Brave new world: telecommunications data in detecting and prosecuting crime and the right to privacy

ARTEMIS CHATZISTAVROU
Lawyer, Athens Bar Association | Defense, Special Tribunal for Lebanon | LL.M. UNICRI

Act 1

"O brave new world"
William Shakespeare
(*The Tempest,* Act V, Scene I)

Had this famous line been written for today's world, the main points of exclamation would have been technology and its advancements along with crisis and its fall-backs. The latter should not be seen though as simply affecting economic structures. The crisis has equally affected our social, cultural, and moral structures and has visible impact on criminal behaviour and delinquency. Already in 2011, the United Nations (UN) Office on Drugs and Crime in its report *Monitoring the Impact of Economic Crisis on Crime* found that "economic factors play an important role in the evolution of crime trends" with statistical modelling suggesting a relationship between economic changes and at least one of the crimes of intentional homicide, robbery, and autotheft.[1]

At the same time, criminal methods are evolving, particularly with the assistance of information and communication technology. Cyber-

[1] UN Office on Drugs and Crime, *Monitoring the Impact of Economic Crisis on Crime*, 2011, executive summary.

crime walks hand in hand with traditional crime, forming the new category of "cyber-enabled crime".[2] However, this paper will not address the trending criminal modus operandi; instead it will examine how technologically advanced methods of crime prevention, detection, analysis and prosecution function and what challenges such methods present for the right to privacy.

A homicide, a terrorist attack or an auto-theft is committed: instinctively it is assumed that the perpetrator(s) must have had at least a classic mobile phone – even old-fashioned – either in use or simply in possession. Such an assumption can be confirmed by recent figures of the International Telecommunication Union according to which 99.7% of world's population has a mobile-cellular telephone subscription.[3] The relevance between crime and telephone usage may not be immediately apparent but takes shape when related to crime detection.

In the usual course of their commercial enterprise, the telecommunication service providers collect data from the mobile phone activity within their network with a view to serve their commercial purposes. By way of illustrative example, billing, profit making or system managing would not be possible without the collection of such data. It is evident that this data is collected and retained with a very specific and limited purpose. However the collection of data has reached such an extent that it is reasonable to claim that "in 2016 it would seem that much more data is held on the individual by corporations than that held by the state".[4]

The state, realising the vastness of this pool of information and its potential usefulness for other purposes, has begun requesting and ob-

[2] See http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime, last accessed 11 November 2016.

[3] International Telecommunication Union, 'Key 2005-2016 ICT data for the world, by geographic regions and by level of development, for mobile-cellular telephone subscriptions'.

[4] UN Office of the High Commissioner for Human Rights, 'Report of the Special Rapporteur on the right to privacy', Joseph A. Cannataci, A/HRC/31/64, 8 March 2016, para. 9.

taining access to telecommunications data – call data records in particular – with a view to assist criminal investigations or to use them as evidence in judicial proceedings. The following circular phenomenon is observed: citizens through their subscription to telecommunication service providers and the use of mobile phones provide their data to these companies. The latter provide them to governmental institutions, who in turn use them against a certain number of citizens (suspects, accused) for the security of the majority of citizens; but also to the detriment of their right to privacy.

Crime detection, prevention and prosecution seem new – brave new. However, this bravery is clearly affecting an old concept: the right to privacy. As it has been emphatically stated "[p]rivacy has never been more at the forefront of political, judicial and personal consciousness than in 2016".[5]

Putting aside the contractual expectations of the subscribers to the telecommunications service providers, mobile phone users also have a reasonable expectation of respect to their privacy rights. The collection, retention and further use of call data records and of any accompanying personal data contain information that affect the right to privacy of those whose data has been recorded. Since the subsequent use of data surpasses the limited initial commercial scope of their collection, there is a need for regulation of this practice on a clear and solid legal basis. The mere fact that such information may assist and facilitate crime prevention and detection and judicial proceedings does not automatically legitimise it. As a significant number of the world's population has a mobile phone subscription, the data collected will most likely relate to people that have no connection to any crime. Any ordinary citizen's telecommunication records could end up being analysed by investigators in a manner that could be excessively intrusive, disproportionate, and even unnecessary. Recently, the problematic of the collection of call data records was described by the UN High Commissioner for Human Rights as a very serious interference with the right to pri-

[5] Report of the Special Rapporteur, para. 48.

vacy.[6]

This paper will firstly make an effort to define the two major components at stake: telecommunications data records collected and used for crime detection and prosecution and privacy. The latter will be further analysed in relation to the relevant existing general legal framework about its core notion and its limitations. Recent practice in domestic and international level will shed more light by focusing on the interplay specifically between the use of call data records as evidence and privacy. There remains, however, a question though to be answered: are we brave enough?

