THE MICROSOFT IRELAND CASE, THE CLOUD ACT AND THE CYBERSPACE SOVEREIGNTY TRILEMMA

POST-TERRITORIAL TECHNOLOGIES AND COMPANIES QUESTION REGULATORY STATE MONOPOLIES

Paul De Hert and Johannes Thumfart

Abstract: The Microsoft Ireland case has been heard by the Supreme Court in the beginning of 2018 and dropped due to the introduction of the CLOUD Act in May 2018, which has been issued in order to resolve the fundamental problems at the core of this case. This contribution focusses on two key features of this development: the conflicting and often chaotic approaches to the notion of sovereignty of many of the actors involved and the remarkable move of a private company such as Microsoft to trigger regulation at a time, in which companies, technologies, data flows and governments transgress borders, challenging territorial comprehensions of the world order.

Table of contents

INTRODUCTION AND REFLECTION ON THE DIFFICULTY OF CLASSICAL TERRITORIAL CONCEPTS

The *Microsoft Ireland* case was heard by the Supreme Court in February 2018. It was dropped due to the introduction of the CLOUD Act in May 2018, which has been passed in order to resolve the fundamental problems at the core of this case and which has been pushed by Microsoft's unyielding position in the case. This contribution examines the *Microsoft Ireland* case and its regulatory effects as paradigmatic for two recent developments at the intersection of law, society, technology and international relations: the conflicting and often chaotic approaches to the notion of sovereignty of many of the players involved and the remarkable move of a private company to trigger regulation in a world where companies, technologies, data flows and governments transgress borders with growing acceptance of the inadequacy of older territorial comprehensions of the international order.

In brief, the facts of the case: On December 4th 2013, a magistrate judge in the Southern District of New York was involved in a case concerning drug-trafficking and evidence stored in the cloud. As part of this investigation, he issued a warrant directing Microsoft to produce all emails and information associated with an individual costumer account. The suspect, however, in spite of being a resident of the US, had registered for his account as a resident of Ireland. And at the time, it had been the policy of the company to store email content in the data center nearest to the customer's self-declared country of residence.[1] So, while the account information was held on Microsoft's servers in the US, the emails were stored on a server in Ireland. Subse-

[1] It is a good indicator for the normative de facto power of companies that Microsoft already internally changed its regarding policy, which is discussed in the last chapter of this contribution. Whilst it made the whole world debate about the *Microsoft Ireland* case, at Microsoft internally, the reason for the conflict was already resolved since a while in a way that only appears to be merely technical. The company now stores the data of a customer automatically in the location closest to its most frequent location. With this choice, Microsoft took a step towards the de facto creation of a zone of probable jurisdiction, even more disquieting since this creation is done by an algorithm. See: Matsakis, Louise, «Microsoft's Supreme Court Case Has Big Implications For Data», *Wired*, 27.2.2018: https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/, accessed 13.1.2020.

quently, when confronted with the production order by the judge, the company complied with providing the account information but refused to turn over the emails, arguing that a US judge has no authority to issue a warrant for information stored abroad. In May 2014, a federal magistrate judge disagreed with Microsoft and ordered it to turn over the emails.

A series of appeals by Microsoft followed, which ended up before the US Supreme Court by the beginning of 2018 and attracted an unusual degree of public interest. 289 different groups and individuals from 37 countries signed 23 legal briefs supporting Microsoft's position. During the global debate that this case set in motion, it became increasingly understood as a *pars pro toto* for the growing iceberg of extraterritorial production orders concerning digital data.[2] The outcome of the case would have been problematic for the US Government either way: if it had won the case, other «wrong», i.e. poorly regulated countries, would have gotten the wrong message and would have started asking all kinds of data from big Internet players, mostly situated in the US. If it had lost the case, it simply would have lost the legal battle, which, of course, was undesirable.

As a way of escaping this dilemma, the US legislator, set in motion by the case and the global debate around it, intervened and came up with the CLOUD Act in March 2018. This act – short for: Clarifying Lawful Overseas Use of Data – clarified the legal framework in making extraterritorial data production orders legally possible, as long as the data is within a U.S company's «possession, custody or control», irrespective of where the data is located.[3] In a turn away from multilateralism – a move typical for the Trump

[2] In 2014, in the UK alone, for which we have such self-reported numbers, law enforcement officials sought costumer data for at least 53 947 separate user accounts controlled by American Internet firms. As an estimation, by 2019, 55% of the consumer Internet population will use personal cloud storage and 86% of data processing will happen remotely, in cloud centers. In general, since most Internet firms headquarter in the US, but most users are located outside of the US, and data is frequently stored in a third country, the access to extraterritorial evidence is a mass phenomenon on a global scale. Numbers according to: WOODS, A. K., «Against Data Exceptionalism», *Stanford Law Review*, April 2016, Vol 68, 729–789, pp. 741, 743.

[3] On the 23th of March 2018 the U.S, adopted the *Clarifying Oversees Use of Data (CLOUD Act),* which revises portions of the 1986 Stored Communications Act (SCA), introduces four main changes. First section 103 of the Cloud Act extends the jurisdictional scope of warrants and subpoenas requiring electronic communication and remote computing service providers the

administration – it also foresees bilateral executive agreements concerning extraterritorial data production orders.

The text of the first and, therefore, probably paradigmatic of these bilateral agreements, the UK-US CLOUD Act Agreement, was released on October 7, 2019. It underlined the turn away from territory as a limiting principle of data production orders to other, more subtle restrictions: E.g. citizens and residents of the US are exempted from access by UK law enforcement and vice versa. An additional focus is being put on fundamental rights issues, i. e. restrictions regarding crimes punished with death penalty in the US and restrictions regarding crimes related to limitations of the freedom of speech in the UK.[4] Whilst the bilateral nature of the CLOUD Act is problematic because it infinitely increases the bargaining power of the US, where most tech firms are situated, the included provisions can be regarded as an important step towards the development of a post-territorial legal framework for the obtaining of e-evidence.

In a *first section*, this contribution will examine the circumstances which allowed a relatively petty case such as the Microsoft Ireland case to unfold such a surprising amount of impact. In order to do so, it will examine the historical context and – with the necessary epistemic precautions at hand[5] – attempt to reconstruct the intentions of the actors

«*preservation, backup, or content disclosure of electronic communications*» irrespective of where the data is located insofar the same is within a U.S company's «*possession, custody or control*» (U.S.C. § 2713.); Secondly the same section establishes the framework according to which, service providers might challenge an SCA warrant (2703(h)(2); Third, a new added subsection directs the courts to conduct a limited comity analysis to balance certain factors relevant to cross-border transfers of data (section 2703 f); Finally, section 105 sets the parameters for foreign governments to enter into executive agreements with the United States and based on which U.S companies will be enabled to respond to cross-border data requests.

4 Daskal, Jennifer & Swire, Peter: The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards, Tuesday, October 8, 2019 https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards, accessed 13.1.2020.

5 Ultimately, intentions are the object of the classic Skinnerian method of intellectual history, but they are, in general, a difficult object of historical research, since they cannot be empirically proven. See: Johannes Thumfart, «Archäologie – Ideengeschichte – Topik. Zur Gegenüberstellung der Methoden Foucaults und Skinners», in Busen, A. & Weiß, A. (eds.): *Ansätze und Methoden zur Erforschung politischer Ideen*. Nomos: Berlin 2013, 127–148, p. 137.

involved. This will also provide insights in the position of the US government, showing that the conflict at the heart of this case is rather structural than political.

The *second section* will provide a look at this structural conflict in light of three more or less well-known scenarios proposed in the cyberspace literature: *cyber-anarchy*, *hyper-sovereignty* and *Internet Balkanization*. As exotic as these labels might seem, they are a helpful tool for the understanding of a fundamental deadlock that we call *cyberspace sovereignty trilemma*.

The first of these three scenarios, *cyber-anarchy,* has been named and criticized by the legal theorist Jack Goldsmith.[6] According to this scenario, cyberspace is an «a-geographical» and «boundary-destroying means of communication»,[7] and as such cannot be regulated by national regulations at all.[8] (In contrast to Goldsmith, we speak of *post-territoriality*[9] of cyberspace.)

The second scenario, *hyper-sovereignty*, is named after a term used in the theory of international relations.[10] In the context of this contribution, hyper-sovereignty (from Greek *hyper*, «overly») denotes transgressive state actions in terms of territory – a tendency towards extraterritorial agency –, which is caused by the adaption of states to the

6 GOLDSMITH, J L., «Against Cyberanarchy», *University of Chicago Law Occasional Paper*, 1999, No. 40. Similar to the authors of this essay, Goldsmith opposes such justification of cyber-anarchy.

7 Id. pp. 1, 4.

8 As will be elaborated below, in section 2, Goldsmith developed this model not to endorse it, but to oppose it.

9 Obviously, the Internet is not simply non-territorial, as this case makes also clear. The Internet is based on material infrastructure that does occupy a territory. The term «post-territorial» is elaborated further in section 2. In this context, the term has been first used regarding the difficulties with identifying the territory of origin of cyber-attacks, something very rare in non-digital, so called «kinetic» conflicts. Johannes Thumfart, «Francisco de Vitoria and the Nomos of the Code: The Digital Common and Natural Law, Digital Communication as Human Right, Just Cyberwarfare», in Beneyto, J. & Corti, J. (eds.), *At the origins of Modernity. Francisco de Vitoria and the Discovery of International Law,* Springer: Basel 2017, 197–217, p. 211.

10 Only having structural similarity with the issues discussed in this contribution, Hobson uses the term to denote the hegemony of developed nations over the developing world. John Hobson, «Decolonising Sovereignty. Globalisation and the Return of Hyper-Sovereignty», in Schuett, R. & Stirk M. P. (eds.) *The Concept of the State in International Relations: Philosophy, Sovereignty and Cosmopolitanism*. Edinburgh UP: Edinburg 2015, 135–162.

post-territoriality of cyberspace. This geographical transgression is accompanied by actions of states that are transgressive in terms of the rule of law, in a sense that extraterritorial enforcement jurisdiction is per se illegal under international law.

The third scenario, which is often, and wrongly so, perceived as the solution of the problem of cyber-anarchy and hyper-sovereignty alike, is *Internet Balkanization,* i. e. the division of the Internet according to national borders. It has been circulating in the respective literature for a while and also employed in one of the Amicus Curiae briefs concerning the Microsoft Ireland case.[11]

Regarding the Microsoft Ireland case, one can conclude: If the defenders of Irish sovereignty, mostly located within the EU, had won, this would have only increased the tendency towards Internet Balkanization. Due to the introduction of the CLOUD Act, a tendency towards a regulatory deficit is avoided that could be hyperbolically understood as cyber-anarchy. On the other hand, the missing judicial checks under the CLOUD Act, especially regarding warrants issued by foreign governments, could lead to an increase in hyper-sovereignty, in particular, if the safeguards regarding fundamental rights are not renewed in every bilateral agreement.

