DOI 10.5817/MUJLT2018-1-2

"LAGOM JURISDICTION" – WHAT VIKING DRINKING ETIQUETTE CAN TEACH US ABOUT INTERNET JURISDICTION AND GOOGLE FRANCE[*]

by

DAN JERKER B. SVANTESSON[**]

The law of Internet jurisdiction is facing a crisis. While there is widespread and growing recognition that we cannot anchor Internet jurisdiction in the outdated, typically overstated, and often misunderstood, territoriality principle, few realistic alternatives have been advanced so far.

This article seeks to provide an insight into the conceptual mess that is the international law on jurisdiction; focusing specifically on the concepts of sovereignty and jurisdiction, with limited attention also given to the impact of comity, and international human rights law. These issues are studied through the lens of the so-called Google France case that comes before the CJEU in 2018. The article argues that we may usefully turn to the Swedish "lagom" concept – which allegedly stems from Viking era drinking etiquette – as a guiding principle for how we approach Internet jurisdiction.

KEY WORDS

Lagom, Comity, Google France, Internet Jurisdiction, Sovereignty, Vikings

---

[*] This article draws, and expands, on research findings discussed in: Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press; Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing; and Svantesson, D. (2017) *Time for international law to take the Internet seriously.* [online] OUPblog. Available from: https://blog.oup.com/2017/10/international-law-internet/ [Accessed 7 October 2017].
I thank the two anonymous reviewers for their valuable feedback.

[**] dasvante@bond.edu.au, Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia).

1. INTRODUCTION

At the time of writing, the Court of Justice of the European Union (CJEU) is about to determine a matter regarding jurisdiction and sovereignty that goes to the very core of the Internet; the consequences of which may indeed seriously impact the future of the Internet.

The matter in question arose out of the famous (or notorious) Google Spain – right to be forgotten – case decided by the CJEU in May 2014. As is well-known, in that decision the Court recognised, or rather articulated some would say, a right variously referred to as the "right to be forgotten", the "right to delisting", and the "right to de-referencing". However, the CJEU was never asked to deal with the scope of jurisdiction question; that is, in this case the geographical scope of reach of any order requiring "delisting". As I have discussed elsewhere, Google saw the order aslimited to the EU, while the Article 29 Working Party and some of the European Data Protection Authorities (DPAs) saw the order as requiring a broader implementation of any delisting order.[1] Consequently, there now is considerable controversy about how widely – geographically speaking – search engines need to delist search results based on the so-called "right to be forgotten".

In a media release of 12 June 2015, the French data protection authority – the Commission Nationale de Informatique et Libertés (CNIL) – stated, amongst other things, that:

> *"CNIL considers that in order to be effective, delisting must be carried out on all extensions of the search engine and that the service provided by Google search constitutes a single processing. In this context, the President of the CNIL has put Google on notice to proceed, within a period of fifteen (15) days, to the requested delisting on the whole data processing and thus on all extensions of the search engine."*[2]

This dispute – commonly referred to as the Google France case – has now reached the CJEU with the following questions having been referred

---

[1] See e.g. Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press; Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[2] CNIL. (2015) *CNIL orders Google to apply delisting on all domain names of the search engine* 12 June. [online] Available from: http://www.cnil.fr/english/news-and-events/news/article/cni-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine [Accessed 2 April 2017].

to it by the Conseil d'État of France:

> *"1. Must the "right to de-referencing", as established by the Court of Justice of the European Union in its judgment of 13 May 2014 on the basis of the provisions of Articles 12 (b) and 14 (a) of Directive [95/46/EC] of 24 October 1995, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de--referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46/EC] of 24 October 1995?*
>
> *2. In the event that Question 1 is answered in the negative, must the "right to de-referencing", as established by the Court of Justice of the European Union in the judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester's name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States of the European Union?*
>
> *3. Moreover, in addition to the obligation mentioned in Question 2, must the "right to de-referencing", as established by the Court of Justice of the European Union in its judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the "geo-blocking" technique, from searches conducted on the basis of the requester's name from an IP address deemed to be located in the State of residence of the person benefiting from the "right to de-referencing", or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive [95/46/EC] of 24 October 1995, regardless of the domain name used by the internet user conducting the search?"*[3]

[3] Google Inc. v. Commission nationale de l'informatique et des libertés (2017), C-507/17.

Thus, a bit simplified the CJEU has been asked to rule on the following: Must a search engine operator deploy the de-referencing to all of the domain names used by its search engine?

If not, must a search engine operator only remove the links on the domain name corresponding to the State in which the request is deemed to have been made or on the national extensions used by that search engine for all of the Member States of the European Union?

