Andreas von Arnauld, Freiheit und Regulierung in der Cyberwelt: Transnationaler Schutz der Privatsphäre aus Sicht des Völkerrechts, in: Freiheit und Regulierung in der Cyberwelt – Rechtsidentifikation zwischen Quelle und Gericht, Berichte DGIR Bd. 47, Heidelberg 2016.

Summary

Freedom and Regulation in the Cyber World: Transnational Protection of Privacy from the Perspective of Public International Law

by Prof. Dr. Andreas von Arnauld, Walther Schücking Institute, Kiel

I. Cyber World Amidst Changing Paradigms

1. The predominant view regarding the internet at any given time is reflected in the discussions on its adequate legal regime. A first phase was dominated by the libertarian idea of a de-nationalised space of unlimited opportunities which later gave way to a conception of the internet as a medium for global development. For several years now, we have found ourselves in a third phase of the discussion with a focus on security and protection against threats.

II. Threats to Privacy on the Internet

2. As the programmes "Prism" (NSA) and "Tempora" (GCHQ) show, surveillance of large parts of global internet communication is both technically feasible and carried out in practice. Additionally, large-scale private "data mining" takes place. Detailed user profiles that can be related to real persons are generated, especially for advertising purposes. Often enough, security services access these private databases to circumvent restrictions on data collection by public authorities.

3. The challenges to data protection are essentially familiar, net communication merely intensifying many known problems. It is not necessary to develop a new *lex digitalis*. What is necessary, however, is the adaption of the law as it stands to the specificities of internet communication.

4. The internet makes it possible to access the same set of data from practically anywhere in the world. This is in stark contrast to a traditionally territory-oriented international law that aims at delimitating jurisdictional spheres and mitigating conflicts of jurisdiction by differentiation between jurisdiction to prescribe and jurisdiction to enforce.

5. Internet Access Providers and Internet Service Providers have a vast amount of private or even intimate data at their disposition. Though the mediatisation of private actors in international law has been modified in many respects, binding them to data protection standards presupposes either voluntary self-commitment or national legislation.

6. Technological standards and programming delineate the possibility and modalities of communication in cyberspace. Privacy is threatened if programmes are specifically designed to collect data. Attempts by individual States to regulate these codes are confronted with a plurality of competing jurisdictions. Furthermore, it has proven difficult to counteract an established code.

III. Possible Approaches to the Protection of Privacy on the Internet

1. Point of Departure: A Global Right to Digital Privacy

7. When searching for a global solution, a starting point is needed which has potentially universal bearing without, for the time being, requiring uniform standards in detail. Furthermore, effective implementation must be possible by decentralised means. Human rights-based "constitutional vocabulary" is needed to hedge in transnational threats to privacy. A global right to digital privacy is a realistic utopian project to which international jurisprudence should contribute. Such a right can be based on, inter alia, Art. 17 ICCPR and Art. 8 ECHR. Its transnational effects, however, are not yet fully established.

8. For binding public authorities to human rights, a territorial nexus is a sufficient, but not a necessary condition. To take the infrastructure of internet communication as a reference point leads to arbitrary results and practically invites evasive practices. Physical control over territory or over persons has in large part been rendered unnecessary by technological progress. A functional approach is therefore required, taking into account a State's power to act and to cause effect. Here it becomes necessary to distinguish between negative and positive obligations. Only positive obligations are limited by the sovereign rights of other States and connected to authority and control over territory or persons.

9. There must not be any distinction between nationals and non-nationals with regard to the surveillance of external telecommunication as the right to privacy is entrenched in human dignity – and as foreigners do not *per se* present a greater threat to national security.

2. Concretisations: Possible Approaches to Regulation

a) Negative Obligations: The Duty to Respect Digital Privacy

10. Any collection, retention, processing or transfer of personal data constitutes an interference with the right to privacy. Such interferences are only permissible when authorised by laws that (i) are publicly accessible; (ii) tie the collection of, access to and use of data to specific legitimate aims; (iii) contain sufficiently precise provisions on the reasons for and the procedure and duration of the interference as well as on the categories of persons who may be placed under surveillance; and (iv) provide for effective safeguards against abuse.