We think that this deadlock of the cyberspace sovereignty trilemma is not inevitable, but rather owed to an understanding of sovereignty in mostly territorial terms. Our *third section* tries to surpass such a territorial understanding of sovereignty. It takes a look at legal theorist Hans Kelsen's non-empirical conception of sovereignty, which he developed already in 1920, in *Das Problem der Souveränität,* and which he later, in his *General theory of Law and State* from 1925, extended towards a critique of an understanding of legal territoriality in geographical-empirical terms. According to Kelsen, an

[11] Brief amici curiae of Former Law Enforcement, National Security, and Intelligence Officials in support of neither party filed, pp. 9f. In this scenario, states try to put the post-territorial features of the Internet back into the bottle and counteract cyber-anarchy and hyper-sovereignty alike by building barriers to trans-border traffic and trans-border business. For example, by geo-blocking or the practice of re-localization of data, which includes the compulsory storing of data about citizens of a nation on the territory of that very nation – a policy that could prevent situations such as the Microsoft Ireland case. A good example for such a practice is Russia: SAVELYEV, A.: «Russia's new personal data localization regulations: A step forward or a self-imposed sanction?», *Computer, Law & Security Review,* 2016, 32, 128–145. Will be elaborated further in section 2.

empirical understanding of legal territoriality is based on what is called in philosophy the *is-ought-fallacy*,[12] the confusion of empirical concepts with normative ones. From Kelsen's work in that field, a new, post-territorial, non-empirical idea of sovereignty will be developed, which might sound groundbreaking, but actually just conceptualizes existing practices such as the CLOUD Act and corresponds to what is common sense in philosophy since Kant and Hume.

The *fourth section* will discuss which seems, besides the issue of post-territoriality to which it is however connected, the most novel feature of the *Microsoft Ireland* case and the debate that it triggered: The role of a private company such as Microsoft pushing publicly for regulatory change and not by lobbying. Here, too, it will be just conceptualized what is already international reality, for example in non-state transnational multi-stakeholder-models of Internet governance such as ICANN, which already involve companies as regulatory actors. We will show that, with or without regulatory actions taken by states, cyberspace is already heavily regulated by companies, in part as de facto regulation by technical design, in part by private coercive actions, for example concerning the censorship of hate-speech. If one takes a post-territorial understanding of sovereignty seriously, companies seem to possess normative power that is comparable to states, since what they lack foremost in comparison to states is jurisdiction over territory. Transnational companies can also serve as an important counterweight to state power in regard to regulation making, because they are not restricted by territorial borders or the logics of public property. The CLOUD Act even increased this regulative function of companies. Not only because it is the outcome of an attempt of Microsoft to trigger regulation, but also because by permitting direct collaboration between the US tech sector and foreign governments, it makes the tech company itself «the only real

[12] Social Darwinists, for example, are guilty of the *is-ought-fallacy* par excellence since they claim that the proverbial observed «laws of the jungle» need to be decisive to how humans live. Similarly, pre-modern political thought, i. e. thought before Hume and Kant, regularly cited observations concerning the social life of ants to justify human social hierarchies. According to the argumentation in this contribution, reducing the possibilities of legal territoriality to the borders of observable empirical-geographical territory is based on the same fallacy.

fail-safe to prevent a technology company from inadvertently acceding to a harmful data request.»[13]

1. *Microsoft Ireland's* context, motives and arguments: the Snowden shadow at work?

«One could imagine a world in which the Snowden disclosures had never occurred and as a consequence: (1) Microsoft would not resist the warrant in the first instance and (2) even if it did, privacy groups and foreign governments would not come to its aid. But we do not live in that world».[14] These words accurately describe the close relation between *Microsoft Ireland,* its historical context in the post-Snowden era and the political motivation of its actors. Later on, it will be discussed why not all is *Snowden* in this case (as was understood by the US Government). But let us start with underlining how much is *Snowden* in this case. We recall some major outcomes of the Snowden revelations in June 2013 and the subsequent debate:

First, the Snowden (or NSA) affair created *international tensions* that are still on-going today. For example, the leaders of Brazil, France and Germany sent clear messages in the direction of the US that – unlike it might have seemed before – cyberspace is politically relevant to them and they regard the NSA's surveillance as an interference in their domestic affairs. Spokespersons of the EU, whose antitrust chief Joaquin Almunia had been personally under surveillance, were likewise indignant.[15] Although as part of so called «hybrid warfare»,[16] the Russian interest in cyber-war dates back way further than

---

13 Guliani, Neema Singh & Shah, Naureen, «Proposed CLOUD Act Would Let Bad Foreign Governments Demand Data From US Companies Without Checks and Balances», ACLU, https://www.aclu.org/blog/privacy-technology/consumer-privacy/proposed-cloud-act-would-let-bad-foreign-governments-demand, accessed 13.1.2020.

14 Woods, Andrew Keane, «Whatever happens in US v. Microsoft, three themes will persist», *Scotusblog*, 8.2.2018, http://www.scotusblog.com/2018/02/symposium-whatever-happens-us-v-microsoft-three-themes-will-persist/, accessed 13.1.2020.

15 Ball, James & Hopkins, Nick, «GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief», *The Guardian*, 20.12.2013 https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner, accessed 13.1.2020.

16 The label might be dangerously misleading inasmuch as it unnecessarily exaggerates already existing tensions. RENZ, B. & SMITH, H., «Russia and Hybrid Warfare. Going beyond the label»,

2013, one might also argue that Russia intensified its endeavors to oppose the US in the digital sector, starting with achieving a remarkable propaganda victory by granting Snowden asylum, but also by adopting a legal regime of increasing data localization.[17]

Second, the Snowden-revelations led to a dramatic *decline of trust of citizens in institutions,* since they included not only the NSA, but a number of international secret services. This trust dimension with its «populist quality»[18] brought about a synchronized global political debate in civil societies concerning surveillance, probably the first of its kind.

Third, there is the *economic effect* of the Snowden-revelations. Since they suggested a seamless collaboration between the NSA and the US's digital sector that has already been named before the Snowden-revelations a «cyber-industrial complex»,[19] the Snowden-revelations led to a decline of trust of states and individuals in the US's digital industry. As a first reaction, governments in Europe and China limited their cooperation with the US digital industry.[20] Individual consumers were at least feared to act in a similar way, which is of great importance to the digital industry, since it is built on consumer trust and reputation effects.[21] The US digital sector was therefore confronted with the problem of how to counteract the disastrous effect of the NSA-scandal on all

Aleksandri Papers 1/2016, https://www.stratcomcoe.org/bettina-renz-and-hanna-smith-russia-and-hybrid-warfare-going-beyond-label, accessed 13.1.2020.

17 SAVELYEV, A.: «Russia's new personal data localization regulations: A step forward or a self-imposed sanction?», *Computer, Law & Security Review,* 2016, 32, 128–145.

18 David Fidler, «Introduction» in Fidler, D. (Ed.): *The Snowden Reader,* Indiana University Press: Indiana 2015, 2-14, p. 12.

19 BRITO, J. & WATKINS, T., «Loving the cyber bomb? The dangers of threat infation in cybersecurity policy», *Working Paper Mercatus Center at George Mason University* 2011, 11–24, pp. 1–34.

20 Miller, Claire Cain, «Revelations of N.S.A. Spying Cost U.S. Tech Companies», *The New York Times*, 21.3.2014, https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html, accessed 13.1.2020.

21 HAUCAP, J. & HEIMESHOFF, U., «Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?», *International Economics and Economic Policy,* 2014, 11, pp. 49–61.

brands that headquarter in the US, which led, for example, to Apple's iPhone-standoff with the US government in 2016.[22]

When Microsoft was asked in 2013 to produce the emails of a suspected drug-trafficker that were stored in Ireland, it, understood this request as both, granting an opportunity to repair its damaged reputation and to re-gain consumer trust, but also including the dangerous possibility to become engaged in an increasingly heated international conflict concerning sovereignty in cyberspace, and therefore «become the proverbial meat in the sandwich».[23] Thus, in its objections to the warrant, Microsoft employed the main themes of the post-Snowden debate. It underlined that committing to the judge's request would «violate the territorial integrity of sovereign nations and circumvent the commitments made by the US in mutual legal assistance treaties»[24] and added «courts in the US lack authority to issue warrants for extraterritorial searches and seizures.»[25] Complying with the warrant, Microsoft argued, could «damage US foreign relations»[26] And «the government's unilateral exercise of law enforcement powers within the territory of Ireland puts at risk the US information technology sector's continued ability to compete globally.»[27]

Besides the conflict with territorial jurisdiction, Microsoft also gave the case a reading in regard to privacy, which fitted well within the post-Snowden context. It argued that the Fourth Amendment's particularity requirement was violated because the warrant «does not limit the Government's search to any specific facility or physical premises,

22 Khamooshim Arash, «Breaking Down Apple's iPhone Fight With the U.S. Government», *The New York Times*, 21.3.2016, https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html, accessed 13.1.2020.

23 SVANTESSON, D. & GERRY, F., «Access to extraterritorial evidence: The Microsoft cloud case and beyond», *Computer Law & Security Review,* 2015, 31, 478-489, p. 478.

24 Microsoft's Objections to the Magistrate's Order denying Microsoft's motion to vacate in part a search warrant seeking costumer information located outside the United States, p. 1.

25 Ibid., p. 17

26 Ibid., p. 29

27 Ibid., p. 29

but instead extends it to all digital information within Microsoft's possession *anywhere* in the world».[28]

When the DOJ (Department of Justice) got involved in the case, Microsoft employed once more the main themes of the post-Snowden debate. In its response to the DOJ, it openly criticized the «Extraterritorial Application» of US law, which this request implied, and also pointed towards the grave «implications for international comity» that this case could unfold.[29] Of course, it also made sure that the refusal to comply with the production order was communicated to the global public as one of the most influential digital companies finally standing up against the US government in defense of privacy rights. In this respect, Microsoft's decision to pursue this case up to the Supreme Court can also be criticized as a PR-campaign that instrumentalizes the limited capacities of the highest court of the world's most powerful democracy for PR-reasons.

Other tech companies, of course, were in a similar situation as Microsoft and took its side. Ebay, Hewlett-Packard, Salesforce, Cisco et al. filed an Amicus Curiae brief supporting Microsoft. In the brief, the tone became very drastic. Two well-put, self-explanatory headlines read: «The District Court's ruling would harm American businesses economically and potentially subject them to civil and criminal liability abroad», «The District Court's decision would undermine international agreements and understandings and spur retaliation by foreign governments.»[30] IBM, Amazon, Apple, Facebook, Mozilla and others later issued similar briefs.

---

28 Ibid.,. p. 27

29 Reply in Support of Microsoft's Objections to the Magistrate's Order denying Microsoft's motion to vacate in part a search warrant seeking costumer information located outside the United States, p. 12.

30 The Amicus Curiae brief by the US digital industry also puts a number to the economic damages done by the NSA-scandal and, unlike the briefs by Microsoft, mentions it explicitly: «Recent revelations about US intelligence practices have heightened foreign sensitivities about the US government's access to data abroad, generated distrust of US companies by foreign officials and customers, and led to calls to cease doing business with US communications companies and cloud service providers. This has put US companies at a competitive disadvantage with respect to their foreign competitors. Studies have estimated that this distrust will result in tens of billions of dollars in lost business by US companies over the next few years» Brief of Verizon Communications Inc., Cisco Systems, Inc., Hewlett-Packard Co., Ebay Inc., salesforce.com, and infor, as Amici Curiae in Support of Appellant, p. 10.

Likewise, members of the EU parliament, EU national trade organizations and EU Data Protection and Privacy Scholars filed Amicus briefs in favor of Microsoft, underlying that, also from a European perspective, «EU rules apply to the email account covered by the warrant in issue in this case» and, therefore, a mutual legal assistance treaty (MLAT) should be used.[31] Just as concerning the other Amicus briefs filed by foreign governments and foreign interest groups, one should not underestimate the degree to which the opportunity for «nation branding» contributed to this unprecedented global keenness to take position in a case that was back then not even discussed at the Supreme Court.[32]

Against the claim that it exerted its jurisdiction extraterritorially if it obtained the email from Ireland, the US government argued that it was Microsoft who needed to do the extraterritorial search, not the government, and the company was obliged to do so because the data was, extraterritorial or not, in its control, «regardless of the location of that information»[33]

Concerning this aspect, ACLU and EFF issued an amicus brief arguing that Microsoft conducting extraterritorial searches on the government's behalf was the same as the government extending its enforcement jurisdiction extraterritorially. Bringing the government's far-fetched argument to an even further-fetched conclusion -which probably, too, can only be understood with the Snowden & NSA-context in mind-, ACLU and EFF reasoned that an exemption of search from general regulations regarding warrants according to the Fourth Amendment could have dramatic consequences: «Accepting the government's argument could lead to massive over-collection of data. On this theory, a

31 Brief of *Amici Curiae* Jan Philipp Albrecht, Sophie In`T Veld, Viviane Reding, Birgit Sippel, and Axel Voss, Members of the European Parliament in Support of Respondent Microsoft Corporation, p. 5.

