

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Contribution to growth

De Streel, Alexandre; Hocepied, Christian

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

[Link to publication](#)

Citation for published version (HARVARD):
De Streel, A & Hocepied, C 2019, *Contribution to growth: european digital single market : delivering improved rights for European citizens and businesses*. European Parliament, Luxembourg.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Contribution to Growth: European Digital Single Market

Delivering improved rights for
European citizens and
businesses

Abstract

This study reviews all the rules adopted during the 8th Parliamentary legislature (2014-2019) to strengthen the Digital Single Market. On that basis, the report analyses the rights and obligations as well as the institutions and procedures created or improved in the main policy fields of the Digital Single Market (e-commerce and online platforms, e-government, data and AI, cybersecurity, consumer protection and electronic communications networks and services). Finally, the report identifies remaining gaps and possible actions for the forthcoming Parliament's legislature.

This document has been prepared for the IMCO Committee at the request of the Policy Department A of the European Parliament.

This document was requested by the European Parliament's Committee on the Internal Market and Consumer Protection.

AUTHORS

Prof. Dr Alexandre de STREEL, University of Namur and CERRE (Centre on Regulation in Europe)
Christian HOCEPIED, University of Namur
With the assistance of Michael LOGNOUL and Zorana ROSIC, University of Namur

ADMINISTRATOR RESPONSIBLE

Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT

Irene VERNACOTOLA

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Economic, Scientific and Quality of Life Policies
European Parliament
L-2929 - Luxembourg
Email: Poldep-Economy-Science@ep.europa.eu

Manuscript completed: May 2019

Date of publication: May 2019

© European Union, 2019

This document is available on the internet at:
<http://www.europarl.europa.eu/supporting-analyses>

DISCLAIMER AND COPYRIGHT

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

For citation purposes, the study should be referenced as: de STREEL, A., *Contribution to Growth: European Digital Single Market. Delivering improved rights for European citizens and businesses*, Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019

CONTENTS

LIST OF FIGURES	4
LIST OF TABLES	4
LIST OF ABBREVIATIONS	5
EXECUTIVE SUMMARY	6
1. INTRODUCTION	11
2. POLICY AND REGULATORY TECHNIQUES TO BUILD THE DIGITAL SINGLE MARKET	13
2.1 EU substantive rules: Unification or harmonisation of national rules	14
2.2. EU procedural rules: Unification or harmonisation of enforcement	17
2.3. Non regulatory techniques to reduce national divergences	18
3. MAIN ACHIEVEMENTS DURING THE 8TH PARLIAMENTARY LEGISLATURE	19
3.1. E-commerce and Online platforms	23
3.2. E-Government	28
3.3. Data and Artificial Intelligence	32
3.4. Security	36
3.5. Consumer Protection in the digital era	40
3.6. Electronic Communications Networks and Services	42
4. FUTURE POTENTIAL OF THE DIGITAL SINGLE MARKET AND POSSIBLE INITIATIVES	46
4.1 Applying and evaluating the newly adopted rules	47
4.2. Digitalizing and deepening the single market	47
4.3. Smart policy and regulatory techniques	50
REFERENCES	51
ANNEX LIST OF DIGITAL SINGLE MARKET LEGAL INSTRUMENTS	53

LIST OF FIGURES

Figure 1:	The Six Building blocks of the Digital Single Market	12
Figure 1:	Feedback loops between platform scale-up and single market	49

LIST OF TABLES

Table 1:	Main achievements of the 8th legislature to stimulate the Digital Single Market	9
Table 2:	List of legal instruments adopted or proposed during the 8th Legislature to build the Digital Single Market	21
Table 3:	EU rules regarding e-commerce and online platforms	26
Table 4:	EU rules regarding e-government	31
Table 5:	EU rules regarding data and AI	35
Table 6:	EU rules regarding security	37
Table 7:	EU rules regarding consumer protection	41
Table 8:	EU rules regarding electronic communications networks and services	45

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programme Interface
AVMS	Audio-Visual Media Services
BEREC	Body of European Regulators for Electronic Communications
CPC	Consumer Protection Cooperation
CSIRT	Computer Security Incident Reponse Team
DCD	Digital Content Directive
DESI	Digital Economy and Society Index
DSM	Digital Single Market
EECC	European Electronic Communications Code
EESSI	Electronic Exchange of Social Security Information
EIDAS	electronic IDentification, Authentication and trust Services
ENISA	European Network Information Security Agency
ERGA	European Regulators Group for Audiovisual Media Services
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
HPC	High Performance Computing
IOT	Internet of Things
NIS	Network Information Security
P2B	Platform-to-Business
PSI	Public Sector Information
RSPG	Radio Spectrum Policy Group
TLS	Internet Top Level Domain
UCPD	Unfair Commercial Practices Directive
VAT	Value Added Tax

EXECUTIVE SUMMARY

In May 2015, the European Commission launched a very ambitious agenda to strengthen the Digital Single Market (DSM) for Europe that led to a very intense activity of the European Parliament in this field during the 8th legislature (2014-2019). This Study analyses (i) the barriers eliminated or reduced by specific DSM legislative measures, (ii) the specific rights and obligations as well as the legal institutions or procedures introduced or improved by those measures and (iii) the remaining gaps and possible actions for the forthcoming Parliament's legislature. The Annex lists all the specific legislative measures adopted during the 8th legislature.

The Study is organised as follows: (i) the first section explains the policy techniques used by the EU institutions to stimulate the DSM (*how* it was achieved), (ii) the second section reviews the different measures adopted in the main building blocks of the DSM, the rights and obligation they have established and the barriers to the internal market they have removed (*what* was achieved) and (iii) the third section proposes future reforms for the next Parliamentary legislature.

1. Policy and regulatory techniques to achieve the Digital Single Market

The EU institutions may rely on **diverse policy techniques to build the Digital Single Market** and remove barriers to trade between Member States. Some techniques are regulatory and aim, on the one hand, to unify or harmonise across the EU the substantive rules and, on the other hand, to unify or harmonise the enforcement of those rules. Other techniques are non-regulatory and rely on action plans, policy benchmarking or financial support.

EU unification and harmonisation of the substantive rules can be achieved with hard law, in particular Regulations that are directly applicable or Directives that need to be transposed into national law. They can also be stimulated with the soft-law, in particular with Recommendations or Guidelines giving interpretation of existing EU laws or recommending particular approach in national laws or with Codes of conduct or Memorandum of Understanding to involve more closely stakeholders in the elaboration of the rules (participatory regulation). **In the digital field, Regulations have been used extensively** and represent a higher proportion of legislative acts than in other EU policy fields. In addition, **several Recommendations and Guidelines** have been adopted to ensure a common interpretation of those rules. Finally, multiple **Codes of conduct** were agreed by the industry to supplement or substitute the adoption of hard-law.

However, common EU rules are not enough to achieve the single market if those rules are implemented by national authorities differently across the Member States. This is why many institutional and procedural rules are needed to **unify or harmonise across the EU the enforcement mechanisms**. They should respect the constitutional and procedural autonomy of the Member States. **In the digital field, many procedural rules were adopted to improve the quality of the national enforcement agencies as well as their cooperation at the EU level**, in particular through the establishment or the strengthening of EU networks of agencies.

Next to rules, **non-regulatory actions** are also key to stimulate the single market, in particular in area where the adoption of legislation is difficult or not appropriate. In the digital field, numerous **policy action plans** were adopted to coordinate EU and national digital policies. **Benchmarking** of national digital policies to diffuse best practices across the Member States are also common. Finally, increasing amount of **EU funds** have been allocated to digital initiatives.

2. Main achievements in removing barriers in the Digital Single Market during the 8th legislature

During the 8th legislature, the European Parliament and the other EU institutions have been very active in the digital field. To review the numerous achievement, we present **the DSM measures into six building blocks**. The two first blocks relate to the digital services used by European consumers and citizens: the e-commerce and online platforms and the e-government services. The three successive blocks are horizontal and necessary to ensure the development of and the trust in private and public digital services; they relate to data and AI, security and the specific consumer protection for the digital era. Finally, the last block relates to the infrastructures on which the digital applications are provided: the electronic communications networks and services. Most of policy actions **during the 8th legislature took place for e-commerce and online platforms as well as for data and AI**.

For each building block, we analyse, as summarised in Table 1 below, how the specific DSM measures (i) **directly facilitate cross-border trade** by removing specific barriers to the single market, (ii) **unify or harmonise the national substantive rules** which indirectly ease cross-border operations and create specific rights and obligations and (iii) **unify or harmonise the enforcement** of those rules and establish legal institutions and procedures which also indirectly ease cross-border operations.

