

Digital Regulations and the Risk of a Securitized Internet

by Kevin Kalomeni

Among the hotly debated topics in Brussels these days, digital innovation is no doubt high on the agenda. Cybersecurity and privacy are natural concerns in light of the upcoming European elections but several other issues are also present, particularly in the realm of copyright rules and efforts to counter the spread of “fake news”.

The European Parliament’s adoption last September of a position on digital copyright rules is an example of the increased willingness of European institutions to use regulations to tackle potential risks in the digital domain.¹ In this way, the EU has not only made important strides in the realm of digital copyright regulations, it has also re-confirmed its role as a global norms setter.

¹ European Parliament, *Parliament Adopts Its Position on Digital Copyright Rules*, 12 September 2018, <http://www.europarl.europa.eu/news/en/press-room/20180906IPR12103>.

Nevertheless, a misconception seems to pervade a number of these well-intentioned EU efforts. While Margrethe Vestager, the European Commissioner for Competition, initiated a series of investigations against the market dominance of big tech oligopolies, such as the GAFAs (Google, Apple, Facebook and Amazon), some of these regulations may inadvertently end up reinforcing these technological giants.

The digital copyright rules and especially article 13 of these regulations² is a good example of the outdated conceptions that some European parliamentary members have on digital technology. In effect, article 13 calls for collaboration between electronic platforms and rights holders to verify the copyright status of the content

² European Commission, *Proposal for a Directive on Copyright in the Digital Single Market* (COM/2016/593), 14 September 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0593>.

Kevin Kalomeni is a Marie-Curie PHD student at LUISS University (Rome) and Université Laval (Québec) within the frame of the GEM-STONES research programme, conducting researches on regulatory cooperation within preferential trade agreements and crypto-assets.

published in these platforms, including through automatic content recognition (ACR) or filters, both of which are rather problematic.

The current technological level of ACR does not permit to distinguish with certainty posts that contain legal content from those violating legislative requirements, such as infringements of intellectual property. This shortcoming was rapidly identified and presented to the President of the European Parliament, Antonio Tajani, in a 2018 letter authored by Vint Cerf, co-inventor of the TCP/IP, and Tim Berners-Lee, inventor of the World Wide Web.³

In response, the EU rushed to adopt an exception for online encyclopaedias, such as Wikipedia, which would otherwise have been threatened with fines and closure.⁴ However, the EU continues to underestimate the effects that online filters may have on voluntary projects of knowledge sharing. An illustrative example is given by Facebook's decision in 2011 to censor a post containing an image of the celebrated painting by Gustave Courbet "L'Origine du monde" and deactivate the user's account due to its no-nudity policy.⁵

³ Vint Cerf et al., *Article 13 of the EU Copyright Directive Threatens the Internet*, letter to Antonio Tajani, President of the European Parliament, 12 June 2018, <https://www.eff.org/files/2018/06/12/article13letter.pdf>.

⁴ Cory Doctorow, "The EU's Copyright Proposal is Extremely Bad News for Everyone, Even (Especially!) Wikipedia", in *Deeplinks Blog*, 7 June 2018, <https://www.eff.org/node/98924>.

⁵ Perrine Signoret, "Censure de 'L'Origine du monde': une faute de Facebook reconnue, mais pas sur le fond", in *Le Monde*, 15 March 2018, [https://www.lemonde.fr/pixels/article/2018/03/15/censure-de-l-origine-du-](https://www.lemonde.fr/pixels/article/2018/03/15/censure-de-l-origine-du)

In a slightly more nuanced fashion, the recently adopted "EU Code of Practice on Disinformation"⁶ that is meant to force major tech companies such as Facebook, Twitter and Google to counter the spread of "fake news", also suffers from similar shortcomings. While the code remains voluntary, its efforts to prioritize and rank sources according to their "trustworthiness" or call for partnerships with third-party fact-checking organizations might have similar unintended consequences.