32 Melissa Aronczyk & Stanislav Budnitsky: «Nation branding and Internet governance: Framing debates over freedom and sovereignty» in Kohl, U. (ed.), *The net and the nation-state: Multidisciplinary perspectives on Internet governance*, Cambridge UP: Cambridge, 2017, 48–65.

33 Government's brief in support of the Magistrate's Judge's decision to uphold a warrant ordering Microsoft to disclose records within its custody and control, p. 7

warrant would not be required to copy all electronic communications, unless and until officers sought to view some of the data».[34]

So far, all actors discussed are driven by their *Snowden* understandings. But what about the US government? Of course it was not exactly happy about the fact that Irish law should interfere with its investigation of a relatively petty crime supposedly committed by an US-resident on US territory. However, on the level of legal arguments, the motivation of the US government and its backers is more complex than that and, in a sense, based on a deeper understanding of the differences between the Snowden context and its NSA-problem and the case at hand than the one which dominated global public opinion.

As clear as the connection between the Microsoft-case and the Snowden-revelations are if examined on the level of the perception or the interest of the public, it should not be forgotten that regarding the underlying legal structures, both do not only have nothing in common, but rather are diametrically opposed. NSA-surveillance is based on FISA (Foreign Intelligence Surveillance Act) and a general great amount of liberty of military institutions to act abroad. In terms of territoriality, within the US, FISA and the actions of the NSA have been criticized foremost because they used the relative liberty of military institutions in an extraterritorial context in order to conduct intra-territorial warrantless searches and therefore circumvent civil liberties.[35]

At *Microsoft Ireland*, on the other hand, one had tried to resolve an issue that at least Microsoft perceived as an international one by the usually domestic legal instrument of SCA (Stored Communications Act). This incongruence, for example, is perfectly understood by the backers of the US government, which are mostly situated in the US and concerned with the privacy of data stored by US-based companies. «SCA is both a sword

[34] Brief for Brennan Center for Justice at NYU School of Law, American Civil Liberties Union Foundation, Electronic Frontier Foundation, Restore the Fourth, Inc. and R street Institute as *Amici Curiae* in Support of Respondent, p. 16

[35] Thumfart, Johannes, «Der militärisch-digitale Komplex», *Die Tageszeitung*, 5.5.2013,http://www.taz.de/!5068185/, accessed 13.1.2020.

and a shield», they argue according to Woods' summary of their position.[36] If US law cannot be adopted to extraterritorial data, this also means that users cannot enjoy the privacy rights regarding their data stored by US enterprises abroad as guaranteed by the SCA. To them, as it was the basis of the NSA-scandal, applying extraterritorial categories to domestic cases is the real threat.

There are also other, obvious, reasons why the Microsoft Ireland case is exactly not the same as the Snowden-NSA situation. Unlike military surveillance that is foremost extraterritorial, criminal procedures are largely domestically and conducted according to legally regulated processes. This means foremost that suspects who are targeted by the regarding procedures have means to combat these procedures legally, whereas the problem of the NSA case was exactly that citizens were targeted who have not elected the US government and who practically enjoy no means to defend themselves in the US legal system.

2. *Microsoft Ireland* and the Cyberspace Sovereignty Trilemma (anarchy, hyper-sovereignty or balkanization)

Whilst *Microsoft Ireland* is in some way determined by the Snowden-revelations, both are also an expression of a greater, structural crisis regarding the relatively slow adaption of legal standards to contemporary technological realities.

In the past -or better: during the fading interim period of the classical Westphalian model-, the law of sovereign nations provided the regulatory framework for their politics, their economies and societies. But, since its development by Jean Bodin in the 16th century, the concept of sovereignty was, at least in retrospect, strongly related to the controllability, identity, and, in part, hermetic qualities of a territory. The Internet, on the other hand, was, since its intellectual beginnings as a defense project of RAND corporation, designed to be decentralized to withstand attacks on single nodes.[37] The end-

[36] Woods, Andrew Keane, «Whatever happens in US v. Microsoft, three themes will persist», *Scotusblog*, 8.2.2018, http://www.scotusblog.com/2018/02/symposium-whatever-happens-us-v-microsoft-three-themes-will-persist/, accessed 13.1.2020.

[37] Johannes Thumfart, «El Internet no es, ni siquiera es una esfera publica: una ontología negativa política entre la Cibernética, Platón, Deleuze, Heidegger y Habermas», in: Thumfart,

to-end-principle and packet-switching, its technical foundation, inherently work towards decentralization. Especially the rise of cloud-computing led to an increasing degree of geographical distribution of data. Between 2005 and 2012 alone, during the dawn of cloud computing, cross-border Internet traffic grew 18-fold.[38] As an estimation, by 2019, 55% of the consumer Internet population use personal cloud storage and 86% of data processing happens remotely, in cloud centers.[39]

Of course, the Internet is based on a material infrastructure that occupies a certain territory. It would therefore be wrong to simply speak of the *non-territoriality* of the Internet. However, the high amount of distribution of data that the Internet makes possible, can, as a last consequence, actually amount to the *post-territoriality* of data, [40] i. e. a situation in which it does not make sense to think of data as something that occupies an identifiable territory at all.

Google, for instance, breaks up its emails and stores them on different servers all over the world and moves them constantly around in an automatized process. Therefore, the company itself cannot fully determine where data is actually stored at any given moment in time.[41] The *Microsoft Ireland* case is comparably classical compared to such,

J. & Aguirre, M. (eds.), *Pensar Internet*, Universidad Iberoamericana: México D.F., 2017, 55–82, p. 58ff.

38 McKinsey Global Institute, «Globalfows in a digital age: How trade, finance, people, and data connect the world economy», April 2014, https://www.mckinsey.com/business-functions/strategy-and-corporate-fnance/our-insights/global-fows-in-a- digital-age, accessed 13.1.2020.

39 WOODS, A.K., «Against Data Exceptionalism», *Stanford Law Review*, April 2016, Vol 68, 729–789, pp. 741

40 In this context, the term has been first used regarding the difficulties with identifying the territory of origin of cyber-attacks, something very rare in non-digital, so called «kinetic» conflicts. Johannes Thumfart, «Francisco de Vitoria and the Nomos of the Code: The Digital Common and Natural Law, Digital Communication as Human Right, Just Cyber-warfare», in Beneyto, J. & Corti, J. (eds.), *At the origins of Modernity. Francisco de Vitoria and the Discovery of International Law,* Springer: Basel 2017, 197–217, p. 211.

41 In re Search Warrant No. 16-960-M-01 and No. 16-1061-M to Google, US District Court for the Eastern District of Pennsylvania, 03.02.2017, page 7, p. 28, http://www.paed.uscourts.gov/documents/opinions/17d0077p.pdf, accessed 13.1.2020.

genuinely post-territorial developments, for which the Cloud Act, since it is based on who controls the data, rather than the location of data, is a possible answer.[42]

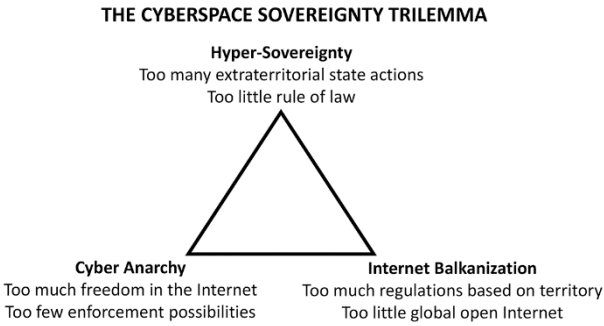
Whilst really existing post-territoriality is an extreme case (as philosophers, respectively mathematicians would say: a teleological, asymptotic concept), especially in regard to its relation to the state, which is usually bound to a territory, the Internet can be regarded as promoting tendencies that are in principle post-territorial, inasmuch as local distribution simultaneously limits and expands the possible field of a state's actions

This post-territorial scope of cyberspace has created a *crisis of the state in the digital age*[43] inasmuch as its confronts states with a trilemma regarding cyberspace sovereignty. Either states accept a scenario of *cyber-anarchy*,[44] and lose sovereignty on their own territory because of restrictions in terms of enforcement jurisdiction imposed on their sovereignty by the post-territoriality of the Internet. Or, as a reaction to this threat, they will adopt a policy of *hyper-sovereignty*: Once adjusted to the post-territorial realm of cyberspace, their sovereignty will transform into an unregulated hyper-sovereignty that is bound to create international and domestic conflicts due to its extraterritorial reach and corresponding extra-legality. As last consequence, international conflicts, which are inevitably created by hyper-sovereignty, lead to the third scenario, *Internet Balkanization.* In this scenario, states attempt to increasingly re-territorialize the post-territorial scope of the Internet by adopting policies of geo-blocking, re-localization of data and regulations bound to territory, which is a threat to the cultural and scientific function of the open Internet. Let us take a closer look at the trilemma represented by these three scenarios (*figure below*):

[42] It is worth noting here that the *Microsoft Ireland* case could not have been brought before the Supreme Court by Google because it has another, business model concerning the storage of information.

[43] The expression «*The crisis of the state in the digital age»* is coined by Owen. T. Owen, *Disruptive Power. The Crisis of the State in the Digital Age,* Oxford UP: Oxford 2015.

[44] GOLDSMITH, J L., «Against Cyberanarchy», *University of Chicago Law Occasional Paper*, 1999, No. 40.



Firstly, Cyber-anarchy. Before the Snowden-revelations, cyber-anarchy has been the predominant theme of the debate regarding the relationship between cyberspace and the state. Already in 1996, Perry Barlow in his *Declaration of the Independence of Cyberspace*[45] argued that cyberspace was post-territorial and that states, who are funded on territoriality, had «no sovereignty» in cyberspace. Although Barlow's lofty, natural-law-style manifesto has been ridiculed many times, its basic opposition of territoriality and cyberspace remains true. Cybercriminals and political activists alike take advantage of extraterritoriality in order to avoid state persecution.

This, of course, was, also since the beginnings of the Internet perceived as a challenge by lawyers. Already in 1999, legal theorist Jack Goldsmith created the scenario of cyber-anarchy in order to denounce those who opposed a stricter regulation of cyberspace. Cyber-anarchy, according to Goldsmith, is based on the idea that «the application of geographically based conceptions of legal regulation and choice of law to a-geographical cyberspace activity either makes no sense or leads to hopeless confusion.»[46] Whilst Goldsmith criticizes this idea, it has been immensely influential in both ways: as an, in part hyperbolical, concept dominating public perception and as an adequate description of actual problems concerning the rule of law in cyberspace.

---

45 Barlow, John Perry, «A Declaration of the Independence of Cyberspace», https://www.eff.org/de/cyberspace-independence, accessed 13.1.2020.