Regarding **e-commerce and online platforms**, some of the main impediments to cross-border trade have been removed or reduced with the cross-border portability of some digital content, the prohibition of unjustified geo-blocking, the simplification of VAT declaration and collection, the improvement of eu. Top Level Domain and the new copyright rules facilitating access to online TV and radio content across borders. Moreover, several national rules on the operations of online platforms have been harmonised, in particular for platforms offering audio-visual media services and intermediation services as well as platforms hosting illegal or harmful online content. To ensure effective and harmonised enforcement of those rules, ERGA - the network of national media regulators - has been strengthened.

Regarding **e-government**, which remains a national competence, the EU institutions can merely stimulate the adoption and the diffusion of best practices across the Member States as well as facilitate the interoperability between the different national public services, as for example by the setting up a single digital gateway. The EU is also leading by example by digitizing its own public services.

Regarding **data and AI**, data location requirements have been limited. Moreover, several national rules on the governance of data have been harmonised in order to ease cross-border data businesses and the movement of data across the EU while ensuring strict privacy protection and respecting EU values and fundamental rights. This is the case for personal data with the now famous General Data Protection Regulation (GDPR), for public data with the new Open Data and Public Sector Information Directive and for non-personal and non-public data where best practices for data sharing have been established. To ensure effective and harmonised enforcement of data protection rules, a new European Data Protection Board (EDBP) has been established between the national data protection authorities. In addition, a plan to stimulate AI in Europe has been coordinated between the EU and the Member States and new EU funds are being made available.

Regarding **security**, an EU cyber-security culture is emerging. New cooperation between cybersecurity agencies have been set up, ENISA will become an EU level Cybersecurity agency, a new EU Competence Centre has been set up and EU funds have been made available to strengthen network security.

Regarding **consumer protection**, an adaptation of the existing consumer acquis to the characteristics of the digital sector, in particular the lack of monetary prices and the difficulties to understand the

functioning of algorithms, has been adopted. A strengthening of the cooperation between national consumer protection authorities has also been agreed.

Regarding **electronic communications networks and services**, rules were adopted to deal with specific cross-border issues such as international roaming calls or international calls. EU harmonised rules were reviewed in order to ease entry and spectrum use, thereby stimulating private investment and to protect consumers. The cooperation between national regulatory authorities was slightly strengthened with the reform of BEREC. More EU funds were made available to support the deployment of new fibre and 5G infrastructures.



Table 1: Main achievements of the 8th legislature to stimulate the Digital Single Market

	E-commerce and online Platforms	E-Government	Data and AI	Security	Consumer protection in the digital era	Electronic communications networks and services
EU rules facilitating cross-border trade	<ul style="list-style-type: none"> - Cross-border portability content - Geo-blocking - VAT e-commerce - Cross-border parcel delivery - .eu top domain level - Facilitating cross-border access to online TV and radio content 	<ul style="list-style-type: none"> - Digital Single Gateway - VAT One Stop shop 	<ul style="list-style-type: none"> - Limitation of data location requirements 	<ul style="list-style-type: none"> EU cybersecurity certification 		<ul style="list-style-type: none"> - International roaming - International calls - EU numbering space
Unification or harmonisation of national rules	<ul style="list-style-type: none"> - Media services - Transparency for online platforms - Effective removal of illegal content online 	<ul style="list-style-type: none"> - Interoperability framework 	<ul style="list-style-type: none"> - Personal data: protection of privacy - Public data: openness - Private data: sharing 	<ul style="list-style-type: none"> - NIS requirements and notification 	<ul style="list-style-type: none"> - Adaptation of the consumer protection rules to the characteristics of digital economy 	<ul style="list-style-type: none"> - Adaptation of telecoms rules to stimulate investment in very high capacity infrastructures (fibre and 5G) while protection consumers - Better coordination of spectrum assignment, in particular the 700 MHz band
Unification or harmonisation of national enforcement	<ul style="list-style-type: none"> - DG COMP Sector enquiry on e-commerce - Strengthening of ERGA 		<ul style="list-style-type: none"> - Establishment of EDPB 	<ul style="list-style-type: none"> - Cooperation in large scale incidents - Network of CSIRT - Strengthening ENISA - EU Cybersecurity Industrial, Technology and Research Centre 	<ul style="list-style-type: none"> - Strengthening CPC Network 	<ul style="list-style-type: none"> - Strengthening of BEREC - Strengthening RSPG
Action plan and coordination of national strategies		<ul style="list-style-type: none"> - eGov Action Plan 	<ul style="list-style-type: none"> - Coordination of AI Strategies 			

3. Future potential of the Digital Single Market and possible initiatives for the next legislature

As many regulatory and non-regulatory actions have been taken during the 8th legislature, the first task is to **implement those new rules in an effective and harmonised manner** across Europe. This is particularly important because most of those EU substantive rules are implemented by national authorities. Then the **efficiency and the effectiveness of the rules and their enforcement should be evaluated**, in particular the impacts on the economy and the society.

However, evaluating the effects of the actions already adopted will not be enough given the importance of the digital technologies for the European economy and society, the rapid pace of evolution of those technologies and the increasing global competition for digital leadership. To respond to changes, the **pace of reform should remain important during the forthcoming 9th legislature**.

Regarding the objectives and policy fields, we have identified the following **priorities**:

- (i) **Make the EU a technological powerhouse for the emerging and important technologies** such as AI, quantum computing, security of connected devices or data exchanges that should be designed and developed according to European values enshrined in the Treaties and the Charter of Fundamental Rights;
- (ii) Stimulate the **development of online platforms**: (i) start-up should be stimulated by rules ensuring a level playing and access to the main capabilities for digital innovation (in particular data) and to the eco-system of products that are used by consumers, (ii) scale-up should be stimulated by one set of rules and enforcement all over Europe, (iii) and significant platforms should be subject to an increased duty of care;
- (iii) Stimulate **e-government**: given the potential benefits of digital public services, the EU should stimulate the adoption and the diffusion of national and cross-borders e-government services as well as the adoption of digital technologies, such as blockchain, to improve public regulation.

Regarding the **policy and regulatory techniques**, we recommend the reliance of **principles-based legislation** that can easily adapt to fast and unpredictable technology and market evolutions **complemented with codes of conduct** agreed with all the digital players (firms, consumers associations, NGOs ...) under the auspices of EU institutions and with a close monitoring by the EU institutions. We also recommend that the **enforcement of those rules is more Europeanised** either with the continuous strengthening of the cooperation network of national regulatory authorities or with the **establishment of a EU regulator for significant platforms** as it was done some years ago for the significant banks with the creation of the Single Supervisory Mechanism within the European Central Bank. The **regulatory authorities in Europe should also size the potential of digital technologies**, such as big data or AI, to improve their operations (*RegTech*). To go further when feasible, enforcement may be automatized in the computer code as it is the case for smart contracts or privacy by design (more generally, *compliance by design*).

Those regulatory actions should be **complemented with non-regulatory initiatives**, in particular the monitoring and exchange of best practices of key digital national policies, the increasing smart use of EU funds to stimulate the deployment and the adoption of key digital networks and services and the development of the digital skills of EU workers and citizens.

1. INTRODUCTION

The Digital Market Strategy

On 6 May 2015, the European Commission launched its Digital Market Strategy for Europe,¹ announcing ambitious legislative steps towards a connected digital single market. The Strategy was built on three pillars:

- *Better access for consumers and businesses to online goods and services across Europe* – by removing of key differences between the online and offline worlds to break down barriers to cross-border online activity;
- *Creating the right conditions for digital networks and services to flourish* – by fostering high-speed, secure and trustworthy infrastructures and content services, through the right regulatory conditions for innovation, investment, fair competition and a level playing field; and
- *Maximising the growth potential of our European Digital Economy* – by promoting investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competitiveness as well as better public services, inclusiveness and skills.

