Institut für Öffentliches Recht

Völkerrecht und Rechtsvergleichung

UNI FREIBURG

Freiburger Informationspapiere zum Völkerrecht und Öffentlichen Recht

Silja Vöneky (Hrsg.)

Freiburg 3/2015
ISSN 2192-6077

Silja Vöneky (Hrsg.)
Freiburger Informationspapiere zum Völkerrecht und Öffentlichen Recht

SECURITY INTERESTS, HUMAN RIGHTS, AND ESPIONAGE IN THE SECOND MACHINE AGE – NSA MASS SURVEILLANCE AND THE FRAMEWORK OF PUBLIC INTERNATIONAL LAW

by Silja Vöneky

Freiburg 3/2015

Silja Vöneky (Hrsg.) - Institut für Öffentliches Recht
Abteilung 2 (Völkerrecht und Rechtsvergleichung)
Rechtswissenschaftliche Fakultät
Universität Freiburg
Platz der Alten Synagoge 1
79098 Freiburg im Breisgau
voelkerrecht@jura.uni-freiburg.de

Freiburger Informationspapiere zum Völkerrecht und Öffentlichen Recht
ISSN 2192-6077
www.fiponline.de

Content

"The same tools that make it possible to monitor the word in greater detail also give governments and their adversaries the ability to monitor what people are doing and who they are communicating with. There`s a genuine tension between our ability to know more and our ability to prevent others from knowing about us. When information was mostly analog and local, the laws of physics created an automatic zone of privacy. In a digital world, privacy requires explicitly designed institutions, incentives, laws, technologies, or norms about which information flows are permitted or prevented and which are encouraged or discouraged."

Erik Brynjolfsson/Andrew McAfee, The Second Machine Age, 2014, 253

A. Introduction[1]

States argue that their existence, State security and the safety of their populations depend on the information that they gather without the consent of those States and individuals which are the aim of the secret information gathering. For a State to exist or not to exist seems to depend on its decision to spy or not to spy.

The phenomenon of espionage is not a new one, but has always been a common practice in international relations in both times of war and times of peace.[2] But in contrast to the time of the cold war, there is a twofold radical change concerning espionage: on the one hand, there is a radical change of the means of espionage and, on the other, a radical change of the focus of security concerns in the 21st century.

The radical change of the means of espionage is caused by the new tools of the digital world, the second machine age: Today the capacity of governments – besides companies, non-state actors, and even individuals – to keep people under surveillance, to intercept and to collect data has increased to

[1] I am grateful to Mr. Felix Beck and Mr. Jakob Jürgensen for their support and valuable impact. The final version of this paper will be published soon.

[2] Schaller, C., Spies, in R. Wolfrum (ed.), Max Planck Encyclopedia of Public International Law (MPEPIL), Vol. IX, 2012, p. 435, para. 2.

an unprecedented scale.[3] We can now speak of digital mass surveillance and bulk information that is gathered by different entities.[4]

These new tools of espionage come together with new major concerns in security issues; the major concerns today are the unknowns and the so-called "black swans". The latter are understood as very rare cases whose probability of occurrence is not (but close to) zero and which have potentially huge consequences.[5] These are things and persons we do not know yet, but which are able to kill people, damage our environment and economy, destabilize our governments and hence endanger the existence of a State and a society now or in the near future.

How are these two radical changes linked? One can give an example that concerns a current debate: During the last two years there was an intense discussion on biosecurity issues. The notion of biosecurity describes the problem of dual use in the biological sciences. There nobody knows how to rationalize or quantify the risk of bioterrorism, i.e. the misuse of biological agents by terrorists. But if a society and its State organs do not know whether there is a concrete danger of misuse of certain viruses it is difficult to argue that there is a need for certain tools to prevent these kinds of terrorist attacks, for instance by establishing a new dual use research of concern-commission that evaluates experiments or by setting rules of non-publication if the results of experiments could be misused by criminals.[6] All the tools to prevent bioterrorism would limit the freedom of research; and as freedom of research is a human right as well, this may be done only if it can

---

[3] Cf. for instance Report of the Office of the United Nations High Commissioner for Human Rights (OHCHR), The right to privacy in the digital age, Human Rights Council, UN Doc. A/HRC/27/37, 30 June 2014, p. 3. The report is based on GA Res. 68/167, December 10, 2013.

