1. The growing issue of “digital sovereignty”

The CJEU decision in the Schrems case\(^1\) is a further step towards the assertion of a EU digital sovereignty. The term “sovereignty” is meant here in its traditional sense: the power to control, \textit{de iure} and \textit{de facto}, a certain space, the activities that in that space are conducted, those who enter such a space, how that space is organized, administer police, judicial and security powers in that space. When the CJEU, in its 2014 \textit{Google Spain} decision\(^2\), states that Google is to be considered established in the EU and therefore subject to EU laws, it is asserting its sovereignty over commercial entities that operate within the European space, albeit via telecommunications networks using technologies such as the Internet.

When the CJEU, a year later, declares that transfer of personal data of European citizens to the US is illegal, it is, in its core, stating that EU law governs the processing of data, not the law of a different State.

---

\(^1\) \textit{Schrems v Data Protection Commissioner [Ireland], C-362/14, of October 6, 2015.} For numerous comments from various perspectives see the special issue of \textit{Il Diritto dell’Informazione e dell’Informatica}, n. 4/5-2015, pp. 683-938

\(^2\) \textit{Google Spain v. Agencia Española de Protección de Datos, Costeja, C-131/12, of May 13, 2014.} The decision has attracted a host of comments. For a comprehensive over-view of the different aspects see G.RESTA – V.ZENO-ZENCOVICH (eds), \textit{Il diritto all’oblio su Internet dopo la sentenza Google Spain}, Roma TrE-Press, 2015 [available on-line at http://ojs.romatrepress.uniroma3.it/index.php/oblio].
The fact that both cases concern personal data should not be misleading. Data protection is considered as one of the distinctive features of the European legal system, of its dominant pre-juridical values, as opposed to a rather different US approach to the same topic. However this has only made it easier – probably thanks to a careful selection in the priority of cases to be decided – for the CJEU to adopt disruptive decisions, which disavow high level institutional positions.

Until the Google Spain decision it was widely believed that processing of data by the great search engine, which is present in practically every moment of our life, was to be considered done on the mainframe computers in the US, and therefore not subject to the EU data protection directive. And transfer of data to that country was guaranteed by an international agreement defined “Safe Harbour” which purportedly guaranteed an analogous level of protection in processing across the Atlantic.

In this last case the aspect of sovereignty is much more noticeable, because the casus belli is expressly indicated as the exercise of sovereign powers by the USA over European data on the basis of the irresistible “Patriot Act”. The CJEU is – looking at things from a realistic perspective – stating that the EU Council inadmissibly renounced to exercising its sovereign powers

---


4 A few days before the Schrems decision, the CJEU issued its judgments in Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság (C-230/14) and in Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate and Others (C-201/14). In the first case the issue concerned the application of Hungarian law to the processing of data by a Slovak based service (EU data protection law “must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered”). In the second case the transfer, without prior consent, of personal taxation data to a social security institution is precluded by EU law. For an overview of the dozen CJEU decisions concerning data protection rendered between 2014 and 2015 see V. ZENO-ZENCOVICH, Data Protection as a Central Issue of ECJ Polices: From Digital Rights Ireland to Data Protection Commissioner [Ireland], in 2016 European Papers, n.1, pp. 369-373
in reaching the “Safe Harbour” agreement with the US. The CJEU is – via the strong case of the protection of fundamental individual rights – drawing the line on sovereign powers and – very clearly – affirming judicial supremacy over issues of the highest political level, such as international policy.

The Schrems decision surely needs to be analyzed from the perspective of two international super-powers facing each other for the control of an essential resource such as global telecommunication network. This confrontation was already very clear in the SWIFT\(^5\) and PNR\(^6\) controversies in which data of bank clients and of airline passengers were, unknowingly or forcibly, communicated to and used by US authorities. Here we have moved to a more general and wider level, because it includes all sorts of data, from the most diverse sources, allowing in-depth profiling.