At the same time, the Commission stressed, that these actions must “*go hand-in-hand with efforts to boost digital skills and learning across society and to facilitate the creation of innovative start-ups*” and that “*enhancing the use of digital technologies and online services should become a horizontal policy, covering all sectors of the economy and of the public sector.*”² The European Parliament welcomed this programme in a Resolution of 19 January 2016 on a Digital Single Market Act and called for ambitious actions.³

Aims of this Study

This study aims to update, for the Digital Single Market, the findings related to EU digital policies of Civic Consulting Study (2014) on the Contribution of the Internal Market and Consumer Protection to Growth. To do that this Study analyses (i) the barriers eliminated or reduced by specific DSM legislative measures adopted during the 8th legislature (2014-2019), (ii) the specific rights and obligations as well as the legal institutions or procedures introduced or strengthened by those measures and (iii) the potential future initiatives that should be elaborated and discussed during the forthcoming 9th legislature. This Study focuses on legal issues and is complemented by the companion economic study on the benefits of the European Digital Single done by Dr. Scott Marcus and his team at Bruegel.

To analyse the numerous achievement, we organise the DSM measures into six building blocks following Maciejewski (2015:19) as explained in Figure 1 below.

¹ Communication from the Commission of 6 May 2015, A Digital Single Market Strategy for Europe, COM(2015) 192. See <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market> and <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market>

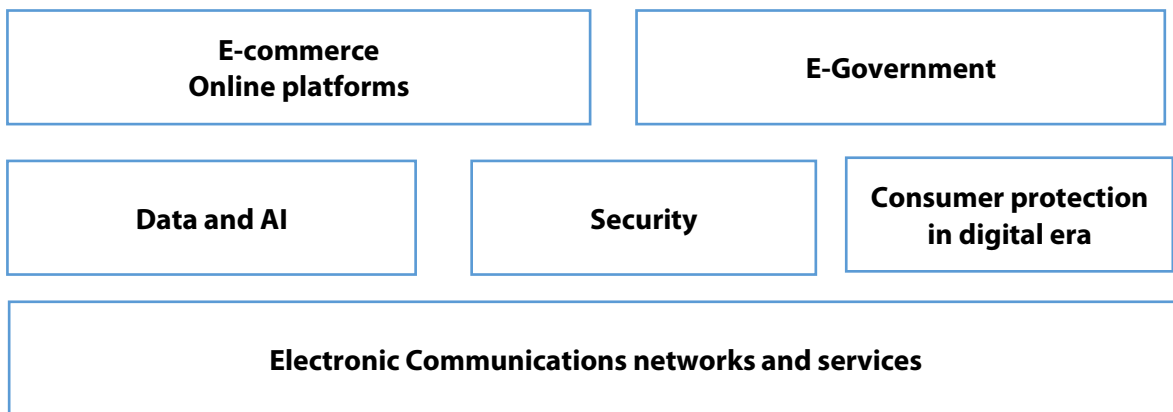
² Idem, p. 2.

³ 2015/2147 (INI).

The two first blocks relate to private and public digital applications used by European consumers and citizens: the e-commerce and online platforms and the e-government services.

The three successive blocks are horizontal and necessary to ensure the development of and the trust in private and public digital services: they relate to data and AI, security and the specific consumer protection for the digital era. Finally, the last block relates to the infrastructures on which digital applications are provided: the electronic communications networks and services.

Figure 1: The Six Building blocks of the Digital Single Market



The Study is organised as follows: After this brief introduction the first section explains the policy techniques used by the EU institutions to stimulate the DSM (*how* it was achieved). Then, the second section reviews the different measures adopted in the main building blocks of the DSM, the rights and obligation they have established and the barriers to the internal market they have removed (*what* was achieved). Finally, the third section proposes future reforms for the next Parliamentary legislature. The Annex lists all the specific legislative measures introduced during the 8th Parliamentary legislature.

2. POLICY AND REGULATORY TECHNIQUES TO BUILD THE DIGITAL SINGLE MARKET

KEY FINDINGS

The EU institutions may rely on **diverse policy techniques to build the Digital Single Market** and remove barriers to trade between Member States. Some techniques are regulatory and aim, on the one hand, to unify or harmonise across the EU the substantive rules and, on the other hand, to unify or harmonise the enforcement of those rules. Other techniques are non-regulatory and rely on action plans, policy benchmarking or financial support.

EU unification and harmonisation of the substantive rules can be achieved with hard law, in particular Regulations that are directly applicable or Directives that need to be transposed into national law. They can also be stimulated with the soft-law, in particular with Recommendations or Guidelines giving interpretation of existing EU laws or recommending particular approach in national laws or with Codes of conduct or Memorandum of Understanding to involve more closely stakeholders in the elaboration of the rules (participatory regulation). **In the digital field, Regulations have been used extensively** and represent a higher proportion of legislative acts than in other EU policy fields. In addition, **several Recommendations and Guidelines** have been adopted to ensure a common interpretation of those rules. Finally, multiple **Codes of conduct** were agreed by the industry to supplement or substitute the adoption of hard-law.

However, common EU rules are not enough to achieve the single market if those rules are implemented by national authorities differently across the Member States. This is why many institutional and procedural rules are needed to **unify or harmonise across the EU the enforcement mechanisms**. They should respect the constitutional and procedural autonomy of the Member States. **In the digital field, many procedural rules were adopted to improve the quality of the national enforcement agencies as well as their cooperation at the EU level**, in particular through the establishment or the strengthening of EU networks of agencies.

Next to rules, **non-regulatory actions** are also key to stimulate the single market, in particular in area where the adoption of legislation is difficult or not appropriate. In the digital field, numerous **policy action plans** were adopted to coordinate EU and national digital policies. **Benchmarking** of national digital policies to diffuse best practices across the Member States are also common. Finally, increasing amount of **EU funds** have been allocated to digital initiatives.

The Digital Single Market Strategy relies on different regulatory and non-regulatory techniques. Legislation appears to be, by far, the privileged approach. The ‘acquis’ is impressive and will still require many years to be fully implemented because implementation in practice often require periods longer than a Parliament legislature. The number of Commission Communications reflects the absence of executive powers at EU level. Instead of launching specific projects – which the Commission successfully did for example for the Electronic Exchange of Social Security Information (EESSI) – the Commission is obliged to promote best practices and general principles, without certainty of effective results. Another finding is that the Digital Single Market cannot be forced through a top down approach.

Public private partnerships, test projects and other research networks play a key role in developing applications that will give a face to the concept of digital and show its benefits.

The Commission has clearly understood this as reflected by its proposed Digital Europe programme for the period 2021-2027. More than regulation, funding is the lifeblood of digitization.

2.1 EU substantive rules: Unification or harmonisation of national rules

a. Types of EU legal instruments

Regulations are legislative acts that can directly be enforced by national courts in the EU. Regulations must be applied in their entirety across the EU. However, the use of Regulations does not suffice to achieve full harmonization of the national rules. Some provisions of Regulations may not be directly applicable and yet require further implementation measures or interpretations.⁴ **Directives** are legislative acts that set out a goal that all EU countries must achieve. Directives are binding for the Member States, but normally not for citizens and undertakings. It is up to the individual countries to devise their own laws on how to reach these goals. However, national measures transposing Directives must be of a binding character and not merely in the form of administrative practices. Some Directives do however go further than setting goals. They can require Member States to set up national regulatory authorities and give them far-reaching powers. This is the case in the telecom and postal sectors, for the broadcasting sector, data protection and, increasingly, in the area of consumer protection. **Decisions** are binding on those to whom it is addressed (e.g. an EU country or an individual company) and are directly applicable. Decisions are rarely used in the digital sector.⁵

Recommendations can, in principle, not be enforced in national courts. A Recommendation allows the EU institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed. However, national courts have considered that national authorities have not complied with obligations under national law to give reasons for their decisions when these decisions diverged from the line of action recommended by the Commission, without the national authority providing adequate justifications for its own line of action. Recommendations – which can be named ‘guidelines’ or ‘communication’ – go beyond peer pressure and naming and shaming exercises, like the Digital Economy and Society Index (DESI).⁶ Recommendations play an essential role to ensure that national policies – though autonomous – are designed with the better functioning of the EU economy in mind.⁷

⁴ For example, Article 8 GDPR determines 16 as the relevant age of consent for minors when using information society services, but allows Member States to lower the age to 13 years. Many Member States have done so. In addition, the GDPR does not encroach on the principle of procedural autonomy, and Member States legislated on the organization of their national DPA(s) and the rules of procedure to be followed by the latter. On the other hand, the GDPR empowers the European Data Protection Board (EDPB) to adopt interpretative guidelines, stressing that, despite common rules, national practices are susceptible to remain different.

⁵ An example is the 700 MHz spectrum decision 2017/899, which requires that Member States would no later than 30 June 2018, adopt and make public their national plan and schedule (‘national roadmap’), to make this frequency band available for wireless broadband electronic communications services under harmonized technical conditions.