Must a search engine operator use "geo-blocking"? If so, only from an IP address deemed to be located in the State of residence of the person benefiting from the "right to de-referencing", or even, more generally, from an IP address deemed to be located in one of the Member States?

The binary nature of the questions advanced by the Conseil d'État is both crude and inadequate, and I would rather be inclined to a different moulding of the relevant issues. In my view, we can get out of the quagmire and regain firm ground only if we realise that this is not an area that lends itself to such simplistic binary questions.[4] Rather, what we are dealing with – the appropriate protection of personality rights – will always be a matter of degree.

At any rate, as cannot be disputed, the dilemma facing the CJEU goes beyond pure EU law since the EU – unsurprisingly – is subject to international law. Indeed, the fact that e.g. EU law *"is bound to observe international law in its entirety, including customary international law, which is binding upon the institutions of the European Union"*[5] is not in dispute.

Thus, evaluating the Google France matter requires us to consider what international law actually tells us about jurisdiction. And evaluating that question necessitates us considering a range of core concepts in international law – most prominently – the concepts of sovereignty and jurisdiction. However, we need also briefly pay some attention to comity and some relevant aspects of international human rights law. The article then considers whether the way international law deals with Internet jurisdiction could be informed by a perhaps somewhat unorthodox source of wisdom – Viking era drinking etiquette.

However, before discussing how international law deals with

[4] I provide a detailed discussion of how to approach scope of (remedial) jurisdiction in Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press, pp. 171–190.

[5] Judgement of 21 December 2011, The Air Transport Association of America and Others, C-366/10, EU:C:2011:864 , paragraph 101.

jurisdiction for a case such as this, it is relevant to first make a few observations as to how international law approaches the Internet and the legal issues to which the Internet gives rise.

2. INTERNATIONAL LAW AND THE INTERNET

Unfortunately, Internet-related legal issues are still treated as fringe issues in both public, and private, international law. Anyone doubting this claim need only take a look at the tables of content of textbooks and journals in those respective fields. However, approaching Internet-related legal issues in this manner is becoming increasingly untenable. Let us consider the following:

Tech companies feature prominently on lists ranking the world's most powerful companies. For example, on *Foreign Policy's list of "25 Companies Are More Powerful Than Many Countries"*[6] ten of the listed companies are from the tech industry, and perhaps somewhat less importantly, six of the top 10 companies on *Forbes' list of the world's most valuable brands are tech companies* (with the four top spots being Apple, Google, Microsoft and Facebook).[7]

With its more than two billion users[8], Facebook alone has more "citizens" than any country on earth; and no other communications media comes even close to the Internet's ability to facilitate cross-border interactions – interactions that often have legal implications.

While statistics arguably may be used to prove just about anything, the message stemming from the above is clear and beyond intelligent dispute – cross-border Internet-related legal issues are central matters in society and need to be treated as such also in public, and private, international law.

A particularly relevant matter is that of Internet jurisdiction. The harms caused by the current dysfunctional approach that international law takes to jurisdiction are as palpable as they are diverse. The territoriality-centric approach to jurisdiction causes severe obstacles for law enforcement's fight

---

[6] Khanna, P. (2016) *These 25 Companies Are More Powerful Than Many Countries*. [online] Foreign Policy. Available from: http://foreignpolicy.com/2016/03/15/these-25-companies-are-more-powerful-than-many-countries-multinational-corporate-wealth-power/

[7] Forbes. *The World's Most Valuable Brands.* [online] Forbes.com. Available from: https://www.forbes.com/powerful-brands/list/#

[8] Constine, J. (2017) *Facebook now has 2 billion monthly users… and responsibility.* [online] Techscrunch.com. Available from: https://techcrunch.com/2017/06/27/facebook-2-billion-users/ [Accessed 27 June 2017].

against both traditional – and cyber – crime, it undermines the protection of important human rights, it amounts to an obstacle for e-commerce and it creates uncertainties that undermine the stability online with an increased risk for cyber conflict as the result. Thus, Internet jurisdiction is one of our most important and urgent legal challenges. And we all need to get involved.

3. INTERNATIONAL LAW, SOVEREIGNTY AND JURISDICTION

Having attended a range of workshops and other meetings relating to the way we should approach Internet-related legal matters, it seems to me that the label "international law" sometimes is used as a lawyers' version of the well-known children's game "Simon says". In that game, all proposed actions are to be ignored unless prefaced with the phrase "Simon says", in which case the instructions must immediately be complied with.

