013,[[48]](#footnote-48) the Supreme Court in the so-called Pirate Bay saga confirmed the lawfulness of an injunction order against all national ISPs, on the basis of article 39*bis* CCP, to block access to content which is hosted by a server linked to the main domain name ‘thepiratebay.org’, and such by employing all possible technical means, including at least by blocking all domain names that refer to main domain name “thepiratebay.org”. According to the Supreme Court, such a judicial order does not impose a general monitoring obligation upon the ISPs under Article 21§1 of the e-commerce Act of 11 March 2003 (now: article XII.20§1 of the New Commercial Code). It has been questioned[[49]](#footnote-49) whether the judgment of the Supreme Court complies with the prohibition of a general monitoring obligation and with Article 3 of the Directive of 29 April 2004 on the enforcement of IP rights:[[50]](#footnote-50)

‘1 Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights covered by this Directive. Those measures, procedures and remedies shall be fair and equitable and shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays.

2. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.’

Kerkhofs and Van Linthout read in article 39*bis* CCP and the judgment of the Supreme Court a possibility to block foreign websites.[[51]](#footnote-51)

# New legislation

|  |
| --- |
| **Question 12** |
| Is there any new legislation prepared or proposed concerning the above mentioned issues? If so, please indicate what are the intended changes and what reasons for them? |

The law of 27 December 2004[[52]](#footnote-52) modified article 88*bis* CCP, but the relevant provisions have not yet entered into force. The amendments include, first, the requirements of proportionality in relation to the privacy and subsidiarity in relation to any other investigatory act; second, the requirement for the operator of an electronic communications networks or the provider of an electronic communications service to provide the investigative judge or public prosecutor with an estimate of costs in case they act in view of establishing an offense referred to in Article 145 § 3 of the Electronic Communications Act of 13 June 2005. If the actual costs are higher than the ones listed in the Royal Decree of 9 January 2003, than the decision lies with the Chief Prosecutor of the jurisdiction of the public prosecutor, or with the first President of the Court of Appeal of the jurisdiction of the investigative judge.

Following the attacks against the magazine Charlie Hebdo in January 2015, the Belgian legislator announced its intention to add offence such as “encouraging, inciting or provoking terrorism” (article 140*bis* and following of the Criminal Code) to the list of offences in article 90*ter* CCP that justify an interception measure.



Co-funded by the Prevention of and Fight against Crime Programme of the European Union

# Annex 1 Bibliography

## Doctrine

De Hert, Paul and Boulet, Gertjan, “Cybercrime report for Belgium”, I*nternational Review of Penal Law (RIDP/IRPL)*, 2013, issue 84, no. 1-2, 48 pp., <http://www.penal.org/IMG/pdf/RIDP_2013_1_2_CD_Annexe.pdf>

Kerkhofs, Jan and Van Linthout, Philippe, *Cybercrime*, Politeia, Brussels, 2013, 639 pp.

## EU legislation

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54-65

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJL 195, 2.6.2004, pp. 16-25.

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, pp. 33-50.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, pp. 1-16.

## EU case law

European Court of Justice (Grand Chamber), Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, 8 April 2014.

## Belgian Acts

Act of 26 December 2013 inserting article XII in book XII, “Law of the electronic economy”, of the New Commercial Code, *Belgian Official Journal*, 14 January 2014.

Act of 15 December 2013 inserting a Book XII, entitled "Law of the electronic economy," in the New Commercial Code, and inserting definitions specific to Book XII and of enforcement provisions specific to Book XII, in the Books I and XV of the New Commercial Code, *Belgian Official Journal*, 14 January 2014.

Act of 30 July 2013 amending Articles 2, 126 and 145 of the Act of 13 June 2005 on electronic communications and Article 90decies of the Code of Criminal Procedure, *Belgian Official Journal,* 23 August 2013.

Act of 28 December 2011 concerning diverse provisions relating to justice II, *Belgian Official Journal*, 30 December 2011.

Act of 10 January 2010 modifying the Act of 7 May 1999 on gambling, gambling establishment and the protection of players**,** *Belgian Official Journal*, 1 February 2010.

Civil Contingencies Act of 15 May 2007, *Belgian Official Journal*, 31 July 2007.

Programme Act of 20 July 2005, *Belgian Official Journal*, 29 July 2005.

Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 20 June 2005.

Act of 27 December 2004 containing various provisions, *Belgian Official Journal*, 31 December 2004.

Act of 11 March 2003 on Certain Legal Aspects of the Information Society Services, *Belgian Official Journal*, 17 March 2003

Act of 11 March 2003 on Certain Legal Aspects of Information Society Services as defined in Article 77 of the Constitution, *Belgian Official Journal*, 17 March 2003.

