RIPE

ESTABLISHING JURISDICTION ONLINE

THE PROBLEM OF THE ACCESS-BASED JURISDICTIONAL PRINCIPLE

Sara Solmone, 23 October 2017

What does State jurisdiction mean online?

- Traditionally, State jurisdiction has been established by relying primarily on the **territorial criterion** (i.e. a State can exercise jurisdiction over acts committed within its territory and over people located within its borders).

- Due to the Internet's apparently borderless nature, it is **difficult to ascertain the meaning of State jurisdiction in cyberspace**.

- States are applying the **access-based jurisdictional approach**.

Aim of the presentation

- To answer two main questions:

  ❖What are the **implications** of the access-based jurisdictional approach on the **fulfilment of freedom of expression online**?

  ❖Are there **other jurisdictional criteria** that are better suited to establish jurisdiction over online content in a way that is compatible with freedom of expression requirements?

- To **introduce** a highly controversial jurisdictional criterion, **jurisdiction based on data location**, and to discuss the critiques that it has attracted.

The access-based jurisdictional approach

- **Two distinctive elements** define the access-based jurisdictional approach:

  ❖ this approach is used by national courts to establish jurisdiction over content published online but **uploaded and hosted in foreign countries**;

  ❖ the basis upon which jurisdiction in exercised is that **content published online can be accessed** from within the territory of the country exercising jurisdiction.

The *Perrin v. United Kingdom* case

Perrin v. United Kingdom [2005] ECHR 5446/03

What happened: Some pictures of a sexual nature were uploaded on Mr. Perrin's website. The pictures had been uploaded and hosted in the US, where Mr. Perrin's company was located. Those pictures were legal in the US and illegal in the UK, where Mr. Perrin lived.

What the UK Court found: The UK Courts established that they had jurisdiction over the case due to the fact that the pictures were accessible from within the UK territory. Mr. Perrin was sentenced to 30-month imprisonment.

What the European Court of Human Rights (ECtHR) found: The ECtHR accepted that the UK Court had jurisdiction over the images published online and found that Mr Perrin's conviction did not violate the applicant's right to freedom of expression.

Key characteristic of the access-based jurisdiction

- The accessibility of online content published abroad from within the territory of a given State has been used to justify the exercise of State jurisdiction and specifically the application of the objective territorial principle:

  i.e. **publishing content online is equated to having committed an act within the territory of the State where that content can be accessed.**

Critiques to the access-based jurisdiction

- Establishing jurisdiction based on access has the overall effect of **imposing restrictions on the freedom of expression** of Internet users located in foreign countries.

- **No thorough analysis** of the link between the perpetrator of the unlawful act, the illegal content published online and the State that exercises jurisdiction has been conducted (Korf 2014).

The importance of a clear and close nexus

- **Geneva Internet Disputes Resolution Policy** (Topic 1, Proposal 2) rejects the access-based jurisdictional approach as it "allows any country to enjoy jurisdiction over […] websites which do not make use of technological ways of filtering users".

- Official documents issued by the below international authorities in the field of freedom of expression state that jurisdiction over content published online should be limited to States to which those cases "**have a real and substantial connection**" or "**are most closely associated**":

  - The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression;
  - Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media
  - Organization of American States (OAS) Special Rapporteur on Freedom of Expression
  - African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information
  - Inter-American Commission on Human Rights (IACHR) Special Rapporteur for Freedom of Expression

Establishing jurisdiction online: which could be the criteria?

- The **criteria identified in the above mentioned international declarations** are:

  - ❖ the place where the author of the content is **established/resides**;
  - ❖ the place from where the content is **uploaded/published**;
  - ❖ the State/public at which the content is specifically **directed**.

- Even in a borderless environment such as the Internet, **territory is seen as a central element** in establishing jurisdiction.

- The territorial principle is **not useful** in all those cases where it cannot be established the place where the content has been uploaded or even who uploaded it.

The Targeting Test

- The targeting test seems **better suited** to establish which State has jurisdiction in a non-physical environment such as the cyberspace.

- The targeting test permits to **by-pass the obstacles** represented by the unknown location of the person who uploaded some content online or the place where the content was uploaded from.

- For the targeting test to be satisfied it is **sufficient to establish** that the content published online was **targeting** an audience located within a given State, regardless of where the content was originally uploaded from or who uploaded it.

- However, the **difficulty** associated with the targeting test is that so far there is no consensus as to the criteria upon which this test should be based.

Jurisdiction based on data location: the *Microsoft Corp. v. the United States* case

Microsoft Corp. v. the United States, 829 F.3d 197 (2d Cir. 2016)

What happened: The US government asked Microsoft to seize an email account that had been set up by one of its customers and to disclose its content. The account was believed to be used in conjunction with illegal drug trafficking. Most of the account's content was stored outside the US, in Microsoft's Dublin data centre. Microsoft refused to hand over the Dublin-based data.