These approaches may result in delegating further powers to large tech giants, allowing them to moderate information based on the rather malleable criteria of "real news". In this they are called to rely on mainstream news organizations, allowing users to quickly identify the provenance of a news story. Mainstream news organizations, however, themselves may at times produce, relay or rely on false information.⁷

Over time, such a reliance may become a liability for big tech companies, all the more so in the context of increasingly polarized societies and news outlets. To mitigate human political bias, social media firms may eventually decide to further their adoption of algorithms that produce automated fact-checking, which would result in reinforcing the "homogenization" of the media

[monde-une-faute-de-facebook-reconnue-mais-pas-sur-le-fond_5271666_4408996.html](https://www.eff.org/files/2018/06/12/article13letter.pdf).

⁶ European Commission, *Code of Practice on Disinformation*, 26 September 2018, <https://europa.eu/!Hp98Ty>.

⁷ Laurent Bigot, "Rétablir la vérité via le fact-checking: l'ambivalence des médias face aux fausses informations", *Le Temps des médias*, No. 30 (2018), p. 62-76.

ecosystem and pre-existing biases in society.⁸

In the realm of digital copyright and “fake news”, therefore, the European Union may have inadvertently strengthened the dominance of the big technological companies, increasingly considered as the Internet’s “gate-keepers”. This is extremely problematic as it indirectly reinforces the power of major Internet service providers, by delegating control and regulation to them. Essentially, these companies are being asked to police themselves and employ their technological infrastructure to assist governments in their security efforts.

Among the available options, the use of “filter by design” based on ACR is one of the most problematic. For instance, the decision by Google to design a search engine that meets the censorship requests of the Chinese Government is one worrisome development in this domain.⁹

Two conflicting visions are identifiable in these debates. On the one hand, stands a traditional approach to the hierarchical relationship between authority and society. Such views privilege the concentration of power and responsibilities in the hands of few actors that are then subjected to top-down regulations. On the other, the complex reality of modern life

is increasingly characterized by a decentralization of power and influence and a growing embrace of the virtues of communal self-organization.

This latter approach views public or private entities seeking to control cyber-space with suspicion, preferring diffused power structures and a decentralization of network actors. These tend to embrace management modalities that share some similarities with worker cooperatives, in which users or workers hold a direct stake in a given platform or company. For instance, the widespread use of open source code is a good illustration of this collective ownership over the means of production.

While in the short-to-medium term the former approach may be more efficient in terms of scalability, resources management and speed, it is particularly vulnerable to security threats. Concentrating power may appear as an attractive shortcut to manage new digital challenges. However, it also creates oligopolistic structures, due to a winner-takes-all approach and suffers from a high concentration of risk.

Indeed, compiling and storing data in a central database may effectively ease the task of hackers, which can exploit human vulnerabilities typical in large bureaucratic organizations. Furthermore, aggressors with limited resources can focus all their efforts on single organizations. A decentralized organization may therefore be preferable, as hacking one node will not compromise the entire system, as demonstrated by research conducted

⁸ Hannah Devlin, “AI Programs Exhibit Racial and Gender Biases, Research Reveals”, in *The Guardian*, 13 April 2017, <https://gu.com/p/69m9x>.

⁹ Alex Hern, “Google ‘Working on Censored Search Engine’ for China”, in *The Guardian*, 2 August 2018, <https://gu.com/p/94yyq>.

by the University of South Alabama.¹⁰

Often at the vanguard in defending consumer rights, EU institutions are poised to be the new battleground where these two mentalities, a vertical versus decentralized approach, fight over the future of Europe's regulatory framework.

Vertical approaches do not always come out on top in Brussels, as evidenced by the recent adoption of the General Data Protection Regulation (GDPR) and the second version of the Payment Services Directive (PSD2). Both regulations reflect the will and ability of the EU to promote a less centralized market structure and empower consumers.

The GDPR, enforced throughout the EU since May 2018, places individual, user rights over data at the cornerstone of its regulation.¹¹ As a result, and for the first time, consumers can enjoy real ownership of their data.

Following on from the GDPR, the recently adopted PSD2 seeks to create a level playing field between financial and technological companies.¹² In effect, consumers will have the possibility to request their account data and provide them to third party service providers.