[4] OHCHR, UN Doc. A/HRC/27/37 (n. 3), p. 3.

[5] Cf. Taleb, N. N., The Black Swan: The Impact of the Highly Improbable, 2007, p. 44 et seq.

[6] For further details see Vöneky, S., Biosecurity – Freedom, Responsibility, and Legitimacy of Research, Ordnung der Wissenschaft 2/2015, p. 117 et seq., available at: http://www.ordnungderwissenschaft.de/.

be justified. Abstract dangers alone do not seem to be sufficient to limit this right. Hence it seems rational for a government that wants to protect human rights to minimize the unknowns and to substantiate whether there are concrete dangers for the people of a country.

And one can go a step further: If the unknowns and the so-called "black swans" are the big concerns of our security in the 21st century, it is not astonishing that information gathering is one of the main and most important tools to make a society safe and to secure the existence of a State. And information gathering today, in the second machine age, is a very smooth tool: it is clean; it is beneath the surface of our everyday life; usually we do not see, hear or feel it. There is no clicking in the telephone in contrast to – for instance – the secret police action in the former German Democratic Republic. So big data based and internet based espionage is not virtual but it seems to be. Besides this, secret internet based data collection is a tool that we are used to. Digital information gathering is integrated into our daily life in commercial contexts: we are used to the fact that while surfing the internet, advertisements pop up that correlate to our interests and wishes and often there was no express informed consent beforehand given beforehand. This does not mean – and it shall not be stated – that the collecting of internet user data by companies for commercial purposes is the same as secret internet based espionage by a State organ, as the National Security Agency (NSA) in the US, or by private companies on their behalf. But the lines are blurred.

Hence it is not astonishing that there were huge demonstrations against the Pershing NATO missiles during the 1980s in Germany, but that there are nearly no demonstrations against NSA activities and other information gathering by foreign States or companies on behalf of foreign States today. The modern tools to fight security dangers are smart, clean and without an angst-inducing symbolic manifestation.[7]

---

[7] Cf. for instance Chita-Tegmark, M., Terminator Robots and AI Risk, Huffington Post, 02.03.2015, available at: http://www.huffingtonpost.com/meia-chitategmark/terminator-robots-and-ai-risk_b_6788918.html.

The situation is even more complicated as those persons, who endanger a society, live in the middle of free and democratic States: it is neither so much the Taliban in Afghanistan nor even the so-called "Islamic State" (IS) in Syria and Iraq which can destabilize Germany or the US. The main enemy is embedded in our society: the terrorists of 9/11 studied and lived in Hamburg; the Boston and Paris terrorists studied and/or lived in the US and France.[8] European newspapers are full of news that terrorist fighters are coming back to western countries, after having fought for the IS. According to a certain rationale, every citizen of Germany, France, the US etc. can be the next Mohammed Atta, Dzokhar Tsarnaev, or "Jihadi John"; therefore, everybody seems to be a legitimate aim of secret data collection.

So a diffuse and abstract danger to the public is answered and shadowed by diffuse and abstract observation, a meta-observation: an observation that has a rational aim (decrease the unknowns), often no manifestation, and hence nearly no burden to our daily life – at least as long as our assets are not frozen, we are not detained, we are not denied access to another State