Law of 30 November 1998 Law on the Intelligence and Security Services, *Belgian Official Journal,* 18 December 1998.

Act of 11 January 1993 on preventing use of the financial system for purposes of laundering money and terrorism financing, *Belgian Official Journal*, 9 February 2005.

Act of 21 March 1991 on the reform of certain economic public enterprises, *Belgian Official Journal,* 10 February 2009.

## Belgian Royal Decrees

Royal Decree of 19 September 2013 regarding the execution of the Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 8 October 2013.

Royal Decree of 31 January 2013 replacing the annex to Royal decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal,* 4 March 2013.

Royal Decree of 8 February 2011 modifying the Royal Decree of 9 January 2003 regarding the execution of Royal decree of 9 January 2003 regarding the execution of Article 46*bis* §2, paragraph 1er, 88*bis* §2, paragraph 1 and 3 ad 90*quater* §2 paragraph 3 CCP and of Article 109ter, E, §2 the Act of 21 March 1991 on the reform of certain economic public enterprises, *Belgian Official Journal*, 23 February 2011.

Royal Decree of 12 October 2010 determining the conditions of the legal collaboration obligation in case of judicial requests on electronic communications by the intelligence and security services, *Belgian Official Journal*, 8 November 2011.

Royal Decree of 13 April 2005 regarding the amicable settlement for breaches of the Act of 11 March 2003 on Certain Legal Aspects of the Information Society Services, *Belgian Official Journal,* 10 May 2005

Royal Decree of 7 May 2003 establishing the modalities under which the free movement of an information society service may be limited, *Belgian Official Journal,* 7 July 2003.

Royal Decree of 4 April 2003 ruling on the sending of publicity via e-mail, *Belgian Official Journal*, 28 May 2003.

Royal decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications’, *Belgian Official Journal,* 10 February 2003.

## Belgian case law

Supreme Court, 22 October 2013, P.13.0550.N/1.

Supreme Court, 4 September 2012, A.R. P.11.1906.N/18.

Supreme Court, 18 January 2011, P.10.1347.N.

Supreme Court, 3 February 2004, P.03.1427.N.

## Other materials

Advanced Cyber Defence Centre, Deliverable 1.8.1 – Legal Requirements (first iteration), 31 January 2014, 153 pp., <http://www.acdc-project.eu/wp-content/uploads/2014/11/ACDC_D1.8.1_Legal_Requirements.pdf>

Child Focus, Annual report 2013, 44 pp., <http://www.childfocus.be/sites/default/files/jaarverslag_2013_nl_lr_0.pdf>

Dhont, Jan and Dumont, David, “New Belgian Royal Decree Introducing Broad Data Retention Obligations”, interview with Nymity, January 2014, 4 pp., <http://www.nymity.com/~/media/Nymity/Files/Interviews/2014/2014-01-dhontdumont.aspx%E2%80%9D>

Belgian Privacy Commission, 2013 annual report, <http://www.privacycommission.be/nl/jaarverslag> (Dutch version) and <http://www.privacycommission.be/fr/rapport-annuel> (French version), 99 pp.

Belgian Privacy Commission, “Adviesaanvraag inzake het voorontwerp van wet en het ontwerp van koninklijk besluit inzake dataretentie, en het ontwerp van koninklijk besluit inzake de medewerkingsplicht (A/09/012)” (Request for advice concerning the proposals for a Law and Royal Decree on data retention, and concerning the proposal for a Royal Decree on the duty to cooperate), Advice nr 20/2009 of 1 July 2009, 14 pp., <http://www.privacycommission.be/sites/privacycommission/files/documents/advies_20_2009_1.pdf>

Flanders News.be, “Child porn taken down too slowly”, 10 October 2014, <http://deredactie.be/cm/vrtnieuws.english/News/1.2115016>

Järvinen, Heini, “Belgian NGO’s challenging the data retention law”, EDRi 12 March 2014, <http://edri.org/belgian-ngos-challenging-data-retention-law/>

Van Eecke, Patrick and Fierens, Alexis, “In pirate bay case, Belgian Supreme Court confirms lawfulness of generic ip blocking injunctions”, 13 January 2014, [http://www.lexgo.be/en/papers/IP-or-IT-or-TELECOM/IT%20law/page,3.html](http://www.lexgo.be/en/papers/IP-or-IT-or-TELECOM/IT%20law/page%2C3.html)

