Digital Clearinghouse

Background Note

for the meeting of the Digital Clearing House of 16 June 2021[*]

New Ways of Enforcing Law in the Digital Society

Towards data-based and experimental enforcement

Alexandre de Streel and Inge Graef [**]

[*] The Digital clearinghouse project is organised by the University of Namur, the University of Tilburg and the European Policy Centre with the support of the Open Society Foundations, Omidyar Network and the King Baudouin Foundation. Please visit the website: https://www.digitalclearinghouse.org/

[**] Professor, University of Namur and NADI and Academic Co-Director Centre on Regulation in Europe (CERRE); Associate Professor, Tilburg University, TILEC and TILT. This Note is partly based on A. de Streel and M. Ledger, *New Ways of Oversight for the Digital Economy*, CERRE Issue Paper, February 2021

Table

1. Introduction and aim of the Note

With States around the world seeking to regulate digital platforms, the question arises as to how regulatory enforcement can be carried out. Even if the right regulatory models are put in place, a lack of effective oversight may undermine and even discredit public intervention. The oversight of platforms is particularly challenging given some of the key characteristics of the platform economy:

- the number, size, and (sometimes global) reach of platforms;
- the large information asymmetry between platforms and enforcement authorities;
- a high level of innovation and complexity in the business models;
- the impact of platforms on society in general and on fundamental rights such as privacy and freedom of expression.

To date, there is little in European Union (EU) legislation specifically targeting enforcement mechanisms of the rules applicable to platforms.[1] Except for broader policy areas (such as data protection, consumer protection, competition or audio-visual media services), the platform economy is not supervised by a specific regulator and there are multiple enforcement systems at the national level. However, this situation is set to change since the European Commission is proposing tighter oversight mechanisms in the recently proposed Digital Services Act (DSA)[2] and the Digital Markets Act (DMA).[3]

Given the novelty of many of the regulatory issues in the digital economy and the (still) many unknowns, the complexity and the dynamism of digital technologies and markets, as well as the large information asymmetry between the regulator and the digital platforms, new ways of enforcement need to be applied. Those new ways should adapt past regulatory enforcement practices to the new characteristics of the digital economy. In particular, to improve their operations, regulators could be inspired by the ways of working of the digital platforms they will oversee.

After this introduction, section 2 suggests the emergence of an ecosystem of enforcement involving the regulators, the platforms and their users. Then, section 3 suggests the move towards data and AI based enforcement. Finally, Section 4 suggests the move towards experimental enforcement. The Note aims to put forward some options and to stimulate discussion around models of enforcement of the platform economy.

2. Towards an ecosystem of oversight and enforcement

New ways of enforcing rules in the digital society could be based on the concept of **ecosystem of oversight and enforcement** where the regulator orchestrates the meeting of the public interest and the supervision of the rules by the platforms and their (business and end) users. In some Member States, this may require a cultural shift for the regulator as noted by several French regulators: *"Instead of telling economic stakeholders how to behave, the aim is to empower consumers/users to create market incentives. To be successful, this approach requires a cultural shift within the State. It means recognising*

[1] On the EU regulation of digital platforms, see A. de Streel, A. Kuczerawy and M. Ledger, "Online Platforms and Services", in *Electronic communications, Audiovisual Services and the Internet: EU Competition Law and Regulation*, 4th ed., Sweet & Maxwell, 2019, pp.125-157.

[2] Proposal of the Commission of 15 December 2020 for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31, COM(2020) 825.

[3] Proposal of the Commission of 15 December 2020 for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842.

that the State is not the sole guarantor of the public interest: every stakeholder, every user is given the ability to influence regulation".[4]

To do so, the regulator has a central role in issuing general and individual guidance, stimulating and overseeing the adoption of codes of conducts. The regulator should be supported by internal compliance mechanisms within the digital platforms, proactive users of the platforms, and, in some cases, independent auditors.

2.1. Regulatory guidance

(a) General guidance

First and foremost, regulators should **guide on what is expected from platforms** (in general) and how they intend to oversee the application of the rules.[5] A culture of dialogue, trust, and transparency should be established, and this could start with the establishment of **initial general guidance.**

Platforms, users, and other interested parties can shape guidance if the regulator provides room for input during its process of elaboration, in particular through open consultation processes. This will promote wide acceptance of the guidance, while also making sure that this general guidance is informed and considers the evolution of technology, business processes, and media consumption.