The controversy: Microsoft argued that the Stored Communications Act (SCA) does not have extraterritorial effect and therefore does not apply to material stored abroad. The US government maintained that an SCA warrant requires that the service provider disclose the data stored on its facilities, regardless of the location of the latter.

What the Court found: the US Court of Appeals for the Second Circuit found that the warrant provisions of the SCA could not be applied to content located in a foreign country and therefore subjected to the jurisdiction of a foreign State.

The problem of jurisdiction based on data location

- Establishing jurisdiction based on the place where the data is located is highly controversial and has received **several critiques**:

  ❖ “Unstable and arbitrary jurisdictional criterion: **data are extremely mobile**, change location frequently and are divided among different countries” (Daskal 2015);

  ❖The owner of the data has **no control** over where the data are located (Daskal 2015);

  ❖It leads to an “**unsatisfactory”** result (Daskal 2016; Harvard Law Review 2016).

The problem of jurisdiction based on data location

- On the other hand, granting the extraterritorial application of the laws of a State to data stored in a foreign State presents many difficulties as well:

  - ❖It could lead to the **violation of the foreign State's sovereignty** (Daskal 2015);

  - ❖The ISPs might be **uncertain as to the laws** with which they are bound to comply (Daskal 2015).

- Two points have been raised by both the critics of the data location criterion and those who favour the extraterritorial application of national laws to data stored abroad:

  - ❖**Risk of data localisation** (Daskal 2015; Granick 2016);

  - ❖**Privacy concerns** (Daskal 2015; Granick 2016).

Conclusions

- Due to the general uncertainty as to the meaning of State jurisdiction online, some national courts in Europe are adopting the access-based criterion in order to establish jurisdiction over content hosted abroad. This fact has **negative effects on the fulfilment of human rights online**.
- Some **consensus** at the international level exists on limiting State jurisdiction only to cases were a genuine link can be found between the State establishing jurisdiction and the content published online/person publishing it.
- The **targeting test** seems better suited to establish jurisdiction in a non-physical environment than the territorial principle.
- The **data location** jurisdictional principle is highly controversial and raises several concerns, especially with regard to **sovereignty and privacy**.

RIPE

THANK YOU

Email: s.solmone@uel.ac.uk

RIPE

Questions?

References

Perrin v. the United Kingdom [2005] ECHR 5446/03, available at http://echr.coe.int/sites/search_eng/pages/search.aspx#{"fulltext":["applicationnumber:\"5446/03\""],"subcategory":["e-reports"]}.

Microsoft Corp. v. the United States, 829 F.3d 197 (2d Cir. 2016).

Mika Hayashi, 'Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace' in Carlo Focarelli (ed) Le Nuove Frontiere del Diritto Internazionale (Morlacchi Editore, 2008).

A Gillespie, 'Jurisdictional issues concerning online child pornography' (2012) 20 Int J Law Info Tech 170.

D Korf, The rule of law on the Internet and in the wider digital world. Issue Paper published by the Council of Europe Commissioner for Human Rights, 2014. Available at https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2 (Accessed: 14 September 2015).

Research Division of the European Court of Human Rights "Internet: Case Law of the European Court of Human Rights", 2015, available at http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.

Office of the Special Rapporteur for Freedom of Expression Inter-American Commission on Human Rights "Freedom of expression and the Internet", 2013, available at http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf (Accessed: 05 July 2016)

Organization for Security and Co-operation in Europe "Joint declaration on freedom of expression and the Internet", 2011, available at http://www.osce.org/fom/78309 (Accessed: 05 July 2016).

University of Geneva, *Geneva Internet Disputes Resolution Policies 1.0.* Available at: https://geneva-internet-disputes.ch/ (Accessed: 14 August 2017)

Daskal, J (2015) 'The Microsoft Warrant Case: The Policy Issues', *Just Security*, 8 September. Available at: https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues/?print (Accessed: 20 October 2017)

Daskal, J (2016) 'Three Key Takeaways: The 2d Circuit Ruling in The Microsoft Warrant Case', *Just Security*, 14 July. Available at: https://www.justsecurity.org/32041/key-takeaways-2d-circuit-ruling-microsoft-warrant-case (accessed: 20 October 2017)

Granick, J (2016) 'The Microsoft Ireland Case and the Future of Digital Privacy', *Just Security*, 18 July. Available at: https://www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy/ (Accessed: 20 October 2017)

Harvard Law Review (2016) *Microsoft Corp. v. United States*. Available at: https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/ (Accessed: 20 Octonber 2017)