E-Portfolio Activity 3: Competing Interests – Michael Geiger

When looking at Germany's legal orientation in the context of cybercrime legislation and criminal investigations, two central aspects stand out. On the one hand, these relate to the internal alignment of laws and authorities, which is to receive a large number of additional powers through the IT Security Act 2.0 and can thus restrict the freedom of private individuals. On the other hand, Germany's external orientation can be perceived in an international context as a supranational sovereignty that relies on the interdependence and cooperation of nations in order to strengthen international criminal prosecution, but this also threatens to restrict national sovereignty according to Article 2 of the United Nations Charter (UNRIC, N.D.).

In 2020, the German Ministry of the Interior submitted the draft of the IT Security Act 2.0 for departmental approval. Among other things, the rules for the use of components in the area of the so-called critical infrastructure are to be defined therein. According to the law, the responsibilities and tasks of the BSI will be significantly expanded. In the future, the office should actively carry out port scans, lure attackers into honey pots and search for unprotected systems (Federal Gazette, 2021). The BSI should even be allowed to store user information that arises during digital communication between citizens and administrative bodies of the federal government, but also parliamentarians, for a period of 18 months. Critics are talking about data retention of a special kind. Because the metadata alone that is created when citizens communicate digitally with parliamentarians and federal authorities says a lot about what worries individual citizens, about their political activities and their personal projects.

The situation is similar with company data. The obligation to report so-called critical IT components is particularly controversial. Information that is then ultimately also available to the Ministry of the Interior via the BSI, since the IT Security Act 2.0 also stipulates that the BSI remains a subordinate authority of the Federal Ministry of the Interior and therefore has extensive powers to collect data and this data could be requested by the Ministry of the Interior. This means that the Federal Ministry of the Interior can use the very extensive overview of the situation in the country, which not only results from lists of critical IT components or log data of digital communication, for its political work. This can be advantageous for targeted planning and risk management, but it also harbors risks, since the information collected could also be misused.

According to Kloiber & Lassen (2020), there is broad agreement in the IT security community that a federal office that is supposed to be responsible for IT security must quickly identify and close vulnerabilities. But this task is thwarted if, as a dependent and subordinate authority of the Ministry of the Interior, it has to work together with an authority whose task is to penetrate systems, hack and crack encryption.

With regard to Germany's international positioning, it is striking that this differs from that of other western countries. In March 2021, the federal government published a position paper on the application of international law in cyberspace. What is particularly striking about this statement is the wide scope that the Federal Republic of Germany intends for state sovereignty on the Internet (The Federal Government, 2021). Human rights and other limits to sovereignty hardly appear in the paper, which should be viewed critically. If the understanding of state sovereignty in cyberspace is

too broad, there is a risk of considerable restrictions on freedom on the Internet. State sovereignty is a cornerstone of international law. It states that every state is entitled to its own sovereign territory on which it can exercise its sovereignty independently of other states. However, this does not entail unrestricted freedom for states to arbitrarily exercise their own state power on their own territory. Human rights prevent such an approach, among other things, as limitations on state sovereignty (Schmitd. 2021).

Unlike Great Britain and the employees of the US government, Germany considers state sovereignty in cyberspace to be an independently vulnerable rule of international law, which could also be affected if more specific rules such as the ban on intervention or the use of force do not apply (The Federal Government, 2021). Sovereignty thus takes on the character of a kind of “catch-all rule” for a wide variety of interventions.

There is a violation of territorial integrity if digital measures cause physical damage or functional impairments on foreign territory. However, physical or functional impairments that are negligible do not constitute a violation. In doing so, the Federal Republic of Germany has established a meaningful threshold for violations of territorial sovereignty, which prevents countermeasures being taken in response to any access to foreign network infrastructure. According to the position paper, even an impairment of critical infrastructure does not automatically lead to a violation of state sovereignty. Overall, the German position on territorial integrity is therefore amenable to an individual, meaningful assessment of interstate conflicts. For example, according to the German position, hacking into the power grid that causes damage and subsequent power failure would probably be contrary to international law, but mere espionage via the Internet would not.

This positioning shows the difficult role of the internet in the context of national sovereignty and which tensions can arise in the international context. A well-considered assessment of criminal liability and the consequences of state interference in national sovereignty is important, since this must be protected and respected in principle, but an overly strict interpretation could be used by interest groups to provoke conflicts.

References:

UNRIC (N.D.) Die Charta der Vereinten Nationen. Available from: https://unric.org/de/charta/ [Access 18 September 2022].

Bundesanzeiger (2021) Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme. *Bundesanzeiger Verlag*. Available from: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27l_2022_32_inhaltsverz%27%5D__1663488269571 [Accessed 19 September 2022].

Kloiber, M. & Welchering, P. (2020) Kritik am Entwurf zum IT-Sicherheitsgesetz 2.0. *Deutschlandfunk*. Available from: https://www.deutschlandfunk.de/bsi-soll-ausgebaut-werden-kritik-am-entwurf-zum-it-100.html [Accessed 19 September 2022].

The Federal Government (2021) On the Application of International Law in Cyberspace. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf [Accessed 19 September 2022].

Schmidt, R. (2021) Grenzenlose Souveränität im Cyberspace. Verfassungsblog on Matters Consitutional. Available from: https://verfassungsblog.de/grenzenlose-souveranitat-im-cyberspace/ [Accessed 19 September 2022].