Act 2: Defining Bravery

1. *Telecommunications data*

Before embarking on further discussion, it is important to define which data is described by the term telecommunications data that is usually requested from the telecommunication service providers and used for investigation and prosecution. At the outset, it has to be noted that this analysis does not concern the content of telecommunications or the practice of call interceptions and wire-tapping. The term telecommunications data is used with reference to the so-called "call data records" that are mere metadata linked to the mobile phone activity. In an effort to draw the line in relation to the content of the telecommunications, these are data "about the telecommunications", not the communication itself.[7] Call data records are also known under the term traffic data and comprise of the following categories of information: i) source and destination of a communication (number of the caller and of the receiver of the call; ii) date, time and duration of a communication; iii) type of a communication (voice call or Short Message Service (SMS)); iv) the International Mobile Equipment Identity (IMEI) number

[6] UN, Office of the High Commissioner for Human Rights, Report of the Office of the UN High Commissioner for Human Rights, 'The right to privacy in the digital age', A/HRC/27/37, 30 June 2014, para. 20.

[7] *Ibid*., para. 19.

that allows the identification of the communication equipment; and v) the cell tower sector that handled the communication (usually at the start of the call or both at the start and end).[8]

The telecommunications service providers maintain also files containing the predicted coverage of the cell towers of their network for system managing reasons. Such files when combined with the metadata regarding the cell tower handling the call can, under certain conditions, demonstrate even in approximation the purported location of the caller. Along with this set of data, the telecommunications providers keep databases that link the specific phone number to identifying personal data, such as names, addresses, even bank account numbers (subscribers' databases).

A combination of the traffic data, the predicted coverage and the subscribers' information can result in pinpointing a specific mobile phone and its user as being approximately located in an area at a certain date and time. It becomes obvious that such data is a powerful tool at the hands of enforcement authorities. What further militates for a cautious and regulated use is the fact that they are automatically processed when provided by the telecommunication service providers.

2. *Privacy*

CORE CONTENT

Even if there is universal recognition that the right to privacy is fundamental in the human rights arsenal, to date there is no universally accepted and binding definition of the concept. Linked to human dignity and freedom, the right to privacy guarantees that people are free from unreasonable intrusions into their lives, property and correspondence. From a human rights law theoretical perspective, it belongs to the negative rights, with its holders being entitled to enjoy this right

[8] See for example: European Union (EU), Directive 2006/24/EC 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, 15 March 2006, Article 5.

without interference emanating from the state, but also from natural or legal persons.[9] However, as it will be further explored, privacy is not unlimited. The lack of clear definition though covers both its aspects; that of its core content and that of the permissible limitations.

There exists a plethora of international legal instruments safeguarding the right to privacy. In international law, article 12 of the Universal Declaration on Human Rights[10] and article 17 of the International Covenant on Civil and Political Rights (ICCPR) provide the basic, however not binding, legal framework.[11] In particular, article 17 of ICCPR provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

With a view to interpret article 17, in 1988 the UN Human Rights Committee (UN HR Committee) issued General Comment 16. The right to privacy is described therein as encompassing a range of interests, including the privacy of communications.[12]

In its recent resolution 28/16 entitled "[t]he right to privacy in the digital age", the UN HR Committee established the mandate of the Special Rapporteur on the right to privacy for three years, emphasizing how challenging can be the protection of the right to privacy due to the rapid development of information technology.[13] Pursuant to this reso-

[9] UN HR Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), 'The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation', 8 April 1988, para. 1.

[10] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III), article 12.

[11] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, UN Treaty Series, vol. 999, p. 171, article 17.

[12] UN HR Committee, CCPR General Comment No. 16: Article 17 (Right to Privacy), 'The right to respect of privacy, family, home and correspondence, and protection of honour and reputation', 8 April 1988, para. 8.

