Access to communications metadata regardless of the severity of the crime

Dr. Maria Tzanou, Keele University
Published in Leading Internet Case Law http://www.cecileparkmedia.com/leading-internet-case-law/article_template.asp?Contents=Yes&from=eclr&ID=1243

Overview

In an Opinion delivered on 3rd May 2018 in the case C-207/16 *Ministerio Fiscal* (‘*Ministerio Fiscal’),* Advocate General (AG) Saugmandsgaard Øe proposed that criminal offences that are not particularly serious may justify in certain cases disclosure of electronic communications metadata. The AG’s Opinion might come as a slight surprise to privacy advocates after the seminal decisions of the Court of Justice of the European Union (‘CJEU’) in *Digital Rights Ireland* (C-293/12 and 594/12) (‘*Digital Rights*’), *Schrems* (C-362/13) and *Tele2* and *Watson* (C-203/15 and C-698/15) (‘T*ele2*’). Yet, a more careful reading of the AG’s Opinion does not reveal a rupture from the previous line of the CJEU’s surveillance case-law; it merely states that there could be certain flexibility in the interpretation of the requirements of targeted metadata surveillance as soon as this does not pose a serious interference to the fundamental rights to privacy (Article 7 of the EU Charter of Fundamental Rights (EUCFR)) and data protection (Article 8 EUCFR).

Factual background

On 16 February 2015, Mr Hernández Sierra, a Spanish national, was the a victim of a robbery that resulted in the theft of his wallet and his mobile telephone and left him seriously injured. Following this incident, the police requested the Court of Preliminary Investigation in Tarragona, Spain to order the various telephone operators to communicate a) the telephone numbers which had been activated, between 16 and 27 February 2015, with the ‘International Mobile Equipment Identity’ (IMEI) code - the unique identification code, consisting of 15 digits, generally found inside the battery compartment of a mobile phone- of the stolen mobile telephone; and, b) the personal data of the owners or users of all the telephone numbers corresponding to the SIM cards activated by that IMEI code. The Court of Preliminary Investigation refused that request, on the grounds that the Spanish Criminal Code limited the communication of the data retained by the telephone operators to serious offences, namely, those punishable by a term of imprisonment of more than five years, while the facts at issue did not constitute a serious offence.

The preliminary reference questions

The Spanish Public Prosecutor’s Office (Ministerio Fiscal) -the only party to the proceedings- appealed against that order before the Provincial Court of Tarragona, which decided to stay the proceedings and refer two preliminary questions to the CJEU which concerned the interpretation of the concept of ‘serious crime’. More particularly, in its first question, the Provincial Court asked whether the sufficient seriousness of offences, as a criterion which justifies interference with the fundamental rights recognised by Articles 7 and 8 EUCFR, can be determined by taking into account only the sentence which may be imposed in respect of the offence investigated, or whether it is also necessary to identify in the criminal conduct particular levels of harm to individual and/or collective legally-protected interests. If the CJEU were to find in favour of the former, namely that the seriousness of the offence can be determined only on the basis of the prescribed sentence, the Spanish Court in its second question requested a clarification on what should be the minimum threshold for this and whether a minimum of three years’ imprisonment would be compatible with the requirements of EU law.

Legal background

The preliminary reference questions of the Spanish Court concern the interpretation of the concept of 'serious crime' as a criterion for the assessment of the lawfulness and proportionality of the interference of metadata surveillance measures with the rights to privacy and data protection enshrined in Articles 7 and 8 EUCFR. In order to fully understand the legal context within which the concept of 'serious crime' appeared, we need to take a look at two judgments of the CJEU which referred to this: *Digital Rights* and *Tele2*.

Digital Rights

In *Digital Rights*, the CJEU annulled Directive 2006/24/EC (the 'Data Retention Directive') on the basis that the mass, indiscriminate metadata retention that this established interfered disproportionately with the fundamental rights to privacy and data protection in the light of Article 52 (1) EUCFR. Article 52 (1) EUCFR provides that any limitation on the exercise of the rights and freedoms recognised by the Charter should i) be provided for by law, ii) meet objectives of general interest recognised by the EU, iii) be necessary and proportionate, and iv) respect the essence of those rights and freedoms. It should be recalled that the Data Retention Directive obliged the providers of publicly available electronic communications services or networks to retain communications' metadata generated or processed by them, in order to ensure that these were available for the purpose of the investigation, detection and prosecution of serious crime. The CJEU held in that case that the purpose of fighting 'serious crime', such as terrorism or organised crime, is indeed an 'objective of general interest' recognised by the EU and while metadata retention can be a 'valuable tool for criminal investigations', such an objective of general interest, 'however fundamental it may be, does not, in itself, justify a retention measure such as that established by [the Data Retention] Directive being considered to be necessary for the purpose of that fight'.

Tele2

In *Tele2,* the CJEU had to consider national metadata retention laws -the Swedish one and the UK's Data Retention and Investigatory Powers Act 2014 ('DRIPA')- after the invalidation of the EU Data Retention Directive. It held that EU law precludes national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all metadata of all subscribers and registered users relating to all means of electronic communication. It also stated that EU law precludes national legislation governing the protection and security of electronic communications metadata and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, '*is not restricted solely to fighting serious crime*' (emphasis added), 'where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.'