Van Eecke, Patrick, “Data retention obligations. Legal issues”, presentation of 12 December 2013, <http://events.belnet.be/sites/default/files/Patrick%20Van%20Eecke_Data%20retention.pdf>

Vodafone, Law Enforcement Disclosure Report Legal Annexe June 2014, 88 pp, <http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf>

# Annex 2 List of abbreviations

ADCD Advanced Cyber Defence Centre

BIPT Belgian Institute for Postal Services and Telecommunications

CC Criminal Code

CCP Code of Criminal Procedure

CERT Computer Emergency Response Team

DNS Domain Name Server

IAP Internet Access Provider

IP Intellectual Property

IP-address Internet Protocol Address

IMEI International Mobile Station Equipment Identity

IMSI International Mobile Subscriber Identity (IMSI);

IRISS Increasing resilience in surveillance societies

ISP Internet Service Provider

LEA Law enforcement authority

# Annex 3 Questionnaire: cooperation of ISP with law enforcement

1. How providers of publicly available telecommunication technologies are classified in the legal system of your country?

2. What are the regulations concerning data retention by IAPs (i.e. providers of publicly available electronic communications services or of public communications networks) and ISPs (i.e. providers of information society services)N

3. Are there traffic data related to technologies such as Facebook, blogs or other   information society services covered by your national legislation?

4. What data are kept by ISP, IAP?

5. What are the legal regulations enabling law enforcement and judicial authorities  to obtain data from IAP, ISP with particular stress on social networking sites?

6. What are the legal requirements for an access of traffic data, stored content (eg. e-mail message) and subscriber’s data by LE/judicial authorities from ISPs?

7. Are there any laws, policies or arrangements for the remuneration of costs incurred by ISPs when providing LEAs with requested data?

8. What are the legal regulations concerning taking down and blocking illegal content on the Internet before start of criminal proceedings and during criminal proceedings (powers of law enforcement and powers and obligation of service providers), what problems of taking down and blocking could be indicated?

9. Were there any research projects concerning cooperation between LEA and ISP/IAP in fighting cybercrime in your country? If yes, please specify and shortly describe the results. What are the main problems of cooperation?

10. What problems of cooperation between LE/judicial authorities with ISP/IAP can be indicated on the base of judicial decisions/judgments?

11. What is the effectiveness of investigation and prosecution of illegal content crimes and child abuse on the internet in your country according to available statistical data and research?

12. Is there any new legislation prepared or proposed concerning the above mentioned issues? If so, please indicate what are the intended changes and what reasons for them.