⁶ <https://digital-agenda-data.eu/datasets/desi/indicators>

⁷ For example, the Commission sets out principles and guidance on business to business (B2B) data sharing agreements, as well as on business to government (B2G) data sharing agreements, promoting voluntary harmonisation of practices across the EU.

b. Objectives of legal instruments

More than the instrument chosen, the content and nature of the solutions chosen to tackle the remaining barriers to the digital single market matters. This content can diverge on the following aspects.

Negative and positive integration

European integration studies firstly distinguish between negative and positive integration. **Negative integration** refers to provisions in EU law (or case-law) requiring Member States to remove certain national measures, no matter how the obstacle disappear.⁸ **Positive integration** addresses the fragmentation resulting from national rules with the adoption of common rules and regulatory standards across the EU, i.e. requires the Member States to adopt specific rules or principles and not only to prohibit Member States to enact measures restricting trade.

Country of origin and country of destination

Another distinction is between, on the one hand, the home state control or country of origin principle (mutual recognition) and, on the other hand, the country of destination' principle.⁹ The country of origin principle is the cornerstone of the Services Directive,¹⁰ but the Directive excludes several services from its scope, notably financial services, transport, telecommunications network services, gambling, health and certain social services.

In the telecommunications sector, the Commission proposed in 2013 to introduce the country of origin principle for the provision of electronic communications networks and services¹¹ to remove unnecessary obstacles in the authorisation regime and in the rules applying to service provision so that an authorisation obtained in one Member State is valid in all Member States, and that operators can provide services on the basis of consistent and stable application of regulatory obligations. But the proposal was not accepted. Besides the fear of some Member States to lose the control of operators active in their jurisdictions, the main reason seems to have been that every Member State would depend on the market surveillance of its neighbours. Consequently, weaknesses in the organisation of market surveillance in one single Member State could seriously undermine the efforts taken by other Member States and creates a weak link in the chain.

The reluctance of Member States to accept the country of origin principle implies that the country of destination principle underlies most of the EU legislation governing the Digital Single Market. The AVMS Directive, the e-commerce Directive and some copyright rules constitute exceptions.

⁸ An example of such provision is Article 92 of the EEC, which prohibits any discrimination on the basis of residence or nationality by providers of electronic communications networks or services, unless such different treatment is objectively justified.

⁹ This distinction originates from the Court of Justice, when specifying the underlying principles of the free movement of goods enshrined in the TFEU (at the time EEC Treaty) in respectively Case 120/78 *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein* and Case C-267/91 and C-268/91, *Keck and Mithouard*,.

¹⁰ Directive 2006/123 of 12 December 2006 on services in the internal market, OJEU L 376, 27.12.2006, p. 36.

¹¹ Article 3 of the proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627.

This fact explains largely why the voluminous acquis could not tackle yet the fragmentation of national markets remains in the EU.

Maximum and minimum harmonization

The country of destination principle is thus one of the causes of the regulatory fragmentation of the single market because Member States impose more detailed and often more onerous obligations than those listed in the EU rules (regulatory gold-plating). To deal with this unintended consequence of harmonization legislation, maximum harmonisation is becoming more common. This does not mean that EU law would replace national law and constitute a uniform law applicable to the whole EU. Member States can still regulate the sector or activity as far as they do not impose more stringent obligations as regards the issues covered explicitly by the EU instruments.

However, the success of measures aimed at maximum harmonisation may be undermined by national legislation circumventing the scheme laid down in European rules.¹² In addition, given the preference of some for a high level of protection, the maximum harmonization risks being set at a level that dissuades commercial offers and investment, bringing the contrary of the aim pursued of boosting the offer of digital services and investment in digital networks.¹³

Maximum harmonisation is a goal worth pursuing, but is not the silver bullet to bring the single market. Even in the case of maximum harmonization, there is no guarantee that the rules will be enforced identically in each Member State. Indeed, new legislation, however well-designed, cannot avoid all regulatory gaps and implementation deficits, so that the need for more detailed rule-making and coordination on a transnational basis persist. The enforcement of Union harmonisation legislation remains the Member States' competence. The Court of Justice acknowledges the principle of procedural autonomy of the Member States, meaning that the actions necessary to achieve the objectives set forward by regulations or directives continue to be carried out by Member States' civil servants, except in the areas where the EU legislation gives specified implementation powers to an EU-body. However, until now EU legislator has been reluctant to give implementation powers to EU bodies.¹⁴

¹² An example is provided by the Electronic Communications Authorization Directive which regulates the fees that Member States can ask to telecommunications operators to deploy their electronic communications networks. Local authorities in the Member States are however not precluded to impose annual taxes on network installations such as antennas as long as the 'triggering' factor of the taxes is not related to the authorization to deploy a network. In practice, it might be difficult to establish what the precise 'triggering' factor.

¹³ And deregulation by the EU is legally not straightforward to pursue in the case of shared competences. Indeed, Article 2(2) TFEU implies that the Member States may maintain (or further expand) regulation in all domains where the EU would decide to abolish regulation.

¹⁴ In addition, the case law of the EU Court of Justice does not accept the granting of a wide margin of discretion to EU regulatory bodies. See Case C-270/12, United Kingdom v Parliament and Council, [2014].

2.2. EU procedural rules: Unification or harmonisation of enforcement

The Court of Justice stressed in its case law the balance between the autonomy of national systems to enforce EU law and the imperative of effective and uniform enforcement of EU law across all Member States.¹⁵ However, the concept of effectiveness remains subjective. National patterns of regulation and governance differ, notably, with respect to the power, autonomy and resources allocated to the bodies entrusted with the enforcement of the EU in the various domains of the digital sector. For this reason, the EU has in this 'two-tiered system', sought, where politically acceptable by the Member States, to regulate the regulators that deal directly with the addressees of regulation. However, any stringent or intrusive procedures allowing the Commission to interfere with the decision-making of national regulators are doomed to be blocked by political vetoes from adversely affected member states, or seeking to avoid precedents.

An alternative route was therefore followed: establishing EU enforcement networks grouping national authorities entrusted with the implementation of the EU rules concerned.¹⁶ For example, in the framework of the reform of the Consumer Protection Cooperation (CPC) Regulation, the Commission promoted harmonized rules governing the powers of enforcement authorities and the manner in which they can cooperate. The GDPR also requires, on the one hand, stronger enforcement powers for the national DPAs, while, on the other, ensuring that the DPAs coordinate their approaches via the EDPB. The EDPB's binding dispute resolution system can even lead to harmonised decisions, even in individual cases. This procedure is, today, likely a model to follow in other domains.

Next to public enforcement, the main aim of out of court mechanism is to facilitate dispute resolution by reducing their cost and speed. Moreover, out of court dispute resolution mechanism contribute to the single market in two ways:

- Directly, in the case of on-line resolution mechanisms. The best example is the internet platform created by the European Commission for the settlement of disputes arising from e-commerce. The whole out-of-court dispute resolution processes takes place on the internet, which means that long and expensive trials are avoided and that the European consumer's trust in cross-border shopping is strengthened.
- Indirectly as European legal principles and precedents will more easily be used in such procedures than in formal court proceedings, which are often constrained by the national judicial traditions and vocabulary. For example, the creation of a uniform European insurance market has been facilitated by the application of out-of-court insurance dispute resolution through the European consumer protection regulations under Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution.

¹⁵ Referring to the third paragraph of Article 288 TFEU, the Court held: 'Although that provision leaves Member States to choose the ways and means of ensuring that the directive is implemented, that freedom does not affect the obligation imposed on all the Member States to which the directive is addressed, to adopt, in their national legal systems, all the measures necessary to ensure that the directive is fully effective, in accordance with the objective that it pursues': Case 14/83, *Sabine von Colson et Elisabeth Kamann v. Land Nordrhein-Westfalen*, , ECLI:EU:C:1984:153, point 145.

¹⁶ Commission Communication "EU Law: Better Results through Better Application", 13.12.2016, Pages 5-6.

2.3. Non regulatory techniques to reduce national divergences

Because of the limits of harmonizing or unifying rules at EU level, alternative approaches should be considered to foster the digital single market. Those can be based on EU policy plans to try to influence and possibly coordinating policy actions at the national level, monitoring and benchmarking of national policies to stimulate an exchange of best practices among the Member States or financing support with EU funds. Indeed, EU financing can be a powerful means to accelerate cross-border cooperation.¹⁷

¹⁷ For example in the area of standard setting, the Commission proposes to speed up the standard setting process in five priority domains: 5G, cloud computing, internet of things, data technologies and cybersecurity, and to co-finance the testing and experimentation of technologies to accelerate standards setting, including in relevant public-private partnerships.