The regulator could envisage the adoption of **more specific guidance to address particular problems** (such as terrorist content or child sexual abuse). Some processes may be particularly complex because they imply collaboration and reporting mechanisms between platforms, regulators, law enforcement authorities, users, and civil society. This collaboration could be detailed in codes of conduct or similar documents which could also provide examples of best practices. They should be adopted with the active input of platforms.

Guidance should also be subject to **regular evaluation and review** to make sure it is still fit for purpose.

(b) Individualised guidance

Regulators could provide **individual guidance to particular platforms**. This guidance can be seen as a form of "soft enforcement" of rules when their interpretation is not clear, hence needs to be clarified through implementation. An example of this can be found at the EU level in the field of consumer protection when following coordinated actions, the Consumer Protection Cooperation (CPC) Authorities adopt Common Positions in which they inform the digital platforms about their concerns. The CPC Authorities and the Commission then discuss with the specific digital platforms to ensure compliance with EU consumer laws. [6]

Besides, akin to rules that exist in other closely related areas such as consumer contracts in the telecommunications sector,[7] the regulator could envisage giving special guidance to platforms on their **Terms and Conditions (T&C)**. The regulator could even conduct an ex-ante review/screening of the T&C (and changes proposed to T&C) of very large platforms given their crucial role in shaping what is allowed or not on the platform thereby giving the users the required confidence that they are validated by a public oversight body. Indeed, there is an increasingly important body of legislation that applies to

[4] See French regulators, New regulatory mechanisms – data-driven regulation, July 2019 at p.3.
[5] For instance, see Commission Staff Working Document of 25 May 2016 on Guidance on the implementation/application of the Directive 2005/29 on Unfair commercial practices, SWD(2016) 163, Section 5.2.
[6] Coordinated actions taken by the Consumer Protection Cooperation (CPC) Network: https://ec.europa.eu/info/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions_en
[7] See EECC, arts. 102-104.

contracts between online providers and consumers/users.[8] Some legislation is also in place at the EU level to frame the T&Cs between platforms and business users.[9] To date, it is often unclear how the application of these rules is overseen, and this may also fall within the remit of regulators.

Start-ups in particular often lack experience and capabilities to understand the regulatory environment, and advice could be given by regulators through dedicated channels.

2.2. Codes of conduct

The regulator should **also stimulate and oversee the adoption of codes of conduct**. This is often foreseen by EU law for the digital economy.[10] In practice, there are many examples of codes of conduct developed at the EU level, which have been adopted by platforms under the oversight of the European Commission to deal with illegal or harmful content and products.[11] Codes of conduct by platforms can either serve to **translate legal obligations into operational measures or can be developed to address further issues** not covered by the legislation.[12]

As codes of conduct should be developed and complied with by platforms, there is a risk that such form of self-regulation becomes self-serving and/or is not well enforced. Therefore, those codes should comply with the **principles for better self-and co-regulation** proposed by the European Commission.[13] Those principles ensure, on the one hand, that rules are prepared openly and by as many as possible relevant actors representing different interests and values and, on the other hand, that they are monitored in a way that is sufficiently open and autonomous and are sanctioned when violated.

2.3. Internal tools of platforms

Regulators could be supported by internal compliance mechanisms within the digital platforms. Internal oversight tools are methods developed by the platforms themselves to make sure they respect the rules in place. The EU law applicable to digital platforms already imposes some of those mechanisms.

Risk assessments **-** Platforms could be required by law or incentivised[14] to conduct risk assessments to review whether their products and services comply with the regulatory requirements or whether users are particularly exposed to certain risks. The GDPR contains such a requirement in the form of a data protection impact assessment[15] and the proposed DSA foresees that very large online platforms should conduct risk assessments of how their services are used to disseminate illegal content, of any negative effects for the exercise of fundamental rights and the intentional manipulation of their services harming the protection of public health, minors, civic discourse or on electoral processes and public security.[16] It may also be possible to request platforms to carry risk assessments with the help of independent

[8] See in particular Council Directive 93/13 of 5 April 1993 on unfair terms in consumer contracts, OJ [1993] L 95/29 as amended; Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ [2019] L 136/1; AVMSD, art.28b(3).