2. Sovereignty as jurisdiction

This is not the forum for such an examination. Suffice it to note, however, that there is no reason why networks and all the activities that are directly or indirectly done through them should not be an object of great attention by super-powers, considering their strategic importance in all fields. In this indispensable general frame one is however brought to consider more specific legal aspects not only because the starting point is a decision by the EU’s highest court, but also because it has to be compared with other decisions by other courts across the Atlantic\(^7\). Here the notion of

\(^5\) See the “Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program” in the OJEU L8 of January 13, 2010.

\(^6\) See the “Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security” in the OJEU L215 of August 11, 2012. But see now the sweeping Directive 2016/681 “on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime” which clearly reflects a change in policy after the Paris and Brussels terrorist attacks.

\(^7\) See e.g. In re Microsoft, 15 F. Supp. 3\(^{rd}\) 466 (S.D.N.Y 2014) holding that data held by Microsoft in Ireland was under US jurisdiction and therefore subject to a US warrant issued under the Electronic Communications Privacy Act (as amended by the Patriot Act).
sovereignty is translated in the elegant and technical term of jurisdiction: but establishing that a Court has jurisdiction – and generally this is done by the courts themselves – is in itself the expression of sovereign powers. The power to set rules is coupled with the power to establish how, when, and to what extent those rules may or must be applied. In this sense even in the hypothetical case in which the CJEU were to have established that the “Safe Harbour” agreement was perfectly in line with EU law, the decision would have been nonetheless an expression of sovereignty. And one should add that – even more in the case of the electronic communications – it is not sufficient to assert sovereignty: this must be recognized by other States.

The Schrems decision is useful, in this respect, to discard a certain idea of activities on the telecom networks, and through the most known of the technical procedures, the Internet, as being a-territorial and therefore not subject to State sovereignty. This idea which dates back to the first age of the Internet and its spontaneous development has been amply superseded by the progressive expansion of State intervention and regulation of networks and of activities which are conducted on them.

3. Sovereignty over the material segments of a network

Networks are in a great measure composed of physical elements (cables, switching boxes, and computers) which must be located somewhere within the territory of the State. Even when the network uses significant segments of wireless communications, these must be transmitted and must be received by physical antennas and radio-bases. On these elements the State can quite lawfully exert its powers preventing them to operate or imposing that they should operate according to certain technical or

---

8 The idea is challenged by W. HEINTSCHEL VON HEINEGG, Legal Implications of Territorial Sovereignty in Cyberspace, in C.CZOSSECK, R. OTTIS, K. ZIOLKOWSKY (eds), 4th International Conference on Cyber Conflict, 2012 NATO CCD COE Publications, at p.9 [available on-line at https://ccdcoe.org/sites/default/files/multimedia/pdf/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf].

9 However it had been criticized nearly 20 years ago: see T.S. WU, Cyberspace Sovereignty? The Internet and the International System, 10 Harv. J. L&Tech. 647 (1997)
administrative instructions. The fact that the content of communications is intangible does not mean that the State cannot, again both de facto and de jure, prevent circulation of certain contents, access to foreign sites, or access from abroad, and in general may legitimately – and regularly do so also in democratic countries – control and apprehend the content of digital communications. All these interventions are clear evidence that States – or in the case of supranational entities, such as the EU, delegated by its Members – exercise day by day their sovereign powers on telecommunication networks, from minute aspects to much more complex and in-depth interventions.

Establishing how personal data which are collected through networks should be processed, and if and at what conditions they may be transferred to other countries is very simply the expression of the functioning of sovereign powers according to a rule-of-law system. The law, whether in the form of a general provision or in the form of a Court order – establishes what can legally be done. If the party or the parties do not abide there will be sanctions of progressive intensity up to the closing down of certain activities and the arrest of the natural persons engaged in them.