1. In that regard, see: Act of 11 January 1993 on preventing use of the financial system for purposes of laundering money and terrorism financing, *Belgian Official Journal*, 9 February 2005. [↑](#footnote-ref-1)
2. For instance, Article 181 Civil Contingencies Act of 15 May 2007 (*Belgian Official Journal*, 31 July 2007) provides that the Minister competent for internal affairs or his delegates may seize everyone and/or everything in the framework of interventions for civil contingency missions, if there are no public services or sufficient means available. Vodafone stated that Article 181 of the Civil Contingencies Act could include the communications data and/or network of Vodafone. See Vodafone, Law Enforcement Disclosure Report Legal Annexe June 2014, p. 14, <http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf> [↑](#footnote-ref-2)
3. Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 20 June 2005. [↑](#footnote-ref-3)
4. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, pp. 33-50. [↑](#footnote-ref-4)
5. Compare with Article 2(a) of the Framework Directive. [↑](#footnote-ref-5)
6. The definition is identical to the definition provided in Article 2(d) of the Framework Directive. [↑](#footnote-ref-6)
7. Compare with Article 2(c) of the Framework Directive. [↑](#footnote-ref-7)
8. Jan Kerkhofs and Philippe van Linthout, *Cybercrime*, Politeia, Brussels, 2013, p. 396. [↑](#footnote-ref-8)
9. Act of 15 December 2013 inserting a Book XII, entitled "Law of the electronic economy," in the New Commercial Code, and inserting definitions specific to Book XII and of enforcement provisions specific to Book XII, in the Books I and XV of the New Commercial Code, *Belgian Official Journal*, 14 January 2014. [↑](#footnote-ref-9)
10. Act of 26 December 2013 inserting article XII in book XII, “Law of the electronic economy”, of the New Commercial Code, *Belgian Official Journal*, 14 January 2014. [↑](#footnote-ref-10)
11. Act of 11 March 2003 on Certain Legal Aspects of the Information Society Services, *Belgian Official Journal*, 17 March 2003; and Act of 11 March 2003 on Certain Legal Aspects of Information Society Services as defined in Article 77 of the Constitution, *Belgian Official Journal*, 17 March 2003. [↑](#footnote-ref-11)
12. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, pp. 1-16. [↑](#footnote-ref-12)
13. Supreme Court, 18 January 2011, P.10.1347.N. [↑](#footnote-ref-13)
14. Act of 30 July 2013 amending Articles 2, 126 and 145 of the Act of 13 June 2005 on electronic communications and Article 90decies of the Code of Criminal Procedure, *Belgian Official Journal,* 23 August 2013. [↑](#footnote-ref-14)
15. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54-65; On 8 April 2014, the European Court of Justice declared the Data Retention Directive to be invalid: European Court of Justice (Grand Chamber), Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, 8 April 2014. [↑](#footnote-ref-15)
16. Royal Decree of 19 September 2013 regarding the execution of the Act of 13 June 2005 on electronic communications, *Belgian Official Journal*, 8 October 2013. [↑](#footnote-ref-16)
17. Act of 21 March 1991 on the reform of certain economic public enterprises, *Belgian Official Journal,* 10 February 2009. [↑](#footnote-ref-17)
18. Compare with Article 46*bis* CPP (see below). [↑](#footnote-ref-18)
19. Compare with Article 88*bis* CPP (see below). [↑](#footnote-ref-19)
20. Act of 30 November 1998 Law on the Intelligence and Security Services, *Belgian Official Journal,* 18 December 1998. [↑](#footnote-ref-20)
21. Jan Kerkhofs and Philippe van Linthout, *Cybercrime*, Politeia, Brussels, 2013, pp. 396-397. [↑](#footnote-ref-21)
22. Jan Dhont and David Dumont, “New Belgian Royal Decree Introducing Broad Data Retention Obligations”, interview with Nymity, January 2014, p. 2, <http://www.nymity.com/~/media/Nymity/Files/Interviews/2014/2014-01-dhontdumont.aspx%E2%80%9D> [↑](#footnote-ref-22)
23. Article 2 of the Royal decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications’, *Belgian Official Journal,* 10 February 2003. [↑](#footnote-ref-23)
24. Royal decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal,* 10 February 2003. [↑](#footnote-ref-24)
25. Royal Decree of 12 October 2010 determining the conditions of the legal collaboration obligation in case of judicial requests on electronic communications by the intelligence and security services, *Belgian Official Journal*, 8 November 2011. [↑](#footnote-ref-25)
26. Jan Kerkhofs and Philippe van Linthout, *Cybercrime*, Politeia, Brussels, 2013, p. 396. [↑](#footnote-ref-26)
27. Programme Act of 20 July 2005, *Belgian Official Journal*, 29 July 2005. [↑](#footnote-ref-27)
28. Criminal fines are multiplied by a factor to counter the effects of currency inflation. Act of 28 December 2011 concerning diverse provisions relating to justice II (*Belgian Official Journal*, 30 December 2011) raised the surcharges (décimes additionnels or opdeciemen) to fifty surcharges. The fines are thus multiplied by factor 6. [↑](#footnote-ref-28)
