

## **The Legality of Internet Blackouts in Times of Crisis An Assessment at the Intersection of Human Rights Law, Humanitarian Law and Internet Governance Principles**

*Matthias C. Kettemann*  
University of Graz, Austria

– Draft –

### **1. Introduction**

- On 28 January 2011, Egyptian authorities ordered the country's Internet Service Providers to shut down. On 5 March 2011, Libya shut down its data traffic. Already in 2009, Iran had greatly reduced connection speed, and China had shut down the Internet in the region of Xinjiang. What connects all of these cases of Internet blackouts in times of crisis is the lasting conviction by governments that shutting down information and communication channels in times of crisis increases the country's stability and security, as defined by the ruling authority. Given the potential of information and communication technologies (ICTs) it is highly likely that this pattern will continue in times to come. Therefore, an evaluation of the legal framework that governs Internet shutdowns is urgently required.
- Against this background I will enquire whether states can shut down the Internet because of reasons of "national security" and what international rules limit their behavior. After an introduction (section 1), I will elaborate on the normative frame provided by human rights law (section 2), humanitarian law (section 3) and by Internet Governance Principles (section 4). In my conclusions, I will show that Internet blackouts do not occur within a legal black hole and are only legal in very specific situations (section 5). The legal framework I will develop in my paper will help assess states' actions, point out their legal limits, and frame the response of the international community.

### **2. Internet Shutdowns and Human Rights Law**

- What limits does human rights law set for states to shut down the Internet in times of crisis?
- The Internet has become "the public space of the 21st century – the world's town square, classroom, marketplace, coffeehouse, and nightclub."<sup>1</sup> As a room where opinion are shaped and articulated, the Internet therefore needs to be protected.

---

<sup>1</sup> Secretary of State Hillary Rodham Clinton, Internet Rights and Wrong: Choices and Challenges in a Networked World, George Washington University, Washington, D.C., 15 February 2011, <http://www.state.gov/secretary/rm/2011/02/156619.htm>

- Communicator, recipient and the content of the communication are protected through human rights law.
- Articles 19 of the Universal Declaration of Human Rights<sup>2</sup> and the International Covenant on Civil and Political Rights (ICCPR) provide a very broad level of protection which has developed into a number of different freedoms: freedom of opinion, freedom of expression, freedom of information, freedom of thought, right to privacy ....<sup>3</sup>
- Arguing that the essence of the rights and freedoms protected by Article 19 has crystallized into a norm of international customary law I will affirm the norm's applicability independent of state commitments. This crystallization process has been consistent.<sup>4</sup> The applicability of the protection to the Internet is clear.<sup>5</sup> Based on this practice the Security Council, in Resolution 1970 of 26 February 2011, underlined "the need to respect the freedoms of peaceful assembly and of expression, including freedom of the media" and, in Resolution 1973 of 17 March 2011, condemned the "acts of violence and intimidation committed by the Libyan authorities against journalists, media professionals and associated personnel".
- Additionally, the vast array of activities the Internet is used for today makes Article 22 (freedom of assembly; as an institutionalized form of freedom of expression) and Article 25 (right to political participation) relevant for a human rights-based analysis of Internet shutdowns.
- Apart from these individual human rights protection guarantees I will also argue that the Internet enjoys institutional protection pursuant to Article 19 (3) in connection with Article 2 (1) and (2) of the ICCPR as a medium for individuals to enjoy their information and communication rights and freedoms.
- After having painted in broad strokes the human rights protection regime, I will analyze under which conditions states can legally limit information and communication rights and freedoms through Internet shutdowns.

---

<sup>2</sup> „Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers“.

<sup>3</sup> Freedom to express an opinion (Art 19 para. 2 ICCPR, Art 10 para. 1 ECHR, Art 13 ACHR, Art 9 para. 2 AfrCHR); freedom of opinion (Art 19 para. 1 ICCPR, Art 10 para. 1 ECHR); freedom of information (retrieval: Art 19 para. 1 ICCPR, Art 13 ACHR; reception and re-communication: Art 19 para. 1 ICCPR, Art 10 ECHR, Art 13 ACHR, Art 9 para. 1 AfrCHR); freedom of thought (Art 18 ICCPR, Art 9 ECHR, Art 13 ACHR); right to privacy (Art 17 ICCPR, Art 10 ECHR, Art 11 para. 2 ACHR) and protection of one's correspondence (Art 8 para. 1 ECHR, Art 11 para. 2 ACHR).

<sup>4</sup> Mary Rundle and Malcolm Birdling, *Filtering and the International System: A Question of Commitment*, in: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press) 2008 (<http://opennet.net/accessdenied>), 73-103.

