Privacy and Jurisdiction in the Global Network Society

Gry Hasselbalch, May 2010

In the network society, the right to privacy is challenged by new automated methods of collecting data and global information networks used to their full potential by both state actors and non-state actors. New technologies hold a potential for increasingly sophisticated methods of state's intelligence gathering and police investigations. Moreover, with the introduction of the internet, a space for private parties as data disseminators, collectors and processors has been created. This development has expanded the primarily negative scope of Article 8 of the European Convention of Human Rights to include also positive obligations. In its case law, the European Court of Human Rights (ECHR) has on several occasions addressed the challenges of technological progress to the right to privacy and stipulated the positive obligations of states when securing the appropriate balance between the benefits of technologies and the right to privacy. In some aspects the stipulations are rather clear however, there are some implications of the ECHR's application of a primarily territorial definition of jurisdiction to the question of global information networks that creates a level of uncertainty as to the essence of state parties' to the convention obligations.

Safeguards and Transparency

The ECHR case law provide clear stipulations on the requirements of state parties in regards to the handling of personal data when using advanced automated methods for intelligence gathering. Here, the stronger future potential and challenges of new technologies when processing, recording, organising, storing, altering, collecting, searching, retrieving and transmitting personal data is emphasized.[i] And thus technological progress is recognized to require even greater safeguards for the protection of personal data (detailed rules on duration, storage, usage, access of third parties, procedures for preservation and destruction of data) in order to guarantee against risks of abuse [ii]. In this context, it must be noted that the very existence of a legislation which allows a system for the secret monitoring of e.g. telecommunications the ECHR acknowledges to entail a threat to all of those whom the legislation may be applied and thus amount to an interference of their privacy [iii]. When the prevention of serious crime and terrorism are put forward as legitimate aims for the electronic collection and processing of data, the question of proportionality will be assessed on the basis of the balance struck between the benefits of technologies and the protection of rights but also the quality of the domestic law[iv] Here, the sophisticated development of technologies is stressed by the ECHR to require an increased transparency in the law of the aims and procedures put in place [v].

Protection of Minors

The positive obligations of states in regards to the adaptation of measures designed to secure respect for private life in the sphere of the relations between private parties online are less clear. In general, the case law on internet activities is still limited. In *KU v. Finland*[vi] the ECHR held that the state had failed its positive obligations when not providing an efficient legislation to protect the physical and moral integrity of a minor online (§ 43) and emphasised the greater importance of the state's positive obligations in regards to the protection of minors (criminal law provisions through effective investigation and prosecution) (§ 46). An anonymous person had placed a fake ad of a 12 year old boy on a website effecting several sexual advances to the boy. However, the identity of the person who had placed the ad could not be obtained from the ISP due to the domestic legislation in place at that time ("malicious misrepresentation" was not stipulated as an offence that gave the police a right to obtain the identification data from the ISP). Importantly, the case illustrated the ECHR expectations' to a state party's response to the specifically anonymous potential for acts of crime that the internet had introduced. The government had failed to respond to this technological progress by not putting in place a system to protect children online (§48). It was further accentuated that the right to freedom of expression and privacy is not absolute online and that it is the legislators' task to provide the framework for reconciling the various claims which compete for protection in this context (§49).

The Challenge of the Global Information Network

State parties to the ECHR have an obligation to secure the rights of their citizens within their *jurisdiction* (ECHR, Article 1). Jurisdiction is in ECHR case law understood as primarily territorial[vii]– "physically placed and described"[viii]– other bases of jurisdiction being exceptional and requiring special justification[ix]. However, the global nature of information networks with the absence of physical frontiers, challenge this territorial definition of jurisdiction, especially in cases of the protection of privacy, when activities conducted in one jurisdiction has effects in multiple jurisdictions, and thus can create a level of uncertainty as to a state's obligations.