At workshops and other meetings, I have too often seen the phrase "international law says" play a very similar role. Too often, proposed actions are ignored – regardless of their intrinsic value, merit or sensibility – while at the same time, any instructions prefaced with the phrase "international law says" are treated as almost holy – regardless of their lack of intrinsic value, lack of merit and lack of sensibility. The problems caused by this are augmented by the lack of scrutiny directed at whether international law also "says" other things that in fact contradict and clash with the first statement as to what "international law says".

I think there are at least two, related, reasons for this. First, international law – and even more so commentaries on international law – are replete with absolutist statements that are better suited for the political arena than they are for law; statements that then can be (ab)used in the pursuit of particular positions in legal discussions. Consider, for example, the following statement made by the Permanent Court of Arbitration in *the Island of Palmas case*:

> *"[t]erritorial sovereignty, as has already been said, involves the exclusive right to display the activities of a State."*[9]

Such a statement is clearly overly broad and open to abuse. To see that

[9] Island of Palmas (Neth. v. U. S.), 2 R. I. A. A 829, 838 (Perm. Ct. Arb. 1928).

this is so, we need only consider that it is incompatible with the nationality principle and the effects doctrine.

Second, international law is complex and inaccessible to the degree that many non-experts are forced to uncritically accept the preaching of those who claim to "know" what international law "says". This means that claims as to what international law "says" too rarely are disputed. Put simply, those who speak with conviction about what international law instructs us to do are too rarely challenged.

In this section, I want to briefly discuss *the concept of sovereignty* – a key concepts for the Google France matter, and for international law generally and a concept that I argue is much less settled than is commonly thought. I also briefly discuss *the concept of jurisdiction* and how the two concepts relate to each other.

3.1 SOVEREIGNTY – A (MISUSED) KEY CONCEPT

Perhaps the most fundamental concept in international law is the concept of sovereignty. And while various aspects of the sovereignty concept have been debated more or less constantly, reading the international law textbooks provides the sensation that sovereignty has a well-established meaning. For example, as Endicott puts it:

> *"Sovereignty, it seems, is: absolute power within a community, and absolute independence externally, and full power as a legal person in international law."*[10]

Turning to primary sources, the conventional starting point for discussions of sovereignty is found in *the Island of Palmas* case which teaches that:

> *"Sovereignty […] signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."*[11]

Put simply, conventional thinking treats the concept of sovereignty as a right to independence and exclusiveness.

Yet this conventional wisdom has come under fire recently, and the true

[10] Endicott, T. (2010) The Logic of Freedom and Power. In: Besson, S. and Tasioulas, J. (eds.) *The Philosophy of International Law*. Oxford: Oxford University Press, pp. 245–259.

[11] Island of Palmas (Neth. v. U. S.), 2 R. I. A. A 829, 838 (Perm. Ct. Arb. 1928).

nature of the concept of sovereignty is in fact far less settled than we often are led to believe. Important aspects of the current debate are showcased with great clarity in an excellent *Symposium on Sovereignty, Cyberspace, and the Tallinn Manual 2.0* published in 2017 in the American Journal of International Law Unbound.[12]

In their contribution, *Gary P. Corn* (a Staff Judge Advocate, United States Cyber Command) and *Robert Taylor* (a Former Principal Deputy General Counsel, U. S. Department of Defense) argue that:

> *„Some argue that […] sovereignty is itself a binding rule of international law that precludes virtually any action by one state in the territory of another that violates the domestic law of that other state, absent consent. However, law and state practice instead indicate that sovereignty serves as a principle of international law that guides state interactions, but is not itself a binding rule that dictates results under international law. While this principle of sovereignty, including territorial sovereignty, should factor into the conduct of every cyber operation, it does not establish an absolute bar against individual or collective state cyber operations that affect cyberinfrastructure within another state, provided that the effects do not rise to the level of an unlawful use of force or an unlawful intervention."*[13]

While stated in the context of state cyber operations, these observations have much broader impact, and indeed, much broader appeal. In essence, *Corn and Taylor* argue that: (a) sovereignty is an underlying principle that cannot be violated *per se*, (b) but that sovereignty, as expressed in the relatively clear proscriptions against unlawful use of force and unlawful interventions, can be violated, and that (c) everything else is a grey-zone in relation to which the underlying principle of sovereignty tells us little or nothing.[14]

---

[12] Ginsburg, T. (2017). Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0. *AJIL Unbound*, 111, pp. 205–206. Available from: doi: 10.1017/aju.2017.58

[13] Corn, G. and Taylor, R. (2017) Sovereignty in the Age of Cyber. *AJIL Unbound*, 111, pp. 207–212. Available from: doi: 10.1017/aju.2017.57