---

[8] Mohammend Atta, one of the 9/11 terrorists, the hijacker-pilot of American Airlines Flight 11, studied for many years at the Technische Universität Hamburg-Harburg, Germany; Tamerlan Tsarnaev, one of the terrorists of the Boston Marathon Bombing, studied at the Bunker Hill Community College, Boston/, US; Dzokhar Tsarnaev, the second Boston Marathon Bombing terrorist, studied at the University of Massachusetts, Dartmouth, US and had been an US citizen since 2012, cf. Finn, P. et al., Tamerlan Tsarnaev and Dzhokhar Tsarnaev were refugees from brutal Chechen conflict, Washington Post, April 19, 2013, available at: http://wpo.st/2UP80; US Federal Bureau of Investigation, Updates on Investigation Into Multiple Explosions in Boston, available at: http://www.fbi.gov/news/updates-on-investigation-into-multiple-explosions-in-boston/updates-on-investigation-into-multiple-explosions-in-boston; Ross, A., Der Körper der Muslime, Frankfurter Allgemeine Zeitung, March 4, 2015, p. 3. The "Islamic State" militant known as "Jihadi John", who has been pictured in the videos of the beheadings of Western hostages, is a British national from west London who finished his computing degree at the University of Westminster, United Kingdom, in 2009, cf. BBC news, 26.02.2015, available at: http://www.bbc.com/news/uk-31637090 (all internet sources last retrieved March 13, 2015).

and we are not killed by a drone missile strike. But the latter are very rare consequences one of us will hardly ever face.

B. The Framework of Public International Law

It is not astonishing that public international law has a rather ambivalent approach towards espionage. The very banal reason is that the States have an ambivalent approach to espionage. The main elements of the espionage framework according to international law are the following.

Firstly, to fight enemies and protect one`s own population from attacks, stemming from terrorists or other states, is a legitimate aim according to international law. Some even argue that there is a "responsibility to protect" as an emerging norm of international law9 and hence sovereignty includes the States' duty to protect their populations from mass atrocities and crimes.[10] Even if one does not want to rely on the rather vague concept of responsibility to protect, one can deduce such a duty from the human rights of life and health that are laid down in human rights treaties: a State has to protect these human rights not only against infringements by State officials, but also against infringements by private actors, and protect its population.[11]

Secondly, there is neither a general prohibition of espionage in international law nor a general justification of espionage in international law.[12] Even according to the laws of war – the humanitarian law – a spy is not a combat-

---

[9] Cf. Winkelmann, I., Responsibility to Protect, MPEPIL (n. 2), Vol. VIII, 2012, p. 965, para. 1, 22; International Commission on Intervention and Sovereignty, The Responsibility to Protect – Report of the International Commission on Intervention and State Sovereignty, 2001, available at: http://responsibilitytoprotect.org/ICISS%20Report.pdf (last retrieved March 13, 2015), para. 2.24.

[10] Cf. UN General Assembly, 2005 World Summit Outcome, September 16, 2005 UN Doc. A/RES/60/1, para. 138.

[11] Cf. Art. 6 ICCPR: „Every human being has the inherent right to life. This right shall be protected by law." Tomuschat, C., International Covenant on Civil and Political Rights, MPEPIL (no. 2), Vol. V, 2012,p. 639, para. 18-19.

[12] Ewer, W./Thienel, T., Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, p. 30, 31.

ant,[13] hence not a prisoner of war and espionage can be prosecuted according to the criminal laws of a State when a spy is captured during wartime for espionage.[14] So even in an international armed conflict – although it is allowed for combatants to attack and kill enemy combatants if there is a military aim and no excessive so-called collateral damage – there is no per se justification for espionage according to international law.

Thirdly, espionage for the purpose of preventing terrorism nevertheless is part of the system of collective security.[15] The UN Security Council has clearly stated many times that it regards "any act of terrorism […] as a threat to peace and security"[16] and strongly urged States to prevent the transit of terrorists to and from countries, arms for terrorists, and financing that would support terrorists.[17] The Council is recalling that all States must cooperate fully in the fight against terrorism, in order to find and bring to justice any person who supports, facilitates, participates or attempts to participate in the financing, planning, preparation or commission of terrorist acts.[18] So today intelligence cooperation has become an accepted instrument for combating

---

[13] Cf. Annex to the Convention respecting the Laws and Customs of War on Land ('Hague IV'), concluded October 18, 1907, entry into force January 26, 1910, 205 CTS 277, Art. 29-30; Protocol I Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts ('Additional Protocol I'), adopted June 8, 1977, entry into force December 7, 1978, 1125 UNTS 3, Art. 46 para. 1.

[14] Cf. Geneva Convention relative to the Treatment of Prisoners of War, concluded August 12, 1949, entry into force October 21, 1950, 75 UNTS 135 ('Geneva Convention III'), Art. 5 para. 3.