[9] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ [2019] L 186/55

[10] Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ [2000] L 178/1, art.16; GDPR, art.40; AVMSD, art.4a.

[11] For a summary, see S. Broughton-Micova and A. de Streel, Digital Services Act: Deepening the internal market and clarifying responsibilities for digital services, CERRE Report, December 2020. For instance in the field of online disinformation (Code of Practice) or online hate speech (Code of Practice)

[12] DSA Proposal envisages both these possibilities at arts 35 and 36.

[13] Those principles are available at : https://ec.europa.eu/digital-single-market/en/best-practice-principles-better-self-and-co-regulation. See also M. Finck, Digital co-regulation: designing a supranational legal framework for the platform economy, 43 *European Law* Review, 2018, pp. 47-68.

[14] A platform could be incentivised to carry out risk assessments where for instance, the sanctions could be reduced or delayed if a risk assessment has been made.

[15] GDPR, art.35.

[16] Prop DSA, art.26.

auditors,[17] experts and/or with the involvement of users, and civil society. In any event, regulators should provide a clear framework on risk assessments concerning frequency, reporting and involvement of third parties.

Appointment of compliance officer **-** Compliance officers already exist to monitor and ensure compliance with the GDPR[18] and are also foreseen in the proposed DSA for very large online platforms.[19] Among the important tasks linked to oversight, we highlight (i) a duty of cooperation with the regulator in charge,[20] and (ii) a duty to inform the management and the employees of the obligations to be complied with.

Accountability **-** While requirements for risk assessments and the appointment of compliance officers are helpful as internal tools, they should not be employed by platforms to increase their discretion over how the applicable rules should be interpreted and interpreted. To prevent such risks, a duty of accountability could be imposed to make platforms responsible for proactively showing compliance with the applicable rules. Inspiration can be drawn from the GDPR's principle of accountability, which requires data controllers to demonstrate to the data protection authority upon request that adequate measures have been taken to ensure that their data processing activities comply with the GDPR.[21] The imposition of a duty of accountability would fit in a shift in thinking from purely negative duties to refrain from harmful practices towards positive duties to show compliance with the rules. Such a shift would not go as far as reversing the burden of proof,[22] but would help address the current information asymmetries between regulators and platforms. The ability to request platforms to show what measures have been implemented to comply with the law can allow regulatory agencies to engage in more proactive monitoring against lower enforcement efforts.[23]

2.4. Empowered and proactive users

The regulators should strive to better **empower the users of platforms to make choices in their best interest** and, in doing so, contribute to making the market work better. This digital literacy role implies that business users and the end-users of the platforms should receive from the platforms as well as from the regulators meaningful information to choose between different platforms. To be meaningful, the information given should take into account users biases and heuristics.

Platforms can be made more **responsible for helping users make good decisions**. As explained in the Guidelines on the protection of online consumers published by the Netherlands Authority for Consumers and Markets (ACM),[24] this implies that the information given should be complete, correct, communicated in an easy to understand manner and be found easily. Moreover, the choice architecture

[17] This possibility is foreseen in article 13 of the proposed DMA.
[18] GDPR, arts.37-39.
[19] Prop DSA, art.32.
[20] Platforms and regulators may need to take urgent action is certain circumstances which will require excellent collaboration between platforms and regulators. Crisis protocols could be established between regulators and platforms which could be activated rapidly in case of need. The regulator could identify potential areas where urgent cooperation may be needed (such as online disinformation) and establish a framework for collaboration with the help of platforms, civil society and other experts. Article 37 of the proposed Digital Services Act foresees that the European Commission can initiate the drawing up of crisis protocols to coordinate a rapid and cross-border response in extraordinary circumstances such as acts of terrorism, pandemics. Compliance officers can be the point of contact for these crisis protocols within platforms.
[21] See for instance GDPR, arts. 5(2) and 24(1).
[22] However, reversals of the burden of proof have been suggested in the form of a presumption in favour of interoperability and in the context of the assessment of mergers in digital ecosystems as well as regarding the abusive nature of self-preferencing behaviour by dominant digital platforms under EU competition law. See Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era' (2019) Expert report for Commissioner Vestager.
[23] See I. Graef and S. Van Berlo, 'Towards Smarter Regulation in the Areas of Competition, Data Protection and Consumer Law: Why Greater Power Should Come with Greater Responsibility', European Journal of Risk Regulation 2020.
[24] See ACM Guidelines of 11 February 2020 on the protection of the online consumer: boundaries of online persuasion.