Intelligence Gathering in the Network Society

In *Weber and Saravia against Germany*[x] the applicants (one German national and one Uruguayan national both residing in Uruguay) claimed among others that the German Fight Against Crime Act's amendments to the G10 Act interfered illegally with the sovereignty of another state (The law, Submissions of the parties, §69). Although not judging on the very ratione personae of this argument (Court's assessment, §72), the ECHR still stressed that the monitoring of international

telecommunications was conducted via interception sites situated on German soil and data was collected and used in Germany, thus emphasizing the physical points of interception, not the virtual. The decision on inadmissibility was made on the grounds that the appropriate data protection safeguards were in accordance with the stipulations of ECHR case law [xi].

In this connection, it is worth noting a recent special rapporteur report from the Human Rights Council which highlighted the increased tracking of cross-border communication in the fight on global terrorism and, in this context, the clash of converging jurisdiction's data protection requirements[xii]. As an example of this, the SWIFT agreement[xiii] on the handling of EU citizens' financial data, currently negotiated between the EC and the US, was rejected by the EU Parliament primarily on the grounds that it did not concur with EU data protection standards and safeguards [xiv]. Here, the transfer of data in "bulks" could e.g. be compared to the UK's indiscriminate system of data collection criticized by the ECHR in the S. and Marper case. In addition, the lack of transparency as to the specifics of the data protection safeguards put in place are as compelling as they were in the Liberty and Other case. However, neither the uncertainty of data protection safeguards or the far reaching nature of the transfer of EU citizens data were the original initiators of the current SWIFT negotiations. The negotiations between the EU and US were only initiated following the physical relocation of the US database to Switzerland.

The Conduct of Private Parties in the Network Society

Perrin against the UK[xv] exemplifies, as *KU v. Finland*, how the ECHR would decide in favor of measures taken by authorities to protect the integrity of minors online. But perhaps more interesting, it illustrates the transjurisdictional implications of online activities. The applicant, a French national residing in the UK, was a majority shareholder of a US company, which had created a website with obscene pornographic images. The site was operated and controlled in the US. However, he was sentenced to 30 months in prison under the UK Obscenity Act 1959 for making the material available online to minors in the UK. In the application to the ECHR, the applicant maintained that because of the worldwide nature of the internet it was unreasonable for publishers to foresee the legal requirements in all individual states where the material could be accessed. Nevertheless, the ECHR underlined that although the images in question might be legal in other states including non-state parties to the convention, the government had not exceeded its margin of appreciation when prosecuting and convicting the applicant within its own territory. The deciding point was here that the images were freely available to anyone surfing the net including minors. The ECHR considered the *effects* of the material and thus regarded the criminal conviction necessary in a democratic society as a measure put in place to protect the morals and rights of minors.

In June 2009, Facebook, the most popular social networking site among minors in Denmark, in their response to a letter from the Danish Data Protection Authority, rejected the Article 29 group's interpretation of online jurisdiction [xvi] by emphasizing the physical placement of their equipment and referencing their adherence to the US/EU Safe Harbor Agreement [xvii]. Remindful of the ECHR decision in Perrin against UK and KU V. Finland, the question left to be answered is how the effectiveness of measures taken by the Danish state to e.g. secure the protection of minors on online social networking sites, such as Facebook, operated in states not parties to the convention, would or could be assessed by the ECHR.

The Essence of Obligations

The global network society challenges the fundamental right to privacy as it is described in human rights instruments such as the European Convention of Human Rights. In this context, the ECHR case law is shaping the positive obligations of states. T he greater need for data protection safeguards when technological progress advances the methods for intelligence gathering is e.g. acknowledged by the ECHR in its case law. Furthermore, the ECHR emphasizes that state parties should be prepared for the new online character of activities that might have an effect on citizens' right to privacy, particularly in the sphere of the protection of minors, and that it is the state's task to reconcile the various claims competing online. However, there is still uncertainty as to the essence of a state's obligations (jurisdiction) in the context of global information systems. The current clashes between the US and EU data protection standards for example illustrate the legal challenges that particularly online technologies and the potential of automated processing and collection of data have effectuated. The ECHR case law dealing with cross-border internet activities is limited, but presently dealt with in other foras such as the Council of Europe's advisory group on the cross-border internet and at the EURODIG and UN Internet Governance Forum [xviii] as well as in instruments such as the Convention against Cyber Crime (2001). These activities might provide an interpretative framework for the question of jurisdiction in the global network society.