[13] UNHRC, Resolution 28/16, 'The right to privacy in the digital age',

lution, the Special Rapporteur will report annually to the UN HR Committee, after studying trends and challenges for the right to privacy and will make recommendations in that regard.[14]

At a regional level, the right to privacy is also included in article 8 of the European Convention on Human Rights (ECHR),[15] articles 7 and 8 (in particular for personal data) of the Charter of Fundamental Rights of the EU,[16] and article 11 of the American Convention on Human Rights.[17] National legislations also form part of the protective framework. In many states this protection is afforded by the Constitution,[18] by Charters of Rights,[19] by other legislation,[20] or by more specific legislation focusing solely on the right to privacy.[21]

LIMITATIONS

However, an *a contrario* reading of Article 17 of the ICCPR demonstrates that the right to privacy is not absolute. The protection offered is against "arbitrary or unlawful" interferences, requiring an assessment on a case-by-case basis. Article 8 of ECHR provides a more enlightening enumeration of exceptions. Interferences with the right to privacy are permissible when they are in accordance with the law and are necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals,

---

A/HRC/28/L.27, 24 March 2015, para. 4.

[14] Ibid.

[15] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, article 8.

[16] EU, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, articles 7 and 8.

[17] Organization of American States, American Convention on Human Rights, 'Pact of San Jose', 22 November 1969, article 11.

[18] United States, Amend. IV, Constitution; Belgium, Article 22, Constitution.

[19] Canada, Canadian Charter of Rights and Freedoms, section 8.

[20] France, Civil Code, Article 9.

[21] New Zealand, Privacy Act 1993, 17 May 1993.

or for the protection of the rights and freedoms of others.[22]

The European Court of Human Rights (ECtHR) and the UN HR Committee have also interpreted the non-absolute character of privacy and held that permissible restrictions to the right to privacy must respect certain guarantees.[23] It appears as common ground that the restriction must be provided for by law, and be necessary in the circumstances and proportionate in relation to the legitimate aim pursued.[24] In essence, the principles of legality, necessity and proportionality are providing guidance when determining whether an interference with the right to privacy is permissible or not.

It is the responsibility of the domestic legislator to enact such laws that provide the appropriate guarantees to prevent any use of personal data that is not consistent with these principles. As relevant ECtHR jurisprudence highlights, such a need is even more acute when related to personal data subject to automatic processing; in particular, when they are used for law enforcement purposes.[25] The domestic law should assure that personal data are relevant and non-excessive in relation to the purpose for which they are registered and that there are guarantees protecting against the improper and abusive use.[26]

CONTROL OF LIMITATIONS

Who is the competent authority to make a determination as to whether an interference with the right to privacy is not arbitrary and lawful? Actions of the executive authorities that interfere with privacy must be scrutinised by an independent and impartial authority, to

[22] ECHR, article 8.

[23] ECtHR, *Malone* v. *United Kingdom*, 2 August 1984, *inter alia* paras 80, 82; UN HR Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, para. 8.

[24] ECtHR, *Uzun v. Germany*, 2 September 2010, paras 77-81. See UN HR Committee, General Comment 31, 'Nature of the general legal obligation on state party to the Covenant', CCPR/C/21/Rev.1/Add. 13, 24 May 2004, para. 6.

[25] ECtHR, *S and Marper* v. the *United Kingdom*, 4 December 2008, para. 103.

[26] ECtHR, *Brunet* v. *France*, 18 September 2014, para. 35.

which the individual whose privacy is at stake can have access. It would be for the state to prove that interference is permissible. According to jurisprudence, this is the case "[e]ven where national security is at stake, [as] the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence".[27]

Elaborating further on the characteristics of the control, according to the jurisprudence of ECtHR, it has to be an "effective control" taking into account the guiding principles of legality and necessity, for example in relation to an investigative measure.[28] Such an effective control can only be assured by the judiciary, [as] the judicial control is the one offering the best guarantees of independence, impartiality, and a proper procedure.[29] Interestingly enough, a Prosecutor who receives instructions and reports to a minister, cannot be considered as independent vis-a-vis the executive authorities.[30]

The aforementioned automatic processing of the data is also relevant in relation to the importance of effective control of the limitations to privacy and of the controlling authority; in particular, in relation to telecommunications data.

Act 3: How the Brave New World Functions

The collection and retention of telecommunications data, but also their subsequent use in criminal investigations and proceedings constitute a certain interference with the right to privacy. The UN Human Rights Council (UNHRC) recognised that "certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private pref-

[27] ECtHR, *Al Nashif* v. *Bulgaria*, 20 June 2002, para. 123.

[28] ECtHR, *Brunet* v. *France*, 18 September 2014, paras 35-36.