46 GOLDSMITH, J L., «Against Cyberanarchy», *University of Chicago Law Occasional Paper*, 1999, No. 40, p.1.

As has been most prominently argued by Morozov,[47] states have expanded their reach as a response to really existing or perceived cyber-anarchy. Take for instance the websites that offered and offer download of illegal content from extraterritorial domains hosted by so called bulletproof hosters. Or take foreign based websites used to commit more serious crimes. Successful persecution of these websites by states, either by using MLAs or by (often more problematic) unilateral measures indicate that there are limits to the idea of cyber-anarchy and that states are not totally disarmed. Unfortunately, concerning an aspect of subversion by extraterritoriality that is within democratic contexts regarded as positive[48] -political activism-, one also witnessed an increasing tendency of states such as Iran and China to limit the freedom that the post-territoriality of digital communication grants by censorship and geo-blocking.[49]

Secondly, there is *Hyper-Sovereignty,* characterized by actions of states in cyberspace that transcend the classical limits imposed on sovereignty, in terms of territory, but also in terms of the rule of law. Hyper-sovereignty is *hyper* (greek, «overly») because it inherently conflicts with the idea of checks, balances and limitations of power which characterizes the national and international rule of law. The excess of hyper-sovereignty becomes especially visible if a state acts extraterritorially as if it was acting on its own territory. Hyper-sovereignty is, to a large extent, a reaction to cyber-anarchy and a mere adapting of enforcement capacities to the digital age. But it is not only the really existing or perceived tendency towards cyber-anarchy that seduces states to exert hyper-sovereignty. As the NSA-scandal has drastically shown, states are also seduced by the seemingly limitless possibilities that the Internet grants to conduct personal surveillance in a relatively cheap and seamless way, to gain omniscience domestically and abroad, and to -in all of that- avoid the prying eyes of a critical democratic public. «Collect it all,

47 Morozov, E., *The net delusion. The Dark Side of Internet Freedom,* PublicAffairs: New York, 2011.

48 Non-democratic states usually perceive the Internet as a means of Western propaganda.

49 Schmidt, Eric & Cohen, Jared: «Web censorship: the net is closing in», *The Guardian*, 23.4.2013, https://www.theguardian.com/technology/2013/apr/23/web-censorship-net-closing-in, accessed 13.1.2020.

sniff it all; know it all, exploit it all», as one of the leaked presentations by the NSA bluntly stated.[50]

Thirdly, there is the scenario of *Internet Balkanization*. As the example of China shows, due to the increasing capacity of contemporary computing, localizing or sealing off the Internet as nationally closed realm became possible, which creates the third scenario of a balkanized[51] or re-localized Internet (aka *SplInternet*[52]) that unties global connections in the interest of state security. As mentioned before, Russia, too, can be understood as having moved in this direction by its requirement to store personal data concerning Russian users physically in the country,[53] which makes it very difficult for smaller foreign companies to compete in the Russian market. Internet Balkanization poses a threat to the global economy, to the cultural and scientific significance of the open Internet and to the Freedom of Speech as a universal right.

In regard to the *Microsoft Ireland* case, it is easy to see that, as long as the Supreme Court did not reach a conclusion, there was a tendency towards a regulatory deficit that

---

50 As a rule of thumb, one could assume that with the decrease of cyber-anarchy, there is an increasing risk of hyper-sovereignty. Both phenomena are, however, not opposed, but ultimately related. Hyper-sovereignty is just another facet of cyber-anarchy, inasmuch as it appears as anarchy of power. The equating of anarchic and hyper-sovereign tendencies in the digital age has also been discussed in light of a juxtaposition of the concepts of law and code: «Our age of the nomos of the code is always in danger of in toto replacement of the law (*nomos*) with the atavistic and more authoritarian code of de facto powers-a replacement that is worse if done by states, corporations and secret services than by smaller actors claiming to be the defendants of the digital commons.» Johannes Thumfart, «Francisco de Vitoria and the Nomos of the Code: The Digital Common and Natural Law, Digital Communication as Human Right, Just Cyber-warfare», in Beneyto, J. & Corti, J. (eds.), *At the origins of Modernity. Francisco de Vitoria and the Discovery of International Law,* Springer: Basel 2017, 197–217, p. 199.

51 Brief amici curiae of Former Law Enforcement, National Security, and Intelligence Officials in support of neither party filed, pp. 9f; Meinrath, Sascha, «We Can't Let the Internet Become Balkanized», *Slate*, 14.10.2013, http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html, accessed 13.1.2020.

52 Searls, Doc, «The SplInternet», Blog, December 2008, http://blogs.harvard.edu/doc/2008/12/16/the-splinternet/, accessed 13.1.2020.

53 SAVELYEV, A.: «Russia's new personal data localization regulations: A step forward or a self-imposed sanction?», *Computer, Law & Security Review,* 2016, 32, 128–145.

could be understood as an expression of the scenario that we have hyperbolically labelled as cyber-anarchy. This, of course, is unacceptable and undermines the rule of law. On the other hand, the CLOUD Act that was issued as a result of the Microsoft Ireland case, due to its lacking emphasis on judicial control and its strong emphasis on bilateral negotiations, could increase a tendency towards hyper-sovereignty. If, finally, Microsoft and its supporters in the EU had won with their -in principle outdated- emphasis of Irish sovereignty, this would have, at first, increased the tendency towards cyber-anarchy, inasmuch as it would have enticed bulletproof hosting in under-regulated territories. Amongst better regulated countries, however, such regulations, which are in an «unnecessarily aggressive»[54] way bound to territory, have a tendency to increase Internet Balkanization, for example by geo-blocking or the compulsory storing of data in the territory of the user's residence.

It is important not to give the empirical fact of the post-territorial functioning of the Internet the last word in a discussion about normativity, because that would mean to commit the error that Hildebrandt exposed as «*cyberspace exceptionalism*».[55] Such a way of arguing -which is highly popular amongst libertarians- basically says that the empirical post-territoriality of the Internet makes the normative concept of the territorial nation-state obsolete. This is, of course, a form of the *is-ought-fallacy* discussed in the next chapter. In addition to the already mentioned costs of Internet Balkanization, due to the post-territorial scope of cyberspace and global business practices associated with it, it is however questionable if approaches based on the primacy of territory represent a viable and sustainable long-term solution. Albeit it is true that normative discussions cannot be based on empirical reality alone, they make little sense -or are only ideological in nature- if they are completely dissolved from empirical facts.

---

54 SVANTESSON, D. & GERRY, F., «Access to extraterritorial evidence: The Microsoft cloud case and beyond», *Computer Law & Security Review,* 2015, 31, 478–489, pp. 488.

55 Hildebrandt discussed similar concepts in regard to what she calls «*cyberspace exceptionalism*» and justly criticizes the confusion of empirical and normative statements at the argumentative base of such cyber-libertarianism, which is in a sense complementary to the discussion of territory in section 3 of this contribution. HILDEBRANDT, M., «The Virtuality of Territorial Borders», *Utrecht Law Review,* 2017, Volume 13, Issue 2, 13–27, p.21.

3. Hans Kelsen on *Lotus* and the illusion of sovereignty and territory as empirical-scientific facts

The trilemma of cyberspace sovereignty, described in the foregoing, is almost unsolvable if one assumes that on the one hand cyberspace is post-territorial and on the other hand sovereignty is necessarily based on territory. These assumptions are responsible for the initial tension between the state and cyberspace at the heart of the trilemma. However, the connection between sovereignty and territory is not as close as it may intuitively seem.

Already in the beginning of the 20th century, in his books on *The Problem of Sovereignty* and *The General Theory of Law and State*,[56] legal theorist Hans Kelsen critically analyzed the connection between territory and sovereignty, and, following Kant, refuted an understanding of sovereignty and legal territoriality based on empirical categories. Territory is an empirical-geographical category, Kelsen argues, while sovereignty and legal territoriality are normative legal categories. Both categories should not be confused. In the following, this important philosophical insight will be applied in order to develop a post-territorial understanding of sovereignty.

Kelsen opens his line of thought with a refutation of the idea that sovereignty implies a literally *higher* location of the state in relation to its subjects as this is suggested by the etymology of sovereignty (from Latin *super,* «above»). «Obviously», Kelsen argues, «it is only an image, when the relationship between the state and other elements is being depicted as a *spatial* relationship. Here, just as in many other cases, an illustration that has been created out of mental convenience turns into an obscuration of the object of knowledge».[57]

Concerning the empirical understanding of sovereignty in general, Kelsen adds the following:

---

[56] Kelsen, H., *Das Problem der Souveränität,* Mohr Siebeck: Tübingen, 1928; Kelsen, H, *General Theory of Law and State*, Harvard UP: Cambridge, 1949.

[57] «Es ist offensichtlich nur ein Bild, wenn das Verhältnis des States zu anderen Elementen als eine *räumliche* Beziehung dargestellt wird. … Wie so oft wird auch hier Denkbequemlichkeit geschaffene Veranschaulichung zu einer Verdunkelung des Erkenntnisgegenstands (…).», Kelsen, H., *Das Problem der Souveränität,* Mohr Siebeck: Tübingen, 1928, p. 6.

> *«The naturalistic direction of modern political sciences (*Staatslehre*) creates a prevailing tendency towards a, -futile and illusionary-, understanding of sovereignty as an empirical-scientific* fact. *It can be proven that something as sovereignty cannot exist as a social reality (…). In the sphere of natural realities, sovereignty must imply roughly freedom and independence of one power from the other (…). In this factual sense (…), no state can be sovereign because even the greatest superpower is being determined by others on all sides, in terms of economic, juridical and cultural life».*[58]

Sovereignty as an empirical-scientific *fact* creates an illusion, Kelsen argues. Pretending that sovereignty implies not only independence and freedom as normative principles, but also as empirical realities, is contradictory, since -and here Kelsen is heavily relying on Kant-, independence and freedom cannot be found in empirical reality at all. Empiric reality constitutes a chain of causes and effects. None of its parts can be factually free and independent since this would contradict the very idea of empirical sciences as a whole.[59]

So, what, then, is sovereignty? «Sovereignty», Kelsen argues further in his book, «is only the order, which is not «contained» in any other order, because it cannot be deduced from another order (…). Only if sovereignty is being understood as a property of the state determined as a legal order, the attempt to understand sovereignty in legal terms makes sense».[60] In another passage, Kelsen writes even clearer:

---

[58] «Die naturalistische Richtung der modernen Staatslehre drängt diese immer wieder – immer wieder vergeblich und um den Preis gröbster Selbsttäuschung – das Souveränitätsproblem im Wege sozialer Tatsachenforschung, die Souveränität als *Faktum* auf naturwissenschaftlich-empirische Weise, womöglich induktiv zu erfassen. Dass es aber für eine auf die soziale Wirklichkeit gerichtete Betrachtung so etwas wie Souveränität nicht geben kann (kann bewiesen werden) (….). In der Spähre der Naturrealität muss Souveränität den Sinn etwa von Freiheit und Unabhängigkeit von einer Macht oder Herrschaft von einer anderen annehmen (…). In diesem faktischen Sinne (…) kann kein Staat (…) souverän sein, ist jeder Staat (…) selbst die politisch gewaltigste Großmacht nach allen Seiten des wirtschaftlichen, rechtlichen und kulturellen Lebens von anderen bestimmt, abhängig, unfrei. », Ibid.: pp. 6f..

[59] Kant makes this argument in the «Antinomies of Pure Reason» in the Critique of Pure Reason.

[60] «Souverän is nur die keiner anderen «enthaltene», weil aus keiner andern ableitbare Ordnung (…) Nur wenn Souveränität als Eigenschaft des als Rechtsordnung bestimmten Staates erkannt wird, kann der (….) Versuch, Souveränität als einen Rechtsbegriff zu denken, einen Sinn erhalten. «, Ibid., pp. 13f.