<sup>5</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/17/27 vom 26.4.2011, 69, 72.

- First, we can determine that any regional or national shutdown or serious slowing of connection speeds touches upon the communication freedoms protected by human rights law. Limitations are possible, but they need to be provided by law, necessary for a specific, legitimate purpose – such as national security – and proportional.
- Often, limitations are based on factual acts without a legal foundation. This makes them a priori illegal.
- But there are some cases where authorities will argue that a shutdown is necessary for national security or the protection of ordre public. Calls to war or to political violence can be seen as a legitimate threat which needs to be stopped.<sup>6</sup> With regard to the extent of the protection of freedom of expression through the International Covenant on Civil and Political Rights, the Human Rights Committee, its supervisory organ, has clearly ruled that “The legitimate objective of safeguarding and indeed strengthening national unity under difficult political circumstances cannot be achieved by attempting to muzzle advocacy of multi-party democracy, democratic tenets and human rights; in this regard the question of deciding which measures might miss the “necessity” test in such situations does not arise.”<sup>7</sup>
- Similarly, in the Syracuse Principles, the High Commission for Human Rights has underlined that national security may not be used to justify arbitrary limitations.<sup>8</sup>
- If a state can show that the aim of the limitation is legitimate, the relationship between the limitation and the goal pursued must still be proportionate.<sup>9</sup> Freedom of expression itself, as the Human Rights Committee stated, must not be endangered itself.<sup>10</sup>
- Expect very limited cases, a blanket regional or national shutdown is therefore unjustifiable under international human rights law.
- What would be justifiable, however, would be a law targeting servers from which dangerous “hate speech” (“Mille Collines servers”) emanates, which could be shut down.

---

<sup>6</sup> Nowak, Commentary to the ICCPR, Art. 19, Rz 54.

<sup>7</sup> Mukong v. Cameroon, U.N. Doc CCPR/C/51/D/458/1991 (1994), para 9.7.

<sup>8</sup> Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/4 (1984), <http://www.uio.no/studier/emner/jus/humanrights/HUMR5503/h09/undervisningsmateriale/SiracusaPrinciples.pdf>, para. 31.

<sup>9</sup> United Nations Human Rights Committee, General Comment No. 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant, U.N. Doc CCPR/C/21/Rev.1/Add.13 (2004), para. 3. Siehe auch Park v. Korea Comm. No. 628/1995, Para. 10.3; Laptsevich v. Belarus Comm. No. 780/1997, Para. 8.2.

<sup>10</sup> United Nations Human Rights Committee, General Comment No. 10: Freedom of Expression (29 June 1983), para. 4.

### **3. Internet Shutdowns and Humanitarian Law**

- What protection does international humanitarian law (IHL) provide for the Internet in cases of conflicts?
- Though questioned by a growing number of scholars, IHL still recognizes the applicability of different regimes to international and non-international armed disputes and the applicability of human rights law in cases of conflicts.
- In addition to protection under HR law, the Internet may also be protected as a “critical infrastructure” under IHL. The deliberate destruction of “works or installations containing dangerous forces”, such as dams, is forbidden under Art. 56 of the First Additional Protocol to the Geneva Conventions. The Internet as such is no „dangerous force“ and a customary addition of the list of objects considered critical infrastructure has not yet been taken place. Thus, only the principle of proportionality (Art 51(5)(b) AP1) could stop Internet shutdowns by one party in a conflict under IHL, if serious consequences might follow.
- Arguing that shutting down the Internet will stop the other party to the conflict from communicating effectively though will regularly allow for shutdowns under IHL in light of the principle of military necessity.

### **4. Internet Shutdowns, Global Obligations and Internet Governance Principles**

- In section 4 I will develop on the limits that the emerging framework provided by Internet Governance Principles sets for states. What duties, I will ask, exist for states with regard to the integrity, stability and functionality of the Internet and in how far do these set limits to Internet shutdowns.
- Violations of the freedom of expression are usually not considered by the international community to be as serious as the violation of the right to life or the prohibition of torture. But what about the interest of the international community in the integrity and stability of the Internet as such? What do recently emerging Internet Governance principles say about that?
- Over the years, international lawyers have increasingly recognized that the Internet is a global, critical resource which needs to be protected: states have a common and shared responsibility, similar to the one existing regard international rivers and lakes.
- The Tunis Commitment clearly commit state to a “people-centred, inclusive and development-oriented Information Society” [...] “premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism” [...]“respecting fully and upholding the Universal Declaration of Human Rights”. States confirm the “universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as

enshrined in the Vienna Declaration.”<sup>11</sup> They also committed to a a stable and secure Internet as a global institution.<sup>12</sup>