[15] Schaller, C., Spies, MPEPIL (n. 2), para. 2, 12.

[16]UN Security Council, Threats to international peace and security caused by terrorist acts, August 4, 2005, UN Doc. S/RES/1618 (2005), para. 1; see also Counter-Terrorism Committee of the UNSC, Security Council Resolutions pertaining to terrorism, http://www.un.org/en/sc/ctc/resources/res-sc.html (last retrieved March 13, 2015).

[17] UN Security Council, UN Doc. S/RES/ 1618 (n. 16), para. 6 .

[18] UN Security Council, UN Doc. S/RES/ 1618 (n. 16), para. 7.

terrorism;[19] it is not only part of the system of collective security but also of the new NATO doctrine after 9/11.[20]

Fourthly, this does not mean that the aim to combat terrorism trumps everything else and no legal limits exist according to international law: States may adopt measures against terrorism only "as may be necessary and appropriate and in accordance with their obligations under international law".[21] So States must ensure that any measures taken must "comply with all of their obligations under international law, in particular international human rights law" as the UN Security Council expressly stated.[22]

C. Espionage and International Human Rights Law

Therefore an important question to answer is whether and, if so, to what extent the existing rules of international human rights law limit espionage.

The protection of private life, as enshrined in Art. 8 European Convention of Human Rights (ECHR)[23] and Art. 17 International Covenant on Civil and Polit-

---

[19] Schaller, C., Spies, MPEPIL (n. 2), para. 2.

[20] NATO, Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, adopted by Heads of State and Government, November 20, 2010, available at: http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf, para. 25; NATO, Partnership Action Plan against Terrorism, November 22, 2002, available at: www.nato.int/cps/en/SID-E86475A7-0E19BA88/natolive/official_texts_19549.htm (both last retrieved March 13, 2015), para. 16.1.2.
rorism, November 22, 2002, available at: www.nato.int/cps/en/SID-E86475A7-0E19BA88/natolive/official_texts_19549.htm (both last retrieved March 13, 2015), para. 16.1.2.

[21] UN Security Council, Threats to international peace and security, September 14, 2005, UN Doc. S/RES/1624, para. 1.

[22] UN Security Council, UN Doc. S/RES/1624 (n. 21), operative clause 2.

[23] European Convention for the Protection of Human Rights and Fundamental Freedoms, concluded November 4, 1950, entry into force September 3, 1953, 213 UNTS 221, amended by Protocols Nos. 11 and 14, ETS No. 005.

ical Rights (ICCPR)[24] – to which e.g. Germany, Russia, and the US are parties[25] –, is aimed at securing information privacy.[26]

One major concern is the answer to the question of whether States Parties to human right treaties are bound by the human rights outside their territory. In my view it is not convincing to argue that human rights do not matter as long as persons outside the territory of the State are the aims and the victims of espionage.[27] In a global order with transnational State activities it is

---

[24] Concluded December 16, 1966, entry into force March 23, 1976, 999 UNTS 171.

[25] List of States Parties available at: http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en (last retrieved March 13, 2015).

[26] Article 17 ICCPR states: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." Art. 8 ECHR states: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." See the clear statement of the state community in GA Res. 68/167 (The right to privacy in the digital age), December 10, 2013: […] 4. *Calls upon* all States: (a) To respect and protect the right to privacy, including in the context of digital communication; (b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; (c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;"

[27] The International Court of Justice (ICJ) and the Human Rights Council clearly supported the extraterritorial application of human right treaties. Cf. ICJ, Advisory Opinion, Legal Consequences of the Construction of a Wall in the Occupied Palestinian

contrary to the object and purpose of human rights, as they are universal values, to restrict their application on the territory of a State party. So it is not the territory of a State which is decisive; instead it is decisive whether a person falls under the jurisdiction of a State: Different from the *Banković* decision[28] of the European Court of Human Rights, one has to argue that jurisdiction of a State is given if a State exercises factual power on the territory of a non-State or third party. Factual power is exercised by doing espionage at the territory of another State. If the protection of the private sphere is a universal human right, a global value, adverse factual effects must be considered to have the same relevance as adverse legal acts. This is at least true if a State has the effective control[29] of the adverse factual effects.