> *«To name sovereignty a property of the state can only be valid (…) inasmuch as the state is being understood as an order and the identity of that order with the legal order is being recognized.«*[61]

Kelsen bases his critique of the understanding of territoriality in empirical terms on the same rejection of the confusion of empirical and normative categories. He writes in his *General Theory of Law and State:*

> *«The unity of the State territory, and therefore, the territorial unity of the state, is a juristic, not a geographical-natural unity. For the territory of a State is in reality nothing but the territorial sphere of validity of the legal order called State.«*[62]

Luckily, Kelsen adds some practical arguments to his reasoning. He references several phenomena of extraterritorial jurisdiction, for example concerning ships under the flag of a nation, which do not make part of the territory of a nation in spite of representing a sphere of validity of national legal norms. A similar situation, he sketches, is given during the occupation of a territory, where a state can perform coercive acts on another territory without incorporating the respective territory. Further, Kelsen adds that a state has the right to attach sanctions to delicts committed within the territory of another state.[63] In the enhanced English version of the text from 1949 -the German original dates from 1925-, Kelsen illustrates this idea with the Lotus case from 1927.[64]

---

61 «Dass Souveränität eine Eigenschaft des Staates sei (…), kann nur insofern Geltung haben, als der Staat als Ordnung und die Identität dieser Ordnung mit der Rechtsordnung erkannt wird.», Ibid., p. 16.

62 Kelsen, H., *General Theory of Law and State*, Harvard UP: Cambridge, 1949, p. 208. Because of this distinction, Kelsen speaks several times with the greatest amount of terminological distance about the «so-called territory of a state». From a merely philosophical point of view, this is an inevitable conclusion from his Kantian epistemology that tries to avoid the *is-ought-fallacy,* the confusion of empirical concepts with normative concepts, which will be explained to non-philosophers some paragraphs below.

63 «That the validity of the national legal order is restricted by the international legal order to a certain space, the so-called territory of the state, does not mean that the national legal order is authorized to regulate only the behavior of individuals living within this space. (…) A state can, without violating international law, attach sanctions to delicts committed within the territory of another state» (Ibid.: p. 209). This passage has also been discussed by Svantesson as an «unequivocal endorsement of jurisprudential legitimacy of extraterritoriality, at least in the context of delicts», SVANTESSON, D.J.B., «A Jurisprudential Justification for Extraterritoriality in (Private) International Law», *Santa Clara Journal of International Law,* 2015, 13, 517–571, p. 542.

64 The Lotus case was the result of a collision between the S.S. Lotus, a French steamer and the S.S. Bozkurt, a Turkish steamer. As a result of the accident, eight Turkish citizens aboard the Bozkurt

> *«In the* Lotus *Case the Permanent Court of International Justice expressed the opinion, in 1927, that there is no rule of International Law which prohibits a State from exercising jurisdiction over a foreigner in respect to an offence committed outside its territory. (….) That the power of the State is limited to its own territory does not mean that no act of the State may be legally carried out outside of this State's territory. The limitation refers in principle only to coercive acts in the wider sense.«*[65]

Kelsen does not elaborate this point further, although it could be understood as the climax of his deconstruction of the understanding of sovereignty in terms of empirical territory. He also seems to fall back to common naiveté in regard to territory in a terminological sense, because he does not relativize the term in this instance (exactly where it would be so important to do so).

Nevertheless, the Lotus-principle provides a good opportunity to illustrate the importance of Kelsen's legal philosophy to the understanding of claims about territoriality and sovereignty in the *Microsoft Ireland case*. *Lotus* has been frequently discussed by the actors in this case, in literature and some of the Amicus Curiae briefs.[66] With its denial of the legitimacy of extraterritorial enforcement jurisdiction, it has been primarily understood as the greatest obstacle for states to gain access to extraterritorial evidence.

However, there are different readings of *Lotus* in relation to cyberspace. Kohl, for example, in her book on *Jurisdiction and the Internet,* emphasizes, just as Kelsen did, that *Lotus* was originally an *extension* of enforcement beyond territory -or, in Kohl's words,

---

drowned. On 7 September 1927, the case was presented before the Permanent Court of International Justice, the judicial branch of the League of Nations, the predecessor of the UN. The issue at stake was Turkey's jurisdiction to try the French lieutenant on watch at the time of the collision. Since the collision occurred on the high seas, France claimed that the state whose flag the vessel flew had exclusive jurisdiction over the matter. The Court, however, rejected France's position stating that there was no rule to that effect in international law.

65 Kelsen, H., *General Theory of Law and State*, Harvard UP: Cambridge, 1949, p. 210.

66 Brief Amicus Curiae of United Nations Special Rapporteur on the Right to Privacy Joseph Cannataci in support of neither party, p. 19; Brief of *Amici Curiae* Jan Philipp Albrecht, Sophie in't Veld, Viviane Reding, Birgit Sippel, and Axel Voss, Members of the European Parliament in Support of Respondent Microsoft Corporation, p. 18; OSULA, A.M., «Transborder access and territorial sovereignty», *Computer Law & Security Review,* 2015, 31, 719–735, p. 726.

the first in a series of «expansion(s) of the territoriality principle», which was owed to an increase of international traffic at the beginning of the 20th century, i. e. a different socio-technological situation that questioned the traditional understanding of territoriality.[67]

Whatever might be the right interpretation of *Lotus* and applicable international public law, one cannot fail to observe that an adaption of the understanding of territoriality to the reality of the post-territorial Internet has taken place since a while in legal practice. Well-known cyberspace-related cases such as *LICRA and UEJF v. Yahoo! Inc. and Yahoo France*[68] and *People v. World Interactive Gaming Corp*[69] already transcend the traditional understanding of the territoriality-principle to the favor of an effects-based, «destination approach».[70] The weaknesses of such an approach is clearly that, according to this logic of universal jurisdiction – as has already been criticized concerning the Lotus case in 1928 – «every individual may be subject to the laws of every State at all times and in all places.»[71] Whilst such a reasoning may have only served as an abstract *reductio ad absurdum* at the time of the Lotus case, it has clearly concrete implications today. In short, the *destination approach* requires that -since every website can be viewed from any part of the globe- every website also complies with any laws anywhere on the globe,

67 «The Permanent Court in Lotus redefined the territoriality principle by abandoning the requirement that the offender must be physically in the territory or that the causative act must have occurred there for there to be a valid territorial claim, in favour of a nexus, which merely required the offender's act to affect the territory. In other words, it allowed for a result-oriented jurisdictional claim. This, no doubt, was more attuned to modern conditions which exposed States frequently and substantially to the effects of conduct by absent actors.», Kohl, U., *Jurisdiction and the Internet. Regulatory Competence over Online Activity*, Cambridge UP: Cambridge, 2007, p. 90.

68 Ibid. pp. 99: *LICRA and UEJF v. Yahoo! Inc. and Yahoo France* concerns France's prohibition of the auctioning of Nazi-memorabilia in France from US-based servers, which was decided to the favor of the French, limited understanding of the Freedom of Speech.

69 Ibid. pp. 102: *People v. World Interactive Gaming Corp* concerns gambling sites targeting an US audience and operated from Antigua, which has been decided against the site's legality.

70 Uta Kohl: «Jurisdiction in Cyberspace», in: Tsagourias, N. & Buchan, R. (eds.), *Research Handbook on International Law and Cyberspace*, Edgar Elgar: Cheltenham, 2015, 30–54, pp. 44f.

71 BRIERLY, J.L.: «The Lotus Case», *Law Quarterly Review*, 1928, 44, 154–175, p. 161.

which is equally impossible and nonsensical. Nevertheless, the destination approach is being used more and more frequently.

As mentioned before, the GDPR has a post-territorial scope inasmuch as its «territorial»-scope is based on the -not even necessarily financially remunerated- participation in the EU market and the monitoring of the behavior of data subjects within the EU, which can be understood as a pure destination approach without any relation to geographical-empirical territory in regard to origin:

> *«This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related a.) to the offering of goods or services, irrespective of whether a payment of the data subject is required, b.) to the monitoring of their behaviour as far as their behaviour takes place within the Union.»*[72]

Additionally, it has been seriously discussed to tax US digital enterprises in Europe for their purely Internet-based, not financially remunerated transactions with European users.[73]

Of course, and justly so, it is a very long path from legislative jurisdiction, which *Lotus* allows, to enforcement jurisdiction, which *Lotus* prohibits. It is therefore probable that only such states will attempt to push such practically universal jurisdiction onto the digital world, which are sure that they can make their voice heard, for example by diplomatic or economic pressure. For Europe, this may include ambitions to strive for the status of a «regulatory superpower»[74], which is, of course, problematic, because such ambitions towards hyper-sovereignty usually bring about conflicts.

For the reason of enforceability alone, it is much easier to regard the so called «origin approach» as the international standard for transborder access, i. e. that -

---

72 GDPR Art. 3,2.

73 Schreuer, Milan, «Targeting Tech Giants, Europe Unveils Digital Tax Proposal», *New York Times*, 21.3.2018, https://www.nytimes.com/2018/03/21/business/europe-tech-digital-tax.html, accessed 13.1.2020.

74 Leonard, Mark, «Connectivity Wars. Weaponizing Interdependence», *European Council on Foreign Relations*, http://www.ecfr.eu/europeanpower/geoeconomics, accessed 13.1.2020.

as this is the predominant opinion concerning the Microsoft Ireland case- the country were the information in question is physically stored has the jurisdiction over the respective information. The weaknesses of this approach are obvious. First, it entices extraterritorial bulletproof hosting in countries with particularly low regulations -hence, fosters a tendency towards what has been called cyber-anarchy earlier in this contribution (section 2). Second, as has been laid out there as well, it will make states that are better regulated work towards Internet balkanization and compulsory re-localization of citizen's data within the grasp of national enforcement jurisdiction.[75]

Sustainable solutions must, indeed, move beyond the gospel of empirical territory and beyond the dichotomy between origin approach and destination approach. They should, with Kelsen, not fall for the fetish of territoriality understood in a geographical-empirical sense, but rather come to an understanding of the limits of state jurisdiction in a purely normative sense that can relate in a more flexible way to empirical territory. This is what we call a «post-territorial» approach to sovereignty in cyberspace.

Just as concerning its empirical meaning laid out in section 2, also concerning its normative function, post-territoriality does not simply amount to non-territoriality, i. e. the complete negation of the empirical fact of territory. Analogue to the fact that the often quoted empirical reality of the «laws of the jungle» does not need to be decisive to how humans live (Social Darwinists are guilty of the *is-ought-fallacy* par excellence), but, nevertheless, a realistic kind of legislation cannot negate that part of human nature completely, a post-territorial approach does not entirely negate the existence of empirical boundaries of a territory, but it does not grant geography the last word when it

[75] Compare with Svantesson and Gerry: «Views such as that «if data is located inside the EU it must benefit from the protections of EU law» are too simplistic as a solution even if they arguably amount to a correct description of the legal landscape under current thinking. (…) Given the fluidity of data storage, it is unnecessarily aggressive to argue that all data located in the EU must automatically be protected by EU data privacy law.« SVANTESSON, D. & GERRY, F., «Access to extraterritorial evidence: The Microsoft cloud case and beyond», *Computer Law & Security Review,* 2015, 31, 478–489, pp. 487f.

comes to the question of how a normative framework for the Internet should be designed. As Hildebrandt puts it, adequate legal models concerning cyberspace, «cannot (...) be grounded in the monopolistic spatiality of territorial sovereignty».[76]

In a post-territorial approach, rather than primarily focusing on the relatively unsubtle, all too tangible argument of territory, details such as the citizenship of the suspect, the nature of the requested data, the nature of the crime, the degree of regulation in the country where the data is stored and the degree of regulation in the country that requests data, and further, the relevance of the crime to the nation leading the investigation should be considered. Overall, such an approach finds its limitation not in territory, but rather in the, at least de jure, universal nature of fundamental rights.