- Now – does the state shutting down the Internet have duties vis-à-vis the international community? And are the global duties of the international community from which emerge concrete obligations if a state cuts the net?
- There exists a customary law erga omnes duty of the state shutting down the Internet towards the international community. This duty can be developed in analogy to the environmental law principles of *sic utere tuo ut alienum non laedas*. States have to do their utmost to refrain from harming other states. Under international law, this duty exists mainly with regard to neighbours. In the times of the Internet, this duty is global. It can therefore be argued that there an erga omnes duty of each state regarding the stability, integrity and functionality of the Internet as such has crystallized into customary law.<sup>13</sup>
- The development towards formalizing these obligations has been supported by the the Council of Europe’s work on the principles regarding the protection and promotion of the universality, integrity and openness of the Internet, including notably the very recent Recommendation of 21 September 2011.<sup>14</sup>
- The duties are enriched by the principles of Internet Governance<sup>15</sup> that have been recently emerging and by the work on the role of human rights in the Internet, including by the Dynamic Coalitions.

---

<sup>11</sup> World Summit on the Information Society, Tunis Commitment, WSIS-05/TUNIS/DOC/7-E, 18.11.2005, Z. 2-3.

<sup>12</sup> World Summit on the Information Society, Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, Z. 29.

<sup>13</sup> Vgl. Rolf H. Weber, New Sovereignty Concepts in the Age of Internet, Journal of Internet Law, August 2010, 12-20 (17).

<sup>14</sup> Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers’ Deputies, [https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec\(2011\)8&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383](https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Rec(2011)8&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383). For the background, see Council of Europe, Ad Hoc Advisory Group on Cross-border Internet (Bertrand de la Chapelle, Wolfgang Kleinwächter, Christian Singer, Rolf H. Weber, Michael V. Yakushev), International and multi-stakeholder co-operation on cross-border Internet. Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder co-operation on cross-border Internet, Council of Europe Doc. H/Inf (2010) 10, 2010, <http://www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI%20Interim%20Report.pdf>.

<sup>15</sup> Declaration by the Committee of Ministers on Internet governance principles, Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers’ Deputies, [https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Del/Dec\(2011\)1121/5.1&Language=lanEnglish&Ver=app8&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864](https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Del/Dec(2011)1121/5.1&Language=lanEnglish&Ver=app8&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864).

- What is especially important is the extent and impact of the need of states to protect human rights and freedoms online and the duty of states to refrain from impacting negatively the global, unhindered and cross-border Internet traffic.
- There are however, not yet, any clear indicators of global duties of action beyond political measures. This tear in the protection blanket must urgently be sewn shut.
- Concluding, Internet Governance Principles, especially those confirming the importance of human rights protection and the obligations of states regarding the integrity, functionality and stability of the Internet in a cross-border context, have crystallized into obligations limiting Internet shutdowns internationally and nationally. A clearly defined obligation of states to react, however, has not yet emerged.

## 5. Conclusions

- It is of great importance, both as a policy and legal matter, to ensure, especially in times of crisis, the viability of information and communication channels. While international human rights law sets clear limits to state attempts to suppress the mobilization and articulation of democratic dissent, an analysis of international humanitarian law provides a more nuanced picture and sets only few limits to shutdowns. The emerging Internet Governance Principles, again, lay down the duties of states regarding the integrity, functionality and stability of the Internet, but also figure as a source for states' human rights obligations.
- It is unlikely that the Security Council will ever conceive Internet shutdowns as serious enough human rights violations to merit a chapter VII resolution. Nevertheless, the reference to both the importance of the freedom of expression and the explicit condemnation of the violence against “journalists, media professionals and associated personnel” in the two recent Libya resolutions sends an important signal. “Associated personnel” should be read, in my mind, to also include bloggers and citizen journalists.
- Though there is no failsafe protection against Internet shutdowns a diversified server landscape can help. A recent Freedom House study has shown that 19 states – among them Egypt, Cuba, Iran, Thailand and Tunisia – have only a very limited and centralized server structure.<sup>16</sup> This should be cause for concern.
- Finally, I'd ask you to keep one thing in mind: There is historically a strong – at least coincidental – connection between Internet filtering, Internet shutdowns and systematic human rights violations against the democratic opposition. By shutting down the Internet in times of crisis, states send an important signal: that they are ready to attack protest movements without international and national control and critique. This is, when the international community and all of its stakeholders must act.

---

<sup>16</sup> Sanja Kelly, Sarah Cook (eds.), Freedom on the Net 2011. A Global Assessment of Internet and Digital Media, Freedom House 2011, <http://www.freedomhouse.org/uploads/fofn/2011/FOTN2011.pdf>, 6-7.