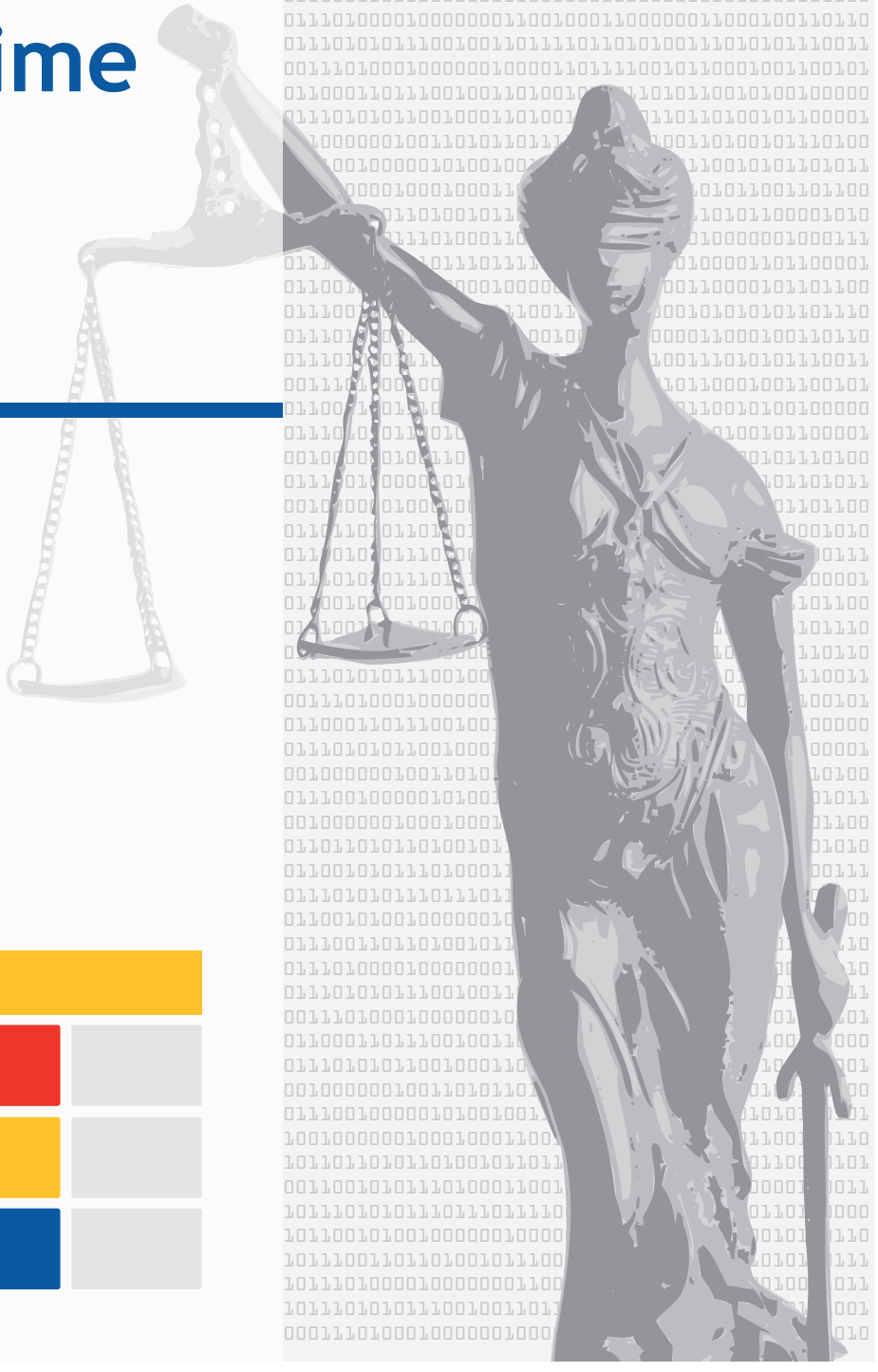
Cybercrime Judicial Monitor

Issue 1 June 2016



Contents

Foreword

The challenges posed by cybercrime and cyber-enabled crimes are recognised at national and international levels. Numerous measures have been taken both by the European Union and the Council of Europe to effectively counter cyber offences. This crime area has also been included in the European Agenda on Security. In 2016, additional attention was focused on the cyber threat by the Netherlands EU Presidency, which prioritises enhanced cooperation among Member States, particularly between their judicial authorities.

Eurojust recognises the pressing need for coordination and cooperation in this field and pursues its efforts in countering cyber offences by facilitating judicial cooperation in operational cases among the Member States and third States. As harmonisation of legislation in the area of cybercrime has hardly been undertaken so far, challenges and best practice extracted from both casework and strategic endeavours may expedite and simplify the work of practitioners in investigating and prosecuting cyber criminals across Europe and beyond. As a step in the direction of documenting and analysing legislation and sharing lessons learned in cybercrime cases at national and European levels, Eurojust has produced a new report, the *Cybercrime Judicial Monitor*.

The impetus for this report came from practitioners, following a series of meetings held at Eurojust since 2014. At the Eurojust tactical meeting on cybercrime of 1 July 2015, participants agreed upon the need for a tool to support prosecutors in their work by highlighting common challenges, possible solutions and lessons learned in cybercrime cases. This view was further confirmed at a subsequent cybercrime meeting at Eurojust on 25 November 2015.

The Cybercrime Judicial Monitor is a product mainly intended for prosecutors, judges and policemen.

Eurojust would like to express its sincere thanks to the Member States' authorities and all other contributors to this report. We hope that it will prove beneficial to your work in the cybercrime domain and look forward to continued good cooperation on possible future reports. We welcome your feedback on this first issue.

Michèle Coninsx

President

Daniela Buruiana

Chair, Eurojust Task Force on Cybercrime

I. Introduction

The inherent borderless, virtual nature of cyberspace, and the often transient nature of data transmitted therein, makes timely and effective judicial cooperation essential in the fight against cybercrime. To further strengthen the support provided to the national authorities in this field, Eurojust has developed a new reporting tool, the *Cybercrime Judicial Monitor* (CJM).

The CJM is designed to assist practitioners in the investigation and prosecution of cybercrime cases by providing information on the applicable legal framework, in-depth analyses of legal proceedings related to cybercrime and selected topics of interest. This is the first issue of the CJM. It focuses mainly on judicial analysis of court decisions. If it is considered to be of interest, Eurojust can continue to prepare further and more detailed versions.

In the absence of a specific obligation on Member States to report cybercrime-related information, the CJM mainly relies upon information shared by national authorities on a voluntary basis, through regular Eurojust channels (e.g. operational and tactical meetings), or in response to dedicated Eurojust questionnaires. The CJM also takes into account relevant information gathered through open source research and via international fora in which Eurojust participates.

The CJM is composed of three main sections: (1) legal updates; (2) judicial analysis; and (3) topic(s) of interest. The legal updates section offers an overview of relevant provisions or legal instruments at Member State, EU and international levels (e.g. UN). The judicial analysis section presents judgments rendered throughout the EU area by offering relevant case studies and/or legal and comparative analyses. The topic(s) of interest section is designed to address topics or issues widely and consistently raised by practitioners, Member States or EU institutions.

In this issue, the judicial analysis chapter presents a number of court decisions rendered by courts in Denmark and Sweden in the past few years, revealing issues of jurisdiction in cyberspace, use of virtual marketplaces to sell drugs and the complications of evidence-gathering in such a situation. A judgment of the Court of Justice of the EU is also presented. It concerns the legitimacy of transferring personal data from EU Member States to the USA and invalidation of the Safe Harbour Agreement between the EU and the USA.

In the topic of interest chapter, an extensive judicial analysis is presented of the court decisions rendered by the Belgian judicial authorities in the so-called 'Yahoo!' case and a related interview with Mr Jan Kerkhofs, Belgian Prosecutor in this case.

II. Legal Update

The objective of this section is to provide information on recent developments in international, EU and national legal instruments relevant to investigation, prosecution and international cooperation in cybercrime cases. Concerning national legal frameworks, this section will focus on the legislation of the EU Member States, Norway, Switzerland and the USA. It will include updates on substantive and procedural criminal law, as well as other laws and regulations that address questions related to cybersecurity, use of information and communication technologies and infrastructures, all of which have implications on legal or practical aspects of investigations and prosecutions of cybercrime.

As the main source of information presented in this section, contributions collected through the Judicial Cybercrime Network will be used. Data available in open sources will serve as a complementary source of information and, if the data concerns national legislative developments, it will be verified with national experts within the Network before being presented in this section. Where available, references to online sources providing the official texts of the legal documents discussed in the section will be included.

In the current issue of the CJM, this section has no substantial content. This section will be developed in the future issues of the CJM. This section is included solely with the intention of providing the reader with a complete overview of the range of sections available in any future issues of the CJM.

III. Judicial Analysis

The objective of this analytical chapter is to provide insight into cybercrime judgments rendered within the EU and at international level. It is intended to help practitioners and offer relevant case studies and/or comparative analyses. The analysis focuses on the most interesting aspects of the case, rather than covering all issues and arguments addressed by the court.

The judgments to be analysed have been selected from the court decisions that have been sent to Eurojust on a voluntary basis by the practitioners of the Member States, as well as relevant decisions found through open source research. This overview of court decisions is not exhaustive and may be broadened and complemented in future reports.