should be logical and fair and default setting should be favourable to users.[25] In its 2020 final report on online platforms and digital advertising, the UK Competition & Markets Authority proposes the imposition of a duty of 'fairness by design' on platforms with strategic market status.[26] The proposal for an EU Data Governance Act requires data intermediaries offering services to data subjects to take up a fiduciary duty to act in the data subjects' best interest when facilitating the exercise of their rights 'in particular by advising data subjects on potential data uses and standard terms and conditions attached to such uses'.[27]

However, empowering users will not be enough. **Users need to be proactive** and regulators should be able to crowdsource information[28] and oversight from the business and the end-users of the platforms to complement their public oversight with private oversight.

2.5. Delegated oversight to independent auditors

Regulators could also be supported by independent auditors or trustees. In this case, the oversight body would oversee "independent platform auditors" who would, in turn, need to make sure that platforms meet standards of accuracy set out by regulators or legislation in their transparency reports. For instance, the EU telecommunications regulation foresees that competent authorities should be allowed to request from electronic communications service providers that they should submit to a security audit carried out by a qualified independent body or a competent authority and make the results thereof available to the competent authority; the cost of the audit should be paid by the provider.[29]

Regulators would retain investigation and enforcement powers towards platforms, but the reporting duties of platforms would be normalised and overseen by independent external auditors who would themselves be overseen by the regulators. Alternatively, regulators could be given the power to call on auditors or experts to assist when they need to carry out special tasks such as on-site inspections or to check and analyse big data.[30]

Questions for the debate

- Do you agree that the new role of a regulatory agency in the fast changing and uncertain digital economy is to orchestrate an ecosystem of enforcement, which implies a cooperative regulatory oversight and enforcement model?

- From your experience, do you think that self-regulation and co-regulation can be effective and which are the conditions for their effectiveness?

- From your experience, do you think that risk assessment can be effective and which are the conditions for their effectiveness?

- How can users be better empowered to make decisions in their interests?

[25] A. de Streel and A.L. Sibony, *Towards Smarter Consumer Protection Rules for the Digital Society*, CERRE Policy Report, October 2017

[26] See UK CMA Online platforms and digital advertising Market study final report of 1 July 2020.

[27] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020, COM(2020) 767 final, art. 11(10) and recital 26.

[28] For examples of information crowdsourcing, see French regulators, New regulatory mechanisms – data-driven regulation, pp.6-9.

[29] EECC, art.41(2b).

[30] The possibility for the European Commission to appoint independent experts/auditors is foreseen in Articles 21.2 and 24.2 of proposed DMA and in Articles 54 and 57 of the proposed DSA.

3. Towards data-based and computational enforcement

Next to orchestrating an effective oversight and enforcement ecosystem, regulators should be capable of understanding the technologies based on data and AI which are increasingly used by the platforms they oversee as well as developing their oversight tools based on data and AI.[31]

3.1. Better use of data and AI by regulatory agencies

To fully understand business models that are increasingly based on data and AI, regulators should have extensive and proportionate **power to request information on databases and algorithms** from platforms and their (business and end) users.[32] Inspiration could perhaps be taken from the financial auditing sector, whereby the normalisation of transparency in financial auditing has been achieved.[33]

However, this investigation power will only be exercised effectively if regulators have the **human and technical capability of analysing and interpreting the very large volumes and variety of data** that will be provided by the platforms.[34] For instance, in the *Google Shopping* antitrust investigation, the Commission had to analyse very significant quantities of real-world data including 5.2 Terabytes of actual search results from Google (around 1.7 billion search queries).[35]

In turn, this requires that the regulator sets up **in-house dedicated teams of data analysis and AI specialists**. For instance, the French authorities have set up the *Pôle d'expertise de la régulation numérique* (PEReN), which offers digital expertise to the French regulatory administrations, and the French Competition Authority has established a digital unit.[36] In the UK, the CMA has set up CMA's Data, Technology and Analytics (DaTA) unit[37] and Ofcom has created an Emerging Technology directorate and data science team. In the Netherlands, the ACM, the Authority for the Financial Markets (AFM) and the Healthcare Authority (NZa) are integrating data science within their operations.[38] Regulators may also conclude partnership agreements with outside vetted and independent researchers as foreseen by the Proposed DSA.[39]