[29] ECtHR, *Uzun* v. *Germany*, 2 December 2010, paras. 71-72; ECtHR, *Klass and others* v. *Germany*, 6 September 1978, para. 55.

[30] ECtHR, *Moulin* v. *France*, 23 November 2010, para. 57.

erences and identity.[31] In this vein, it is evident that any registration of telecommunication data can interfere with privacy, regardless of whether they are actually used for investigation or prosecution.

As such actions risk to be characterised as arbitrary or unlawful interference, the case-by-case assessment becomes of relevance. With a view to guarantee that such interferences are not arbitrary or unlawful, international and domestic jurisdictions have defined specific requirements for the collection and retention and for the admissibility of telecommunications data in criminal proceedings.

There follows a selection of recent examples that deal with the interplay between the use of telecommunications data and the right to privacy. Each of the cases is selected with a view to provide trends in domestic, regional, and even international criminal justice systems. In particular, they provide interesting insights on the permissible limitations of the right to privacy in relation to the collection and use of telecommunications data in criminal investigations and proceedings. These insights could contribute to establishing a more solid framework regulating the functioning of this brave new world.

1. *ECtHR*

The ECtHR has dealt with many cases in relation to Article 8 of the ECHR and as can be seen above has essentially provided the basis of the interpretation and application of the right to privacy. It has not yet addressed the conflicting situation between privacy and the collection and use of telecommunications data in criminal proceeding, but has found that a number of comparable measures interfere with the right to privacy. The ECtHR even found that the existence of legislation providing the possibility of communications information being captured constitutes interference with privacy.[32]

Currently pending, *Ćalović* v. *Montenegro* (no. 18667/11) is the first

[31] UNHRC, Resolution 28/16, 'The right to privacy in the digital age', A/HRC/28/L.27, 24 March 2015, p. 3.

[32] ECtHR, *Weber and Saravia*v. *Germany*, 29 June 2006, para. 78; ECtHR, *Malone v. UK*, 2 August 1984, para. 64.

case before the ECHR concerning the right to privacy against the use of telecommunications data in criminal proceedings. The applicant filed her complaint in 2011 under Article 8 of the ECHR in relation to the powers of the police to access directly all data of the mobile telecommunication provider to which she is subscribed, therefore including her own, in an uncontrolled manner.[33] Earlier this year, the ECtHR communicated certain questions to the parties, including whether there has there been a violation of the applicant's right to respect for her private life, contrary to Article 8; and in the affirmative whether the interference with her right to respect for her private life was in accordance with the law and necessary in terms of Article 8 of the ECHR.[34]

2. *EU*

In the realm of the legal order of the EU, there have been efforts to regulate the collection and retention of data for law enforcement purposes. The regulatory framework is mainly to be found in three key Directives adopted over a period of ten years, with the extent of regulation gradually evolving. Already in 1995, Directive No. 95/46/EC was adopted with a view to regulate the protection of individuals with regard to the processing of personal data and the free movement of such data.[35] Directive No. 2002/58/EC came to complement 95/46/EC in relation to the protection of personal data in the electronic communications sector (EU e Privacy Directive) with a view to harmonise the provisions of the Member States so as to ensure an equivalent level of protection of the right to privacy and to confidentiality.[36] According to the

[33] ECtHR, *Ćalović* v. *Montenegro*, 31 March 2016.

[34] *Ibid*., question 2.

[35] EU, 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, 24 October 1995, Article 1.

[36] EU, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 12 July 2002, Article 1.

e Privacy Directive, EU Members are required to ensure the confidentiality of telecommunications and traffic data through national legislation. Furthermore, the traffic data shall be erased when they are no longer needed for the purpose of the transmission of the communication. The Directive allows restrictions, but only when they constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of un authorised use of the electronic communication system.[37]

In 2006, the highly controversial Directive No. 2006/24/EC was adopted (Data Retention Directive), requiring telecommunication service providers to retain certain categories of data in order to ensure that they are available for the purposes of the investigation, detection and prosecution of serious crime.[38] The providers are obliged to retain data necessary to trace and identify the source and the destination of a communication for a period of six months and up to two years.[39]

Later that year, the Court of Justice of the EU (CJEU) was seized of a question referred by the High Court of Ireland for a preliminary ruling on the validity of the Data Retention Directive. Digital Rights Ireland Ltd brought an action against two ministers of the Irish Government submitting that the Irish authorities unlawfully processed, retained and exercised control over data related to the communications of the mobile phone number owned by it.