Procedures and dates of decisions in Sweden:

District Court of Helsingborg, 15 May 2014

District Court of Malmö, 4 July 2014; Court of Appeal of Skåne and Blekinge, 8 September 2014

District Court of Varberg, 8 January 2015

District Court of Skellefteå, 2 July 2015

District Court of Södertörn, 7 July 2015

Introduction

Between 15 May 2014 and 7 July 2015, judgements were rendered by Swedish courts in five independent cases in which individuals committed criminal offences using hidden marketplaces on the Internet, particularly the *Silk Road* marketplace. The use of this and other similar marketplaces required accessing the Darknet through a Tor web browser, which makes the users anonymous and criminal activities difficult to detect. Some offences were committed using the first version of *Silk Road*, which was closed down by the US Federal Bureau of Investigation in October 2013. *Silk Road 2.0* was subsequently created to replace the initial site, and some of the accused made use of this new marketplace, sometimes together with other sites like *Flugsvamp*, *Agora* and *Sheep Marketplace*. Payments on these marketplaces were mostly made using the virtual currency Bitcoin.

A total of 19 accused were principally charged with drug-related offences, and some in their roles as vendors on *Silk Road* and other sites. Other accused were charged as accomplices or with providing assistance in the commission of the criminal offences.

The court proceedings

The cases focused in general on the underlying crimes and the evidence gathered, rather than on legal issues concerning cybercrime. Interestingly, the District Court of Malmö pointed to the fact that selling drugs in this manner through the *Silk Road* market place was particularly effective and sophisticated, and clearly contributed to lowering the threshold for buying drugs. The possibility to buy drugs anonymously made these substances easily accessible to a vast group of unknown buyers. The Court of Appeal of Skåne and Blekinge concurred with this finding. This view was clearly shared more widely, as the District Court of Varberg and the District Court of Skellefteå also pointed to the dangerous and reckless nature of these activities, as well as to the indifference of the accused to drug abuse, considering that drugs were available to a large number of people without any control as to the identity of the recipients.

The ruling of the court

Of the 19 accused, one was acquitted and the others were convicted and sentenced to a fine, if the role of the accused was limited, and to prison sentences varying from two months to ten years, if the accused had a more significant role in the criminal activities or acted as the vendor. Some of the vendors were also liable to pay a sum of money to the State as confiscated value of crime.

Three of the five cases became final after the decision by the Court of First Instance. The case before the District Court of Södertörn was appealed up to the Supreme Court on the aspect of forfeiture of assets of the accused. The case against a vendor, brought before the District Court of Malmö, was appealed to the Court of Appeal of Skåne and Blekinge and then became final. In that case, the District Court of Malmö first sentenced the accused to imprisonment prison sentence of five and one-half years for committing aggravated drug offences, possession of knives or similar weapons, aggravated possession of drugs and possession of firearms. The prosecution appealed the decision on the charge of aggravated drug offences and pleaded for a higher sentence. The Court of Appeal of Skåne and Blekinge altered the decision of the District Court of Malmö on this charge and sentenced the accused to seven years' imprisonment.

Procedure: The Court of Justice of the EU (Grand Chamber)

Reference for a preliminary ruling under Article 267 TFEU from the High Court of Ireland (*Maximillian Schrems v Data Protection Commissioner,* Case C-362/14)

Date of decision: 6 October 2015

Introduction

The request for a preliminary ruling was referred to the Court of Justice of the EU (ECJ) by the High Court of Ireland in proceedings between an Austrian citizen, a user of Facebook, and the Irish supervisory authority. The proceedings concerned the supervisory authority's refusal to investigate the person's complaint regarding the fact that Facebook Ireland Ltd transfers to the USA the personal data of Facebook users residing in the European Union. The complainant contended that the law and practice of the USA did not ensure adequate protection against surveillance by the intelligence services, in view of the revelations made in 2013 by Edward Snowden. The complainant asked the supervisory authority to exercise its powers to prohibit the transfer of data. The supervisory authority refused to investigate the complaint, due to the fact that, in a decision of 26 July 2002 (the 'Safe Harbour Decision'),[1] the Commission had already recognised that, under the Safe Harbour scheme, the USA ensures an adequate level of protection of the transferred personal data.

The High Court of Ireland wished to ascertain whether the Commission's Safe Harbour Decision had the effect of preventing a national supervisory authority from examining a claim alleging that the third country does not ensure an adequate level of protection and, where appropriate, from suspending the contested transfer of data. The request for a preliminary ruling related, in essence, to the interpretation of Article 25(6) the Data Protection Directive[2] and to the validity of the Commission's Safe Harbour Decision adopted pursuant to the Data Protection Directive.

The court proceedings

The powers of a national supervisory authority in a situation in which the Commission has adopted a decision pursuant to Article 25(6) of the Data Protection Directive

In relation to the powers of a national supervisory authority of a Member State in a situation in which the Commission has adopted a decision such as the Safe Harbour Decision, the ECJ held that the existence of the Commission's decision does not affect the powers available to the

[1] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7). The 'safe harbour' scheme includes a series of principles concerning the protection of personal data, to which US enterprises may subscribe voluntarily.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 (OJ 2003 L 284, p. 1).

national supervisory authorities under the Data Protection Directive. Thus, even if the Commission has adopted a decision recognising that a third country ensures an adequate level of protection, this decision does not prevent a national supervisory authority from examining, with complete independence, a claim of a person contending that the law and practices in force in the third country do not ensure an adequate level of protection of the person's rights and freedoms with regard to the processing of the personal data.

The invalidity of the Safe Harbour Decision

By virtue of Article 25(6) of the Data Protection Directive, the Commission, in order to adopt the Safe Harbour Decision, had to find that the third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection of private lives and basic rights and freedoms of individuals. The ECJ held that the term 'adequate level of protection' must be understood as a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union. Furthermore, the 'adequate level of protection' had to be found by assessing the content of the applicable rules in the third country resulting from the country's domestic law or international commitments, and the practice designed to ensure compliance with those rules. The ECJ found that the Commission failed to comply with the requirement of Article 25(6) of the Data Protection Directive, as the Safe Harbour Decision concerned only the adequacy of the protection provided under the Safe Harbour scheme, without containing sufficient findings regarding the rules from the country's domestic law or international commitments. The features of the scheme, such as its inapplicability to the U.S. public authorities, and the prevalence of US national security, public interest, law enforcement requirements or US law imposed conflicting obligations over the rules of the scheme, allowed the ECJ to find that the Safe Harbour Decision enables interference by the US public authorities with the fundamental rights of the persons whose personal data is transferred from the European Union to the USA. Moreover, the Safe Harbour Decision neither contained any finding regarding the existence in the USA of legal rules intended to limit such interference nor referred to the existence of effective legal protection against the interference.

The ECJ noted that, regarding the level of protection essentially equivalent to that guaranteed within the European Union, legislation authorising the application of measures involving interference with fundamental rights must lay down clear and precise rules governing the scope and application of the measures and impose minimum safeguards for protection against abuse. Legislation that permits the public authorities to access personal data on a generalised basis and, thus, with unlimited ability to interfere with the fundamental right to what is strictly necessary, as well as not providing for any possibility for a person to pursue legal remedies, must be regarded as compromising fundamental rights to respect for private life and to effective judicial protection.

The ruling of the court

The ECJ declared the Safe Harbour Decision invalid, due to the failure to comply with the requirements of Article 25(6) of the Data Protection Directive.

Additionally, the ECJ declared the Safe Harbour Decision invalid because it had the effect of denying the national supervisory authorities the powers derived from Article 28 of the Data Protection Directive, in which a person, in bringing a claim, calls into question whether a Commission's decision, such as the Safe Harbour Decision, is compatible with the protection of the privacy and the fundamental rights and freedoms of individuals. The ECJ held that the Commission did not have competence to restrict the national supervisory authorities' powers referred to in Article 28 of the Data Protection Directive.

Procedure: Supreme Court of Denmark (*Højesteret*, Case no 129/2011)

Date of decision: 10 May 2012

Introduction

On 10 May 2012, the Danish Supreme Court rendered its decision in a case concerning the permissibility of the Danish police to access information on the Facebook and Messenger profiles of a suspect in a criminal investigation into drug trafficking, who at the time of these measures was residing abroad. The Supreme Court decision addressed two intertwined issues. On the one hand, the Supreme Court considered how the measures carried out by the police should be qualified, i.e. as data reading or as secret searches under the Danish Code of Criminal Procedure. On the other hand, the Supreme Court addressed the applicability of the Danish Code of Criminal Procedure to the measures taken, considering that the suspect was not in Denmark at the time of the measures and the information accessed was stored on servers abroad. Decisions in this case had previously been rendered by the District Court of Esbjerg (Retten i Esbjerg) on 20 October 2010 and the Western High Court (Vestre Landsret) on 8 February 2011.

The court proceedings

The defence in its appeal claimed that the police was not authorised to access information on the Facebook and Messenger profiles of the accused, referring in particular to access on one specific date. The prosecution claimed that the secret searches could be conducted under Article 799, cf. 793, para. 1 no. 1, or that secret data reading could take place on the basis of Article 791b of the Danish Code of Criminal Procedure. According to the defence, neither provision should apply. First, nothing existed to be searched, as the information concerned was stored on a server and, thus, the conditions for secret searches were not met. Second, the provisions on secret data

reading did not apply to these measures due to the fact that Facebook and Messenger profiles could not be considered information systems, i.e. a computer or another kind of data processing system.