If one agrees with these arguments the next decisive question to answer is what is protected by the human right of private life, i.e. the right on information privacy: Looking at the object and purpose of this right, one has to argue that not only the targeted preservation of data, but also the general stockpiling of data are interferences with this right.[30] A justification of such interferences not only depends on a legitimate aim, the interference also has to be proportionate:[31] the reasons for the interference therefore have to be sufficient as well as appropriate with respect to the legitimate aim. The disadvantages for the affected individual have to be weighed against the importance of the legitimate aims pursued by the State; in the end a „fair balance" is necessary. So one could argue that preventive data collection is al-

---

Territory, July 9, 2004, ICJ Reports 2004, 136, para. 111; Human Rights Committee, Report of the Human Rights Committee to the 53rd Session of the United Nations General Assembly, UN Doc A/52/40, September 15, 1998. Cf. as well OHCHR, UN Doc. A/HRC/27/37 (n. 2), p. 11 et seq. However, the extraterritorial application of human right treaties is still disputed: The US administrations have always contested this view, referring to the history of the ICCPR, cf. Tomuschat, C., ICCPR, MPEPIL (no. 11), para. 24.

[28] European Court of Human Rights, Banković et al. v. Belgium et al. (decision on admissibility), no. 52207/99, ECHR 2001-XII.

[29] OHCHR, UN Doc. A/HRC/27/37 (n. 3), p. 11.

[30] For an even broader view see OHCHR, UN Doc. A/HRC/27/37 (n. 3), p. 7.

[31] OHCHR, UN Doc. A/HRC/27/37 (n. 3), p. 11.

ways disproportional and hence a violation of the human right of privacy if no actual terrorist threat exists. On the other hand one could argue that as long as we do not see, feel and hear the observation, this kind of meta-observation has only minor effects on privacy and therefore an abstract and diffuse terrorist threat is sufficient to justify this kind of espionage.

However, in any case: any limitation of this right has to be based on a legal rule which must be clear and precise.[32] Most importantly, the legal rule has to name the type of information, the group of affected people, the circumstances of the surveillance and the procedure.[33] In order to deter misuse, especially an effective and independent control mechanism[34] is necessary.[35] Hence the framework of international human rights law governing espionage is much clearer and much stricter than the framework of general international public law.

D. The Supplementary Agreement to the NATO Status of Forces Agreement

However, the question is whether international human rights law trumps other international rules. Apart from the human rights treaties, the 1959/1993 Supplementary Agreement to the NATO Status of Forces Agreement (NATO SOFA Supplementary Agreement)[36] could be decisive as far as espionage in and by Belgium, Canada, France, Germany, the Netherlands,

---

[32] OHCHR, UN Doc. A/HRC/27/37 (n. 3), 32.

[33] European Court of Human Rights, Rotaru v. Romania, no. 28341/95, ECHR 2000-V, para. 57.

[34] Rotaru v. Romania (n. 33), para. 59.

[35] Human Rights Commitee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), April 8, 1988, para.1 et seq.; European Court of Human Rights, Dumitru Popescu v. Romania, no. 71525/01, para. 72 et seq.

[36] Agreement to Supplement the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces with respect to Foreign Forces stationed in the Federal Republic of Germany of August 3, 1959, Federal Law Gazette 1961 II p. 1218, as amended by the agreement of March 18, 1993, Federal Law Gazette 1994 II p. 2594.

UK, and the US is concerned, as these States are Parties to the NATO SOFA Supplementary Agreement and the treaty entails rules that govern the exchange of information, even of personal data.

