A Revolution in the EU regarding National Security? The Court of Justice cases of C-623/17 PI and C-511/18 QdN 6 October 2020

QMUL Criminal Justice Centre Seminar: 5 February 2021, 14:00 – 16:00 (Zoom/Teams) with the participation of the University of Portsmouth and GUARDINT, Sciences-Po CERI Paris ANR Project

On 6 October 2020, the Court of Justice handed down much awaited two judgments – PI and QdN both dealing with the right to privacy and the limitations to interference with that right by both the private sector on behalf of the public sector on grounds of national security, terrorism and serous crime. The Court held that there are circumstances where the concept of national security comes within the competence comes within EU law[i] and what the limitations are on interference with the right to privacy on these grounds are.[ii]

The judgments fit together into an intellectual whole – providing a rich and complex set of reasoning which is not always entirely coherent or easily accessible. In order to examine some of the key issues which arise in these judgments both from the perspective of fundamental rights protection, limits of state action (in particular intelligence service operations), the relationship of the private and public sectors as regards national security, the characteristics of permissible automated analysis of personal data and judicial oversight, we plan this seminar as an entry point into the discussion. These two judgments are neither the beginning of the road (which substantially began with C-293/12 Digital Rights Ireland

Four academic experts from two institutions will present their analysis of the judgments from four quite distinct perspectives which will be followed by discussion and debate. It is intended that the presentations will become available as blogs after revision. We also plan this as the first of a series of events on the two judgments which will bring together an interdisciplinary group of academic experts to examine the importance and impact of the two judgments.

Programme:

Chair: Professor Didier Bigo, Sciences-Po, Paris, GUARDINT and Kings College London

Transforming the Public – Private Divide: What are the transformations which PI and QdN have made as regards the public/private divide and the use of the national security exception to the right to privacy? What is the configuration of the parameters of public/private

partnerships on surveillance and their impact on the determination of the applicability of EU law in the face of Member States' invoking of the national security exception.

Professor Valsamis Mitsilegas QMUL

Changing the actors and their authority? The two judgments provide an intricate and new approach to what powers and responsibilities different actors have in respect of the protection of personal data and its use. In this second presentation we will examine what these changes are and how the Court has redefined the limits of authority by differentiating between agencies and bodies.

Dr Niovi Vavoula, QMUL

Whither automated analysis after PI and QdN? Among the most convoluted parts of the judgments are those dealing with the use of automated analysis in the context of exceptions to the right to privacy and the protection of personal data. In this presentation we will investigate what the Court seems to be determining as regards automated analysis and in particular compare this with its previous analysis of the subject in Opinion 1/15 (EU-Canada PNR).

Dr Elif Kuskonmaz, Portsmouth University

Oversight? both judgments provide extensive new obligations for courts and independent administrative bodies charged with ensuring that state authorities respect to new rules which it has laid down. The character of courts and independent administrative bodies is defined and the powers both a priori and ex post set out in some detail. What kind of a system is under construction here and how does this relate to the existing frameworks in key Member States?

Professor Elspeth Guild, QMUL.

Discussion.

[i] "1. Article 1(3), Article 3 and Article 15(1) of 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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Article 4(2) TEU, must be interpreted as meaning that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive.

[ii] "Article 15(1) of 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), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding legislative measures which, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data. By contrast, Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, does not preclude legislative measures that:

– allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;

– provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;

– provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period that is limited in time to what is strictly necessary;

– provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;

– allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as not precluding national rules which requires providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection, inter alia, of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used, where:

– recourse to automated analysis is limited to situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of an effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed; and where

– recourse to the real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.

3. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), must be interpreted as not being applicable in the field of the protection of the confidentiality of communications and of natural persons as regards the processing of personal data in the context of information society services, such protection being governed by Directive 2002/58, as amended by Directive 2009/136, or by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as appropriate. Article 23(1) of Regulation 2016/679, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, inter alia, personal data relating to those services.

4. A national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality, which it is bound to make under that law, in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights. Article 15(1), interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact." (QdN operative)