The Supreme Court concurred with the arguments of the prosecution and held that the information accessed by the police on the Facebook and Messenger profiles is similar to received and sent e-mails and cannot be considered as information that is part of an ongoing line of communication. The information was stored on the profiles and was accessed using codes obtained through telephone interception. The measures taken by the police are, thus, not to be considered as secret data reading but as secret searches under the aforementioned provisions.

With regard to the applicability of the Danish Code of Criminal Procedure, the defence argued that while the profiles were accessed from Denmark, these measures required a clear legal basis and the authorisation of the States in which the servers were located, in this case the USA and Luxembourg. In addition, a Canadian telecommunications provider had been used during the suspect's stay in Canada, which meant that the authorisation of the Canadian authorities also should have been obtained. The prosecution held that the measures carried out by the police were part of a criminal investigation of the Danish authorities for the purposes of a possible prosecution in Denmark. Accordingly, the investigation was to be carried out in accordance with the Danish Code of Criminal Procedure and a decision by the Supreme Court should be limited to the question whether the conditions set by the Danish Code of Criminal Procedure were met.

The Supreme Court reiterated that the Danish Code of Criminal Procedure was applicable to the measures taken. The criminal offences in question fall under Danish jurisdiction, the investigation was carried out by Danish authorities and the secret measures were undertaken without the involvement of foreign authorities and, thus, the fact that the suspect resided abroad and the information was stored on servers abroad did not alter the applicability of the provisions on secret searches of the Danish Code of Criminal Procedure to the measures carried out by the Danish police.

The ruling of the court

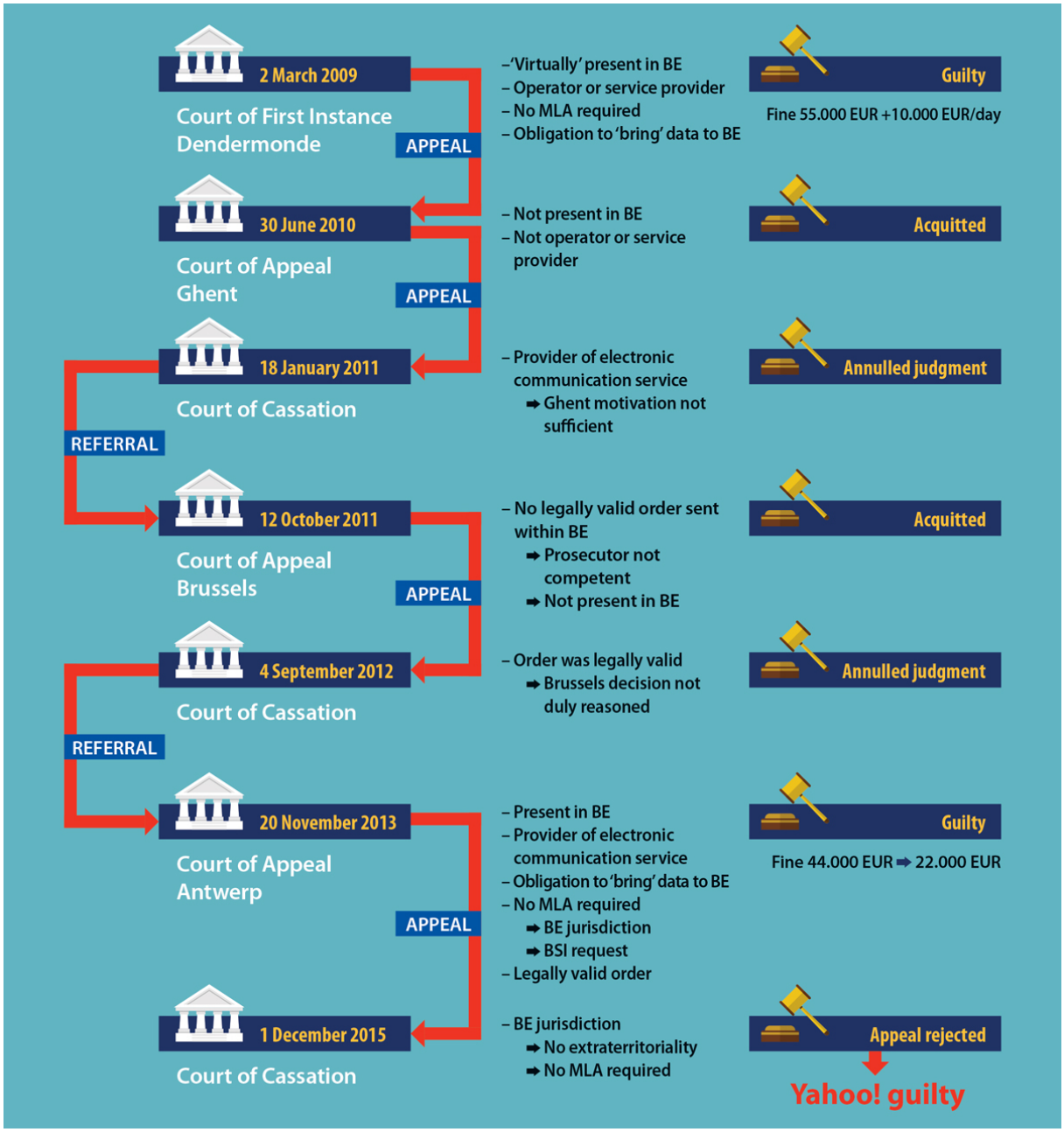
Considering that all conditions set by the applicable provisions were fulfilled, the Supreme Court found that the secret searches of the suspect's Facebook and Messenger profiles by the police were permissible.

IV. Topic of Interest

In this chapter, an extensive judicial analysis is made of the seven Belgian verdicts related to the *'Yahoo!'* case. The legal proceedings in this case lasted from 2008 until end of 2015 and finally resulted in the conviction of Yahoo! Inc.

The chapter contains an in-depth analysis of the Yahoo! court decisions followed by an interview with the public prosecutor who initiated the case.

An overview of the court findings and decisions in the *Yahoo!* case is given below.



IV.i. Analysis of Yahoo! judgments

Introduction

The initial criminal case

In October 2007, a complaint was made by a company, located in the judicial district of Dendermonde (Belgium), regarding purchases (laptops) made online via its webshop by use of stolen credit card data. Subsequently, an investigation was initiated by the public prosecutor in Dendermonde.

The criminals made use of several e-mail accounts to commit the criminal acts. These e-mail accounts belonged to or were provided under the management of Yahoo! Inc., located in California, USA. To further identify the perpetrators, the public prosecutor decided to request Yahoo! to provide identification and registration data (basic subscriber information) linked to the aforementioned e-mail accounts.

The Yahoo! case - background facts

In the context of the abovementioned criminal investigation, with a view to identifying the perpetrators, and pursuant to article 46bis of the Belgian Code of Criminal Procedure (see below), the public prosecutor sent an order to Yahoo! Inc. in November 2007 to provide the following data linked to the Yahoo! e-mail accounts:

1) the full identification/registration data of the person who created/registered the account, including the IP address, date and time (+ time zone) of the registration,

2) the e-mail address associated with the profile,

3) any other personal information that could lead to identification of the user(s) of the account.

Considering that Yahoo! Inc. did not have any local office in Belgium, the order was sent to Yahoo! Inc. via the web addresses through which Yahoo! makes itself available in Belgium to its users for reporting abuse or questions related to security problems.

Yahoo! replied by e-mail that such request was to be submitted in writing, addressed to the address of Yahoo! Custodian of Records in California, U.S.A. The prosecutor subsequently addressed the order by ordinary mail and fax to the mentioned address in February 2008.

Yahoo! responded to the written order by e-mail, stating that all the requested information related to US registered accounts, in relation to which the US Electronic Communications Privacy Act (ECPA) prevents the disclosure without an order to this effect by a US jurisdiction, and thus such requests must be made through the US Department of Justice. Furthermore, Yahoo! suggested that the initiation of a civil 'John Doe legal action' would be an alternative to proceed with this request. In its reply, Yahoo! did not take any stand in relation to its presence – or lack thereof on Belgian territory.

In July 2008, the public prosecutor summoned Yahoo! again to respond to the judicial order. Yahoo! did not react, from which the conclusion was made that it did not intend to comply with the judicial order of the Belgian prosecutor. Consequently, the public prosecutor initiated criminal proceedings against Yahoo!

Procedure: Court of First Instance Dendermonde

Date of decision: 2 March 2009

The charges

The Public Prosecutor's Office accused Yahoo! Inc. of violating article 46bis §2 of the Belgian Code of Criminal Procedure (C.C.P.) by having refused, in the capacity of operator of an electronic communications network or provider of an electronic communications service from whom the public prosecutor required the communication of the data referred to in paragraph 1 of article 46bis C.C.P., to communicate the required data to the public prosecutor. Yahoo! committed this violation within the judicial district of Dendermonde and connected therewith elsewhere in Belgium, at least during the period from 10 December 2007 until the date of the summons (16 September 2008), and in any case on 10 December 2007, 10 March 2008 (dates when Yahoo! replied to the requests of the public prosecutor) and 7 July 2008.