3. MAIN ACHIEVEMENTS DURING THE 8TH PARLIAMENTARY LEGISLATURE

KEY FINDINGS

During the 8th legislature, the European Parliament and the other EU institutions have been very active in the digital field. To review the numerous achievement, we present **the DSM measures into six building blocks**. The two first blocks relate to the digital applications used by European consumers and citizens: the e-commerce and online platforms and the e-government services. The three successive blocks are horizontal and necessary to ensure the development of and the trust in private and public digital services; they relate to data and AI, security and the specific consumer protection for the digital era. Finally, the last block relates to the infrastructures on which the digital applications are provided: the electronic communications networks and services. Most of policy actions **during the 8th legislature took place for e-commerce and online platforms as well for data and AI**.

For each building block, we analyse, as summarised in Table 1 below, how the specific DSM initiatives and measures (i) **directly facilitate cross-border trade** by removing specific barriers to the single market, (ii) **unify or harmonise the national substantive rules** which indirectly ease cross-border operations and create specific rights and obligations and (iii) **unify or harmonise the enforcement** of those rules and establish legal institutions and procedures which also indirectly ease cross-border operations.

Regarding **e-commerce and online platforms**, some of the main impediments to cross-border trade have been removed or reduced with the cross-border portability of some digital content, the prohibition of unjustified geo-blocking, the simplification of VAT declaration, the collection and the improvement of eu. Top Level Domain and the new copyright rules facilitating access to online TV and radio content across borders. Moreover, several national rules on the operations of online platforms have been harmonised, in particular for platforms offering audio-visual media services and intermediation services as well as platforms hosting illegal or harmful online content. To ensure effective and harmonised enforcement of those rules, ERGA - the network of national media regulators - has been strengthened.

Regarding **e-government**, which remains a national competence, the EU institutions can merely stimulate the adoption and the diffusion of best practices across the Member States as well as facilitate the interoperability between the different national public services, as for example by the setting up a single digital gateway. The EU is also leading by example by digitizing its own public services.

Regarding **data and AI**, data location requirements have been limited. Moreover, several national rules on the governance of data have been harmonised in order to ease cross-border data businesses and the movement of data across the EU while ensuring strict privacy protection and respecting EU values and fundamental rights. This is the case for personal data with the now famous General Data Protection Regulation (GDPR), for public data with the new Open Data and Public Sector Information Directive and for non-personal and non-public data where best practices for data sharing have been established. To ensure effective and harmonised enforcement of data protection rules, a new European Data Protection Board (EDBP) has been established between the national data protection authorities. In addition, a plan to stimulate AI in Europe has been coordinated between the EU and the Member States and new EU funds are being made available.

Regarding **security**, an EU cyber-security culture is emerging. New cooperation between cybersecurity agencies have been set up, ENISA will become an EU level Cybersecurity agency, a new EU Competence Centre has been set up and EU funds have been made available to strengthen network security.

Regarding **consumer protection**, an adaptation of the existing consumer acquis to the characteristics of the digital sector, in particular the lack of monetary prices and the difficulties to understand the functioning of algorithms, has been adopted. A strengthening of the cooperation between national consumer protection authorities has also been agreed.

Regarding **electronic communications networks and services**, rules were adopted to deal with specific cross-border issues such as international roaming calls or international calls. EU harmonised rules were reviewed in order to ease entry and spectrum use, thereby stimulating private investment and to protect consumers. The cooperation between national regulatory authorities was slightly strengthened with the reform of BEREC. More EU funds were made available to support the deployment of new fibre and 5G infrastructures.

During the 8th legislature, **digital policy has been a key priority and the EU institutions proposed, agreed or adopted many regulatory and non-regulatory actions** in several policy fields to build the digital single market. The most ambitious reforms have been achieved in the field of *e-commerce and online platforms* to stimulate the digital economy while protecting consumers as well as in the field of *data and AI* to ensure that data become a fifth internal market freedom. Then, some important reforms have been agreed in the field of *security and trust* and an EU cyber-security culture begins to emerge and other important reforms are being negotiated to adapt the *consumer protection rules* to the digital environment. Some reforms have been agreed to adapt the EU rules on *electronic communications networks and services* to the increasing needs of connectivity. Finally, the EU continues to stimulate the deployment of *e-government* in the Member States.

Table 2: List of legal instruments adopted or proposed during the 8th Legislature to build the Digital Single Market

E-commerce and online platforms	E-Government	Data and AI	Security	Consumer protection in the digital era	Electronic communications networks and services
Regulation 2017/1128 on cross-border portability of online content services	Regulation 2018/1724 establishing a Single Digital Gateway	Directive 2015/2366 Payment Services	Directive 2016/1148 on Network Information Security	Regulation 2017/2394 on Consumer Protection Cooperation	Regulation 2015/2120 on Open Internet and International Roaming
Regulation 2017/2454 and Directive 2017//2455 on VAT for e-Commerce		Regulation 2016/679 General Data Protection	Regulation 2019/XXX on EU Cybersecurity Act	Directive 2019/XXX Better enforcement and modernisation of EU consumer protection rules	Regulation 2017/920 on wholesale roaming
Regulation 2018/302 on unjustified geo-blocking		Directive 2016/680 Data Police	Regulation 2019/XXX European Cybersecurity Industrial, Technology and Research Centre	Directive 2019/XXX on contracts for the supply of digital content	Decision 2017/899 on use of 470-790 MHz frequency band
Regulation 2018/644 on cross-border parcel delivery services		Regulation 2018/1488 on European High-Performance Computing Joint Undertaking			Regulation 2017/1953 to promote Internet Connectivity in local communities (Wi-Fi4EU)
Directive 2018/1713 VAT on e-publication		Regulation 2018/1807 on free flow of non-personal data			Directive 2018/1972 on European Electronic Communications Code
Directive 2018/1808 amending Audio-Visual and Media Services		Dir. 2019/XXX on open data and the re-use of public sector information			Regulation 2018/1971 on BEREC
Regulation .2019/XXX on .eu Top Level Domain name		<i>Prop. Reg. e-privacy – (2017/1807)</i>			
Directive 2019/XXX on copyright in the Digital Single Market					
Directive 2019/XXX Copyright and					

E-commerce and online platforms	E-Government	Data and AI	Security	Consumer protection in the digital era	Electronic communications networks and services
broadcasting organisations					
Regulation 2019/XXXX P2C fairness and transparency					
<i>Prop. Reg. on terrorist content online (2018/640)</i>					
Communication on European Agenda for collaborative economy (2016/356)	Communication on EU e-Government Action Plan 2016-2020 (2016/179)	Communication on ICT Standardisation Priorities in DSM (2016/176)	Rec. 2017/1584 on coordinated response to large scale cybersecurity incidents	Guidance on the implementation UCPD (2016/163)	Guidelines on market analysis and SMP (2018)
Competition Sector Enquiry e-commerce (2017/229)	Communication on European Interoperability Framework (2017/134)	Communication on European Cloud Initiative (2016/178)	Communication on Making most of NIS Directive (2017/476)		
Recommendation 2018/344 on illegal content online		Communication on Digitising European Industry (2016/180)			
		Recommendation 2018/790 on access to and preservation of scientific information			
		Guidance on sharing private sector data (2018/125)			
		Communication on Building Trust in Human-Centric Artificial Intelligence (2019/168)			

In green: the legislative acts that have been adopted or agreed between the European Parliament and the Council

In yellow: the legislative acts that have been proposed by the Commission and are negotiated between the European Parliament and the Council

In yellow: important soft-law instruments adopted by the Commission

3.1. E-commerce and Online platforms

As part of the Commission's Digital Single Market strategy and its plan to boost e-commerce and online platforms, the Commission announced several measures to promote e-commerce in early June and late May 2016. The European Parliament adopted an important Resolution on 15 June 2017 on online platforms and the digital single market.¹⁸ Legislation was subsequently approved and soft law in the form of communications and guidelines issued.

The **Regulation 2017/1128 of 14 June 2017 on cross-border portability of online content services in the internal market** ensures that subscribers can watch paid-for online content when they are temporarily outside their country of residence. To achieve its aim without encroaching on the right of rightholders to license their works on exclusive basis per Member State, the Regulation requires providers to verify the subscriber's Member State of residence when the contract for the provision of the service is concluded and renewed. At the same time, the Regulation provides no details on the enforcement. National law and procedures apply in case of breach.