Going one step further and following the Commission's White Paper on AI,[40] regulators may also **develop their own AI tools to process the data to be analysed**. The use of AI by regulators to improve their operations is often referred to as *Suptech* and *Regtech*.[41] In practice, AI techniques are increasingly used by financial regulators[42] and are starting to be used by competition agencies.[43]

---

[31] World Economic Forum, Agile Regulation for the Fourth Industrial Revolution A Toolkit for Regulators, pp.27-31.
[32] Prop DSA, art.31, 41(1) for national authorities and 54(3) for Commission; Proposed DMA, art.19.1.
[33] Online Harms: Bring in the Auditors by Institute for Global Change, available at https://institute.global/policy/online-harms-bring-auditors and Analysis, Applying the Principles of Audit to Online Harms Regulation, 30 July 2020, available at https://institute.global/policy/analysis-applying-principles-audit-online-harms-regulation.
[34] See the very interesting Position paper of Oversight of Algorithms by the Dutch ACM.
[35] See Commission Press Release of 27 June 2017.
[36] See Pôle d'expertise de la régulation numérique (PEReN) and French Competition Authority has established a digital unit.
[37] This DaTA unit has just produced a very interesting paper on how algorithms can reduce competition and harm consumers.
[38] See https://www.acm.nl/nl/organisatie-werken-bij-de-acm-studenten-en-starters-data-science-traineeship-acm-afm-en-nza/data-science-bij-acm-afm-en-nza.
[39] Prop DSA, art.31(1). For examples of such cooperation, see French regulators, New regulatory mechanisms – data-driven regulation, pp.4-5.
[40] Communication White Paper of 19 February 2020 on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65, p.8.
[41] On the topic, see also the Conference organised by the Club of Regulators in cooperation with the OECD Network of Economic Regulators, *RegTechs: Feedback from the First Experiments*, available at: http://chairgovreg.fondation-dauphine.fr/node/708.
[42] See for instance the Data Science/Artificial Intelligence (Datalab) excellence hub created in 2018 within the French financial regulator.
[43] T. Schrepel, Computational Antitrust: An Introduction and Research Agenda, Computational Antitrust project at Stanford University, CodeX Centre (The Stanford Centre for Legal Informatics), January 2021.

AI tools can be used to improve the operations of the regulatory agencies, but they may also be used to **better empower users**. Interesting examples are the *Claudette* project which offers a tool for consumers to check the legality of Terms and Conditions against EU consumer protection rules[44] or the *Open Terms Archive & Scripta Manent* developed by the French *Pôle d'expertise de la régulation numérique* (PEReN) which offers a tool to track the evolution of Terms and Conditions provided by the main digital platforms.[45] Thus, regulators may also stimulate the development and the deployment of AI tools to help the users in their private enforcement.

3.2. Compliance by design

A more radical step consists in by-passing (or supplementing) the regulatory oversight by **"coding" legal requirements directly into the algorithms**.[46] Thereby, the legislative code could be replaced (or supplemented) by the computer code; in the words of Lawrence Lessig, the East Coast rules (the Congress) could be replaced by the West Coast code (the Silicon Valley platforms).[47] This is surely an interesting avenue to pursue as the progress of AI technologies will offer more opportunities for such a model of compliance by design. Already today, some EU laws are imposing such a model, for instance, the GDPR is imposing privacy by design.[48]

However, two important safeguards and cautions are in order. First, not every legal requirement can be coded in an algorithm, in particular, because the legislative rule is often open and subject to interpretation while computer code should be closed and not flexible. Open norms are a feature of the legal system but an imprecise code is a bug in computer programming. Second, the rules must be ultimately decided by an elected legislator and not by privately owned and managed digital platforms. Thus, it is **only the closed rules which have been decided by an elected legislative body that could be coded**.

Questions for the debate

- Do you think AI could contribute to improve your operations as regulatory agencies? If yes, for which tasks and under which conditions? Are you in the process of developing AI tools?

- From your experience, do you think that compliance (privacy, consumer protection, competition …) by design can be effective and which are the conditions for their effectiveness? Should requirements of compliance by design be imposed on all platforms or only on the especially powerful ones?