The applicable law

Article 46bis C.C.P. states 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 an access of the customer files of the operator or of the service provider, to:
>
> 1° the identification of the subscriber or a habitual user of an electronic communications service or of the means used for electronic communication;
>
> 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 commandeer these data. The officer of the criminal investigation department shall communicate this reasoned and written decision and the information obtained within twenty-four hours to the public prosecutor and also the reasons for the extreme urgency.

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

The King determines, upon advice of the Commission for the protection of privacy and based on a 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, available to the public prosecutor and for the police service designated in the same paragraph.

Any person who by virtue of his ministry is aware of the action or otherwise 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.'

Arguments of the defence

The defence contested the offences with which it was charged and brought the following arguments before the Court:

- The public prosecutor should have followed the **mutual legal assistance procedure** and therefore have sent the request via the US authorities in order to receive the data. The requested information namely concerned US registered accounts that are governed by the ECPA, stipulating that such information cannot be transmitted without being ordered to do so by a US jurisdiction.
- The alleged **criminal offence**, i.e. not complying with the judicial order of the public prosecutor, has **not been committed in Belgium**.
- The public prosecutor had **no territorial jurisdiction**, as **Yahoo!** is neither an operator of an electronic communications network established in **Belgium**, nor a provider of an electronic communications service established in Belgium within the meaning of article 46bis C.C.P.

- The public prosecutor did **not have any competence to act** in this matter, given the fact that Yahoo! is **neither an operator** of an electronic communications network **or a provider** of an electronic communications service within the meaning of article 46bis C.C.P.
- The claim of the public prosecutor was disproportionate and violated the principle of subsidiarity.
- Since the period within which the data needs to be transferred is not defined in article 46bis C.C.P., no criminal offence has been committed.
- A moral element was lacking, as Yahoo! did not refuse in any way whatsoever to provide the requested data in its possession.

Court reasoning

Reasoning on substantive matters

1. *Presence of Yahoo! on Belgian territory*

The Court established that the abovementioned e-mail accounts were used in Belgium, under the management of Yahoo!, and therefore within Belgian territory. Furthermore, the Court agreed with the public prosecutor that **Yahoo! is also present within the Belgian territory, both commercially as well as by providing services, even if it is through the Internet or 'virtually'**. This assertion is supported by the fact that Yahoo! also makes itself available on Belgian territory to third parties. Indeed, Yahoo! as an ISP is economically present in Belgium and is reachable via web addresses for its customers. Consequently, Yahoo! is to be deemed accountable in Belgium and should therefore also be capable of replying to queries coming from the Belgian judicial authorities. The Court reasoned that this situation is in fact what occurred in the current case, namely a Belgian public prosecutor requesting information in Belgium from a US national present on Belgian territory at that time.

The Court reiterated that Yahoo! is present within Belgium for economic purposes, pointing to a specific reference to the defendant's statement that one of the reasons for its presence through the Internet in Belgium was to generate 'hits' via its website there to attract advertisers. The Court reasoned that Yahoo! could exclude the IP range of Belgian Internet Access Providers from its servers if it believes it is not capable of complying with Belgian legal obligations or if it considers it does not need to comply with these obligations for alleged privacy reasons. By doing so, Yahoo! would become unreachable as an economic entity within Belgian territory. The fact that Yahoo! does not choose to exclude the IP range, is thus clearly for economic reasons. Thus, the Court concluded that Yahoo! should comply with Belgian laws.

The duty to cooperate pursuant to article 46bis C.C.P. extends to any ISP that provides services and is available in Belgium. Nowhere is it defined that the operator or provider needs to have its registered office in Belgium, nor is any distinction made regarding the nationality of the ISP.

Furthermore, the Court pointed out that the requested information on the basis of article 46bis C.C.P. concerns registration of electronic traffic within Belgian territory and not content data.

2. *Yahoo! as an operator of an electronic communications network or a provider of an electronic communications service*

The Court found that **Yahoo! can indeed be regarded as an operator of an electronic communications network or a provider of an electronic communications service** as defined by article 46bis C.C.P. The Court kept its reasoning quite brief by stating that not only is Yahoo! a portal site or a search engine, but it also offers a free e-mail service. This e-mail service is one of the market leaders in the area of free providers of this service. According to the Court, the Belgian legislator also clearly envisaged such operators and providers when defining the obligations arising from article 46bis C.C.P.

3. *The applicability of ECPA - requirement of MLA procedure*

The Court stated that the **ECPA is not applicable** to electronic traffic that occurs within Belgian territory and is taking place through a service that is offered in Belgium. In this respect, the ECPA cannot undermine Belgian sovereignty in relation to criminal law and criminal procedure, as, otherwise, discriminatory treatment between ISPs established in Belgium or abroad could occur, or ISPs would be encouraged to establish their offices abroad to escape legal accountability in Belgium.

4. *Refusal to cooperate took place in Belgium*

The defence argued that their refusal to cooperate, an obligation which follows from article 46bis C.C.P. according to the Court, had not taken place on Belgian territory. The Court, however, disagreed, stating that a criminal offence is situated where an act or event occurs that is a constitutive element of the criminal offence or that is an indivisible part of it. Furthermore, the data requested pursuant to art. 46bis C.C.P. must be delivered into the hands of the public prosecutor in Dendermonde *(in casu)*, which means that there is an **obligation to deliver** the information in Belgium.

5. *Time limit within which to provide the requested data*

The Court also countered the defendant's argument that the period within which the requested data needs to be transferred is not defined. Article 46bis C.C.P. stipulates that the data needs to be provided within a time limit 'to be defined by the King'. The Court in this respect referred to the Royal Decree of 9 January 2003, implementing article 46bis §2 C.C.P., which stipulates in article 3 that the data must be communicated in real time to the investigating judge, the public prosecutor or the judicial police officer. Article 1.3 of the Royal Decree specifies that 'real time' means the 'minimum time required for the execution of a particular action in accordance with the rules of the art, without interruption and for which appropriate means and staff were employed'.

6. *Proportionality of the measure*

The appropriateness and proportionality of the measure can only be assessed by the public prosecutor. Furthermore, the Court reasoned that the protection granted by the principles of proportionality and subsidiarity is not intended for the operator or the provider, but for the persons whose identification is pursued by the measures taken in the investigation.

7. *Moral element of the criminal offence*

The moral element of this alleged criminal offence only requires general intent, namely committing an act, knowingly and willingly, that is conscious and well informed. The defence wrongfully asserts that the intent and the moral element should be interpreted as the 'wish' to commit an offence. The Court disagreed with this view and argued that the general intent implies that the non-provision of the data, despite the fact that the provision thereof was mandatory, involves a refusal. Consequently, the moral element was indeed met.

Determining the penalty

The Court took several elements into consideration when determining the sentence.

The facts were found to be objectively grave. Given the increasing importance and use of electronic communications and electronic data exchange for committing criminal offences, the Court considered the cooperation from ISPs and other Internet players an essential link in the chain of crime prevention. A refusal to cooperate by not providing data, while under obligation to do so, is proof of a disloyal attitude and should be penalised severely. Yahoo! tested the limits of the law by being persistent in its refusal. Such attitude should be reprimanded severely, according to the Court.

The penalty should not only serve the need for retribution, but also the purpose of special and general prevention. The punishment imposed had to be of such a nature that it would deter the accused from committing such acts in the future and encourage the accused to show respect for the obligations that serve the general interest.

The Court also took into account the lack of a criminal record of the accused, as well as the size of the company.

Restitution/fine for delay in restitution

Article 44 of the Belgian Criminal Code determines that the penalty is pronounced, without prejudice to the restitution. Restitution is intended to terminate an unlawful situation, which in this case means the provision of the data requested by the public prosecutor. The Court agreed with the claim of the public prosecutor to impose a fine for delay in restitution. To produce any effect, this fine needed to be sufficiently high.

The ruling of the court

In view of abovementioned considerations, the Court of First Instance of Dendermonde declared Yahoo! Inc. **guilty** of the criminal offences mentioned in the indictment and ordered Yahoo! to pay a fine of EUR 55 000. In addition, the Court ordered Yahoo! to supply the requested data, subject to a fine of EUR 10 000 per day for delay in communicating the data.

APPEAL

An appeal was lodged against the judgement of the Court of First Instance in Dendermonde:

- On 4 March 2009 by Yahoo! Inc. against all the decisions;
- On 12 March 2009 by the Public Prosecutor's Office against Yahoo! Inc.

Procedure: Court of Appeal Ghent

Date of decision: 30 June 2010

Introduction

The Court of Appeal, although it touched upon the location of the criminals at the time of creation of the e-mail accounts as well as the location of the office of Yahoo! Inc. (USA), did not take a stand regarding the jurisdictional competence of the Belgian prosecutor. The main focus of the Court was to assess whether or not Yahoo! is an operator of an electronic communications network or a provider of an electronic communications service.

Court reasoning

The Court of Appeal considered that the public prosecutor did not indicate in which capacity Yahoo! was being prosecuted (i.e. as an operator of a network or as a provider of a communications service). Moreover, it found the accused credible in its assertion that the Yahoo! free webmail system essentially consists of providing a software application that allows the user to obtain a Yahoo! e-mail address to send and receive messages from any location. According to the Court, this assertion had not been plausibly refuted by the public prosecutor in this case at any time.