In order to illustrate the practical implications of such a non-territorial approach: E.g., accessing meta-data in regard to child pornography stored on the territory of a notoriously under-regulated Internet «rogue state» related to a great number of users in the nation leading the investigation, which is well regulated, is hardly comparable to accessing personal content stored in a country that is well regulated in relation to copyright infringements committed by very few users, which are investigated by a poorly regulated nation.

The U.K.-U.S. CLOUD Act Agreement from October 7, 2019 can be understood as such a turn away from territory as a limiting principle of data production orders to other, more subtle restrictions: E.g. citizens and residents of the US are exempted from access by UK law enforcement and so are UK citizens and residents regarding access by US law enforcement. However, citizens from other nations still aren't protected, which, of course, opens the door to all kinds of abuse.

Another problematic issue are regulations regarding privacy applicable by both parties of the agreement: Whilst they might «promise to induce privacy-enhancing reforms»,[77]

---

[76] HILDEBRANDT, M., «Extraterritorial Jurisdiction to enforce in Cyberspace? Bodin, Schmitt, Grotius, in Cyberspace», *University of Toronto Law Journal,* Spring 2013, Volume 63, Number 2, 196-224, pp. 224.

[77] Daskal, Jennifer & Swire, Peter: The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards, Tuesday, October 8, 2019 https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards, accessed 13.1.2020.

the reforms in question would be triggered by US regulations and therefore signify an attempt to equal the EU in its problematic aspirations to become a «regulatory superpower» in the digital sector, which provides the ground for a number of conflicts.

An additional focus of the U.K.-U.S. CLOUD Act Agreement are fundamental rights issues, i. e. restrictions regarding crimes punished with death penalty in the US and restrictions regarding crimes related to limitations of the freedom of speech in the UK. Whilst the bilateral nature of the CLOUD Act is, in general, problematic because it infinitely increases the bargaining power of the US, where most tech firms are situated, the included provisions can be regarded as an important step towards the development of a post-territorial legal framework for the obtaining of e-evidence.

As these examples make clear, Kelsen's deconstruction of territoriality understood as an empirical category does not only have epistemic and legal significance, but is also highly political.[78] Understanding territory as an empirical fact that limits public sovereignty, i. e. the right of a people to formulate its own norms, in an absolute way, does, in a last instance, also limit the degree of to which life in democracies is indeed self-determined and free in a normative sense. The fetish of an absolute, empirical understanding of territorial sovereignty should not in all cases force a people to live with effects of information stored on another territory or websites operated from another territory. In this context, a rather community-oriented than territory-oriented understanding of sovereignty, as this has been proposed as a solution to the problem of rule of law in cyberspace by Ryngaert and Zoetekouw,[79] is partly intriguing, but bears traces of a substantialization and essentialization of community instead of territory, and, by that, also of the very confusion of normative and empirical categories that is criticized by Kelsen.

---

78 Kelsen discussed the political importance of epistemological relativism to democracy at length. See: KELSEN, H., «Absolutism and Relativism in Philosophy and Politics*», The American Political Science Review*, Oct., 1948, Vol. 42, No. 5, 906–914.

79 Cedric Ryngaert & Mark Zoetekouw, «The end of territory? The re-emergence of community as a principle of jurisdictional order in the Internet era», Kohl, U (ed.), *The Net and the Nation State. Multidisciplinary Perspectives on Internet Governance*, Cambridge UP: Cambridge 2017, 185–201.

Another issue of great importance concerning the relativism of territorial sovereignty, albeit it goes exactly beyond the scope of epistemic relativism, can also be found at Kelsen:[80] Just as the commodity *fetish* in Marx first simplifies and then overshadows the more complex, and in part -let's think about the textile or phone industry- unbearable reality of social relations embodied in a specific product, the fetish of the geographic-empirical understanding of territoriality does not only mask the more complex reality of the arbitrariness and freedom underlying any normative rule (as discussed in the paragraph above), but it also masks a material epistemic reality that is more complex than the one of territories with clear borders. The *Lotus* case, one must remember, only was an issue at all because the tried incident took place in international waters, i. e. in commons. Without the existence of such a space connecting states, but not subordinate to the logic of states and hermetic territories, questions concerning extraterritorial jurisdiction would be hardly such an important problem or probably not even arise.

In general, one can say that the Westphalian model of a world of sovereign states existing within a vacuum -a model that Hildebrandt critically described as «gapless»-,[81] was only an interlude, and not a very realistic one.[82] As modern technologies increasingly globalize the scope of actions and expose the totality of the planet to the effects of human actions -a development that has been geologically labelled as *anthropocene*[83]-, it becomes increasingly clear, that, in a material sense, a great part of the world does not adhere to the logic of mutually excluding sovereign territories at all, but materially consists of commons -such as the high seas, outer space, the moon and antarctica. And whilst the airspaces of course are national, the air within it, and its raising temperature, is common.

---

80 Kelsen implicitly discusses the juxtaposition between commons and sovereignty by discussing subsurface rights and airspace rights as unclear limits of territorial sovereignty.

81 HILDEBRANDT, M., «Extraterritorial Jurisdiction to enforce in Cyberspace? Bodin, Schmitt, Grotius, in Cyberspace», *University of Toronto Law Journal,* Spring 2013, Volume 63, Number 2, 196–224, pp. 206, 208, 222.

82 The coincidence of pre-Westphalian and post-Westphalian models with special regard to cyberspace is at length discussed in: Johannes Thumfart, «Francisco de Vitoria and the Nomos of the Code: The Digital Common and Natural Law, Digital Communication as Human Right, Just Cyberwarfare», in Beneyto, J. & Corti, J. (eds.), *At the origins of Modernity. Francisco de Vitoria and the Discovery of International Law,* Springer: Basel 2017, 197–217.

83 Davies, J., *The Birth of the Anthropocene,* UCPress: Oakland, 2016.

The same holds true for the waters within the 12-miles zone of a nation whose level of pollution depends largely on factors outside of any single nation's jurisdiction.

It is telling that almost all of the unsolved important questions of the 21st century concern the way how we deal with those commons, which were -in last instance- ignored because too many theorists and practitioners confuse this complex, globally entangled empirical reality with the simplifying, in last instance, not even empirical model of sovereignty based on an, in last instance, merely cartographic[84], and as Kelsen underlines, misleadingly impermeable and two-dimensional[85] understanding of territory. As Held writes in his seminal text on the inadequacy of territorial democracy to global problems:

> *«During the period in which nation-states were being forged – and the territorially-bound conception of democracy was consolidated – the idea of a close mesh between geography, political power and democracy could be assumed. It seemed compelling that political power, sovereignty, democracy and citizenship were simply and appropriately bounded by a delimited territorial space. These links were by and large taken for granted and generally unexplicated. But they can be no longer. Globalization, global governance and global challenges raise issues concerning the proper scope of democracy and of a democracy's jurisdiction, given that the relation between decisionmakers and decision-takers is not necessarily symmetrical or congruent with respect to territory.»*[86]

As will be argued in the next part, cyberspace can be regarded as a *global commons*[87] and, especially due to its effect on a variety of stakeholders across the globe, it needs to

---

84 HILDEBRANDT, M., «Extraterritorial Jurisdiction to enforce in Cyberspace? Bodin, Schmitt, Grotius, in Cyberspace», *University of Toronto Law Journal,* Spring 2013, Volume 63, Number 2, 196–224, pp. 206ff.

85 Kelsen, H., *Allgemeine Staatslehre*, Julius Spriner: Berlin, 1925, pp. 142, 139.

86 HELD, D., «Democratic Accountability and Political Effectiveness from a Cosmopolitan Perspective», *Government and Opposition,* April 2004*,* 39(2), 364–391, p. 372.

87 Benkler Y., *The wealth of networks,* Yale University Press: New Haven, 2006; Lessig L., *Free culture,* Penguin: New York, 2005; This question is also discussed in: Johannes Thumfart, «Francisco de Vitoria and the Nomos of the Code: The Digital Common and Natural Law, Digital Communication as Human Right, Just Cyber-warfare», in Beneyto, J. & Corti, J. (eds.), *At the origins of Modernity. Francisco de Vitoria and the Discovery of International Law,* Springer: Basel 2017, 197–217., pp. 201ff.

be considered in its own right, beyond the normative model of territorial sovereignty, but also beyond the state.

4. Beyond lobbying: companies as motors of global regulatory change

The Westphalian «gapless» model of a world of sovereign states and the scenarios presented in the *Cyberspace Sovereignty Trilemma* are not only misleading because their underlying understanding of territorial sovereignty is based on the confusion of empirical and normative models. They are also misleading because they negate that the most important actor in cyberspace is, in fact, not the state, but rather the company. It might be soothing to some that in particular the, in part dramatic, scenario labelled as *cyber-anarchy* and its libertarian advocates negate the great regulative de facto impact that companies have regarding cyberspace. So, instead of following the Westphalian illusion and continuing to pretend that states are all-powerful entities within a vacuum whose Sisyphus task it is to regulate the global Internet all by themselves, one should take a look at the reality of the web, which is largely dominated by profit oriented non-state actors.

This is especially important, because the territorial idea of sovereignty is not only challenged by the post-territoriality of technology, but also by the post-territoriality of companies, and both are intertwined. Sassen, for example, described already in 2006 a process of «denationalization» that is owed to the fact that digital cross-border electronic communication provides an increasingly crucial part of the infrastructure to globally acting companies.[88] And of course, this post-territorial setup is especially impactful concerning enterprises in the digital sector, who do not only use the infrastructure of global digital communication, but play a role in shaping and regulating it. Microsoft, for example, in spite of having its legal seat in the US, maintains an office in almost every country of the world, and even more importantly, around 100 data centers in about 40 different countries, which makes it subject to many different jurisdictions. Just

[88] Saskia Sassen, «The embeddedness of electronic markets: The case of global capital markets», in Knorr Cetina, K. & Preda A. (eds.), *The sociology of financial markets,* Oxford University Press: Oxford, 2006, 17–37, p. 29.

as any multinational, the company is also involved in highly complex schemes to avoid paying taxes by exploiting various loopholes of extraterritoriality.[89]

It is one of the core characteristics of this case, that, in spite of this post-territorial setup, Microsoft repeatedly made the atavistic argument that Ireland's «sovereignty» was violated if it was to submit the emails stored in Ireland to the US government. At the same time, Microsoft's President and Chief Legal Officer Brad Smith coined the *bon mot*: «We need 21st century laws to protect 21st century technology.»[90] This almost contradictory kind of rhetoric has granted Microsoft the support of a variety of different groups who would not have much in common otherwise. It makes it however difficult to conclude what Microsoft actually wants, i. e. how one can understand its regulatory agenda in the *Microsoft Ireland* case, and how this insight can be helpful to an understanding of the regulatory function of companies in cyberspace.

Mattli and Woods distinguish between four types of motives for companies to act as motors of regulatory change:[91] *Corporate newcomers:* When new companies enter a market that is dominated by established companies which profit from regulations working to their favor, these newcomers often push for deregulation. *Corporations at risk*: It can be the case that the economic viability or even the survival of a company depends on new regulatory models.[92] *Corporate levelers of the playing field:* Corporate actors who, faced with more costly and stringent regulations than competitors elsewhere, will

89 Birrell, Ian, «Bill Gates preaches the aid gospel, but is he just a hypocrite?», *The Guardian*, 6.1.2014, https://www.theguardian.com/commentisfree/2014/jan/06/bill-gates-preaches-fighting-poverty-hypocrite-microsoft-tax

90 Remarks of Brad Smith after Supreme Court oral arguments in Microsoft's warrant case. Microsoft YouTube Channel, published 27.02.2018, https://www.youtube.com/watch?v=7L07WCQEM1E, accessed 13.1.2020.