The **Directive 2017/2455 of 5 December 2017 as regards certain Value Added Tax obligations** for the supply of services and the distance sales of goods reduces the border effect on e-Commerce of the country of destination principle in the VAT system in the EU.¹⁹ The Directive introduces a sales threshold (€10,000), under which traders may continue to apply their domestic VAT rules for the online sales of goods and electronic services anywhere in the EU (home country principle) instead of the VAT of the country of destination. The Directive also introduces the home country principle as regards invoicing and record keeping so that retailers would not have to apply the different rules applicable in the Member States where consumers are located. The retailers will no longer be audited by each Member State where they make sales. Finally, the Directive removes the low value consignment relief (LVCR) for the importation of small consignments below €22 from suppliers in third countries. In the same vein, the Directive makes online selling platforms liable for the collection of VAT when acting as intermediaries for the supply of goods imported from non-EU countries when the goods have a value under €150.

Two related Regulations were also adopted: the Council Regulation 2017/2454 of 5 December 2017 on administrative cooperation and combating fraud in the field of value-added tax and the Council Implementing Regulation 2017/2459 of 5 December 2017 on the common system of value-added tax.

The **Regulation 2018/302 of 28 February 2018 on addressing unjustified geo-blocking** removes geo-blocking and other forms of discrimination based on consumers' nationality, place of residence or place of establishment within the internal market by establishing a single set of rules directly applicable throughout.²⁰ However, the Regulation does not apply to financial services, electronic communications services, transport services, audio-visual and gambling services.

¹⁸ 2016/2276 (INI)

¹⁹ As suggested by Naess-Schmidt H. et al. (2012).

²⁰ See also the Questions & Answers on the Geo-blocking Regulation in the context of e-commerce: <https://ec.europa.eu/digital-single-market/en/news/geo-blocking-regulation-questions-and-answers>. Also Poiares Maduro, Monti and Coelho (2016).

Regulation 2018/644 of 18 April 2018 on cross-border parcel delivery services improves price transparency of cross-border parcel delivery services and make the national regulatory oversight of these services more effective. The Regulation imposes a single set of obligations for all delivery services providers throughout the entire EU. On that basis, the Commission adopted the Implementing Regulation 2018/1263 of 20 September 2018 establishing the forms for the submission of information by parcel delivery service providers.

The **Council Directive 2018/1713 of 6 November 2018 on rates of value-added tax applied to books, newspapers and periodicals** complements the measures addressing the fragmentation resulting from the territorial copyright licensing, by phasing out the differences in VAT rates applicable on physical media – that often benefit from lower rates and may sometimes be reduced to 0% - and e-publications, on which the standard VAT rate (a minimum of 15%) currently applies. Decreasing the VAT on e-publications aims to foster on-line cross border sales.

The Directive 2018/1808 of 14 November 2018 adapts the Audio-visual Media Services Directive to changing market realities by extending the scope of the current Directive to video-sharing platforms providers and social media of which the provision of programmes and user-generated videos constitute an essential functionality. It also requires Member States to designate independent regulatory authorities or bodies to implement the rules of the Directive.

The **Regulation 2019/XXX of 19 March 2019 on the implementation and functioning of the .EU Top Level Domain name** aims to improve the attractiveness of the .EU top level domain. It facilitates the eligibility criteria for registration of .EU domains and allows European citizens to register the domain name independently of their place of residence. The Regulation also improves the governance of the .EU domains by setting a multi-stakeholder advisory Council. This body would be independent from the Registry.

The Directive 2019/XXX on copyright in the Digital Single Market introduces an EU-wide ancillary copyright for press publisher, reduces the liability exemption granted by the e-commerce Directive to video-sharing and other platforms,²¹ strengthens the bargaining position of authors and performers vis-à-vis online distributors and requires Member States to set up impartial bodies to facilitate licensing agreements between rights holders and video on-demand platforms.²² However, Member States remain competent to decide on conditions, such as the timing and duration of the assistance and who bears the costs. The Directive complements current EU Copyright Directive as regards possible exceptions.

The **Directive 2019/XXX on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organizations and retransmissions of television and radio programmes** extends the country of origin principle that currently applies to cross-border satellite broadcasting and retransmission of copyrighted content by cable of television and radio programmes

²¹ On that change, see Nordemann (2018).

²² For further information see Kullas and Brombach (2017).

from other Member States. The Directive aims to give broadcasters the possibility making the vast majority of their content available online in other Member States.

The **Regulation 2019/XXX on promoting fairness and transparency for business users of online intermediation services** bans certain unfair practices such as sudden or unexplained account suspensions, increases transparency regarding ranking, data collection and use and differentiated conditions, and provides for new avenues for dispute resolution such as internal compliant-handling system to assist business users and the possibility of relying on mediators.

In May 2015, the EU Commission also intervened directly in the e-commerce sector based on its competition law powers with sector inquiry complementing the Commission's legislative proposals. On 10 May 2017, the Commission published the **final report of the inquiry**.²³

Soft-law was used to foster a common approach of Member States to deal with illegal content and disinformation. Commission **Recommendation 2018/334 on measures to effectively tackle illegal content online** aims to make the detection and the removal of online illegal content more effective, in particular for terrorism content. In addition, a series of codes of conducts have been agreed by some industry players and are closely monitored with the Commission:

- (i) to reduce the online diffusion of **child sexual abuses**, multiple commitments have been taken by digital firms;²⁴
- (ii) to reduce the online diffusion of **terrorist content**, a **Multi-Stakeholders Forum** has been set up in December 2015 between the Internet platforms and the enforcement agencies;²⁵
- (iii) to reduce the diffusion of hate speech, a **Code of conduct of May 2016 on countering illegal hate speech online** has been agreed by the main IT companies (now Facebook, YouTube, Twitter, Microsoft, Instagram, Google+, Dailymotion, Snapchat and Webmedia);²⁶
- (iv) to reduce the sale of counterfeit products on the Internet, a **Memorandum of Understanding of 21 June 2016 on counterfeit products** has been concluded between some online platforms and trademark right-holders in June 2016;²⁷
- and (v) to reduce the diffusion of online fake news and disinformation, a **Code of practice of October 2018 on disinformation** has been agreed by Google, Facebook, Twitter, Mozilla and the trade associations representing the advertising sector.²⁸

²³ COM(2017) 229.

²⁴ Several initiatives were established to fight the diffusion of child sexual abuses online: a CEO Coalition in 2011: <https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kid> (last visited 26 February 2019); an ICT Coalition for Children Online in 2012: <http://www.ictcoalition.eu> (last visited 26 February 2019); and an Industry Alliance to deal with child sexual abuses in 2017: <https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online> (last visited 26 February 2019).

²⁵ An EU Internet Forum was established in 2015: Commission Press release of 3 December 2015, IP/15/6243.

²⁶ https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300

²⁷ https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en

²⁸ <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> Also Renda (2018).

Table 3: EU rules regarding e-commerce and online platforms

<p>EU rules facilitating cross-border trade</p>	<ul style="list-style-type: none"> - Regulation 2017/1128 on cross-border portability of online content introduces a temporary exception to territorial copyright licences, which is directly applicable throughout the EU. - Directive 2017/2455 on VAT for e-commerce harmonises the conditions for the application of the VAT rules for the online sales of goods and electronic services. - Regulation 2018/302 on unjustified geo-blocking prohibits traders to block access to their online interface, or redirect consumers to another version of their online interface than the one sought for by consumers, based on their nationality. This Regulation also prohibits discrimination based on nationality in relation to the application of traders’ general conditions of access to specific goods or services, or the use of means of payment. - Regulation 2018/644 on cross-border parcel delivery requires parcel delivery service providers to provide their National Regulatory Authorities with their applicable tariffs each year (especially cross-border tariffs). NRAs must determine if tariffs are not unreasonably high. Consumer information by delivery service providers is also required. - Regulation 2019/XXX on.eu Top Level Domain improves EU level governance of the .eu domain name management.
<p>Unification or harmonisation of national rules or codes of conduct</p>	<ul style="list-style-type: none"> - The amending Directive 2018/1808 on Audiovisual Media Service harmonizes regulatory obligations imposed on video-sharing platforms providers and social media, in addition to those already covered by the current Directive, including as regards EU content. - Directive 2019/XXX on copyright in the Digital Single Market aims to harmonise national legislations regarding licensing practices, granting of a related right for publishers and availability of mechanisms of adjustment of contracts and dispute settlement. - Directive 2019/XXX on copyright and related rights applicable to certain online transmissions of broadcasting organisations brings similar systems for the clearance of rights by broadcasting organisations in all Member States. - Regulation 2019/XXX on P2B fairness and transparency imposes common general transparency obligations on providers of online intermediation services throughout the EU regarding their commercial terms and conditions, conditions for suspension and/or termination of their contracts, ranking methods, differentiated treatments, on the access to business or user data they provide, and on their rules for businesses on offering different conditions through other means. It also foresees the drawing up of codes of conduct by providers of online intermediation services and online search engines to contribute to the proper application of the regulation, under the impulsion of the Commission.