Following these considerations, the Court elaborated on the general aspects of sending messages through electronic communications networks. The Court began by presenting some relevant concepts as defined by Belgian law, such as 'electronic mail', 'email strictu sensu' and 'electronic communication'; definitions for which it also referred to the European Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. In relation to these concepts, the Court stated that, in principle, an electronic message is not directly transmitted from the sender to the receiver, but is realised through intermediary communications services (ISPs, providers of specific email services or mobile networks).The sending and receiving of an e-mail is done through mail servers. The e-mail client, i.e. a program that is used for sending and receiving e-mail through a mail server, makes an e-mail account with a linked e-mail address available to the e-mail users.

After this elaboration of general concepts, the Court continued with the elements of the current case.

1. *Created and used email accounts - location*

With respect to the e-mail accounts used by the criminals, the Court reasoned that these were issued and allocated by Yahoo! to several persons. Moreover, the Court found credible, and at least insufficiently disproven to its satisfaction, that these e-mail accounts were requested and created upon the request of persons who were not located in Belgium at that time. Following from this finding, at the time of application and granting of these accounts, the third-party applicants probably did not make use of operators of a communications network or the services of a provider of an electronic communication service established in Belgium. The accounts, as such, belonging to Yahoo! are located within US territory, within a webmail system managed there by the accused.

2. *Presence of Yahoo! on Belgian territory*

The Court of Appeal argued that the identification data requested by the public prosecutor were located in the USA, on the electronic equipment and webmail system owned by the accused. These identification data cannot be consulted or viewed from Belgian territory. The Court did not follow the public prosecutor in his argumentation regarding the presence of Yahoo! on Belgian territory. It found that **any establishment, place of business or real seat of the accused within Belgian territory had not been credibly established**. Yahoo! also does not employ any staff in Belgium. The fact that the public prosecutor can reach the portal site of Yahoo! electronically from Belgium is only the result of the use made of existing public networks, interconnections and service providers of electronic communications via the Internet. According to the Court, it has not been sufficiently established in the case that Yahoo!, either as a network operator or as a provider of a communications service, plays any role or acts as an intermediary in the transfer of data from Belgium to the portal site of Yahoo!. The Court continued by stating that even if a foreign company is visible on a computer screen in Belgium, this company cannot therefore be deemed to be present on Belgian territory and perform activities falling within the scope of article 46bis C.C.P.

3. *Yahoo! as an operator of an electronic communications network or a provider of an electronic communications service*

As to the question whether Yahoo! can be regarded as either an operator or a provider, the Court of Appeal was of the opinion that hardly any attention was paid to the technical aspects of this case during the preliminary examination.

The Court referred to the definitions of 'electronic communications network' and 'electronic communication service' as stipulated in the Belgian Law of 13 June 2005 on electronic communications:

- '*Electronic communications network*: the active or passive transmission systems and, where appropriate, switching or routing equipment and other resources which permit the transfer of signals by wire, radio, optical or other electromagnetic means, provided they are used for the transmission of signals other than radio broadcasting and television.
- *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 communications, except (a) services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, except (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[s] and excluding (c) radio broadcasting and television.'

The Court noted that the Law of 13 June 2005 on electronic communications constitutes the transposition into Belgian national law of several EU Directives. Furthermore, the Court found that the legislator's intention was clearly to use the same terminology in article 46bis C.C.P. as in the Law of 13 June 2005. Thus, the meaning of the concepts of 'operator of an electronic communications network' and 'provider of an electronic communications service' in both legal provisions is the same.

According to the Court, the path to the portal site of the accused is provided through existing networks and services, owned or operated by persons other than the accused. Yahoo! solely uses the infrastructure and existing communications ('networks' and 'services' within the meaning of article 46bis C.C.P.) for purposes of its webmail service. This webmail system should be considered as a network application/software, which is not intended to create and preserve network connections and network transport. As stated by the Court, no proof was provided that the accused intervenes in the transmission of data communicated from the e-mail accounts. It is the provider of Internet access who is integrally responsible for the actual transport or transfer of signals over the Internet. This Internet Access Provider is the provider of an electronic communications service as mentioned in article 46bis C.C.P. Nowhere has the accused, as a mere provider of webmail, been established to have had control over the electronic communications service offered or over the electronic communications network. Likewise, no indication has been given that Yahoo! is, in this instance, the company responsible for the management of the network or the infrastructure and with control over it. Therefore, the provision of a webmail

system, as developed by Yahoo! and made available to the users of the Internet, cannot be qualified as an electronic communications service in accordance with Belgian law.

Consequently, the Court concluded that **it had not convincingly been established that the accused would have to be considered as an 'operator of an electronic communications network' or as a 'provider of an electronic communications service'** within the meaning of article 46bis C.C.P. Therefore, the material conditions for applying article 46bis C.C.P. were not fulfilled according to the Court of Appeal.

The ruling of the court

The Court of Appeal in Ghent annulled the appealed judgment and **acquitted** Yahoo! Inc. from prosecution concerning the fact described in the introductory summons.

APPEAL

An appeal was lodged against the judgment of the Court of Appeal in Ghent:

- On 12 July 2010 by the Public Prosecutor's Office against all the decisions.

Procedure: Court of Cassation

Date of decision: 18 January 2011

Court reasoning

Admissibility of the appeal

The defendant pleaded that the appeal was inadmissible. It claimed that the appeal was only directed against the decision of the Court of Appeal relating to the concepts of 'operator of an electronic communications network' and 'provider of an electronic communications service', and not against the Court's decision that Yahoo! is not present in Belgium. Moreover, the assessment of the capacity of the defendant (i.e. operator or provider) is an assessment of facts, which does not fall under the competence of the Court of Cassation (being competent for verifying the interpretation of the law).

The Court of Cassation, however, found that the Court of Appeal did not take any decision on the competence of the Belgian judicial authorities, except in the context of the assessment whether or not Yahoo! is an operator of an electronic communications network or a provider of an

electronic communications service. The appeal judges considered whether Yahoo! provides such services in Belgium. They did not, however, draw any conclusions with respect to the jurisdiction of the Belgian Courts. Furthermore, the appeal does not request an investigation of the facts, but rather a legal assessment of the meaning of the concepts of 'operator of an electronic communications network' and 'provider of an electronic communications service'.

For these reasons, the Court of Cassation rejected the ground of inadmissibility of the appeal.

Legal assessment

The Court of Cassation elaborated on the meaning of the concepts of 'operator of an electronic communications network' and 'provider of an electronic communications service' as stipulated in article 46bis C.C.P. The Court disagreed with the Court of Appeal's judgment that the content of these concepts in article 46bis C.C.P. has the same meaning and content as the Law of 13 June 2005 on electronic communications. In fact, the 'provider of an electronic communications service' in the sense of article 46bis C.C.P. is not only the Belgian operator within the meaning of the Law of 13 June 2005, but also any company that provides electronic communications services, including, among other things, the transmission of communications data. As a consequence, the obligation to cooperate under article 46bis C.C.P. 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 aforementioned Law of 13 June 2005 or that only provide their electronic communications services through their own infrastructure. This obligation also applies to any company that provides a service that consists wholly or mainly in transferring signals through electronic communications networks. Therefore, **someone who provides a service that consists of enabling its customers to obtain, or to receive or distribute information through, an electronic network, can be a provider of an electronic communications service.**

Based on these findings, the Court concluded that the appeal judges had not been able to lawfully decide that the defendant is not a provider of an electronic communications service within the meaning of article 46bis C.C.P.

The ruling of the court

The Court of Cassation **annulled the judgment** of the Court of Appeal in Ghent and referred the case to the Court of Appeal in Brussels.

Procedure: Court of Appeal Brussels

Date of decision: 12 October 2011

Introduction

In its ruling, the Court of Appeal in Brussels focused on the territorial jurisdiction of the Belgian authorities and the validity of the judicial order sent by the public prosecutor. The Court's reasoning, by extension, also implicitly rejects the virtual presence of Yahoo! on Belgian territory.

Court reasoning

The appeal judges considered that the Belgian government exercises its competence from and within the Belgian territory. A Belgian public prosecutor therefore does not have jurisdiction to exercise its office and conduct or order investigative measures outside Belgian territory. The Court was of the opinion that the public prosecutor did not address, within Belgian territory, any valid order to the accused to communicate information within the meaning of article 46bis C.C.P. The mere fact that reaching Yahoo! from Belgian territory is technically possible by electronic or other means of communication is not sufficient for this purpose. Hence, the **e-mails and written mail containing the judicial order, sent by the public prosecutor to the available Yahoo! (web) addresses, were not considered to be valid requests**. As a consequence, the appeal judges found that Yahoo! did not violate article 46bis C.C.P. by not complying with the request of the public prosecutor addressed to a location in the USA.

Considering the above, the Court concluded that the facts of the indictment were not proven.

The ruling of the court

The Court of Appeal in Brussels **acquitted** Yahoo! Inc. of every charge and discharged it from prosecution.

APPEAL

An appeal was lodged against the judgment of the Court of Appeal in Brussels:

- On 12 October 2011 by the public prosecutor's office against the decisions connected with the accused.