It would be naïf to assume that this expression of sovereign powers is a specific feature of the EU political and legal system. In the USA governance of global networks has been significantly out-sourced to private actors who are operating within the US legal system. The first and most obvious example is that of ICANN, the body entrusted with the role of setting naming procedures and other aspects of operations over the

---

10 Clearly in this sense W. HEINTSCHEL VON HEINEGG, Legal Implications etc., fn.9, at p.9f. “The fact that the components of the internet are located on a State’s sovereign territory but form, at the same time, part of the global internet, does not indicate a waiver of the exercise of such territorial jurisdiction” (K. ZIOLKOWSKI, General Principles of International Law as Applicable in Cyberspace, in K. ZIOLKOWSI (ed), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013, 135. at p.162) [available online at https://ccdcoe.org/publications/books/Peacetime-Regime.pdf ]

11 The concern over a growing Data Nationalism is expressed by A.CHANDER, U.P.LE, 64 Emory L.J 677 (2015)
But also when most great on-line service providers (such as Google, Facebook, E-bay, Wikipedia, etc.) in their general terms of service state that the applicable law is US law, often indicating also a domestic jurisdiction, they are ultimately stating that US law – and therefore US sovereign power – governs the global network. This conflict – in first place a conflict of systems and therefore a conflict of laws – does not appear to be resolvable through well-known and experimented rules of international private and procedural law. The problem is not what national private law should apply to the legal relationship and which is the competent judge. In these cases what is at stake is public regulation of networks, which cannot be solved by rules applicable to private actors.

Using the CJEU case as an example, its decision is not about Mr. Schrems’ personal data (hypothetically Facebook might have agreed to segregate his data and to process them in Europe) but about the personal data of all EU citizens. Clearly this is an issue which could not have been tackled effectively by private law litigation.

4. The “territory” of Internet

As mentioned before, the fact that personal data was chosen as the bone of contention with the US in no way means that the effects of the Schrems decision are limited to this aspect. One can easily image the extension of EU laws – id est EU sovereignty – to consumer e-commerce transactions between Europe and the US, the application of EU IP or competition laws.

---

12 The ICANN qualifies itself as a NGO but is governed by US law and acts on behalf of and reports to the US Department of Commerce: see K. ZIOLKOWSI, General Principles of International Law as Applicable in Cyberspace, fn.11, at p. 157.


14 See T. MAURER et al., Technological Sovereignty, fn 3
to big data held across the Atlantic but comprising significant “European” data, or the extent or limits of processing of public data outside the EU boundaries\textsuperscript{15}. And all this without considering the scorching issue of taxation of business activities which are done through electronic communications.

One of the obvious consequences of the CJEU decision is the need to define clearly the boundaries of EU sovereignty over telecommunication networks. In the first place where do they start/end?\textsuperscript{16} The answer is not obvious considering the overseas extensions of many European countries: Denmark with Greenland, the Netherlands with its possessions in the Caribbean, France with its D.O.M. and T.O.M., and the UK with its dozens of islands in every ocean of the world. One should also consider that most of the inhabitants of such faraway places hold a EU citizenship and therefore are entitled to the same rights as motherland citizens and are subject to the same laws. And citizens – and citizenship – are one of the essential elements of sovereignty\textsuperscript{17}.

This element needs to be carefully considered in a multiplicity of cases:

\textsuperscript{15} The approach by J. DASKAL, \textit{The Un-Territoriality of Data}, in \textit{125 Yale L.J} 326 (2015) is that data is not connected with any specific territory; and is disconnected from citizenship. At least in the EU this second statement does not appear to be applicable. Data protection is considered a fundamental right under article 8 of the European Charter of Fundamental Rights, and therefore surely is an entitlement which is strongly attached to citizenship. For the complex constitutional issues arising from the use of cloud computing in the field of data held by public bodies (and therefore object of sovereign ‘command and control’) and the interaction with EU law see F. CARDARELLI, \textit{Amministrazione digitale, trasparenza e principio di legalità}, in \textit{Diritto Informazione e Informatica} 2015, 227 (at p. 250f).