4. Towards experimental enforcement

4.1. Innovation and firms' experimentation

[44] http://claudette.eui.eu/use-our-tools/index.html

[45] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/team-blog/article/open-terms-archive-scripta-manent

[46] For instance platforms could limit the ability for anonymous adults to contact children as suggested in para 29 of the UK government's response to the consultation on the Online Harms White Paper, 15 December 2020.

[47] L. Lessig, *Code and other laws of cyberspace*, Basic Books, 1999.

[48] GDPR, art.25(1): *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.* See for more details the Guidelines 4/2019 of the European Data Protection Board of 20 October 2020 on Data Protection by Design and by Default.

Regulators should provide support for innovations at the design, proof of concept and testing stages, or for the further ongoing development of existing innovative products/services.

To achieve such an objective, the **legislator may directly provide in the law innovation exemptions or experimentation clauses**.[49] For instance, to allow innovation in the development of Autonomous Vehicle while ensuring safety, the new Approval and Market Surveillance of Vehicles Regulation includes a procedure for manufacturers to obtain, under specific cumulative conditions, a type-approval if they use new technologies or new concepts that prevent from complying with the relevant requirements.[50] These type-approvals can only be issued if the manufacturer (i) justifies why new technologies or concepts prevent compliance with the relevant requirements; (ii) ensures a level of safety equivalent to that provided by the relevant requirements, and (iii) provides test results to ensure a similar safety level.

Another possibility is that **regulators offer regulatory sandboxes** to innovators to experiment with new products or services with a temporary exemption of regulation. For instance, the UK Financial Conduct Authority has a sandboxes programme[51] and France Experimentation, a department of the French administration, can suspend the application of regulation for innovators.[52]

4.2. Regulatory experimentation

Given the novelty of many regulatory issues and remaining unknowns, errors of type 1 (over-intervention) and type 2 (under-intervention) are inevitable but they should be minimised. One way to minimise errors is to learn from experience. NESTA, a UK innovation foundation, calls for an 'anticipatory regulation' stating that: [53]

> *"When regulators have to take on new functions for which they lack an established playbook, or need to deal with uncertain market developments, a flexible, iterative learning approach is needed rather than a 'solve-and-leave' mentality. Where regulations are being developed for a new area or introduce substantial changes, it is difficult to know exactly what the impacts will be. Utilising a more experimental, trial and error approach, at least at the beginning, rather than immediately creating definitive rules can help build evidence on what works to achieve the desired outcomes. Standards, testbeds/sandboxes, or exhorting best practice are different ways in which regulators can provide more flexible interventions.*"

Experimentation can be done *ex ante* before regulatory action is adopted by running A/B testing of different types and design of the intervention. One of the advantages of digital technologies is that such experiments are less costly to run than before and indeed, online platforms now commonly run A/B testing before launching new products or services. Such A/B testing may take place in different manners. One possibility is that the regulators require the platforms to test with their users' different product changes and report the results to the regulator for it to decide the best course of action. Another possibility is to allow the regulator to access the algorithm to analyse the outcome delivered by such an algorithm of different courses of action.[54]

---

[49] World Economic Forum, Agile Regulation for the Fourth Industrial Revolution A Toolkit for Regulators, p.16.
[50] Regulation 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, OJ [2018] L 151/1, art.39.
[51] https://www.fca.org.uk/firms/innovation/regulatory-sandbox-prepare-application;
[52] https://www.modernisation.gouv.fr/nos-actions/france-experimentation/france-experimentation-le-registre-des-experimentations-ouvertes.
[53] Armstrong et al, Renewing regulation 'Anticipatory regulation' in an age of disruption, NESTA, March 2019, p.27.
[54] G. Parker, G. Petropoulos and M. Van Alstyne, Platform Mergers and Antitrust, January 2021.

More generally, any form of regulatory intervention is an experiment that should be **evaluated *ex post*** by assessing the relevance, effectiveness, and efficiency of the intervention after some time of implementation.[55]

Questions for the debate

- How can regulation promote – instead of impede – the development and the diffusion of innovation? Do you have to apply innovation exemption/experimentation clause? Do you offer regulatory sandboxes?

- Do you see interest and added-value in requiring more experimentation to be done by the regulated undertaking in the design of regulatory remedies and in adapting those remedies over time?

[55] On ex post regulatory evaluation: Commission Staff Working Document of 7 July 2017, Better Regulation Guidelines, SWD(2017)350, Chapter VI.