Procedure: Court of Cassation
Date of decision: 4 September 2012

Court reasoning

Legal assessment

The Court of Cassation assessed the judicial order sent by the public prosecutor to the defendant under article 46bis C.C.P. The article stipulates in §1 that 'the public prosecutor is entitled to request, by means of a motivated and written decision, the cooperation of an operator or service provider'. Furthermore, §2 of the same article determines that 'each operator of an electronic communications network and each provider of an electronic communication service, must communicate the requested information to the public prosecutor'.

The Court disagreed with the ruling of the Court of Appeal in Brussels that no valid request was addressed by the public prosecutor to the defendant. On the contrary, the Court of Cassation found that the **public prosecutor did formulate a legally valid request on Belgian territory** and addressed it, from Belgian territory, to an entity to which such a request could be addressed. The fact that the public prosecutor sends his written request from Belgium to a foreign address, in accordance with article 46bis C.C.P., does not invalidate the request.

Consequently, the Court of Cassation concluded that the decision of the Court of Appeal was not duly reasoned on the legal grounds.

The ruling of the court

The Court of Cassation **annulled the judgment** of the Court of Appeal in Brussels and referred the case to the Court of Appeal in Antwerp.

Procedure: Court of Appeal Antwerp

Date of decision: 20 November 2013

Court reasoning

Admissibility of the appeal

The defendant put forward a new ground for inadmissibility, alleging that the governmental appointment of Mr Kerkhofs, deputy public prosecutor at the Court of First Instance in Dendermonde at that time, would not have been legal. The Court of Appeal, however, pointed out that the appointment in accordance with article 326 of the Judicial Code does not provide that this decision should be taken or motivated any differently than justified by the necessities of the service. The governmental appointment refers to a letter of the Attorney General in Antwerp, in which the importance of the case and its highly technical nature are underlined. From this letter, the Court found that the needs of the service, which required this delegation, were demonstrated. The Court consequently did not find the governmental appointment illegal and therefore dismissed the defendant's claim.

Reasoning on substantive matters

1. *Presence of Yahoo! on Belgian territory*

The Court of Appeal concurred with the reasoning of the judges of the Court of First Instance with respect to the **territorial presence of Yahoo! in Belgium**. Yahoo! is indeed providing services in Belgium. In addition, the Court stated that the fact that Yahoo! offers its webmail services in Belgium is reinforced by the fact that advertising is adapted, taking into account the location and the language.

2. *Yahoo! as an operator of an electronic communications network or a provider of an electronic communications service*

The Court of Appeal found that Yahoo! can be considered as **a provider of an electronic communication service**, amongst other things because it is transmitting communication data through its webmail service. The Court based its argumentation on evidence provided by the public prosecutor, which showed that sending an e-mail from sender to receiver occurs mainly, if not exclusively (when both sender and receiver have Yahoo! accounts), via the mail servers of the defendant. This evidence constituted sufficient proof for the Court that Yahoo!, to provide its mail service, is the main or only provider responsible for transmitting signals via electronic communications networks.

The Court thus established that Yahoo! is present on Belgian territory and can be considered as a provider of an electronic communication service. Therefore, Yahoo! is obliged to comply with the requirements of article 46bis C.C.P.

3. Data to be transferred in Belgium

The defendant disputed that the requested **data needed to be transferred and 'handed over' in Belgium.** According to the defence, the public prosecutor needed to get the data. The Court, however, rejected this point of view by referring once more to the rationale used by the first judge: the offence is committed in Belgium and, consequently, Belgian legislation applies. The wording of article 46bis §2 C.C.P. clearly implies an active obligation to give the claimed data to the public prosecutor when requested.

4. Requirement of MLA procedure

The Court continued its reasoning by adding that a lengthy **MLA procedure** (as implied by the defence) was **unnecessary** in this case given the Belgian jurisdiction. Moreover, the Court added that MLA was also not required under American legislation in the current situation.

5. Legal validity of the judicial order

Contrary to the Brussels Court of Appeal, the Court also found that the public prosecutor asked Yahoo! in a **legal and valid manner**, via e-mail, fax and letter, for the data in relation to the e-mail accounts used in Belgium. The Court mentioned that article 46bis C.C.P. does not require any fixed form in this respect.

6. Moral element of the criminal offence

As to the intent of the defence, the violation occurred knowingly, and Yahoo! refused systematically to provide the requested data, satisfying the Court's criterion of intent.

Considering the abovementioned arguments, the Court of Appeal concluded that the facts were proven.

The ruling of the court

In view of the abovementioned considerations, the Court of Appeal in Antwerp confirmed the judgment of the Court of First Instance, thereby declaring Yahoo! Inc. **guilty** of the criminal offences mentioned in the indictment. Yahoo! was ordered to pay a fine of EUR 44 000, with suspension of execution during a period of three years from the date of the Court decision of the amount of EUR 22 000; so that EUR 22 000 remained active.

The Court did not order the restitution and the accessory daily fine (taking into account the fact that the public prosecutor no longer insisted on restitution).

APPEAL

An appeal was lodged against the judgment of the Court of Appeal in Antwerp:

- By Yahoo! Inc. against all decisions.

Procedure: Court of Cassation

Date of decision: 1 December 2015

Court reasoning

Legal assessment

1. *Extraterritorial jurisdiction*

The defendant argued before the Court that the compulsory obligation for it to cooperate under article 46bis C.C.P., as a US-based company, entailed unlawful extraterritorial jurisdiction. It therefore claimed a violation of Article 2 §1 of the Charter of the United Nations, determining the sovereign equality of States, and Article 46bis C.C.P., as well as a misjudgment of the rule of customary international law stating that a State in principle has no extra-territorial jurisdiction.

With regard to the interpretation of the law, the Court of Cassation stated that, in general, a State can only impose coercive measures on its own territory with a view to enforcing its laws. A sufficient territorial link between the measure and the territory needs to be present. Such a link is determined by the nature and the scope of the coercive measure. The Court continued by asserting that the obligation, imposed under article 46bis §2 C.C.P., for operators and providers to cooperate is indeed a coercive measure. The measure is, however, limited in scope, as it does not require the presence of Belgian authorities abroad or any material action outside Belgian territory. Moreover, the offence in the sense of article 46bis §2 C.C.P is committed in the place in which the requested data need to be obtained and received. Therefore, the place in which the operator or provider has established his office is irrelevant to the fact that the crime is punishable in Belgium. Two conclusions can be drawn from the preceding argument: (1) the **measure** consisting of the **obligation for operators or service providers who are economically active in Belgium (*see infra*), to provide such data** is **taken on Belgian territory**; and (2) a judge who convicts an operator or service provider established abroad for denying to comply with this obligation coerces **compliance with a measure taken in Belgium**. Consequently, **no extraterritorial jurisdiction was exerted**. This interpretation is the only correct interpretation of the law; any other interpretation, as given by the defence, is unlawful.

In respect to the presence of Yahoo! on Belgian territory, the Court concurred with the reasoning of the appeal judges and found that **Yahoo!, as a provider of a free webmail service, is indeed present on Belgian territory** considering it actively participates in Belgian economic life by

using the .be domain, showing publicity in the local language and being reachable in Belgium for users via a complaint mailbox and a FAQ desk. Likewise, the Court referred once more to the reasons given by the Court of Appeal to conclude that they did not exercise extraterritorial jurisdiction by declaring Yahoo! guilty and condemning it for violating article 46bis §2 C.C.P.

Therefore, the Court did not accept the defendant's legal remedy.

2. *Requirement of MLA procedure*

The second legal remedy brought by the defence is a violation of article 17.1 of the Convention agreed upon between the Kingdom of Belgium and the United States of America concerning judicial cooperation in criminal matters of 28 January 1988, and of article 46bis C.C.P. According to Yahoo!, the public prosecutor should have followed the procedure as laid down in article 17.1 of the Convention, which stipulates that all requests for legal assistance should be sent and executed via a central authority of each of the countries, the central authority for Belgium being the Minister of Justice and the central authority for the USA being the Attorney General or his/her representatives. As the prosecutor did not send his request via the US central authority, the defence argued that the request of the prosecutor consequently lacked legal (coercive) effect.

This legal remedy was inferred from the first legal remedy claiming unlawful extraterritorial jurisdiction, which was rejected by the Court as it was based on a wrong interpretation of the law. The Court therefore declared the second legal remedy inadmissible.

The ruling of the court

The Court of Cassation **rejected the appeal**.

CONCLUSION

After the seven court rulings, all legal remedies have been exhausted in this case. Hence, following the ruling of the Court of Cassation, the judgment of the Court of Appeal in Antwerp, which found Yahoo! Inc. guilty, became the final decision in the Yahoo! case.

Thus Yahoo! Inc. was found guilty of violating article 46bis §2 C.C.P. by having refused, in the capacity of provider of an electronic communications service from whom the public prosecutor required the communication of the data referred to in paragraph 1 of article 46bis C.C.P., to communicate the identification data to the public prosecutor.