[14] Corn and Taylor state:*"Through both custom and treaty, international law establishes clear proscriptions against unlawful uses of force and prohibits certain interventions among states. And while questions remain as to the specific scope and scale of cyber-generated effects that would violate these binding norms, the rules provide a reasonably clear framework for assessing the legality of state activities in cyberspace above these thresholds, including available response options for states. Below these thresholds, there is insufficient evidence of either state practice or opinio juris to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states "actions in cyberspace"."* Corn, G. and Taylor, R. (2017) Sovereignty in the Age of Cyber. *AJIL Unbound*, 111, pp. 207–208. Available from: doi: 10.1017/aju.2017.57

I agree with *Corn and Taylor* that sovereignty is an underlying principle that cannot be violated *per se*. As I have argued together with *Polcak* in a discussion about dignity and sovereignty:

> *„The problem is that both of these concepts [sovereignty and privacy] too often are treated as rights on their own while they both actually consist of subsets of rights. For example, […] sovereignty is protected by tools such as jurisdictional exclusiveness over the state's territory and the duty of non--interference placed on other states."*[15]

However, in the sharpest contrast imaginable, *Schmitt and Vihul* point to international law cases where the activities in dispute where held to *"only constituted violations of sovereignty, not unlawful interventions or uses of force"*[16] and suggests that, in the light of such cases

> *"no conclusion can be drawn other than that the principle of sovereignty operates as a primary rule of international law."*[17]

This is, unsurprisingly, in line with how the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* approaches sovereignty.[18] *Schmitt and Vihul* also noted, in relation to their work on he Tallinn Manual 2.0:

> *"In Tallinn Manual 2.0, we, together with the seventeen other members of the so-called "International Group of Experts", found that violations of sovereignty could be based on two different grounds: "(1) the degree of infringement upon the target state's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions.""*[19]

While it may seem counterintuitive at a first glance, I suspect that the end result here is that *Schmitt and Vihul* give sovereignty a more limited scope of operation than do *Corn and Taylor*. After all, according to S*chmitt*

---

[15] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing, p. 63.

[16] Schmitt, M. gen. ed. (2017) *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. New York: Cambridge University Press.

[17] Ibid. At 215.

[18] Rule 4 states: *"A State must not conduct cyber operations that violate the sovereignty of another State"*.

[19] Schmitt, M. and Vihul, L. (2017). Sovereignty in Cyberspace: Lex Lata Vel Non? *AJIL Unbound*, 111, pp. 213–218. Available from: doi: 10.1017/aju.2017.55., p. 215.

and Vihul – assuming they are indeed endorsing the Tallinn Manual 2.0 definition just alluded to – violations of sovereignty must stem from one of the two different grounds they put forward, grounds that correspond with the conventional view of sovereignty. In contrast, while *Corn and Taylor* do not recognise sovereignty as a right that can be violated *per se*, they do see it as the foundation for two distinct rights – protection against the unlawful uses of force and unlawful interventions – that can be violated, as well as the foundation for a grey area.

Be that as it may, the fact that experts on this level take so fundamentally different positions on such a centrally important matter is no doubt telling in itself – also the very core concepts of international law remain in contention. And in the end, I suggest that the reality is that both *Schmitt/Vihul* and *Corn/Taylor* are wrong in part and right in part, although admittedly I am closer to side with *Corn and Taylo*r.

On my reading of the *lex lata*, sovereignty is not a right capable of being violated *per se*, rather it is as *Corn and Taylor* note the foundation for the relatively clear proscriptions against unlawful use of force and unlawful interventions. In addition, the principle of sovereignty is the foundation for a selection of other recognised international wrongs to which S*chmitt and Vihul*, as well as *Spector*, direct our attention.[20]

In other words, at this stage only two principles have sprung from the principle of sovereignty; that is proscriptions against use of force and unlawful intervention. And in addition to those rules there are pockets of clarity in what otherwise is a grey-zone. Those pockets are represented by the cases *Schmitt, Vihul* and *Spector* mention but they do not currently form comprehensive and defined rules and they certainly do not transform the principle of sovereignty into a norm of international law capable of being violated as such.