In its landmark judgment of 8 April 2014, the Grand Chamber of the CJEU held that communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives

[37] *Ibid*., Articles 5-6 and 15.

[38] European Union (EU), Directive 2006/24/EC 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, 15 March 2006, Articles 1 and 3.

[39] *Ibid*., Article 6.

of the persons whose data has been retained"[40] and that the retention of these data for the purpose of access by the national authorities, "directly and specifically affects private life".[41] The interference was found to be "wide-ranging" and particularly serious. The CJEU pointed out that the retention and use of the data, without the knowledge of the subscriber, can cause in the minds of the people a feeling of being subject to constant surveillance.

The Data Retention Directive was, in essence, annulled, as the data retention obligations went beyond what was strictly necessary for the purpose of the fight against a serious crime and violated the EU Charter of Fundamental rights, as constituting serious interference with the fundamental right to the protection of personal data as per Articles 7 and 8 of the Charter.

This evolution almost immediately triggered two "sequel" cases to the Digital Rights Ireland that are currently pending before the CJEU. Tele 2 Sverige, a Swedish telecommunication services provider, and private parties in the United Kingdom are challenging their respective domestic data retention laws, based on the grounds that the CJEU used to annul the Data Retention Directive, as imposing general data retention obligations. The CJEU will have to make a pronouncement on the question referred that concerns the compatibility of national data retention laws to the Charter of Fundamental Rights of the EU and the EU e-Privacy Directive.[42]

On 19 July 2016, the Advocate General issued an opinion on the joined cases, which – even if not binding – validates general data retention obligations for electronic communications providers, provided that appropriate safeguards are in place. The opinion considers that

---

[40] CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd* v. *Minister for Communications, Marine and Natural Resources and others*, Judgment, 8 April 2014, para. 27.

[41] *Ibid*., para. 29.

[42] CJEU, Joined Cases C-203/15, *Tele2 Sverige AB* v *Post-och telestyrelsen* and C-698/15, *Secretary of State for Home Department* v *Tom Watson and Others*, Opinion of Advocate General, 19 July 2016, para. 2.

such national legislation imposing general obligations upon telecommunications service providers to retain traffic data may be compatible with EU law, but only in relation to the fight against serious crimes and if accompanied by appropriate safeguards.[43]

In particular, the obligation to retain telecommunications data should be laid down by legislative or regulatory measures offering accessibility, foresee ability, and adequate protection against arbitrary interference. Further, it must respect the essence of the right to respect for private life and the right to the protection of personal data laid down by the Charter. With regards to the aim served, this should be the fight against serious crime and does not encompass ordinary offences or non-criminal proceedings. Access to, period of retention, protection and security of the data must be limited to what is strictly necessary. The principle of proportionality is also referred as one of the safeguards in the sense that serious risks caused by the general data retention obligation must not be "disproportionate to the advantages it offers in the fight against serious crime" in a democratic society.[44]

Such strict safeguards as listed in the opinion limit to the extent necessary the intrusion to personal life and an effort to draw the very thin line between the right to privacy and investigation and prosecution of serious crimes. The relevant judgement would hopefully provide more clear guidance to the EU states and would allow for more harmonised domestic legislations.

3. *Special Tribunal for Lebanon(STL)*

An interesting example from the international legal sphere can be seen at the jurisprudence of the STL, that has jurisdiction over persons responsible for the attack of 14 February 2005 resulting in the death of former Lebanese Prime Minister Rafiq Hariri and in the death or injury of other persons.[45] The Prosecution's case against the four (currently) Accused relies to a great extent upon telecommunications data which,

[43] *Ibid.*, para. 7.
[44] *Ibid.*, para. 263.
[45] STL, Statute, Article 1.

according to the Prosecution, are collections of relevant portions of call data business records generated and maintained by three Lebanese communication service providers.[46]

According to Rules 149(C) and (D) of the Rules of Procedure and Evidence that provide the general rule of evidence admissibility, any relevant evidence which is deemed to have probative value can be admitted, unless the probative value is substantially outweighed by the need to ensure a fair trial – in particular, if the evidence is obtained in violation of the rights of the suspect or accused.[47] Further, Rule 162(B) functioning as procedural safeguard allows for the exclusion of evidence if it has been obtained in violation of international standards on human rights.[48]