The Court ruled in this case:

In relation to substantive law, that:

- Even without having an office established in Belgium, Yahoo! is indeed (virtually) present within Belgian territory
- Yahoo! is a provider of an electronic communications service
- Article 46bis C.C.P. was applicable in this case, which also entailed that Yahoo! was required to transfer the requested data to the public prosecutor in Belgium and that Yahoo!'s refusal to cooperate took place in Belgium

In relation to procedural law, that:

- The judicial order sent by the public prosecutor to Yahoo! in the USA on the basis of article 46bis C.C.P. was legally valid
- The public prosecutor, by sending his judicial order to a service provider in the USA on the basis of article 46bis C.C.P., did not exercise any extraterritorial jurisdiction, and, as a consequence, the public prosecutor was not required to follow the MLA procedure for sending his request

The Court's interpretation in relation to the jurisdiction of the Belgian prosecutor in this context is quite interesting. The Court considers that the prosecutor's direct request to a foreign ISP to provide ('bring') data without having to send an MLA request is a mere implementation of Belgian jurisdiction on its own territory, given the fact that the crime happened on Belgian territory and the public prosecutor therefore was competent to act and request measures from and within Belgian territory. At no time did the prosecutor act extraterritorially.

IV.ii. Interview with Jan Kerkhofs

Jan Kerkhofs is a Federal Magistrate in the counter-terrorism and cybercrime unit of the Belgian Federal Prosecutor's Office in Brussels. He deals with federal and international terrorism and high-profile cybercrime cases on a daily basis, with a special focus on online investigation techniques and trans-border gathering of digital evidence and traces.

Previously, Mr Kerkhofs was Public Prosecutor in the District of Dendermonde, Belgium, specialised in cybercrime, special investigation methods and serious organised crime, and was appointed as the leading magistrate in matters of cybercrime for the region of East Flanders.

Mr Kerkhofs is a nationally and internationally recognised cybercrime expert. He is a member of the Belgian Cybercrime Expertise Network (Belgian National Cybercrime Taskforce) and the Belgian National Platform on Telecommunication. He is a government expert and advisor in matters of cybercrime, counter-terrorism and special investigation methods. He is also assigned as expert of the Belgian delegation in the Convention Committee on Cybercrime (T-CY) of the Council of Europe. He is a magistrate-cybercrime expert for the BCCENTRE (Belgian Cybercrime Centre of Excellence for Training, Research and Education). He is trainer at the National Criminal Investigation School of the Belgian Federal Police and is co-responsible for the training in cybercrime of newly appointed magistrates and specialised magistrates at the Belgian Judicial Training Institute (IGO). He also gives training in counter-terrorism and cybercrime matters for several law enforcement agencies, bar associations and international institutions (Council of Europe, TAIEX, ERA, EJTN, ICCT). He publishes regularly on the subject of cybercrime and is, together with investigating judge Philippe Van Linthout, the author of Cybercrime, the Belgian handbook and field manual on the topic.

➢ **Why did you initiate judicial proceedings against Yahoo?**

Yahoo! was a provider that adopted a policy of not providing basic subscriber information without an MLA request. Microsoft, having an office in Brussels, cooperated quite well ; Google - with no offices in Belgium- also cooperated in similar cases; and Facebook has a portal on their servers where Belgian law enforcement authorities can upload warrants that are prioritised and dealt with by Facebook staff in the USA.

We did not understand this; why an Internet player, being omnipresent and omnipotent, would on the one hand want to propagate that it is universally present around the globe, but, on the other hand, when requested to respond to Belgian justice, claims that it is located and only present in the USA? When you open your computer and go to www.yahoo.com, you'll notice that Yahoo! is in your country, offering services and doing business customised to your citizens and region.

We initiated criminal proceedings against Yahoo! at the moment when it was clear that they refused to cooperate in a direct way – without MLA – in supplying basic subscriber information. I don't think that they expected that we would indeed follow through and sue them. I didn't go solo, though. My superiors within the Public Prosecution Service in Belgium shared my point of view on the jurisdictional competence in this case and agreed to proceed with the prosecution.

➢ **What was your reasoning when prosecuting Yahoo!?**

At that time, we could not base our argumentation on the Convention on Cybercrime (C.C.) [which entered into force in Belgium on 1 December 2012], but I actually applied the same philosophy, i.e. more specifically, the principles laid down in article 18 of the C.C., determining that 'a service provider offering its services in the territory of the Party' needs to comply with a production order of that Party. This is exactly how article 18 C.C. needs to be interpreted and applied.

In Belgium, we have an article (46bis) in the criminal procedure code that states very clearly that every operator and service provider of electronic communications is obliged to respond to a request for basic subscriber information from a prosecutor or judge. With regard to the question whether or not Yahoo! was an 'operator or service provider…', this was a firmly debated judicial thesis at the time. I had few fans along the way, mainly only from law enforcement. The academic world had quite a strong and different standpoint on the notions of operator and service provider, as well on as the need to send an MLA request to obtain data. According to them, the jurisdiction cannot be 'activated' outside Belgium without MLA. However, it was our standpoint that the coercion does not come from our judicial powers, it stems from the law, and Yahoo! voluntarily accepted that law and our Belgian jurisdiction by providing services on Belgian territory. In that perspective, it's not up to the prosecutor to go and get it abroad with MLA, it's up to the ISP to bring the basic subscriber information in the prosecutor's hands; so why should we ask for mutual legal assistance if we don't need it legally?

➢ **Did you ask the US authorities for their point of view?**

The US Department of Justice itself stated that it did not have any issue with direct requests to and cooperation with US-based ISPs; as this is even stipulated in US legislation. ISPs are free to create their own policy in this respect. Defense lawyers, during the court proceedings in Antwerp, stated that MLA with the USA worked well in practice at that time (2008-2009). I then

asked for an expert opinion on the timeframe needed to receive a reply to such an MLA request sent to Yahoo!: on average between 23 and 52 weeks! If you consider the data retention rules we had at that time in Europe, then receiving data 52 weeks later is useless. The US DoJ was and is always cooperative, but since they have a very large number of major Internet players on their soil, they are confronted with a massive workload to serve the whole world. It was therefore unacceptable that a US-based provider such as Yahoo! had a policy to redirect every Belgian request for something so mainstream as basic subscriber information through this bottleneck, in disrespect with Belgian law.

- **Was the initial criminal case -online purchases with defrauded credit cards- eventually successfully resolved?**

No, the case was dismissed. Indeed, the investigations stalled because due to the fact that we could not continue without the information from Yahoo!

- **Are you fully satisfied with the outcome of the Yahoo! case?**

Yes. The Court of Cassation unequivocally took a stand on how it perceives jurisdiction and territoriality, and how this jurisdiction can have an effect across borders.

For the legislator and countries that guard their sovereignty (as well as for some academics), the earth is flat for ages. The problem is, however, that when you look through the telescope, you see it is a globe. The reality is today that we have to apply legislation that is produced for a flat earth, which does not work well for the cyber globe. So you have to interpret and apply the legislation in a way compatible with a round earth, as did the Court of Cassation.

- **Is it necessary to develop new international legislation to regulate jurisdiction in cyberspace or is it feasible to address this nationally by interpreting domestic legislation?**

It would be great to agree on this at international level, but even at EU level it would already be difficult. And we need to have the USA on board because all the big providers are based there.

The Budapest Convention, signed and ratified by many countries, was ahead of its time and is still quite time resistant. It would be good if those countries at least could already agree to trust each other in their cooperation and for example agree that foreign authorities can directly request information from providers on their territory. But this is not that simple, because you have several legislative principles that differ even between the Parties to the Convention (e.g. freedom of speech, 4th Amendment, etc.). So there are many differences. Moreover, what do you do with countries that are not Parties to the Convention? How do you determine jurisdiction then?

Jurisdiction is based on national sovereignty. However, you cannot apply classical jurisdiction principles in a vacuum called cyber. You cannot stop bits and bytes at the border. Jurisdiction in cyberspace can therefore only exist as a global concept where you make agreements internationally on how to apply it. Thus in a way you disregard the traditional notion of jurisdiction, but you agree among each other how jurisdiction will apply.

The Cybercrime Convention has article 18 and each of the Parties should have similar legislation adopted in line with this article. Indeed, in relation to other topics such as remote searching and

access to computer systems, also the explanatory notes of the Convention, such as article 293 do not even oppose to jurisdiction with an extraterritorial or a cross border effect. It is simply not clearly defined how to apply it because it was too difficult to regulate this in 2001. We are not of the opinion that we did anything wrong or acted unilaterally in the Yahoo case; it was a territorial issue that was solved territorially. This however does not mean we've found the solution; I merely kicked a tree until an apple fell out in order to prove gravity. But I didn't invent gravity and I realise that same gravity can cause avalanches.

I'm well aware that the day may come that a direct request from a prosecutor would be addressed to a Belgian operator or service provider to provide subscriber information on a person who has insulted the King of a country where this offence is punishable with a death sentence; what would we do then? This hypothetical situation would just be another confirmation of the fact that the earth is a globe, and we have to deal with the situation as it is and look for possible solutions.

You will never get everyone aligned. Look at Eurojust' s work; concluding a JIT between two civil law countries is fairly easy, but try to do the same with common and civil law countries and you have to agree on how you can cooperate and exchange and use evidence consistent with two very different legal law traditions.

- **Referring to the assessment of the proportionality which Yahoo! used in its defense, what is your opinion on the assumption of service providers and operators that they have a say in this?**

ISPs doing business in Europe should be obliged to have an office in Europe and store data there, so that they have to comply with European legislation and not have to do the double criminality check anymore, and not have to deal with different judicial frameworks. If you allow freedom of business to be combined with choice of jurisdiction, providers – as all other people – will use it to their profit.