There is one more point made by *Corn and Taylor*, to which I want to draw attention:

> *„The fact that states have developed vastly different regimes to govern the air, space, and maritime domains underscores the fallacy of a universal rule of sovereignty with a clear application to the domain of cyberspace.*

[20] Schmitt, M. and Vihul, L. (2017). Sovereignty in Cyberspace: Lex Lata Vel Non? *AJIL Unbound*, 111, pp. 213–218. Available from: doi: 10.1017/aju.2017.55.; and Spector, P. (2017). In Defense of Sovereignty, in the Wake of Tallinn 2.0. *AJIL Unbound*, 111, pp. 219–223. Available from: doi: 10.1017/aju.2017.56

The principle of sovereignty is universal, but its application to the unique particularities of the cyberspace domain remains for states to determine through state practice and/or the development of treaty rules."[21]

This is a very important observation. Not only does it provide support for the idea that sovereignty is an underlying principle rather than a right *per se*, it also highlights that whatever way in which sovereignty is dealt with in other areas, there is scope for applying it differently in the online environment. After all, if sovereignty takes the shape of *lex specialis* in other fields, it can do so in the relation to the Internet arena as well, should we conclude that that is the better option.

Before moving on to consider the concept of jurisdiction, it is interesting to pause to consider what the above means for the Google France matter. In doing so, two things stand out.

First, orders requiring global de-listing, or indeed any form of de-listing going beyond the European Union, are difficult to reconcile with the traditional understanding of sovereignty. Put simply, deciding what content is accessible, for example in New Zealand, is an exercise of a State function for New Zealand. Thus, where the EU determines what is delisted for Internet users in New Zealand, it is arguably interfering with New Zealand's sovereignty.

Second, on the more sophisticated reading of the concept of sovereignty envisaged above – that of sovereignty as a principle of international law – we need to assess how cross-border de-listing orders fit in what currently is a grey-zone. In other words, under the more sophisticated reading of the concept of sovereignty, the CJEU has considerable scope to use its creativity to contribute to a fruitful and balanced development of the international law on sovereignty.

3.2 JURISDICTION – A (MISUNDERSTOOD) KEY CONCEPT

There are many notions regarding jurisdiction in general, and Internet jurisdiction in particular, that are widely relied upon in the academic community and beyond. The two key sources for those notions are the (in)famous *Lotus case* (1927)[22], and the widely cited, but poorly understood, *Harvard Draft Convention on Jurisdiction with Respect to Crime*

[21] Corn, G. and Taylor, R. (2017) Sovereignty in the Age of Cyber. *AJIL Unbound*, 111, pp. 207–212. Available from: doi: 10.1017/aju.2017.57

[22] S.S. "Lotus" (France v. Turkey) (1927) PCIJ Series A, No. 10.

(1935)[23] – both seen to put the supremacy of the territoriality principle beyond question. With a sleep-walking like acceptance, these authorities are treated as clear, exhaustive and almighty.

However, those who have truly studied jurisdiction in detail generally take a different view. For example, *Ryngaert*[24] and *Mann*[25] have both questioned whether the *Lotus* decision remains good law. And as I have sought to show elsewhere, pretty much every aspect of how we classify jurisdictional claims – including the distinction between jurisdiction under public international law and jurisdiction under private international law, as well as the distinction between territorial and extraterritorial jurisdiction – is less settled than it often is portrayed as being and may usefully be called into question.[26]

At any rate, if we adopt the conventional classification of jurisdiction; legislative, adjudicative and enforcement, what we are dealing with in Google France must clearly fall within so-called *enforcement jurisdiction*. But what does that mean in practical terms? To gain an insight into some form of mainstream view of the applicable international law, we can usefully draw upon the conclusions reached by-the group of eminent experts who, in 2017, produced the Tallinn Manual 2.0. As noted in the Tallinn Manual 2.0:

> *"States generally do not possess enforcement authority outside their territory. Rather, such jurisdiction is an exclusive attribute of sovereignty and, as such, may only be exercised extraterritorially with the consent of the State in which the jurisdiction is to be exercised or pursuant to a specific allocation of authority under international law."*[27]

The implications of this for the Google France matter seem undisputable. In the absence of a specific ground to point to that takes the de-listing orders outside the scope of this general rule, a de-listing order going beyond the European Union, is difficult to reconcile with the traditional

[23] Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime (1935) A*merican Journal of International Law,* 29 Supp 443.

[24] Ryngaert, C. (2015) *Jurisdiction in International Law*. 2nd edition. Oxford: Oxford University Press, p. 34.

[25] Mann, F. (1996) The doctrine of Jurisdiction in International Law. In: Karl M Meesen (ed.), *Extraterritorial Jurisdiction in Theory and Practice*. Kluwer Law International, p. 66.

[26] See further: Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press, in particular pp. 159–170.

[27] Schmitt, M. gen. ed. (2017) *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. New York: Cambridge University Press, pp. 52–53.

understanding of the limits international law imposes on enforcement jurisdiction.