Art. 3 of the Agreement, dealing with the cooperation of the German authorities and authorities of the forces of the other States Parties, states:

> "1. In accordance with the obligations imposed by the North Atlantic Treaty upon the contracting parties thereto to render mutual assistance, the German authorities and the authorities of the forces shall cooperate closely to ensure the implementation of the NATO Status of Forces Agreement and of the present Agreement.
>
> 2. The cooperation provided for in paragraph 1 of this Article shall extend in particular
>
> (a) to the furtherance and safeguarding of the security, as well as to the protection of the property, of the Federal Republic, of the sending States and of the forces, and *especially to the collection, exchange and protection of all information which is of significance for these purposes;*
>
> (b) to the furtherance and safeguarding of the security, as well as to the protection of the property, of Germans, of members of the forces and members of the civilian components and dependents, as well as of nationals of the sending States who do not belong to these categories of persons.
>
> 3. (a) German authorities and the authorities of a Force shall, by taking appropriate measures, ensure close and reciprocal liaison within the scope of the cooperation provided for in paragraphs 1 and 2 of this Article. *Personal data shall be passed on solely for the purposes envisaged in the NATO Status of Forces Agreement and in the present Agreement. Restrictions in possible applications based on the legislation of the Contracting Party supplying the information shall be observed*.

> (b) This paragraph shall not impose an obligation on a Contracting Party to carry out measures which would contravene its laws or *conflict with its predominant interests with regard to the protection of the security of the State or of public safety*. […]"

The NATO SOFA Supplementary Agreement expressly lays down the duty to cooperate and exchange all information which is of significance for the furtherance and safeguarding of the security of the States Parties and their troops.[37] As can be concluded from the wording of Art. 3 para. 3, States Parties are allowed "to pass" even "personal data" for the purposes envisaged in the NATO Status of Forces Agreement and in the NATO SOFA Supplementary Agreement. Only if a State Party is "supplying" information, "restrictions in possible applications based on the legislation" of that Party "shall be observed".[38] Para. 3 of Art. 3 was included in the treaty in 1993. The obvious object and purpose of the amendment was to determine the limits of the exchange of personal data between the States Parties. Nevertheless one could conclude from Art. 3 NATO SOFA Supplementary Agreement that this treaty

[37] The NATO SOFA Supplementary Agreement is currently the only international treaty in force in this area: In June 2013, Germany negotiated with the Governments of France, UK, and US, and the administrative agreements of 1968 with these States were nullified by mutual agreement in August 2013, cf. Federal Foreign Office, Verwaltungsvereinbarungen zum G10-Gesetz mit USA und Großbritannien außer Kraft, August 2, 2013 http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Meldungen/2013/130802-G10Gesetz.html; Federal Foreign Office, Verwaltungsvereinbarung zum G10-Gesetz mit Frankreich außer Kraft, August 6, 2013, http://www.auswaertiges-amt.de/DE/Infoservice/Presse/Meldungen/2013/130806_G10_Frankreich.html; see also Gutschker, T. et al., Amerika darf Deutsche abhören, Franfurter Allgemeine Sonntagszeitung, July 7, 2013, p. 1, available at: http://www.faz.net/-gpg-7b2ag (all internet sources last retrieved March 13, 2015).

[38] In German the wording of Art. 3 para. 3 reads: "Personenbezogene Daten werden ausschließlich zu den im NATO-Truppenstatut und in diesem Abkommen vorgesehenen Zwecken *übermittelt*. Einschränkungen der *Verwendungsmöglichkeiten*, die auf den Rechtsvorschriften der *übermittelnden Vertragspartei* beruhen, werden beachtet." The text of the agreement was authenticated in German, English, and French in the sense of Art. 33 Vienna Convention of the Law of Treaties.

does not lay down limits in regard to espionage; on the contrary the treaty stresses that security is a legitimate aim and common concern of all States Parties and that in the end only the protection of *the security interests of one State Party or of the public safety of that Party* trumps the common security concern (Art. 3 para. 3 lit. b: *"conflict with its predominant interests with regard to the protection of the security of the State or of public safety")*. This means, as a first result, that espionage is not prohibited by the NATO SOFA Supplementary Agreement, and that – if espionage is justified by the security interests of one State Party, which is usually the case – all the data collected by espionage need not be passed on to another State Party.