11. Interferences are only allowed for the protection of community interests of paramount importance and must be necessary in a democratic society. The principle of proportionality prods States towards data reduction and area-specific regulations. It is vital that data may be collected only for strictly predetermined, specific purposes; this also limits permissible data transfer. "Big data" is not a viable concept for security agencies.

b) Positive Obligations: The Duty to Protect Digital Privacy

12. The right to digital privacy, inter alia, obligates the State to protect persons on territory under its control against encroachments by others. Generally, States enjoy a wide margin of discretion in this regard, especially in the field of foreign affairs.

13. Sovereignty and immunity limit the possible reactions towards other States to, mostly, diplomatic means and, if applicable, inter-State complaints. Insofar as acts of surveillance amount to an arrogation of public authority on another State's territory, that State might even resort to counter-measures. More options for exerting influence are given in the context of negotiating and concluding international treaties. When agreeing to the transboundary transfer of data, a comparable level of data protection must be guaranteed. Stricter international regulation of secret service activities seems less promising. Finally, no-spy agreements treat data protection as a club good and do not contribute to solving the problem globally.

14. Concerning domestic private corporations, the *lex lata* does not yet obligate States to regulate their external activities. However, public outrage and the model presented by EU data protection standards could contribute, each in their way, to the development of a human-rights based no-harm rule. Alternatively (or accompanying this process), best practices could be agreed on. These, in turn, could be used to substantiate the inter-State standard of due diligence.

15. The principle of consent which is a key element of civil data protection law is in a process of erosion. The quality of consent given can be raised by privacy by default measures. Where necessary, the legislator may also protect the users' privacy irrespectively of their consent. The traditionally behaviour-oriented data protection law must be complemented by a genuine "technology law" realising privacy by design. "Big data" raises serious concerns also with a view to private data collection.

16. The ECJ's "Google" judgment (C-131/12 of 13 May 2014) is not an expression of European imperialism in the field of data protection. Extraterritorial effects of EU data protection laws are not due to an extension of the EU's jurisdiction to prescribe but a consequence of technological development. Providers of internet services must conform to the data protection laws effective in the EU when operating there, otherwise a dis-targeting of IP addresses from EU member States is technologically possible. Where EU standards interfere with a right to market access, a fair balance has to be struck. This means acknowledging that the company has its feet planted firmly on two grounds, i.e. different legal orders. Indirectly, the required proportionality test becomes the place for realising practical concordance (*praktische Konkordanz*) between competing jurisdictions.

c) Necessity of a Fair Balance

17. There are legitimate reasons for private and public data collection; at this time, however, it seems important to strengthen the protection of privacy in the internet. A cautious and well-balanced unilateralism – especially from the EU and its Member States – may provide important momentum towards the establishment of a global right to digital privacy.

IV. On the Road to a Transnational Regime of Privacy Protection

18. Given its blurring of boundaries between public and private law, internet law is particularly apt as a reference field of "transnational law". At the same time, it does remain important to differentiate between public and private actors.

19. States are called upon, in particular, to protect people on their territories against seizure of personal data and to prevent human rights violations by external activities

of their domestic companies. They serve an important function also as norm-entrepreneurs on the international plane. Their legislative function can benefit from the advice of data protection commissioners, ideally complemented by networking among the commissioners themselves. On the level of international organizations, the United Nations, in particular, have the important task of supplying a forum and of supporting the evolution of a global right to digital privacy.

20. In the process of developing adequate rules for the protection of privacy in the internet it is vital to involve the "net community" (represented by commercial as well as non-profit organisations) in a multi-stakeholder setting. However, even a polycentric and interactive regulatory culture demands a public law framework in order to avoid the conservation of private power structures.