	<ul style="list-style-type: none"> - Proposed Regulation on preventing the dissemination of terrorist content online aims to harmonises the rules regarding the diffusion and removal of online terrorist content. - Recommendation 2018/344 on illegal content online calls upon Member States and hosting service providers to take effective, appropriate and proportionate measures to tackle illegal content online, through guidance on the mechanisms of notice and action and of proactive measures by automated means.
<p>Unification or harmonisation of national enforcement</p>	<ul style="list-style-type: none"> - Commission’s e-commerce sector inquiry investigated whether companies erected barriers affecting European cross-border e-commerce (for example, restrictions in agreements between suppliers and distributors) and prompted companies to review their commercial practices on their own initiative. - Regulation 2018/302 on geo-blocking provides for the designation in each Member State, of a body responsible for providing practical assistance to consumers in case of disputes between them and traders arising from the application of the regulation. - Amending Directive 2018/1808 on Audiovisual Media Service harmonises the guarantees of independence of media regulators throughout the EU and strengthen the status of the European Regulators Group for Audiovisual Media Services (ERGA), which was set up in 2014 to facilitate cooperation between the regulatory bodies in the EU, as provided for in the AVMS directive. - Directive 2019/XXX on copyright in the Digital Single Market provides for an alternative dispute resolution mechanism. - Regulation 2019/XXX on P2B fairness and transparency aims to require providers of online intermediation services to designate mediators through their terms and conditions to settle disputes with business users out of court. - Recommendation 2018/344 on illegal content online encourages Member States and hosting service providers to allow for the use of out of court dispute settlement mechanisms.

3.2. E-Government

Many citizens and businesses embrace the possibilities of digital technology and expect the same kind of online experience from the public sector. This is often not the case. Authorities are expected to provide user-friendly information online, digitise procedures as much as possible and make them accessible to cross-border users, re-use information provided by citizens and companies as much as possible, including in a cross-border context.

The Commission presented in April 2016 its **e-Government Action Plan 2016-2020**²⁹ and the European Parliament adopted a Resolution on this Action Plan in May 2017.³⁰ The Plan contains 20 measures, of which the following three regulatory measures:

- The **Regulation 2018/1724 of 2 October 2018 establishing a single digital gateway** aims to provide access to information, procedures and assistance and problem-solving services to help citizens and businesses make the most of the single market. The gateway will allow citizens and businesses to access and carry out administrative procedures online, hence taking advantages of the single market in an easier way, which is less time-consuming and less expensive. A centralised access to all information necessary for those who want to use their rights to mobility in the EU will be provided. Member States have to create full online access to the most important and used procedures. This information should be accurate, complete, up-to-date, and available in at least two languages: that of the Member State, plus at least one other official language of the Union.
- The **Council Directive 2017/2455 of 5 December 2017 as regards certain value-added tax obligations** for supplies of services and distance sales of goods extends the single electronic mechanism for registration and payment of VAT. The Directive extends the existing OSS (also called Mini-One-Stop-Shop or MOSS), that currently applies to electronic services, to EU online sales of tangible goods and services other than electronic services as well as to online sales of goods from third countries which have an intrinsic value not exceeding €150. The MOSS in operation since January 2015 allows companies selling electronic services (telecommunications, broadcasting or electronically supplied services) to customers in more than one EU country to declare and pay all the VAT due via a web portal in their own Member State (instead of having to register for VAT in each Member State in which they have customers). VAT revenues are then transferred from the home tax administration to the relevant Member States, i.e. the home countries of the customers to which the company has sold electronic services.

Among the 20 measures of the Action Plan, some were calls upon the Member States to strengthen existing cooperation in the following domains: (i) eIDAS services including eID and eSignature; (ii) the European e-Justice Portal as a one-stop shop for information on European justice issues; (iii) the

²⁹ COM(2016) 179.

³⁰ 2016/2273 (INI).

electronic interconnection of insolvency registers, (iv) the Business Registers Interconnection System (BRIS);³¹ and (v) the deployment and take-up of the INSPIRE Directive data infrastructure.³²

Other measures consist in commitments by the Commission to coordinate or support Member States' actions: (i) a revised version of the European Interoperability Framework (EIF) and the support its take-up by national administrations;³³ (ii) the establishment of the Electronic Exchange of Social Security Information (EESSI), the IT system to support social security institutions across the EU to exchange information more rapidly and securely;³⁴ (iii) support Member States in the development of cross-border eHealth services with the establishment of the European eHealth Digital Service Infrastructure (eHDSI or eHealth DSI);³⁵ (iv) a pilot for the launch of the 'once-only' principle (TOOP) project for businesses across borders;³⁶ (v) the transition of Member States towards full e-procurement and use of contract registers;³⁷ (vi) the development of a prototype for European Catalogue of ICT standards for public procurement.³⁸

However, the 2016 e-Government Action Plan does not mention the replacement of the paper-format customs procedures with EU-wide electronic procedures to create a more efficient and modern customs environment.

³¹ The BRIS interconnects the central, commercial and companies registers (typically referred to as business registers) to create a more business-friendly legal and fiscal environment in a cross-border context. In addition, BRIS provides a single point of access via the European e-Justice Portal³¹, through which citizens, businesses and public administrations can search for information on companies and their branches opened in other Member States.

³² <https://inspire-reference.jrc.ec.europa.eu/> The objective is promoting the development of end-user applications, so as to harvest from citizens and business more efficiently the data provided through Spatial Data (INSPIRE) for EU-level policy making and implementation. The INSPIRE portal invites stakeholders to actively participate by adding to the dedicated tools and apps catalogues with entries that contribute to both the production or use of INSPIRE.

³³ COM(2017) 134. The Framework is accompanied by the Interoperability Action Plan, which outlines priorities that should support the implementation of the EIF from 2016 to 2020. 47 open ended recommendations on how to improve governance of their interoperability activities and establish cross-organisational relationships are provided in the annex to the Action plan

³⁴ In particular Regulation 987/2009 of 16 September 2009 laying down the procedure for implementing Regulation 883/2004 on the coordination of social security systems, as amended, OJ L 284, 30.10.2009, p.1. The Commission in July 2017 made the central EESSI system available. Following this, Member States have two years to finalise their national implementation of EESSI and to connect their social security institutions to the cross-border electronic exchanges. All communication between national institutions on cross-border social security files will take place through EESSI: social security institutions will exchange structured electronic documents and follow commonly agreed procedures. These documents will be routed through EESSI to the correct destination in another Member State.

³⁵ See <https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Mission>. The European Commission and the national healthcare systems provide the communication infrastructure jointly. Twelve EU Member States started exchanging patient data, backed by the Connecting Europe Facility (CEF). eHDSI shares patient summaries and e-prescriptions in a safe way across borders.

³⁶ TOOP has a budget of € 8 million funded by the Horizon 2020 programme from the European Union. The consortium is composed of participants from 21 countries. The project has the ultimate goal of promoting cross-border cooperation among authorities and offering control and transparency opportunities regarding business operations across borders.

³⁷ To date, achievements related mainly to aspects such as the prequalification of economic operators (ESPD and eCertis) and e-invoicing. Under the Connecting Europe Facility (CEF), EU funding is available to support e-invoicing activities. The Multi-Stakeholder Expert Group on e-Procurement (EXEP) provides a link between the Commission and the stakeholders in the Member States and plays an important role for a successful transition to e-procurement.

³⁸ A number of standards are available on the 'joinup' portal of the EU Commission.