¹⁰ Renuka Prasad Pasupulati and Jordan Shropshire, "Analysis of Centralized and Decentralized Cloud Architectures", in *IEEE SoutheastCon 2016*, 30 March-3 April 2016, p. 1-7.

¹¹ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data..., <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

¹² European Commission, *Payment Services (PSD2) - Directive (EU) 2015/2366*, <https://europa.eu/!qG83XW>.

This will enable consumers' access to a wide range of financial services without having to go through banks as intermediaries.

Nevertheless, these regulations and compliance efforts continue to benefit large companies over smaller firms, who suffer from less visibility and user confidence, which in turn limits their ability to grow and attract more following.¹³

Such challenges require another approach to data ownership. Consumers should in fact not be forced to entirely give up control of their information in exchange for using a service. One proposition might be to force firms to pay consumers directly for the use of their data. Another option could include the establishment of a public managed fund where such assets would be deposited, as recently proposed by Ryan Avent in an article for the *MIT Technology Review*.¹⁴

Overall, the EU level remains the only arena where European citizens and consumers have the ability to fight for their rights and influence the future. Nevertheless, this should not mean giving a blank check for power concentration in the hands of EU institutions or corporate leaders.

¹³ Mark Scott, Laurens Cerulus and Laura Kayali, "Six Months In, Europe's Privacy Revolution Favors Google, Facebook", in *Politico*, 23 November 2018, <https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook>.

¹⁴ Ryan Avent, "A Digital Capitalism Marx Might Enjoy", in *MIT Technology Review*, Vol. 121, No. 4 (July/August 2018), p. 18-19, <https://www.technologyreview.com/s/611480>.

Decentralization, non-censorship and transparency are causes worth fighting for. Combatting an excessive securitization of the Internet and data usage will be key to promote a more open, fair and transparent digital domain.

As the EU seeks to develop a “third way” between the US and Chinese models of top-down centralization and censorship respectively, an approach that begins with an effort to develop and strengthen new networks of small and medium size enterprises in the tech and cyber domain across Europe may prove beneficial to strengthen forms of economic and communal organization. The parallel with worker cooperatives and efforts to foster clusters of start-ups in certain domains could be embraced as reference points.

Ultimately, restoring citizen rights and providing avenues for individuals to gain control of their data will also strengthen trust in EU institutions and breath much needed fresh air into the EU’s own norms and values while also benefitting European resilience and defence against digital threats.

5 December 2018

Istituto Affari Internazionali (IAI)

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*Affarinternazionali*), two book series (*Quaderni IAI* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via Angelo Brunetti, 9 - I-00186 Rome, Italy

T +39 06 3224360

F + 39 06 3224363

iai@iai.it

www.iai.it

Latest IAI COMMENTARIES

Director: Andrea Dessì (a.dessi@iai.it)

- 18 | 66 Kevin Kalomeni, *Digital Regulations and the Risk of a Securitized Internet*
- 18 | 65 Jesse Colzani, *Transatlantic Tensions, Oil Imports and the Euro's Ambitions in International Trade*
- 18 | 64 Margherita Bianchi and Alessandro Valentini, *Brexit and the Future of European Energy Integration: The Stakes*
- 18 | 63 Nathalie Tocci, *The Demise of the International Liberal Order and the Future of the European Project*
- 18 | 62 Claudia Astarita, *A New Frontier of West-China Competition: Academia and International Education*
- 18 | 61 Nicola Bilotta, *Chinese Banks and Foreign Owned Subsidiaries Eye Latin American Markets: A New Challenge for the US?*
- 18 | 60 Riccardo Alcaro, *The US Mid-Term Elections: The Stakes for Europe*
- 18 | 59 Sara Candido, *Europe's Many Souls: Abandoned Places and the Struggle for a European Dream*
- 18 | 58 Giovanni Santambrogio, *A New Narrative for an Old Project: Re-Imagining Europe*
- 18 | 57 Tobias Pietz, *The Civilian CSDP Compact: Strengthening or Repurposing EU Civilian Crisis Management?*