29. Article 145 § 3, 1° of the Law of 13 June 2005 on electronic communications punishes anyone who makes fraudulent electronic communications through a network of electronic communication in order to provide oneself or another an unlawful advantage’; Article 145 § 3*bis* of the Law of 13 June 2005 on electronic communications incriminates "the person who uses an electronic communications network or an electronic communications service or other electronic means to annoy or cause damage to his correspondent and the person installing any device intended to commit the offence and the attempt to commit it ". [↑](#footnote-ref-29)
30. Royal decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal,* 10 February 2003. [↑](#footnote-ref-30)
31. Royal Decree of 8 February 2011 modifying the Royal Decree of 9 January 2003 regarding the execution of Royal decree of 9 January 2003 regarding the execution of Article 46*bis* §2, paragraph 1er, 88*bis* §2, paragraph 1 and 3 ad 90*quater* §2 paragraph 3 CCP and of Article 109*ter*, E, §2 the Act of 21 March 1991 on the reform of certain economic public enterprises, *Belgian Official Journal*, 23 February 2011. [↑](#footnote-ref-31)
32. Royal Decree of 31 January 2013 replacing the annex to Royal decree of 9 January 2003 regarding the legal duty to cooperate with judicial requests regarding electronic communications, *Belgian Official Journal,* 4 March 2013. [↑](#footnote-ref-32)
33. These authorities are listed in the Royal Decree of 7 May 2003 establishing the modalities under which the free movement of an information society service may be limited, *Belgian Official Journal,* 7 July 2003. Another Royal Decree of 13 April 2005 fixes the level of administrative fees that can be proposed in case of infringement to the law: Royal Decree of 13 April 2005 regarding the amicable settlement for breaches of the Act of 11 March 2003 on Certain Legal Aspects of the Information Society Services, *Belgian Official Journal,* 10 May 2005. A third Royal Decree of 4 April 2003 rules on the sending of publicity via e-mail: Royal Decree of 4 April 2003 ruling on the sending of publicity via e-mail, *Belgian Official Journal*, 28 May 2003. [↑](#footnote-ref-33)
34. Act of 10 January 2010 modifying the Act of 7 May 1999 on gambling, gambling establishment and the protection of players**,** *Belgian Official Journal*, 1 February 2010. [↑](#footnote-ref-34)
35. Flanders News.be, “Child porn taken down too slowly”, 10 October 2014, <http://deredactie.be/cm/vrtnieuws.english/News/1.2115016> [↑](#footnote-ref-35)
36. Child Focus, Annual report 2013, pp. 28-29, <http://www.childfocus.be/sites/default/files/jaarverslag_2013_nl_lr_0.pdf> [↑](#footnote-ref-36)
37. <http://irissproject.eu/> [↑](#footnote-ref-37)
38. Gertjan Boulet, “Regulating Surveillance: The Belgian case”, IRISS Deliverable 2.3: The Legal Perspective, pp. 49 – 52, 31 January 2013, <http://irissproject.eu/wp-cont...emocracy-report-D2.3-IRISS.pdf> . A revised version of the contribution, titled “The Belgian Case: Pinpointing Legal and Illegal Surveillance” is forthcoming in an IRISS book. [↑](#footnote-ref-38)
39. <http://www.acdc-project.eu/> [↑](#footnote-ref-39)
40. Advanced Cyber Defence Centre, Deliverable 1.8.1 – Legal Requirements (first iteration), 31 January 2014, <http://www.acdc-project.eu/wp-content/uploads/2014/11/ACDC_D1.8.1_Legal_Requirements.pdf> [↑](#footnote-ref-40)
41. European Court of Justice (Grand Chamber), Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, 8 April 2014. [↑](#footnote-ref-41)
42. Heini Järvinen, “Belgian NGO’s challenging the data retention law”, EDRi 12 March 2014, <http://edri.org/belgian-ngos-challenging-data-retention-law/> [↑](#footnote-ref-42)
43. The Dutch and French versions of the 2013 annual report of the Privacy Commission are available at <http://www.privacycommission.be/nl/jaarverslag> and <http://www.privacycommission.be/fr/rapport-annuel>, see pp. 22-23. [↑](#footnote-ref-43)
44. Belgian Privacy Commission, “Adviesaanvraag inzake het voorontwerp van wet en het ontwerp van koninklijk besluit inzake dataretentie, en het ontwerp van koninklijk besluit inzake de medewerkingsplicht (A/09/012)” (Request for advice concerning the proposals for a Law and Royal Decree on data retention, and concerning the proposal for a Royal Decree on the duty to cooperate), Advice nr 20/2009 of 1 July 2009, <http://www.privacycommission.be/sites/privacycommission/files/documents/advies_20_2009_1.pdf> [↑](#footnote-ref-44)
45. Supreme Court, 4 September 2012, A.R. P.11.1906.N/18. [↑](#footnote-ref-45)
46. Supreme Court, 3 February 2004, P.03.1427.N. [↑](#footnote-ref-46)
47. Jan Kerkhofs and Philippe van Linthout, *Cybercrime*, Politeia, Brussels, 2013, p. 160. [↑](#footnote-ref-47)
48. Supreme Court, 22 October 2013, P.13.0550.N/1. [↑](#footnote-ref-48)
49. Patrick van Eecke and Alexis Fieris, “In pirate bay case, Belgian Supreme Court confirms lawfulness of generic IP blocking injunctions”, 13 January 2014, [http://www.lexgo.be/en/papers/IP-or-IT-or-TELECOM/IT%20law/page,3.html](http://www.lexgo.be/en/papers/IP-or-IT-or-TELECOM/IT%20law/page%2C3.html) [↑](#footnote-ref-49)
50. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 195, 2.6. 004, pp. 16-25. [↑](#footnote-ref-50)
51. Jan Kerkhofs and Philippe van Linthout, *Cybercrime*, Politeia, Brussels, 2013, p. 179. [↑](#footnote-ref-51)
52. Act of 27 December 2004 containing various provisions, *Belgian Official Journal*, 31 December 2004. [↑](#footnote-ref-52)