\textsuperscript{16} See P.W. FRANZESE, \textit{Sovereignty in Cyberspace: Can It Exist?}, \textit{64 Air Force L.Rev.} 1 (2009): “States must be able to establish a cyberspace border that a state can both monitor and control. Without the capability to perform this function, the concept of sovereignty in cyberspace is meaningless” (at p. 39)

\textsuperscript{17} It would appear that in the cases in which the data is processed (allegedly unlawfully) outside the EU, the EU would be applying the so-called passive personality principle (see B. PIRKER, \textit{Territorial Sovereignty and Integrity and the Challenges of Cyberspace}, in K. ZIOLKOWSI (ed), \textit{Peacetime Regime for State Activities in Cyberspace}. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013, 189 (at p. 196) [available on-line at \url{https://ccdcoe.org/publications/books/Peacetime-Regime.pdf}]. For an approach which relates jurisdiction to citizenship see C. RYNGAERT, M. ZOETEKOUW, \textit{The End of Territory? The Re-Emergence of Community as a Principle of Jurisdictional Order in the Internet Era}, available on-line at \url{http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523354}.
a) When a EU citizen accesses the network from Europe and reaches a website outside the EU.

b) When a non-EU citizen accesses, from Europe, a website outside the EU.

c) When a EU citizen accesses a European website from outside the EU.\(^{18}\)

Clearly the growing tension between the need for an open and authentically global network and the assertion of sovereign rights over one’s territory and one’s citizens requires more than simple good will\(^{19}\).

The first point that should be considered is what may be called an appropriate “frame of mind”. The dominant idea has been – as one has seen in the first part of this paper – that the Internet, being global, is essentially a-territorial and can live thanks to its self-determined rules. Behind this idea there seem to be several misunderstandings:

a) To put things rather bluntly, from the point of view of sovereignty the Internet simply does not exist. It is only a protocol used to transfer messages (packets of data) using open-to-the-public telecommunication networks. Clearly this protocol exists from an IP law and a regulatory perspective, but being entirely non-material it cannot be an object of sovereignty more than a broadcasting standard or a metric system. There is no sovereignty on the Internet Protocol as there is no sovereignty on those used by Skype or by WhatsApp.

b) This protocol today exists and is used, but tomorrow it could be replaced by some other technology, or, very simply, some States

\(^{18}\) This approach is different from that considered by W. HEINTSCHEL VON HEINEGG, *Legal Implications etc.*, fn.8 (at p. 15) where the case is that of jurisdiction against someone, from abroad, who has conducted harmful acts “against the cyber infrastructure in another State”. The issue that here is considered is, instead, if and when those operating on the Internet can profit from the protection of the laws of the State, and if entities placed outside its territory may be obliged to comply with another State’s rules.

\(^{19}\) The risk being that of a “Balkanization of the Internet into multiple, closed-off systems protected from the extraterritorial reach of foreign-based ISPs” (J. DASKAL, *The Un-Territoriality of Data*, fn.15, at p. 332). Similar concerns are expressed by A.CHANDER, U.P.LE, *Data Nationalism*, fn 11.
might decide to use telecommunication transmission standards incompatible with the Internet protocol\textsuperscript{20}.

c) The fact that the digital impulses that are transmitted are intangible and are sent thanks to a non-material entity (such as the Internet protocol) in no way means that the network itself is intangible. It is, instead, made of extremely tangible, physical objects mostly placed on the sovereign territory of the State. The only significant extra-territorial non-material situation is that of communications coming from an outer-space satellite which can be directly received by the user (\textit{e.g.} a mobile satellite telephone) without the need of a terrestrial infrastructure that distributes them\textsuperscript{21}.

d) States control the physical segments of telecommunication networks and they decide which standards they want to accept. Therefore they decide whether they want to admit, and to what extent, Internet on their networks. Internet has no territory (and therefore poses no sovereignty issues) because from a strictly technical point of view it cannot have one: it “owns” (in the sense of control-and-command) no cables, no satellites, no wave-lengths. These are controlled by States – or supranational entities which have been empowered by States – which therefore will regulate the Internet and any other digital technique used to communicate on the networks and will tend to do so increasingly\textsuperscript{22}.