3.3 THE RELATIONSHIP BETWEEN SOVEREIGNTY AND JURISDICTION

Convention may have us believe that the scope of jurisdiction is determined by the reach of sovereignty. However, few steps can be taken in such a direction without getting tangled in conflicting wisdoms. To bring forward just one illustration; if the scope of jurisdiction is determined by the reach of sovereignty, and sovereignty is delineated by reference to territorial borders, how do we explain recognised forms of extraterritorial jurisdiction, such as jurisdictional claims based on the nationality of an offending party?

More generally, as noted by *Khan*:

> *„[I]n recent years there are increasing signs that the traditional and rather categorical symbiosis between territory and power may no longer lay a legitimate claim for exclusivity. This is hardly deplorable since from an international law perspective, possession and transfer of territory have never been considered an end in itself. L'obsession du territoire of modern States was always meant to serve people, not vice versa."*[28]

All this illustrates that, while there are obvious indirect links between jurisdiction and sovereignty, there is no necessary direct link between these concepts as such. In response to this, some will hasten to drag forward the old argument that jurisdiction ultimately depends on enforcement. However, I seriously question whether people who do so have really thought through the implications of what they then are saying. Surely, we need to distinguish between law, on the one hand, and brute power, on the other hand, even if doing so means that we have to accept (a) that law can be of value even if it cannot be enforced, and (b) that not all enforcement actions are legitimate?

The observations made here as to the relationship between jurisdiction and sovereignty may not have any direct impact on the Google France matter. Nevertheless, they do draw attention to the complexity

[28] See, eg. Khan, D. E. (2012) Territory and Boundaries. In: Bardo Fassbender and Anne Peters (eds.), *The Oxford Handbook of the History of International Law*. Oxford: Oxford University Press, p. 248 (footnote omitted).

of the relevant aspects of international law that must be taken into account by the CJEU.

4. COMITY

To the issues raised above, we may add that both the notion of international comity, and international human rights law can be seen to speak against the crude and simplistic global delisting sought by the CNIL. As to the former, it must be admitted that neither the scope, nor the application, of comity is uncontroversial. In fact, the concept of comity does not lend itself to being easily pinned down. As a result, there are both divergent definitions and divergent views of the value of comity. Here it will have to suffice to note that arguably the most widely used definition would have us view comity in the following terms:

> *„Comity in the legal sense, is neither a matter of absolute obligation on the one hand nor of mere courtesy and good will upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, and to the rights of its own citizens or of other persons who are under the protection of its laws."*[29]

In light of statements such as this, there can be little doubt that the concept of comity may be seen to speak against de-listing order going beyond the European Union.

5. INTERNATIONAL HUMAN RIGHTS LAW

The fact that de-listing orders involve the balancing of different human rights is obvious and need not be elaborated upon. However, one thing that is important to remember is that, as the human rights of non-EU citizens would be affected by the type of orders sought by the CNIL, the CJEU must consider international human rights law; notably the *International Covenant on Civil and Political Rights* (ICCPR), not merely European human rights law. And as was emphasised in the Tallinn Manual 2.0:

> *"restrictions on the right to seek, receive, and impart information pursuant*

[29] Hilton v. Guyot (1895) 159 US 113 (1895), at 164. For a more elaborate discussion of the concept of comity, see, e.g. Briggs, A. (2012) The Hague Academy of International Law, Recueil des Cours, 354 , p. 94.

> *to Article 19 of the ICCPR must satisfy a tripartite test: they must be provided for by law under the clearest and most precise terms possible, foster a legitimate objective recognised by international law, and be necessary to achieve that objective."*[30]

All aspects of this tripartite test may pose a challenge for global delisting orders. Most obviously, it may be difficult to argue that providing the "right to be forgotten" in a situation such as that in Google Spain makes it necessary to delist search results in Fiji, in the Falkland Islands or even in Finland.

6. THE CONCEPT OF "LAGOM"

The above has pointed to the complex international law concepts the CJEU must tackle in adjudicating Google France. But let us now go back in time to the tables of the longhouses in Viking-era Scandinavia. There is a word said to be quite unique to the Swedish language. The word *lagom* means "just enough" or "just right". At least according to folklore, it stems from the phrase *laget om* ("around the team") from the Viking tradition of drinking enough when the drinking horn was passed around, without drinking so much that there is not enough for everyone.