When the Prosecution filed applications to have the traffic data of the accused admitted into evidence, the Defence used this provision, along with evidence to demonstrate that the way in which the telecommunications data of the entire Lebanese population were obtained from Lebanon by the Prosecution of the STL and by its preceding UN International Independent Investigation Commission (UNIIIC) was in violation of the right to privacy. The Defence stressed the importance of a proper judicial oversight to verify the proportionality of the interference in relation to the collection of the telecommunications data and their subsequent use as evidence and requested their exclusion.[49]

It is worth noting the Trial Chamber's *obiter dictum* recognising that "it is evident that human rights standards are evolving to include legal protection of metadata such as call data records from unwarranted dis-

[46] STL, *Prosecutor* v. *Ayyash et al*., Case No. STL-11-01/T/TC, 'Prosecution motion for the admission of red-network-related call sequence tables and related statement', 28 January 2015, para. 2.

[47] STL, 'Rules of Procedure and Evidence', Rule 149.

[48] STL, 'Rules of Procedure and Evidence', Rule 162.

[49] STL, *Prosecutor* v. *Ayyash et al*., Case No. STL-11-01/T/TC, 'Oneissi consolidated response to the prosecution motions for the admission of call sequence tables', 16 February 2015, paras 36-41.

closure to governments and law enforcement agencies".[50] The Trial Chamber nonetheless rejected the Defence arguments. It held that while the collection of telephone metadata may constitute a restriction on the right to privacy, the transfer of the CDRs was neither unlawful nor arbitrary and there was no violation of international standards on human rights. The legal framework establishing UNIIIC and the STL was enough to provide the required legal authorisation for the transfer of data and no other independent judicial oversight was required. Moreover, the transfer was necessary and proportionate to the legitimate aim of investigating the attack of 14 February 2005; in particular, in light of the gravity of the attack under investigation and as long as it serves a narrow and legitimate forensic purpose. As access to the data is strictly limited to staff employed by the Prosecution, Defence Counsel, the Legal Representative for the Victims and the Judges, the intrusion to any right to privacy is minimal.[51]

The issue reached also the appellate stage with the Appeals Chamber upholding the Trial Chamber's decision. Most importantly, it held that there is a compelling case as to the CDRs protection by international standards on the right to privacy. However, it concludes that the transfer of the CDRs in the absence of judicial control did not violate the right to privacy in this case because their transfer was provided for by law, necessary and proportionate. [52]

4. *Greece*

The protection afforded by the Greek Constitution in article 9A is of particular interest as it is not common for the issue of privacy in relation to the collection of personal data to be dealt with at such a norma-

[50] STL, STL-11-01/T/TC, 'Decision on five prosecution motions on call sequence tables and eight witness statements and on the legality of the transfer of call data records to UNIIIC and STL's prosecution', 6 May 2015, para. 86.

[51] *Ibid*., paras 100-110.

[52] STL, Case No. STL-11-01/T/AC/AR126.9, 'Decision on appeal by counsel for Mr Oneissi against the trial chamber's decision on the legality of the transfer of call data records', 28 July 2015, paras 47-60.

tive level. Article 9A was introduced with the constitutional revision of 2001 and provides that:

Every person has the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is assured by an independent authority, which is established and operates as specified by law.[53]

Further, Article 19 provides for an absolutely inviolable secrecy of communication, allowing though for exceptions where the judicial authority shall not be bound for reasons of national security or for the purpose of investigating especially serious crimes, as specified by law.[54] The two Articles, when read in conjunction, offer a high level of protection, as the use of evidence acquired in violation of these provisions is prohibited.[55] Further, Article 370A of the Greek Criminal Code penalises the illegal violation of the privacy of telecommunications, in particular when its scope is the representation not only of the content of the telecommunication, but also of the traffic and position data.[56]

The following example is not drawn from a criminal case and it concerns the use of content of telecommunications; it nonetheless contains certain pronouncements relevant to the problematic under examination in relation to the importance of an independent oversight mechanism.

In 2015, the Multi-member Court of First Instance of Thessaloniki was seized of a civil case where the parties brought as evidence registrations of SMS, without providing any judicial authorisation in relation to their obtention. The Court held that SMS could not be used as evidence in civil proceedings, as this would entail a violation of the constitutional right to private life and of the right of privacy of communications, but also with reference to article 8 of the ECHR. There needs to be an official lift of the privacy of communications for such

[53] Greece, Constitution, Article 9A.

[54] *Ibid*., Article 19.

[55] *Ibid.*, Article 19(3).