E. Espionage – Lost in Fragmentation?

What does this mean for the duties of the State Parties stemming from human rights treaties? How can we bring together the different areas and rules of international law without being lost in fragmentation? As the ICCPR came into force in 1976 according to the *lex posterior* rule, it has precedence over the NATO SOFA Supplementary Agreement, since the latter already came into force in 1959.[39] The NATO SOFA Supplementary Agreement also does not have precedence over human rights treaties as *lex specialis*. The NATO SOFA Supplementary Agreement regulates different areas than the human rights treaties cover. Even para. 3 of Art. 3 NATO SOFA Supplementary Agreement, that was included in the treaty in 1993 and hence could prevail over the ICCPR norms, states that restrictions in applications based on the legislation of the Contracting Party shall be observed; this has to be interpreted as including the rules of international human rights treaties, at least as long as they form part of the national law of the respective State.

A different question is whether the NATO SOFA Supplementary Agreement might be a justification for the limitation of human rights:[40] Indeed one

---

[39] However, the ECHR entered into force in 1953; therefore one could argue that the NATO SOFA Supplementary Agreement has precedence over the ECHR according to the *lex posterior* rule.

[40] Burkhardt and Granow however argue that the NATO SOFA Supplementary Agreement has improved the protection of private data; cf. Burkhardt, F./Granow,

might argue – as shown above – that the NATO SOFA Supplementary Agreement allows espionage by an US organ, as for instance the NSA, or an organ of another State Party in Germany. However, Art. 1 of the Agreement must be taken into account as well. There it is stated that

"the rights and obligations *of the forces* of the Kingdom of Belgium, Canada, the French Republic, the Kingdom of the Netherlands, the United Kingdom of Great Britain and Northern Ireland and the United States of America *in the territory of the Federal Republic of Germany*"

form part of the agreement. Therefore (only) espionage by State organs that form part of "the forces" of these States in the territory of the Federal Republic of Germany is allowed as long as the collection of data is relevant for the security or the protection of the population.[41]

F. Conclusion

Public international law leaves us with a very ambiguous picture in regard to espionage; this is even more true if one looks closer at the legal situation of espionage by foreign States in Germany.

As it was shown above: fighting transnational terrorism is a legitimate aim of the international order and it is part of the new NATO doctrine after 9/11; fighting transnational terrorism is necessary in a democratic society in the interests of national security.[42] Besides, the NATO SOFA Supplementary Agreement – which does not prohibit espionage and even allows the transfer of personal data by State organs – is part of the legal order of the Federal

---

H., Das Abkommen zur Änderung des Zusatzabkommens zum NATO-Truppenstatut (ZA-NTS), NJW 1995, p. 424, 426.

[41] Cf. as well Deiseroth, D., Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf?, ZRP 2013, p. 194, 196.

[42] Wolf, J., Der verfassungsrechtliche Nebel der deutsch-amerikanischen „NSA-Abhöraffäre", JZ 2013, p. 1039, 1046.

Republic of Germany as federal law according to Art. 59 para. 2 of the Grundgesetz,[43] the German Basic Law.

Therefore there are some reasons to argue that there is no violation of the right to privacy even if the new tools of the digital age are used for espionage – at least if they are used by State organs that form part of the forces of Belgium, Canada, France, the Netherlands, UK, or the US in Germany.

If one looks at the broader picture of espionage and international law, what seems to be most important is that in the end it all depends on our answer to the question of if one can argue that secret, preventive mass data collection is always disproportional when no actual terrorist threat exists or if one has to argue that meta-observation and espionage have only few negative factual effects on privacy and therefore an abstract and diffuse terrorist threat is sufficient to justify abstract and diffuse espionage.

In my opinion the global order must be understood as an order with legally-enshrined values. These values are those protected by human rights treaties, as well as the international security and the sovereignty of States, whereby the values enshrined in human rights clearly have primacy. In the end it is up to the States, especially the democratic ones, to emphasize the existence and relevance of human rights: As long as our governments, as long as the citizens of the States, and as long as we are not convinced that large scale secret data collection and large scale espionage is disproportional in regard to the aim to fight terrorism it will be not easy to argue that a human right is violated.

[43] Federal Law Gazette 1949 I p. 1, last amended by law of December 23, 2014, Federal Law Gazette 2014 I p. 2438.