91 Walter Mattli & Ngaire Woods: «In Whose Benefit? Explaining Regulatory Change in Global Politics», in Mattli W. & Woods, N., (eds.) *The Politics of Global Regulation* Princeton UP: Princeton, 2009, 1–43, pp. 32.ff

92 After Tchernobyl, for example, the nuclear energy industry was heavily damaged. As a result, it established the World Association of Nuclear Power Operators (WANO) to establish global standards of safety and transparence.

support societal groups lobbying for more stringent regulations on a wider scale.[93] *Corporate consumers:* Companies are also large-scale consumers. Sometimes, they need to push for a regulation that suits their interest as consumers.[94]

It is hard to put Microsoft within these four types, because concerning the issues at stake in *Microsoft Ireland*, it does not abide to one jurisdiction, but at least according to its own understanding, to as many jurisdictions as it has server farms abroad. Definitely, however, Microsoft fits in the type *corporation at risk* because it must have feared that if the US government had its will, then -as laid out in section 1- it could have suffered disadvantages in comparison to its competitors solely based in the EU, which to prevent must be considered the key motivator of the company's actions.

Following a similar line of argument, Microsoft represents also a type of *corporate leveler of the playing field,* albeit inverted in a topological sense and also inverted concerning its positive relation to stricter regulations. Microsoft points towards stricter EU-privacy regulations not only as an, in parts, resident of the EU, but also as to what could amount to a sizeable advantage of competitors based in the EU, which it wanted to level by improving respective US regulations.

From this perspective, it is kind of ironic that spokespersons of the EU and EU digital enterprises side with Microsoft concerning this case, as also laid out at length in section 1. It is worth examining the Amicus Curiae brief by EU national trade organizations concerning this question. Whilst it also employs the technologically outdated, albeit convenient sovereignty-argument («The US cannot search data on Irish soil») and utters realistic concern about foreign policy implications, it also employs a novel (because non-territorial) argument with the label «*Remote data storage is essential to modern business and social practices*»*:*

[93] For example, within the EU, German corporations during the 1980s teamed up with environmental groups in order to promote the same degree of regulation that was the standard in Germany for every European country.

[94] For example, during the 70s and 80s, as financial sector firms became increasingly dependent on advanced telecommunication services, they pushed for a deregulation of that sector, most of all in Japan, UK and the US.

> *«The modern global economy is driven not just by the flow of goods, but by the flow and exchange of data. Reliance on data flow across borders has become critical to nearly every industry, ranging from companies and products that facilitate the creation and communication of digital content (e.g., Facebook or Twitter) to traditional industries that maintain competitiveness by taking advantage of new methods of data storage and processing. If SCA warrants were to apply to data stored outside of the United States, businesses may retreat from global technological advancement to avoid the government's extraterritorial reach. The economic and social costs of that retreat could be substantial. Just as the rise of transportation networks and international trade once transformed the identity of manufacturers from local operations to national and international firms, the rise of the global digital economy has now altered the basic structure of how and where businesses store and utilize information to deliver products and services to consumers. An open Internet that facilitates the free flow of data across borders is a critical underpinning of modern economic markets in the 21st century».*[95]

It is remarkable that this post-territorial argument is employed nowhere else, also not in the Amicus Curiae brief of the EU Data Protection and Privacy Law Scholars. In any case, it is the only one that can actually explain why EU digital industry and Microsoft, who should be competitors in theory – i. e. if one wrongly assumes that companies have interests limited by national territory- actually fought side by side in this case. Evidently, the degree of collaboration and entanglement between actors on both sides of the Atlantic is so high that inconvenient regulations in the US are understood exactly not as bringing about competitive advantages for the EU's digital industry, but rather also substantial hurdles to common growth and prosperity on both sides of the Atlantic. This, of course, is the case, too, because, as this brief also indicates, not only the EU-US economies are entangled, but their politics as well. Since all European governments entertain good relations with the US, the EU's digital industry seems to feel as threatened by inconvenient US regulation as if it was US American.

Rather than protecting this or that state's sovereignty, what is introduced in the Amicus Curiae brief by EU national trade organizations (in the long quote above), is the *Open Internet* as an interest in itself, which concerns all users. This argument, in the academic

95 Amicus Curiae Brief by EU National Trade Organizations, 6f.

discussion also appearing under the name of digital commons,[96] is interesting, because rather than being based on a right or a domain of a single state, a single company or an individual, it seems to be based on the rights of a post-territorial structure itself.

Multinational companies do not have a very good track record concerning the protection of commons, but to be fair, the respective track record of states is similarly bad. Due to their topographic quality as post-territorial entities, however, multinational companies sometimes have interests that align with the post-territoriality of commons rather than with the territoriality of the nation state. Furthermore, just like non-profit NGOs, transnational companies are exceptionally well equipped to engage on behalf of the commons, because they are not states and therefore can actually understand the commons as not only transcending private, but also public property. This often overlooked non-public characteristic of the commons is, for example, well reflected ICANN's non-state transnational multistakeholder regulation model that has been successfully defended against attempts by authoritarian states such as China and Russia to incorporate Internet regulation in the international, i. e. state dominated framework of the UN.[97]

As the reach of global economy and technology expands, without even intending to do so, companies naturally -not at least due to the expertise that they can afford- become the entities which are most acquainted with international realities beyond the state. This can, in some cases, make them the ones who represent the interest of commons in a normative architecture otherwise dominated by states and their logic of public property. This may sound utopian, but it is a process as old as the institution of modern international law itself. Grotius's first work on international law and its formulation of the modern, still valid commons-based principle of the Freedom of the Seas was the

---

96 Benkler, Y., *The wealth of networks,* Yale University Press: New Haven, 2006; Lessig L., *Free culture,* Penguin: New York, 2005; This question is also discussed in: Johannes Thumfart, «Francisco de Vitoria and the Nomos of the Code: The Digital Common and Natural Law, Digital Communication as Human Right, Just Cyber-warfare», in Beneyto, J & Corti, J (eds.), *At the origins of Modernity. Francisco de Vitoria and the Discovery of International Law,* Springer: Basel 2017, 197–217., pp. 201ff.

97 Eli Dourado: How Russia and the UN are actually planning to take over the Internet, in The Hill, 12 December 2018, http://thehill.com/blogs/congress-blog/technology/295320-how-russia-and-the-un-are-actually-planning-to-take-over-the, accessed 13.1.2020.

result of a work commissioned by the Dutch VOC, who knew the material reality of early modern globalization better than any politician at that time. The VOC simply wanted the right to wage a *bellum iustum privatum*, a private just war, whilst the right to wage wars was before that reserved to states. In order to justify military actions by the VOC, Grotius formulated the still valid, commons-based principle of the Freedom of the Seas.[98]

The VOC-example also points to another fact that is important when contemplating on the contemporary normative role of companies. In the early days of globalization, sovereign companies were not as unthinkable as they are today.[99] Due to its right to wage wars, the Dutch VOC was the first «corporate sovereign».[100] The British East India company, too, has been named by contemporaries «a state in the disguise of a merchant».[101] Many parts of America, were also settled by corporations created expressly for that purpose,[102] the occupation of land being the characteristic of sovereignty *par excellence*, at least according to its classical territorial understanding.

Also, in today's environment of global cyberspace, companies increasingly exert a normative power that makes them comparable to states. For example, a rather fundamental attribute of normative power usually reserved to states is given to digital companies in processes of the self-regulation of hate-speech, where companies become guarantors

98 THUMFART, J., «On Grotius's Mare Liberum and Vitoria's De Indis, Following Agamben and Schmitt», *Grotiana* 2009, 30, 65–87.

99 History, and especially the history of ideas, has simply neglected the normative power of companies, because it is, for a number of reasons a priori dominated by an epistemic focus solely on the state and its territory -the most important one of those reasons being the funding of research in the humanities by states, followed by the state bias of occidental political philosophy since Plato and Aristotle.

100 WILSON, E.: «The VOC, Corporate Sovereignty and the Republican Sub-Text of *De iure praedae*», *Grotiana, 2005-2007, 26-28, 310–340.*

101 Stern P.J., *The State-Company. Corporate Sovereignty and the Early Modern Foundations of the British Empire in India*, Oxford UP: Oxford, 2011, viii, footnote 3.

102 Philip J. Stern, «Bundles of Hyphens»: Corporations as Legal Communities in the Early Modern British Empire in Benton, L. & Ross, R.J. (eds), *Legal Pluralism and Empires, 1500–1850,* New York UP: NY, 2013, 21–48.

and limiters of fundamental rights on their own virtual premises.[103] Perhaps the highest power of a sovereign state are its capacities of military defense. When it comes to cyberwars and cyberattacks, due to digital companies key positions in global networks -although far from perfect- private-public partnerships are the rule, rather than the exception.[104] And the involvement of companies as independent actors in cyber-detterence is discussed. (Footnote: Thumfart, Johannes: Public and Private Just Wars: Distributed Cyber Deterrence based on Vitoria and Grotius. Internet Policy Review. Special Issue on 'Power, Jurisdiction and Surveillance', edited by Monique Mann and Angela Daly. March 2020.

In general, many digital enterprises take on functions traditionally reserved for governments, inasmuch as they are building trust between strangers and producing a safe platform for them to interact, which is the core function of all social media.[105] If one takes Kelsen's definition of sovereignty as the identity and relative independence of an order from other orders seriously, then Internet-based platforms with their respective terms of use seem already to possess features of de facto sovereignty, especially because they are often not adapted, and can impossibly be, to the jurisdictions of the countries, in which their users reside, on whose lives they exert great normative impact. Even greater is the de facto normative impact of Internet-based platforms inasmuch as the disciplinary effect of globally coherent, automated procedures on users' daily lives can hardly be overestimated, especially in regard to informal practices regarding the monitoring of social behavior that create a Foucauldian *Panopticon-effect* in social networks.[106]

Concerning the normative power of Microsoft, the probably most telling detail lies in the fact that, whilst it made the world debate about *Microsoft Ireland,* at Microsoft internally, the reason for the conflict was already resolved since a while in a way that only

---

103 Hui Zhen Gan, «Corporations: The Regulated or the Regulators – The Role of IT Companies in Tackling Online Hate Speech in the EU», *Columbia Journal of European Law,* 2017, 24, 111–121.

104 CARR, M., «Public–private partnerships in national cyber-security strategies», *International Affairs,* 2016, 92: 1, pp. 43–62.

105 Rheingold, H, *The Next Social Revolution*. Basic Books: Cambridge, 2002, pp. 26ff.

106 Thumfart, Johannes, «Warum wir Datenschutz vernachlässigen. Überwachen und Schwafeln», *Die Tageszeitung, 2.6.2013,* http://www.taz.de/!5066384/, accessed 13.1.2020.

appears to be merely technical. The company now stores the data of a customer automatically in the location closest to its most frequent location.[107] With this choice, Microsoft took a step towards the de facto creation of a zone of probable jurisdiction, even more disquieting since this creation is done by an algorithm. Different to the soothing self-image of digital enterprises, «automated processes are not value free; it is widely recognized that machines and automated processes often have assumptions, goals and sometimes values built into them».[108]

As Lessing once wrote, «Code is Law»,[109] or better: «The age of the *nomos of the code* is always in danger of (...) replacement of the law (nomos) by the (...) code of de facto powers, which is a priori without that close relationship to borders and territories that characterize the political or legal nomos.»[110]

Microsoft's agenda in the *Microsoft Ireland* case can especially be considered a success since its outcome, the CLOUD Act, increases the normative power of companies. By permitting the direct collaboration between the US tech sector and foreign governments it makes tech companies themselves «the only real fail-safe to prevent a technology company from inadvertently acceding to a harmful data request.»[111]

---

107 Matsakis, Louise, «Microsoft's Supreme Court Case Has Big Implications For Data», *Wired*, 27.2.2018: https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/, accessed 13.1.2020.