The AG's Opinion

In *Ministerio Fiscal*, AG Saugmandsgaard Øe had to consider whether EU law allows the access of police authorities to metadata retained by electronic communications service providers for the purpose of identifying individuals in the context of a criminal investigation even if this does not constitute a 'serious crime'. The AG commenced his analysis explaining why *Ministerio Fiscal* was different from *Digital Rights* and *Tele2.*

Targeted vs. mass surveillance

According to the AG, the central issue that distinguishes *Ministerio Fiscal* from *Digital Rights* and *Tele2* is the fact that the police request at issue seeks to obtain only data that would make it possible to identify the owners or users of the telephone numbers linked with the SIM cards that were inserted in the stolen mobile telephone. Therefore, it concerns a clearly defined period of short duration (around 12 days); a restricted -rather than unlimited- number of persons capable of being affected by the measure (those who have used the stolen telephone after it was taken or those suspected of being connected with the perpetrators of this crime); personal data (such as forenames, surnames and addresses) related only to the above individuals -and not every type of metadata-; with the aim to gather information about certain natural persons -and not general information about location and communications as such-. The request, thus, entails a targeted measure that can be distinguished from general, indiscriminate surveillance.

Assessing serious crime

Having established that the case at issue concerned targeted rather than mass surveillance, the AG went on to answer the first question of the Spanish Court regarding the factors that must be taken into account for establishing that a crime is sufficiently 'serious' to justify an interference with Articles 7 and 8 EUCFR. The AG recalled that the concept of 'serious crime' does not appear in the ePrivacy Directive, but it was mentioned in the -invalidated- Data Retention Directive and subsequently used by the CJEU in *Tele2* to ensure consistency with EU law of national surveillance measures. The AG considered that before answering the question of the national court he needed to reformulate this as the interference at issue in the case is not 'sufficiently serious'.

'Sufficiently serious' interference

The AG admitted that operations such as those in the present case constitute an interference with Articles 7 and EUCFR even if the personal data concerned are not particularly sensitive, nevertheless this interference is not 'sufficiently serious' to 'give rise to the need for enhanced justification' for the following reasons: it concerns targeted, rather than mass, undifferentiated surveillance; it entails limited harmful effects for the persons concerned; access to the metadata is accompanied by procedural guarantees under Spanish law, such as review by a court; and the type of data requested and the limited scope of the request do not make it possible to 'obtain varied and/or specific information about the persons concerned and therefore do not directly and seriously affect their right to a private life'. Furthermore, Article 15 (1) of the ePrivacy Directive, which lists the objectives capable of justifying national legislation derogating from the principle of confidentiality of electronic communications includes the objective of 'the prevention, investigation, detection and prosecution of criminal offences', without further qualification as to the nature of those offences. Therefore, according to this, the AG opined that only where 'the interference is 'particularly serious', 'the offences capable of justifying such an interference must themselves be particularly serious'. In the case of a non-serious interference, it is necessary to go back to the basic principle that emerges from the wording of article 15 (1) ePrivacy Directive, namely that 'any type of criminal offence is capable of justifying such an interference'.

Commentary and what's next?

It still remains to be seen if AG's Saugmandsgaard Øe Opinion will be adopted by the CJEU. The Opinion, nevertheless, does not seem to deviate substantially from the strict requirements regarding communications metadata surveillance imposed by previous case-law as the factual circumstances are significantly distinct. *Ministerio Fiscal* concerns a measure of targeted surveillance, of limited scope that does not affect every individual and is accompanied by judicial safeguards. In this regard, the Opinion of the AG confirms to an extent what we already

knew from *Digital Rights* and *Tele 2*, that there exist types of targeted surveillance that could be compatible with EU law, even if they concern criminal offences that are not necessarily serious.

Does this mean that Member States, such as the UK, should no longer be concerned about their domestic metadata retention regimes? The answer is unequivocally, no. Measures, such as the Investigatory Powers Act 2016 ('IPA') still do not comply with EU law, no matter whether the CJEU will agree with its AG in *Ministerio Fiscal*. The interception of communications metadata in bulk of every user and the lack of prior review by a court -as mandated in IPA- still presents a serious interference to the fundamental rights to privacy, data protection and freedom of expression and cannot, therefore, allow for access to the retained data for the purposes of fighting any crime -irrespective of its severity-, following the pronouncements of the AG in *Ministerio Fiscal*.

Mass indiscriminate metadata retention for criminal purposes still remains extremely problematic even if the CJEU follows its AG's suggestions in *Ministerio Fiscal*. It should be recalled that in that case, albeit the facts not being very clear, the AG accepted that there was a valid reason for the retention of such metadata by telecommunications' service providers in the first place under Spanish law in compliance with the ePrivacy Directive. If, however, this premise is lacking and communications metadata were not retained in accordance with the ePrivacy Directive, the analysis regarding the seriousness of the interference and the concomitant requirement of seriousness of crime will not be applicable.

The AG's analysis in *Ministerio Fiscal* can be criticised for lacking clear guidance on this point that is fundamental for the CJEU's decision and the criteria that national legislators need to follow in order to put in place surveillance measures that comply with EU law. When should it be considered that the retained by communications' providers metadata to which the police authorities seek access, for the purposes of an investigation, have been archived by the operators in order to comply with an obligation complying with EU law? The AG accepts that this is the case in *Ministerio Fiscal* without any further discussion or clarification on the matter. The Opinion, thus, raises further questions regarding the dichotomy between retention of metadata and access to this by law enforcement authorities (these issues are discussed in detail in my book on *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*). Finally, the AG's justification of access to metadata irrespective of the severity of the crime in cases such as the one at issue on the basis that this does not present a 'serious interference' is artificial, unduly complex and ultimately not convincing. While I agree with his conclusion, the justification should have been based on a simple application of the principle of proportionality in cases of targeted surveillance measures, rather than the creation of an artificial distinction between measures that pose a serious interference to fundamental rights and those that do not, that causes even further uncertainty.

Dr. Maria Tzanou, Lecturer in Law, Keele University, UK
E-mail: m.tzanou@keele.ac.uk