[i] See e.g. Case of S. and Marper v. the United Kingdom, Application no. 30562/04 and 30566/04, §71 *"...bearing in mind the rapid pace of developments in the field of genetics and information technology...."* , §75 *"..their processing through automated means allow the authorities to go well beyond neutral identification"* , §105 *"..the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification"*

[ii]S. and Marper v. the United Kingdom, safeguards detailed in §99, §103 *"The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned...."*. Gabrielle Weber and Cesar Richard Saravia against Germany (dec. admissibility), Application no. 54934/00 safeguards detailed in §95, §93 *"...especially as the technology available for use is continually becoming more sophisticated."*

[iii] Gabrielle Weber and Cesar Richard Saravia against Germany, §78. S. and Marper v. the United Kingdom §67. Case of Liberty and Others v. the United Kingdom, Application no. 58243/00 §56.

[iv] See e.g. S. and Marper v. the United Kingdom §112 *"The court observes that the protection afforded by Article 8 of the convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests"*

[v]Liberty and Others v. the United Kingdom §62 foreseability because of risk of arbitrariness. Gabrielle Weber and Cesar Richard Saravia against Germany, complaints under article 8 ii Quality of the law §93 *"...It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated."*

[vi] CASE OF K.U. v. FINLAND, Application no. 2872/02

[vii]See e.g. Bankovic and others v. Belgium and others (dec. admissibility), Application no. 52207/99, (b) the meaning of the words "within their jurisdiction" §61. Mohamad Ben El Mahi and others against Denmark, Application no. 5853/06, the Court references the preparatory material where the words *"all persons residing within their territory"* is changed with a reference to persons *"within their jurisdiction"* and found no jurisdictional link between any of the applicants and Denmark.

[viii] Joanna Kulesza, INTERNET GOVERNANCE AND THE JURISDICTION OF STATES JUSTIFICATION OF THE NEED FOR AN INTERNATIONAL REGULATION OF CYBERSPACE, 2008, p. 1.

[ix] Case of Ilascu and others v. Moldova and Russia, Application no. 48787/99, §313-319

[x]Gabrielle Weber and Cesar Richard Saravia against Germany (dec. admissibility), Application no. 54934/00.

[xi] The public data retention debate in Germany has since the lodging of the Weber complaint reached new levels in Germany with the introduction of the requirements of the EU Data Retention Directive. See among others a recent development: http://www.vorratsdatenspeicherung.de/content/view/362/79/lang,en/ . See also II.1. in EC's draft evaluation report of the EU Data Retention Directive: http://www.vorratsdatenspeicherung.de/images/RoomDocumentEvaluationDirective200624EC.pdf

[xii] Report of the Special Rapporteur Martin Scheinin on the Promotion and protection of human rights and fundamental freedoms while countering terrorism, Human Rights Council, December 2009.

[xiii]COUNCIL DECISION 2010/16/CFSP/JHA

[xiv]See e.g. The Article 29 Working Party's examination of the agreement: http://www.statewatch.org/news/2010/jan/eu-art-29-cttee-swift.pdf . EDRI's FAQ on the Swift Agreement: http://www.edri.org/files/SWIFT-FAQ-2010-02-09.pdf

[xv] Stephane Laurent Perrin against the United Kingdom (dec. admissibility), Application no. 5446/03

[xvi] See Opinion 1/2008 on data protection issues related to search engines, p. 11 under "Establishment on the territory of a member state (EEA)" - use of cookies requires adherence to the national law in question. Opinion 5/2009 on online social networking under "Who is the data controller?"

[xvii]http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Facebook_Svar.pdf

[xviii] See e.g. Council of Europe BLOGGED Submission to the Internet Governance Forum, Athens, Greece, 30 October to 2 November 2006