Whether this is the proper origins of the word lagom or not, support for the lagom concept as a guiding principle in Viking drinking etiquette can be found in *Hávamál*. Hávamál is a combination of different poems, attributed to the Norse god Odin, presenting advice for living, proper conduct and wisdom.[31] In Verse 19 we can read Odin's instruction to:

> *"Keep not the mead cup but drink thy measure"*.[32]

I think the concept of lagom – with or without a "divine" origin – is apt indeed to describe how we must approach the issue of Internet jurisdiction. Most obviously, neither excess nor abstinence are acceptable paths forward; that is, emptying the drinking horn before everyone has had a chance to get their fair share would be an insult to their dignity, but a refusal to take part in the drinking would be equally insulting to the dignity of others.

---

[30] Schmitt, M. gen. ed. (2017) *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. New York: Cambridge University Press, p. 202.

[31] Hávamál (2018) [online] Wikipedia. Available from: https://en.wikipedia.org/wiki/

[32] Ashliman, D. L., Bray, O. (2003) *Hávamál* [online] Available: from: http://www.pitt.edu/~dash/havamal.html

Similarly, states should not make excessive jurisdictional claims, as doing so offends the dignity of other states, but equally well, they should not decline to exercise jurisdiction where doing so is called for, as also such inactivity may offend the dignity of other states.

Further, the lagom doctrine incorporates a context-specific proportionality. If the drinking horn is large, or the group of people sharing it small, each member can drink more than if the proportions are in the reverse. In the same manner, jurisdictional claims (and their scope) need to be adjusted to the context. However, the comparison goes further than that. In fact, it is possible to link numerous international law concepts to the lagom doctrine.

Consider the concept of "comity" that clearly can be seen in the requirement of not drinking excessively so as to preclude others from partaking. Or why not the "due diligence" requirement that states must ensure that other states' rights and interests are not violated due to activities over which the first state has jurisdiction; whether we are talking about drinking or about jurisdiction, everyone must partake and claim their share.

In the light of the above, perhaps it can be said to be the case that – at their core – our international law principles on jurisdiction are no more advanced than was the Viking-era drinking etiquette? And perhaps they do not need to be?

7. "LAGOM JURISDICTION"AND THE GOOGLE FRANCE MATTER

Sweden is often described as *landet lagom* (i.e. the country of "lagom") and the lagom attitude can perhaps be detected in the approach taken by the Swedish Data Protection Authority (Datainspektionen) as to "right to be forgotten" delisting:

> *"The DPA's assessment is that the obligation to delete search results means that results must be deleted in such a way that they are not shown when searches are made from Sweden. But, there may be situations where search results must be deleted also when searches are made from other countries. This may be the case if there is a specific connection to Sweden and to the data subject, for example if the information on the webpage which is linked to is written in Swedish, addressed to a Swedish audience, contains information about a person that is in Sweden or if the information has been*

published on the Swedish domain.se", says Martin Brinnen, legal advisor within the Swedish DPA."[33]

This approach is interesting, and the "specific connection" requirement seems to be at least a new phrase (be as it may that it shares commonalities with similar concepts). But the idea that e.g. the use of a Swedish domain – on its own – should determine the scope of jurisdiction seems both naive and misguided.

In any case, it is clear that the *Datainspektionen* has made an attempt to approach the territorial scope of delisting orders in a balanced manner, which stands in stark contrast to the excessive approach taken by its French equivalent (the CNIL). This is important even though further work is needed for the correct balance to be struck. If nothing else, the Datainspektionen has proven the appropriateness of the old Swedish saying that *lagom är bäst*; that is,"lagom is best".

8. CONCLUDING REMARKS

The discussion above has sought to suggest that – at their core – our international law principles on jurisdiction are hardly more advanced or sophisticated than was the Viking-era drinking etiquette, and that arguably they do not need to be. However, the above has also demonstrated something else. The discussion of international law has showcased the complex manner in which we articulate these principles, as well as the degree of lacking consensus as to how we should formulate and approach these principles. And in the light of this, absolutist statements as to what "international law says" in relation to sovereignty and jurisdiction must always be met with a healthy dose of scepticism.

The reality is that international law on sovereignty and jurisdiction is largely a grey-zone populated by conflicting legal rules and principles. Much work lies ahead and in the Google France matter, the CJEU is presented with an interesting opportunity to interpret applicable international law in a manner that helps to steer it in a sensible direction.

But Internet jurisdiction is not just a matter for the courts and other law makers. And it is not just a matter for Internet lawyers. Further, it is not just a matter for the public international law crowd, and it is not just a matter

[33] Datainspektionen. (2017) *The right to be forgotten may apply all over the world.* [online] Datainspektionen. Available from: https://www.datainspektionen.se/press/nyheter/theright-to-be-forgotten-may-apply-all-over-the-world/ [Accessed 4 May 2017].

for those inhabiting the domain of private international law – Internet jurisdiction is a key issue in all of these fields. And, importantly, it is a matter we will only be able to address when the experts from these fields join forces and approach jurisdiction in an open-minded manner.