108 KOHL, U., «Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2)», *International Journal of Law and Information Technology*, 2013, Vol. 21, No. 2, 187–234, p. 194.

109 Lessig, Lawrence: «Code is Law. On Liberty in Cyberspace», *Harvard Magazine*, 1.1.2000, https://harvardmagazine.com/2000/01/code-is-law-html, accessed 13.1.2020.

110 Johannes Thumfart, «Francisco de Vitoria and the Nomos of the Code: The Digital Common and Natural Law, Digital Communication as Human Right, Just Cyber-warfare», in Beneyto, J & Corti, J (eds.), *At the origins of Modernity. Francisco de Vitoria and the Discovery of International Law,* Springer: Basel 2017, 197–217, p. 214.

111 Guliani, Neema Singh & Shah, Naureen, «Proposed CLOUD Act Would Let Bad Foreign Governments Demand Data From US Companies Without Checks and Balances», ACLU, https://www.aclu.org/blog/privacy-technology/consumer-privacy/proposed-cloud-act-would-let-bad-foreign-governments-demand, accessed 13.1.2020.

Increasingly, the jurisdiction over material territory seems to be the only thing that companies lack in order to be regarded as sovereign, but this, of course, looks different from a post-territorial perspective.

Concerning the size of its revenues, Microsoft would range between the UAE and Portugal, if it were a state, comparable to companies such as BMW, HP, Amazon, Gazprom and Nestlé.[112] Microsoft founder Bill Gates has largely disassociated from the firm; he is these days better known for running the *Gates Foundation*, whose normative ambitious are way more visible. The foundation, which is still depending on Microsoft's capital, is now the second largest donor to the World Health Organization after the US, and therefore literally taking a seat as equal among states in global policy making.[113] In the field of regulation making, Microsoft showed with the Ireland case that it can trigger a global debate and the issuing of legislation by not assisting a state to obtain evidence and instead bring this before the highest court, which implies a great deal of -primarily financial- de facto power. Even more importantly, it managed to frame a debate that could be realistically understood as an attempt to adjust the highest legal norms to its business model concerning data storage as defending the interests of ordinary citizens regarding privacy, which shows a strong hegemonic influence on global political discourse and helped to gather sympathy not only from users worldwide, but also from trans-sovereign entities such as the EU. Especially concerning this last point, Microsoft differs from Uber's and Google's normative agendas, which both confronted EU-regulations aggressively, albeit with no success.

The last question would be whether that increasing normative role of corporations is necessarily a bad development. Initiatives such as UN Global Compact, which uses the slogan «business as a source of good» and presents itself as being dedicated to «aligning (company) strategies and operations with human rights, labour, environment,

[112] World Bank, Top 100 Countries and States by Revenues, https://blogs.worldbank.org/publicsphere/files/publicsphere/top-100-countries-corporations-by-revenues.jpg, accessed 13.1.2020.

[113] Vidal, John: «Are Gates and Rockefeller using their influence to set agenda in poor states?», *The Guardian,* 15.1.2016, https://www.theguardian.com/global-development/2016/jan/15/bill-gates-rockefeller-influence-agenda-poor-nations-big-pharma-gm-hunger, accessed 13.1.2020.

anti-corruption and the UN Sustainable Development Goals»[114] should always be critically examined in regard to being mere *green washing,* respectively *social washing*.[115] In the same way, as laid out in section 1, *Microsoft Ireland* could also be, in part, interpreted as the hijacking of the highest court of the world's most powerful democracy for a PR-campaign regarding privacy.

On the other hand -and other than widespread anti-corporation bias all across political camps suggests- given the catastrophic historical track-records of states, it is actually kind of absurd to think of states as having to keep their regulatory monopoly to be the sole watchdogs of democracy, human rights and the global commons under any circumstance. Neither Hitler nor Stalin nor Pol Pot were companies, nor is the NSA corporation-owned. Exactly because companies are not states, but equally powerful, they can tackle states in a fundamental way in favor of private interest in general, as this has been the case in *Microsoft Ireland.* Regardless of its surely merely profit-oriented motives and regardless of its weakness in formulating sustainable concepts during this case, Microsoft successfully contested US-American hyper-sovereignty that poses a threat to civil liberties everywhere in the world by leaving the clouded view of national interest and contesting state enforcement jurisdiction in courts. Especially large, multinational companies who can afford long-lasting legal procedures can serve in this way as a means to hedge the power of states. This is especially important in the international sector, which is mostly not really reached by the discourse and the control mechanisms of civil society. By their mere post-territorial power to settle and re-settle, as they had done in the fiscal sector and in the sector of work and market regulations in a manner that was largely disadvantageous to ordinary citizens, companies could also trigger political competition between states concerning better privacy standards that could benefit ordinary citizens.

Unlike states whose leading protagonists are often interested in personal or ideological power, companies ideally follow exclusively economic goals. Whether the involvement

---

114 UN Global Compact: Mission Statement, https://www.unglobalcompact.org/what-is-gc/mission, accessed 13.1.2020.

115 Gancille, Jean-Marc & Siarri, Alexandra: «Après le greenwashing, le socialwashing?», *Libération*, 9.9.2015, http://www.liberation.fr/evenements-libe/2015/09/04/apres-le-greenwashing-le-socialwashing_1375044, accessed 13.1.2020.

of companies in regulatory processes is advantageous or disadvantageous to ordinary citizens therefore depends much on their economic relation to ordinary citizens. If a company depends on individual customers, then it is more likely to engage in normative processes in a way that is advantageous to ordinary citizens. In this way, the dependence of the digital industry on individual consumers, which sets it apart, for example from the financial sector or the arms industry, can contribute to align its normative power with democracy, human rights and the protection of the global commons. From the perspective of such corrective effects of the involvement of companies in regulatory processes, the surge of Public-Private-Partnerships (PPPs) in the cybersecurity sector[116]is to be critically examined inasmuch as it threatens the possibly competitive/corrective relationship between states and companies. Especially in the digital sector, the consolidation of economic power in very few hands signifies a great problem,[117] and should not be reinforced by including state actors in these dynamics of market monopolization, even if that is in fact often the case.

Finally, *Microsoft Ireland* can also be understood as positive to democracies because it dragged the involvement of companies in regulatory processes from the shadowy world of lobbying into the daylight of open debate, where it, in turn, can be contested much easier by global civil society.

But these points only concern what has been called democratic output-legitimacy, i. e. legitimacy through effects.[118] In general, companies are much worse-equipped than states when it comes to democratic legitimacy by internal democratic processes, so called democratic input-legitimacy. *Workplace democracy* might be a trending topic, but with exceptions such as the French *comité d'entreprise,* the German *Betriebsräte*

---

116 CARR, M., «Public–private partnerships in national cyber-security strategies», *International Affairs,*2016*,* 92: 1, 43–62.

117 A. Ezrachi & M. Stucke, *Virtual Competition. The Promise and the Perils of Algorithm-Driven Economy,* Harvard UP: Cambridge, 2016. For a philosophical account see: Johannes Thumfart, «From the Rhizome to the Heavy Tail: Concentration of the Digital Market, Concentration in the Individual, and the Rediscovery of Sovereignty», in: Niermann, I. (ed.), *Concentration*, Fiktion: Berlin, 2015 (E-Book), ca. 35 pp: http://fiktion.cc/books/concentration/, accessed 13.1.2020.

118 SCHARPF, F. W., «Problem-Solving Effectiveness and Democratic Accountability in the EU», *Max Planck Institute for the Study of Societies Working Paper* 03/1, February 2003, http://www.mpifg.de/pu/workpap/wp03-1/wp03-1.html, accessed 13.1.2020.

and the Swedish *Utvecklingsavtalet*, the domain of the enterprise is still far away from functioning and legally mandatory internal democratic procedures and can be compared to dictatorships in this respect.[119]

Conclusion: questioning two dominating ideas (sovereignty as territory and regulatory state monopolies)

It is not very useful to discuss new things with old terms, especially when these new things are not that new, but rather should be part of common understanding by now. The language of law is infused with the primacy of territory, although contemporary legal practices have often little difficulties with extraterritoriality. The respective concepts need to be updated, so that extraterritoriality – if we assume that the distinction between territorial and extraterritorial is still useful – is no longer seen as a bad word, but rather as a phenomenon that needs to be adequately regulated.

The contextual analysis proposed in this contribution has shown that the *Microsoft Ireland* case and especially its surrounding global debate should be understood for the larger part in the *Snowden*-context, although differences between the two phenomena have also been highlighted, which are grounded in the legal and political differences between intelligence operations and criminal law procedures (section 1).

We have concluded that the *Microsoft Ireland* case and its great impact are not to be understood as the expression of a political, but rather of a structural crisis. This structural crisis is owed to what we call the *Cyberspace Sovereignty Trilemma*: the deadlock between cyber-anarchy, hyper-sovereignty and Internet balkanization, which have been identified as the three possible, albeit altogether undesirable hypothetical outcomes of the *Microsoft Ireland* case (section 2).

In order to provide a viable conception for national sovereignty in the digital age, we have developed a post-territorial model of sovereignty from Kelsen's theory of sovereignty, which is based on normative coherency instead of the geographical-empirical fact of territory. Sustainable solutions must move beyond the gospel of territory and

[119] E. Anderson, Private Government: How Employers Rule Our Lives (and Why We Don't Talk About It), Princeton UP, 2017.

come to an understanding of the limits of state jurisdiction in a purely normative sense that can relate in a more flexible way to empirical realities.

It has been concluded that the geographical-empirical boundaries of the nation state should neither be the decisive nor the only criterion for answering the normative question after the reach of sovereignty in the digital age. Likewise, it has been shown that it is equally important not to make the empirical criterion of the post-territoriality of cyberspace the decisive and only criterion for defining the reach of sovereignty. In a post-territorial approach, rather than primarily focusing on territory, details such as the nature of the requested data, the citizenship of the suspect, the nature of the crime, the degree of regulation in the country where the data is stored and the degree of regulation in the country that requests data, and further, the relevance of the crime to the nation leading the investigation should be considered. Some of these criteria are already addressed in the U.K.-U.S. CLOUD Act Agreement from October 2019, which can be considered an important step towards a broader post-territorial regulatory framework regarding e-evidence. This agreement, however, also includes problematic aspects: Its bilateral nature boosts US bargaining power, since most tech firms are located in the US. Further, its tendency to trigger privacy reforms according to US standards in other nations can be regarded as a form of over-reach destined to create conflicts. (section 3)

Finally, we have turned to a second dominating idea in legal thought: the idea of the regulatory monopoly of the state. Just like the idea of sovereignty as territorial, this idea also misleads. Unlike the popular claim goes, even without states taking regulative actions, cyberspace is not free of regulations, but already heavily regulated by companies: in part as de facto regulation by technical design, in part by private coercive actions, for example concerning the censorship of hate-speech, and – as it is the case here – in part by financially well-endowed companies turning to courts. The normative agency of Microsoft is analyzed as an attempt to avoid grave competitive disadvantages in comparison to solely EU-based companies. Besides that, the post-territoriality of global companies is highlighted and the spectrum of interests and range of action that are determined by that post-territoriality are examined. What we find is that, although companies are in general lacking democratic input-legitimacy, they can, because of their topological features and economic interests, under certain circumstances successfully fulfill normative functions to the benefit of ordinary citizens and serve as a counterweight

to the power of states, especially regarding global commons. In light of a post-territorial understanding of sovereignty, it is also examined how far companies already possess features of sovereignty, as this was historically the case, for example regarding the Dutch VOC or the British East India Company. The CLOUD Act, which was the result of the Microsoft Ireland case, is a proof of Microsoft's normative function and the increased normative function of tech companies in general (section 4).