[56] Greece, Criminal Code, article 370(A).

evidence to be used even in civil proceedings.[57]

Of particular interest is the fact that the Court reached that conclusion without an objection or a claim from the parties, but based on its power to control *proprio motu* the legality of the obtained and used evidentiary material.

As a more general comment that is highly relevant to the debate, the Court held that the delivery of justice cannot be done at any price. The Court further linked the issue of privacy to the freedom of communication. The latter would be limited as everyone would live with the "depressing feeling"[58] that any communication could be used against him, more so when the modern technical means provide broad possibilities of manipulation of the registrations; and when manipulation is difficult, if not impossible to be detected.

5. *Canada*

In Canada, the police make certain "production orders" to telecommunications services providers, with a view to obtain the traffic data of cell towers over a specified time period. During an investigation into a series of jewellery store robberies, two such orders reached companies Rogers and Telus. Rogers was required to provide call data records for all phones activated, transmitting and receiving data through 16 cell towers identified by a police officer, while Telus was required to provide similar information for all of its cell towers proximate to 21 municipal addresses. The companies found such orders particularly broad and onerous and applied for a court ruling so as to tailor these orders to respect the privacy interests of their subscribers and to conform to constitutional requirements. By way of illustrative example, Telus was ordered to disclose personal information of at least 9.000 individuals and Rogers had to provide 200.000 records related to 34.000 subscribers.

In relation to the legal framework, the Canadian Charter provides in

[57] Greece, Multi-member Court of First Instance of Thessaloniki, 3256/2015.

[58] *Ibid*.

Section 8 that "[e]veryone has the right to be secure against unreasonable search and seizure".[59] The Canadian Criminal Code, s. 492.2, requires judicial authorisation, on a "reasonable grounds to suspect" standard, to install transmission data recorders, which can capture the telephone numbers of persons sending and receiving communications.[60]

On 14 January 2016, the Superior Court of Justice of Ontario issued its judgment making some interesting findings of relevance to the problematic.[61] Firstly, the Court found that citizens have a "reasonable expectation" of privacy in their cell phone records, based on the Criminal Code provision that requires judicial authorisation on "reasonable grounds to suspect".[62] It further found that actually the telecommunications providers have standing to assert the privacy interests of their clients not only based on their contractual obligations, but also so that justice is properly delivered.[63]

It was further held that the Production Orders to the providers that formed the basis of the police requests for obtaining the call data records were overly broad and far beyond what was reasonably necessary to gather evidence concerning the commission of the crimes under investigation.[64]

Of particular interest are certain useful guidelines provided in the judgment with a view to minimise the intrusion to privacy. According to these guidelines, when police makes such production orders it has to provide: i) an explanation in the Production Order that the request is made in accordance to the principle of incrementalism and minimal intrusion; ii) an explanation as to the relevance of the requested parameters (date, time, cell towers) for the investigation; iii) an explanation as

[59] Canada, 'Canadian Charter of Rights and Freedoms', section 8.

[60] Canada, Criminal Code, s. 492.2.

[61] Canada, Superior Court of Justice of Ontario, R v Rogers and Telus, Judgment, 14 January 2016.

[62] *Ibid*., para. 31.

[63] *Ibid*., paras 37-38.

[64] *Ibid*., para. 43.

to the relevance of the types of records; iv) listing of other parameters permitting a narrower search and producing fewer records; v) a request for specified data, instead of a request for the underlying data; vi) justification for request of underlying data; and vii) confirmation that the types and amounts of data can be meaningfully reviewed.[65]

Epilogue: Are We Brave Enough?

It becomes evident that international and domestic human rights law texts and practice are becoming braver in providing protection to call data records from arbitrary and unwarranted collection disclosure to and use by law enforcement agencies and governments. The latter also become braver in realising the importance of these data for crime detection and prosecution and in requesting access to them more often. It is evident, as well, that the protective framework for privacy is based on sporadic practice, but it seems to evolve on a common ground and to contain at least principles and guidelines that, if harmonised, could contribute to make this brave new world function.

There is, however, a need for an agreement on an updated definition of the notion of privacy that is consistent with the current circumstances and the technological developments. By way of illustrative example, ICCPR was adopted fifty years ago and was interpreted only twenty-two years later for the first time.The core content, but mostly the limitations to the right to privacy, need to be reviewed and developed with a view to make them address the reality and the needs not only for today, but also for tomorrow. The Special Rapporteur on privacy has highlighted that there appears to be a certain consensus amongst several stakeholders for an additional protocol to Article 17 of the ICCPR[66] and he has actually been "urged to promote the start of negotiations on such a protocol with his first mandate".[67] However,

[65] *Ibid*., para. 65.