5. The precedents of sea, air and space

\textsuperscript{20} This was quite common in the past: it is sufficient to think of the competing colour-TV standards in the ’70ies and ’80ies of last century (PAL, German, and SECAM, French).

\textsuperscript{21} see M. MEJIA-KAISER, Space Law and Unauthorised Cyber Activities, in K. ZIOLKOWSKI (ed), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013, 349. But – as far as the Internet is concerned – this is not the ordinary situation. The misunderstanding (“The fundamental mistake”) is clearly pointed out by I. WALDEN. International Telecommunications Law, the Internet and the Regulation of Cyberspace, in K. ZIOLKOWSKI (ed), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013, 261 (at p. 266) [available on line at https://ccdcoe.org/publications/books/Peacetime-Regime.pdf ].

\textsuperscript{22} see P.W. FRANZESE, Sovereignty in Cyberspace, fn.16 : “States have the capability to transform it [cyberspace] in a domain in which they can exert their sovereignty” (at p. 34)
One should instead consider that telecommunication networks are a modern version of extraordinary mediums of communications as have been since antiquity the sea and from the XX century the sky and outer-space23.

The fact that nobody physically “owns” the waves of the sea, the air through which planes fly or airwaves are transmitted, and outer-space is beyond the ordinary control of States, has not prevented the development of common rules which enable international cooperation in maritime, aviation, telecommunication or satellite activities24. Also in these cases one is faced with activities that originate from one country and are destined to other countries, often passing through or over other countries25 or in international spaces26.

23 “It seems logical to assimilate it to the high seas, international airspace and outer space” ; W. HEINTSCHEL VON HEINEGG, Legal Implications etc., fn 8, at p.9; see also P.W. FRANZESE, Sovereignty in Cyberspace, at fn.16 (at p. 40f). The similarity is used also to attempt to establish jurisdiction in private international law issues: see W.GUILLERMO JIMENEZ, A.R. LODDER, Analyzing Approaches to Internet Jurisdiction Based on Model of Harbors and the High Seas, in 29 Intl R.Law, Computers & Techn. 266 (2015).

24 W. HEINTSCHEL VON HEINEGG, Legal Implications etc, fn.8, qualifies cyberspace as a « global common » or a « res communis omnium » (at p.9). K. ZIOLKOWSI, General Principles of International Law as Applicable in Cyberspace, fn.10, at p.167, refers to “the internet as another globally shared resource, and to cyberspace as another common space”. One could express some doubts on such qualifications: it is debatable that underwater cables or telecommunication satellites can be considered such and one should distinguish clearly the element in which they operate (water, air, and outer-space), the physical infrastructure, and the activity that on the infrastructure is conducted. The same author goes further proposing, de lege ferenda, that the internet be considered “common heritage of humankind” (at p. 181). Against the “global commons” theory see P.W. FRANZESE, Sovereignty in Cyberspace, fn.16 (at pp. 14ff); B. PIRKER, Territorial Sovereignty and Integrity and the Challenges of Cyberspace, fn.17, at p. 194f who suggests that “a trusteeship could be a more suitable solution in the future” (ibidem).

25 This poses novel problems. It is well known that the path a communication through the Internet takes depends on a series of factors which are generally autonomous from the decision of the sender. Can one apply customary international rules on passage? Do States have a sovereign right to control (and eventually block or ‘seize’) communications that pass through their territory? W. HEINTSCHEL VON HEINEGG, Legal Implications etc.,fn.8, suggests that this might be restricted on the basis of “customary or conventional rules of international law” (at p. 11). For some possible technological solutions in order to avoid “passage” through certain countries see T. MAURER et al. , Technological Sovereignty, fn 3 (at p. 58f).