To this we may add that, addressing Internet jurisdiction is, in fact, a matter for us all — industry, government, courts, international organisations, civil society, and the academic community — to help achieve useful change. Furthermore, those engaged in capacity-building initiatives must recognise that they need to incorporate capacity building in relation to a sound understanding of the jurisdictional challenges and solutions.

Much work lies ahead. But it is crucially important work and we must now turn our minds to these issues to which we, for far too long, have turned a blind eye.

LIST OF REFERENCES

[1] Ashliman, D. L., Bray, O. (2003) *Hávamál* [online] Available: from: http://www.pitt.edu/~dash/havamal.html

[2] Briggs, A. (2012) The Hague Academy of International Law, Recueil des Cours, 354.

[3] CNIL. (2015) *CNIL orders Google to apply delisting on all domain names of the search engine* 12 June. [online] Available from: http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine [Accessed 2 April 2017].

[4] Constine, J. (2017) *Facebook now has 2 billion monthly users… and responsibility.* [online] Techscrunch.com. Available from: https://techcrunch.com/2017/06/27/facebook-2-billion-users/ [Accessed 27 June 2017].

[5] Corn, G. and Taylor, R. (2017) Sovereignty in the Age of Cyber. *AJIL Unbound*, 111, pp. 207-212. Available from: doi: 10.1017/aju.2017.57.

[6] Datainspektionen. (2017) *The right to be forgotten may apply all over the world*. [online] Datainspektionen. Available from: https://www.datainspektionen.se/press/nyheter/the-right-to-be-forgotten-may-apply-all-over-the-world/ [Accessed 4 May 2017].

[7] Endicott, T. (2010) The Logic of Freedom and Power. In: Besson, S. and Tasioulas, J. (eds.) *The Philosophy of International Law*. Oxford: Oxford University Press, pp. 245–259.

[8] Forbes. *The World's Most Valuable Brands.* Forbes.com [online] Available from: https://www.forbes.com/powerful-brands/list/#.

[9] Ginsburg, T. (2017). Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn

Manual 2.0. *AJIL Unbound*, 111, pp. 205–206. Available from: doi: 10.1017/aju.2017.58

[10] Google Inc. v. Commission nationale de l'informatique et des libertés (2017), C-507/17.

[11] Hávamál (2018) [online] Wikipedia. Available from: https://en.wikipedia.org/wiki/

[12] Hilton v. Guyot (1895) 159 US 113.

[13] Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime. (1935) *American Journal of International Law*, 29 Supp 443.

[14] Island of Palmas (1928), 2 R. I. A. A 829, 838 (Perm. Ct. Arb. 1928).

[15] Judgement of 21 December 2011, The Air Transport Association of America and Others, C-366/10, EU:C:2011:864.

[16] Khan, D. E. (2012) Territory and Boundaries. In: Bardo Fassbender and Anne Peters (eds.), *The Oxford Handbook of the History of International Law*. Oxford: Oxford University Press.

[17] Khanna, P. (2016) *These 25 Companies Are More Powerful Than Many Countries.* [online] Foreign Policy. Available from: http://foreignpolicy.com/2016/03/15/these-25-companies-are-more-powerful-than-many-countries-multinational-corporate-wealth-power/

[18] Mann, F. (1996) The doctrine of Jurisdiction in International Law. In: Karl M Meesen (ed.), *Extraterritorial Jurisdiction in Theory and Practice*. Kluwer Law International.

[19] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[20] Ryngaert, C. (2015) *Jurisdiction in International Law*. 2nd edition. Oxford: Oxford University Press.

[21] Schmitt, M. gen. ed. (2017) *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*. New York: Cambridge University Press.

[22] Schmitt, M. and Vihul, L. (2017). Sovereignty in Cyberspace: Lex Lata Vel Non? *AJIL Unbound*, 111, pp. 213–218. Available from: doi: 10.1017/aju.2017.55

[23] Spector, P. (2017). In Defense of Sovereignty, in the Wake of Tallinn 2.0. *AJIL Unbound*, 111, pp. 219–223. Available from: doi: 10.1017/aju.2017.56

[24] S.S. "Lotus" (France v. Turkey) (1927) PCIJ Series A, No 10.

[25] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press.

[26] Svantesson, D. (2017) *Time for international law to take the Internet seriously.* [online] OUPblog. Available from: https://blog.oup.com/2017/10/international-law-internet/ [Accessed 7 October 2017].