[66] 'Report of the Special Rapporteur', para. 46.

[67] https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf(last accessed 11 November 2016).

consensus needs to be reached beforehand in relation to a common understanding of what is to be protected and which are its limits. In the world of today, to which extent is privacy desirable, in relation to security, crime detection, and prosecution? The Special Rapporteur invited all actors in the field to contribute to such developments for an improved understanding of the right to privacy and is convinced that significant progress is possible.[68]

While speed might be a characteristic of technology, it is not equally applicable to legal advancements. The fact that the right to privacy and its limitations by the use of telecommunications data for law enforcement purposes is in the centre of recent legal debate, does not automatically entail quick legislative reactions. Such reactions are even more challenging in an effort to actually harmonise globally the legislative framework. Already at an EU level – a more limited environment – , the relevant regulation evolved gradually during the last twenty years, but still without reaching a common understanding. The Data Retention Directive has been practically annulled, while there are live issues as to whether national laws are in accordance to the ePrivacy Directive or even harmonised.

The main question to be answered is, finally, which are the limits to privacy? From the jurisprudence presented above, we can at least identify, as a common ground, that there is a reasonable expectation from the citizens for privacy as a minimum. This reasonable expectation is at a first step safeguarded by the principles of legality, necessity and proportionality. However, these principles are interpreted in various ways as there is always a case by case basis assessment.

It is understandable that states would not cede their sovereign prerogative in the law enforcement realm. However, there is a need for harmonisation, as this debate is recurring and it affects more civil liberties than just the right to privacy. As already explained, the UN HR Committee recently appointed the Special Rapporteur on the broader issue of privacy with a mandate for three years. Although this mandate

[68] 'Report of the Special Rapporteur', para. 2.

is limited for the moment and we are yet to see a more detailed second report, it is believed that he could play a more permanent and active role.

It would be unrealistic to imagine him as a global regulating authority performing a case by case assessment for each and every request to lift the privacy of telecommunication data. However, by collecting and analysing the existing legal frameworks and jurisprudence, the Special Rapporteur could prepare and suggest a list of guidelines that could be followed domestically as soft law. Such list could be revisited annually, allowing for flexibility and adaptability to the exigencies of our reality. The guidelines provided by the Court of Ontario are an excellent example of jurisprudence that could be applicable in any situation of lift of privacy anywhere in the world.

Another way to regulate and harmonise globally this problem is by recognising that the protection of privacy in relation to the collection and use of telecommunications data for the detection and prosecution of crime is slowly forming international customary law. The STL Trial Chamber's *obiter dictum* about the evolution of human rights "standards" is pointing to this direction. The difficulty is that we might observe enough state practice, but it is often fragmented and even contradictory to form a concrete *opinion juris* and to be crystallised into a rule of customary international law. As mentioned above, the CJEU found the Data Retention Directive as interfering with the right to privacy, while in the currently pending cases, the Advocate General has suggested that data retention under certain conditions does not constitute interference. The anticipated judgement will be an important additional element to the relevant practice. The first judgment of ECHR on this problematic is also expected to make some shaping pronouncements and to advance the development of a possible customary rule.

The ethical aspect and the impact of this situation on citizens should be always taken into consideration, as we are not far from that situation that was pointed out by the Greek Court of First Instance, where everyone would live with this "depressing feeling" that their personal life and communication is captured on means that can be manipulated

and consequently used against them. It has to be understood that we are still in an infant stage dealing with telecommunications metadata. The day that we will have to regulate a similar situation in relation to collection and use of data from smartphones is approaching and will probably find us unprepared, trying to find solutions and to make *a posteriori* dangerous legal constructions.

The discussion should not focus on how to fully disclose telecommunications data in order to detect and prosecute crime or how to fully protect a rigid right to privacy. As highlighted by the Special Rapporteur, both privacy and security are desiderata and essential in any legal system as "enabling rights rather than ends in themselves".[69]The essence of civil liberties cannot be fulfilled in a state lacking security. The debate should rather revolve and evolve around the idea of how to use telecommunications data, respecting the core of the right to privacy. Our bravery should not only be characterised by legality, but also by reasonable proportionality.

[69] 'Report of the Special Rapporteur', para. 24.