26 An obvious issue is that of submarine cables analyzed by W. HEINTSCHEL VON HEINEGG, Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law, in K. ZIOLKOWSI (ed), Peacetime Regime for State Activities in Cyberspace. International
The content of existing and/or future rules comprises a wide range of issues: from those concerning standards and technological compatibility to identification of the origin of messages or location of those providing services and content.

But the main controversy is – as is clear from the Schrems decision – about the content of what is transferred via the network and what activities may – or may not – and in which manner be conducted. A certain number of indications might be drawn from the so-called “Internet Bill of Rights”, but this covers an extremely limited part of a much wider picture. The governance of such a wide “space” such as global networks surely requires the enumeration of individual rights, but also of duties and obligations; of default rules; of remedies; of ways to solve disputes.

In this respect, in an international perspective, we are still very far away from an even embryonal setting. The Schrems decision outlines the existence of an international dispute (who controls the network, and sets the rules that govern activity conducted over it) which can be settled only through the typical instruments of international law.

---


29 Several others are pointed out by T. MAURER et al., Technological Sovereignty, fn 3 (at p. 63). And there is an on-going controversy between Russia and NATO on the law (if any) applicable to cyber-wars: see A. KRUTSKIKH, A. STRELTSOV, International Law and the Problem of International Information Security, in International Affairs n.6, 2014, 64 [available on line at https://ccdcoe.org/sites/default/files/multimedia/pdf/International_Affairs_No6_2014_International_Law.pdf]: “Some NATO experts develop approaches to regulate
6. International fora for digital governance

To stopgap the vacuum created by the Schrems decision which invalidated the so-called Safe Harbour decision the EU Commission issued in February 2016 a Communication on “Transatlantic Data Flows: Restoring Trust through Strong Safeguards” commonly known as “Privacy Shield”\textsuperscript{31}. The Communication refers to a more general “Umbrella Agreement” between the EU and the USA. Clearly this appears to be a temporary solution and invokes a broader international setting.

It would appear that the natural forum in which to discuss and set common rules is the International Telecommunication Union (ITU) owing to its experience over a century and a half (it was founded in 1865) and the direct connection with the topics of transnational communications\textsuperscript{32}, and to the fact that it expressly allows private actors (such as industry) to play a role in rule-making, a feature which is particularly important considering that most of the actors engaged in shaping the Internet protocols are private\textsuperscript{33}.

ITU has produced a certain amount of decisions and agreements concerning the Internet, but exclusively on technical issues\textsuperscript{34}. One should

\textsuperscript{30} see P.W. FRANZESE, Sovereignty in Cyberspace, fn 16, at p. 32. In the same direction J. DASKAL, The Un-Territoriality of Data, fn. 15

\textsuperscript{31} COM(2016) 117 final issued on 29.2.2016

\textsuperscript{32} In this direction see I. WALDEN. International Telecommunications Law, the Internet and the Regulation of Cyberspace, fn. 21, at p. 271.

\textsuperscript{33} I. WALDEN, International Telecommunications Law, the Internet and the Regulation of Cyberspace, fn. 21, at p. 264, points out the complexity of distinguishing between technical regulation of an infrastructure, and content regulation of a service. The role of
however add that the ITU basic instruments do not contain significant provisions and procedures concerning dispute resolution, which on the one hand significantly reduces the binding force of its resolutions, but at the same time enables its members to find alternative systems to settle disputes and enforce decisions35.

This brings us back to the EU-US dialogue. The occasion for a move towards a stable and mutually satisfactory solution might be the pending Trans-Atlantic Trade and Investment Partnership (TTIP) negotiations between the EU and the USA36. Some political commentators have even suggested that the Schrems decision is a way to strengthen the European position when discussing issues concerning the development of trans-Atlantic electronic services, which is, understandably, one of the main concerns of the US administration which clearly backs its industries in this field (Google, Apple, Facebook, Amazon etc.)37.