Yahoo! accepted Belgian jurisdiction by offering services in Belgium, so they have to obey. By entering Belgian territory, they have thus themselves limited their policy, for which they have maneuvering space in US legislation.

- **Should Europe take more action or guide the development of European regulations in this area?**

Yes urgently, but not only in terms of conventions. We should think out of the box – but always within the law - and combine technical possibilities with legislative framework. Currently the www stands for 'world wild west'. The Internet has developed in a way that we underestimated. Ninety per cent of Internet traffic is spam but it is filtered out. But no management board controls the Internet. Why shouldn't we have a possibility to exclude and shut off a dirty Internet player who does not want to obey the rules? These players are also harmful for ISPs that do comply with the rules and stick to minimum norms. Providing services without notifying where they are located and not working according to the rules should simply not be possible. We don't allow that situation in the analogue world; why should we allow it in the virtual world?

➢ **Did the Yahoo! case have an impact in Belgium?**

Yes, Skype is currently being prosecuted before the Court of First Instance in Mechelen for not complying with an order of the investigating judge to intercept Skype communication offered on Belgian territory. Initially Skype was located in France. Apparently there were some differences with the French government; I've understood that there were also some issues about the question to what extend Skype should be capable of serving justice when it's needed. Skype eventually closed its office in France itself and moved to Luxembourg. It could be a good idea for the EU to take initiatives in these matters to avoid 'forum shopping' of some service providers.

➢ **Are there other providers or operators working in the same way?**

Actually, you would think that operators would be on their guard, but, for instance, Microsoft, with which we had good direct cooperation in the past, has reduced its cooperation in general. Now they only provide the Belgian IP addresses and require an MLA request for other 'foreign' IP addresses. I think this shift in cooperation probably resulted from the fact that Microsoft was criticised for being so cooperative with US Intelligence agencies and law enforcement. In that respect the release of the Snowden-files is the worst thing that could have happened, as law enforcement and the judiciary pay a high price now. Microsoft and other operators moved servers to Ireland, and privacy became a product, not a concern. They now can say to customers: 'we have put our servers in Ireland, which has very strict data protection rules where some intelligence services cannot access them'. As a result, it already happened that Microsoft USA refers us to Microsoft Ireland because they say the requested information is stored on servers in Ireland. So, we have to do the MLA all over again, all because a service provider decides to choose jurisdiction arbitrarily.

➢ **Don't the service providers acknowledge then that they have an obligation to cooperate?**

Well, they say they want to cooperate but that they do not have the obligation to do so. According to them they are nicely cooperating voluntarily, according to us they are obliged to cooperate. But even if you would succeed in convincing every provider to fully cooperate, there will still be the data retention issue. So, even if you would create a framework, international or European, for cooperation with ISPs, if you do not oblige them to retain data, they will not have or keep anything to share.

➢ **In fact, you are saying that the European Union should work on data retention regulations again?**

Yes. However, the problem would still persist that the USA does not have data retention rules. But you could fine tune cooperation and data retention at EU level and regulate that all ISPs providing services in the European Union have to comply with these rules. You could work with an economic license framework where you define what the providing of electronic communications services within the European Union. is, and ISPs offering services within the European Union need to have an EU license and store EU data on EU territory.

➢ **What was the impact at EU or international level of the Yahoo case?**

The case mostly sparked people's interest; it gives food for thought and goes against some conventional ways of thinking. The biggest merit of the case is that people are discussing the case, even at EU and international level; for example, last March, at the EU conference in Amsterdam on jurisdiction in Cyberspace and cooperation with ISPs. Even in Sri Lanka, which ratified the Budapest Convention most recently, they were very interested in the Yahoo! case and the vision behind it.

The concrete impact of the Yahoo! case is that, independent from me, others are now also prosecuting Skype and addressing Microsoft with tough questions in Belgium; and it could trigger other countries to initiate criminal proceedings against ISPs. We also receive requests from numerous other States to send them the case information so they can see how they could approach it. In the end, if everyone starts to address or prosecute these ISPs in a similar way, then some things might start to move and you could create a negotiation position for authorities.

We therefore also warmly call upon other authorities to initiate similar proceedings; not necessarily having the same ideas as we have on jurisdiction, but at least to see how national jurisdiction can have extraterritorial consequences in the sense that a 'non-resident' can be compelled to cooperate. The keywords here are 'voluntary acceptance of jurisdiction' by doing business in a country. To give a comparison: if a US truck driver would drive on a Belgian highway, he could be stopped by the Belgian police; if he would then refuse to hand over his papers and driver's license, saying that all the requested data is stored on servers in the USA, we would not take no for an answer. Why should this be different for the Internet? If a service provider wants to do business in Belgium but does not want to accept Belgian jurisdiction, he should consider excluding the Belgian IP-range from its services and ultimately stay out. This is also what the Court of Appeal of Antwerp confirmed in the Yahoo! case.

➢ **Do you expect that other service providers could be in trouble then?**

Service providers are only in trouble if they choose not to live up to the laws to which they are subjected to. You don't have to be a clairvoyant to see that some services could fall within the scope of the Yahoo! jurisprudence. Take Telegram or Whatsapp, for example. If you see what Whatsapp recently communicated to the public on end-to-end encryption, which is really scary! The product is commercialized as a communication safe haven for everyone, included everyone with bad intentions. It is also shocking that Telegram provides the same services and we do not even know where they are, who they are and where they can be held liable. In Belgium, as well as in almost every other EU Member State, the standards for our national Internet access and service providers are very high. They have to meet numerous legal obligations, technical standards, etc. And then, suddenly, there come these 'internet cowboys' who provide a similar communication service from somewhere in the world without offering any standard and without any concern about public safety or criminal safe havens. Is that fair for those who have to follow the national and European laws? Anyway, I prefer privacy to be in balance with security and safety.

➢ **According to you, where should be the balance between the right to privacy and the need for authorities to protect people's security?**

The last time I checked the European Convention on Human Rights, the right to privacy was still below the article stipulating the right to life.

When I am giving cyber-training and we are discussing data retention and access to data, I sometimes hear people stating that:

'Privacy is of utmost importance and one should not have to worry about being watched by the government. If that then means that you have to live with the fact that some events can happen, that is a compromise you have to make in a democratic state.'

I can get angry when I hear those things. I wonder whether they would repeat it while looking their wife and kids in the eyes and literally saying that they are worth sacrificing at the altar of privacy. It is always easier to be a privacy fundamentalist if someone else's children pay the price. It is easy to do rabble-rousing. I also find privacy important; I guard it every day and took an oath for it. If you would give people the option to choose between preventing a terrorist attack the next day but agreeing to wiretap all telephone lines; or the terrorist attacks to take place without intruding their privacy; what do you think they would choose? The problem is that you have to make those choices in a moment when there are no bombs exploding. Sometimes I wonder if the Data Retention Directive would have been invalidated in the current climate of imminent terrorist threat.

Striking the right balance is very difficult, but it starts with believing in the constitutional State. A democratic State has three components: democracy, rights and the rule of law. Prosecutors and judges took an oath that they will protect your rights and the rule of law. Privacy can only be intruded under constitutional, legal and judicial protection. If you believe in a democratic constitutional State, you should also give your confidence in the judiciary and confident that no one is out to get you for no reason. Don't deprive the judiciary of the tools to do their job just because you are afraid of a dictatorship.

- **How can one explain the different court rulings in this case?**

Definitely at national and EU level, this case was about taking steps in fresh snow without knowing which path was underneath. It was searching for the law and how to apply it. It was the first time that courts were asked how jurisdiction and a production order must be evaluated in an international cyber context. The opinions on these issues differed enormously, not only among magistrates, but also within the academic world. The first judge has delivered great work in all sections of the judgment. Two Courts of Appeal didn't agree with the first judge. The Court of Cassation proved to have a very clear and consistent view on the subject and annulled subsequently the first and second acquittal of Yahoo!. Finally, the Court of Appeal of Antwerp confirmed in the third retrial the judgment of the first instance court.

In the past seven years I have been involved together with expert-colleagues in the national and international training of magistrates in cybercrime. We can still count the number of Belgian court judges we've met in cybercrime training on my two hands. It seems to be very difficult for them to attend a three-days training since they have to guarantee their consistent presence in court. Nevertheless, these are the judges that have to judge high profile cybercrime cases and issues. Prosecutors and more and more also investigating judges are asking for cybercrime training because they are confronted with certain requests such as communication and data interception on the Internet, and they need to know how this works. So training of judicial authorities, i.e. prosecutors, investigating judges, but also court judges is essential to make sure they know what they are dealing with and talking about. Your prior knowledge on how to repair a 1996 Volkswagen, will not serve you when dealing with a 2016 Tesla.

V. The Way Ahead

The *Cybercrime Judicial Monitor* will be distributed during the Eurojust strategic seminar, *Keys to Cyberspace,* scheduled to take place on 2 June 2016. It can also be accessed on the restricted website of the future European Judicial Cybercrime Network.

If found useful, practitioners are encouraged to send relevant national legislative developments, court decisions and information to Eurojust for future issues of the *Cybercrime Judicial Monitor*.

We welcome your feedback on this first issue and suggestions on topics to include in upcoming issues.

Eurojust June 2016

Catalogue number: QP-AG-19-001-EN-N
ISBN: 978-92-9490-358-7
ISSN: 2600-0113
DOI: 10.2812/48013