35 I. WALDEN. International Telecommunications Law, the Internet and the Regulation of Cyberspace, fn. 21, at p. 276 : (“No enforcement mechanism is available in the event of non-compliance”). It is doubtful if the alternative is recourse to the International Court of Justice as suggested by K. ZIOLKOWSI, General Principles of International Law as Applicable in Cyberspace, fn.10, at p. 175. One should however consider that in the case of submarine cables, governed by the 1884 Paris Convention for the Protection of Submarine Telegraph Cables , subsequently extended to telephonic communications by the 1958 Geneva Convention on the High Seas, disputes could be settled on the basis of the procedures set out by the 1982 UN Convention on the Law of the Sea (see W. HEINTSCHEL VON HEINEGG, Protecting Critical Submarine Cyber Infrastructure, fn. 26, at p. 308f.)

36 For obvious reasons the position of the US Trade Representative in the T-TIP negotiations is much clearer on the Internet (see https://ustr.gov/trade-agreements/free-trade-agreements/transatlantic-trade-and-investment-partnership-t-tip/t-tip-15 ). The EU position focuses more on the aspects were it can negotiate at arm’s length, such as e-commerce (see http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_153009.pdf)

37 As the TTIP negotiation is clearly within the general framework of the WTO a series of elements that have already been outlined in that context could be aptly transposed. See I.
7. A holistic perspective on “digital sovereignty”

The Internet protocol is here to stay\(^\text{38}\). It will develop technologically, economically, socially; it will evolve in something different, with a different name. But focusing exclusively on the Internet entails the risks of looking at the problem from a distorted perspective. Sovereignty issues may, hopefully, find a solution looking at the whole picture. And a piecemeal approach is not very promising: data protection is intimately connected to cyber-security; consumer protection with international trade; banking transactions with financial stability; technical standards with investments and returns; law enforcement requires beyond-the-border cyber-investigations\(^\text{39}\).

The obvious first issue is that of the forum where serious negotiations can be started; and the second is the procedures to adopt in decision-making\(^\text{40}\).

---

\(^{38}\) Clearly one cannot speculate here on its developments and its, existing, alternatives, such as the so-called TOR protocol (see E.ÇALIŞKAN, T. MINÁRIK, A-M OSULA. Technical and Legal Overview of the Tor Anonymity Network, CCD COE, Tallinn 2015, available on-line at https://cryptome.org/2015/07/TOR_Anonymity_Network.pdf). At any rate the TOR is the demonstration that the Internet protocol is only one of the many ways to access and use a telecommunication network.


Subsequently one can imagine discussing the various topics, which are all highly sensitive from a political point of view, inasmuch most of them involve the rights of individuals who constantly use the wealth of knowledge and of opportunities offered by the Internet. From a substantive point of view one should note that a great deal of common rules can be extracted from the 2014 OECD “Principles for Internet Policy-Making” which lay out responses for many of the principal issues which interest developed countries and which require international cooperation.

One should however avoid the danger that the debate on these topics be lead and governed by very vocal minorities who have elected the Internet as their no-man’s land that should not fall under the domain of the law.

Not only is it impossible to escape the millenary wisdom of *ubi societas, ibi ius* (and telecommunication networks are a part, a significant part, of


43 The obvious reference is to the so-called “Anonymous” movement which operates online often engaging in disruptive cyber-attacks on those it declares are its enemies.
contemporary societies), but most importantly creating new taboos (the Internet should not be touched by the law) favours the opposite phenomenon: the use, by States, of hidden, covert, if not unlawful practices.\footnote{Several commentators point out that States may have an interest in denying the existence of international law rules that apply to the Internet: “There is growing evidence that States are behaving as if there are few, if any, restraints in the conduct of cyberspace activities” (P.A. WALKER, Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace, in M. MAYBAUM, A-M. OSULA, L. LINDSTROM (Eds.), 7th International Conference on Cyber Conflict, 2015 NATO CCD COE Publications (at pp.97 and 104) (available on-line at \url{https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%20Technological%20Sovereignty%20Missing%20the%20Point.pdf}). Similarly P.W. FRANZESE, Sovereignty in Cyberspace, fn.16 (at pp. 34ff).}