The legal framework for this e-Government initiative is set in the Union Customs Code (UCC), while the implementation of the European electronic customs environment is governed by the Electronic Customs Multi-Annual Strategic Plan (MASP).³⁹

³⁹ MASP Rev. 2017 Version 1.4, 30.11.2017, taxud.a.3(2017)6498377, https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/policy_issues/e-customs_initiative/masp_strategic_plan_en.pdf

Table 4: EU rules regarding e-government

EU rules facilitating cross-border trade	<ul style="list-style-type: none"> - Package on VAT on e-commerce extends the One Stop shop procedure. - Regulation 2018/1724 on Digital Single Gateway sets common rules for centralised access to all information necessary for those who want to use their rights to mobility in the EU. - Member States must connect their social security institutions to the cross-border electronic exchanges EESSI under Regulation 987/2009 of 16 September 2009
Unification or harmonisation of national rules or codes of conduct	<ul style="list-style-type: none"> - See rules on public data explained in Table 5
Unification or harmonisation of national enforcement	<ul style="list-style-type: none"> - Interoperability Action Plan lists 47 recommendations to the Member States to improve the governance of their interoperability activities and establish cross-organisational relationships. - The Commission deployed and runs the core services platform, named "European Central Platform" (ECP) underlying the Business Registers Interconnection System (BRIS). - The Commission in July 2017 made the central EESSI system available. - The Multi-Stakeholder Expert Group on e-Procurement (EXEP) provides a link between the Commission and the stakeholders in the Member States and plays likely an important role for a successful transition to e-procurement. - Under the Interoperability solutions for public administrations, businesses and citizens (ISA) Programme, the collaborative platform 'Joinup' was created to help e-Government professionals share their experience with each other and support them to find, choose, re-use, develop and implement interoperability solutions.

3.3. Data and Artificial Intelligence

In order to foster a thriving European Data Economy, the following actions were undertaken to facilitate the cross-border flow of data in the digital single market while protecting the consumers and data subjects.

The **General Data Protection Regulation (GDPR) 2016/679** provides for a comprehensive set of rules on the processing of personal data of citizens, especially on data subjects rights and freedoms. The GDPR is, firstly, an essential means to foster consumer confidence in the data economy. Secondly, unified rules across the EU are essential for the emergence of big data with adequate critical mass in Europe, which otherwise would be hampered by diverging national requirements. In addition, the network of regulators will ensure that Data Protection Agencies coordinate their approaches in a manner compatible with the implementation of big data analytics in Europe. The **Directive 2016/680** was adopted at the same time to deal with the **processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences** or the execution of criminal penalties

The proposed **e-privacy Regulation** aims to extend the scope of application of the current ePrivacy Directive⁴⁰ to over-the-top (OTT) communication services (such as WhatsApp or Skype), require user consent for the processing of communications data and metadata and increase the level of fines for breaches.

The **Regulation 2018/1807 on the free-flow of non-personal data** requires Member States to remove legal requirements on data localisation. Restrictions on the location of data will only be allowed on grounds of public security, as defined in the Treaties and as interpreted by the EU Court of Justice. Any remaining data localisation requirements will have to be communicated to the European Commission and published online, in order to ensure compliance and transparency. In addition, the Regulation proposes self-regulation to facilitate switching cloud-service-providers for professional users.

The Council **Regulation 2018/1488 of 28 September 2018 establishing the European High-Performance Computing Joint Undertaking** (EuroHPC JU) sets up a public-private partnership to pool European resources to develop top-of-the-range exascale supercomputers for processing big data. The EuroHPC JU will (i) jointly with Participating States, buy and deploy two supercomputers in Europe that will be among the top 5 in the world and at least two other that would today rank in the global top 25 for Europe's private and public users and (ii) support research and innovation activities: developing a European supercomputing ecosystem, stimulating a technology supply industry, and making supercomputing resources in many application areas available to a large number of public and private users. The EU's financial contribution to the EuroHPC JU amounts to € 486 million.⁴¹

⁴⁰ Directive 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p.37.

⁴¹ This budget will be matched by a similar amount from the participating countries. The private members will also provide additional contributions to the value of over EUR 400 million, through participation in the Joint Undertaking's activities.

The **Directive 2019/XXX on Open Data and Public Sector Information (PSI)** reduces market entry barriers by limiting the exceptions that allow public bodies to charge for the re-use of their data more than the marginal costs; increases the availability of data by bringing new types of data into the scope of the Directive, such as data held by public undertakings in the utilities and transport sectors and research data resulting from public funding; minimises the risk of first-mover advantage, by requiring a more transparent process for the establishment of public–private data arrangements and increases business opportunities by encouraging the dissemination of dynamic data via application programming interfaces (APIs).

The Commission **Recommendation 2018/790 of 25 April 2018 on access to and preservation of scientific information** calls for open access to scientific publications resulting from publicly funded research and invites the Member States to implement clear policies in the areas of preservation and re-use of scientific information, infrastructures underpinning the system for access to, preservation, sharing and re-use of scientific information and for promoting their federation within the European Open Science Cloud (EOSC), including the drafting implementation plans and setting concrete objectives and indicators to measure progress.

Regarding data policies, the Commission adopted a series of Communications and the European Parliament adopted a series of Resolutions.

- First, the Commission **Communication of 19 April 2016 on the European Cloud Initiative - Building a competitive data and knowledge economy in Europe** announces several actions and partnerships to support the European Open Science Cloud and to kick-start the European Data Infrastructure and estimates the investments required at €4.7 billion in the period of 5 years.⁴² The European Parliament adopted a **Resolution on 10 March 2016 on a thriving data-driven economy**⁴³ and then a **Resolution on 16 February 2017 on the European Cloud Initiative**.⁴⁴
- In parallel, the Commission **Communication of 19 April 2016 on digitising European Industry - Reaping the full benefits of the Single Market** calls for strengthening the coordination role of the Public Private Partnerships (PPPs) established in H2020 so that they become real aggregation frameworks and ecosystems for digital industrial innovations, including on big data.⁴⁵ The European Parliament adopted a **Resolution on 1 June 2017 on digitising European industry**.⁴⁶
- Then, the Commission **Communication of 10 January 2017 on Building a European data economy** launches a stakeholder’s dialogue on the following issues: free flow of data; access and transfer in relation to machine-generated data; liability and safety in the context of emerging technologies; and portability of non-personal data, interoperability and standards.⁴⁷ The Communication also sets out suggestions for experimenting with common regulatory solutions in a real-life environment.

⁴² COM(2016) 178.

⁴³ 2015/2612 (RSP).

⁴⁴ 2016/2145 (INI).

⁴⁵ COM(2016) 180.

⁴⁶ 2016/2271 (INI).

⁴⁷ COM(2017) 9.

- Finally, the Commission **Communication of 25 April 2018 on a common European data space** puts forward a package of measures to foster a seamless digital area with the scale that will enable the development of new products and services based on data.⁴⁸ The Communication also recommends five key principles should be complied with in contractual Business to Business and Business to Government data sharing agreements: transparency, shared value creation, respect for each other's commercial interests, undistorted competition and minimised data lock-in.

Regarding Artificial Intelligence, the European Parliament adopted an important Resolution on 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics.⁴⁹ The Commission adopted a series of three Communications with different policy action.

- First, the Commission adopted the **Communication of 25 April 2018 on Artificial Intelligence for Europe** which establishes a three-pronged strategy: boost the EU's technological and industrial capacity and AI uptake across the economy, prepare for socio-economic changes and ensure an appropriate ethical and legal framework.⁵⁰
- Then, the Commission adopted the **Communication of 7 December 2018 on a coordinated plan on AI** to create synergies between Member States and increase joint investment with the aim to foster cross-border cooperation and mobilise all players to increase public and private investments to at least € 20 billion annually over the next decade.⁵¹
- Finally, the Commission adopted the **Communication of 8 April 2019 on building trust in human-centric Artificial Intelligence** which proposes seven requirements for trustworthy AI on the basis of the Ethic Guidelines developed by the High-level expert group on AI.⁵² Those key requirements are: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability.

⁴⁸ COM(2018) 232.

⁴⁹ (2015/2103(INL))

⁵⁰ COM(2018) 237.

⁵¹ COM(2018) 795.

⁵² COM(2019) 168.

Table 5: EU rules regarding data and AI

EU rules facilitating cross-border trade	<p>- Regulation 2018/1807 on free-flow of non-personal data provides for removal of Member States' legal requirements of data localisation, except for some specific exceptions. The proposal also foresees that competent national authorities may not be refused access to data based on its location in another Member State .</p>
Unification or harmonisation of national rules or codes of conduct	<ul style="list-style-type: none"> - GDPR 2016/679 establishes common EU rules on most aspects of the processing of personal data. The GDPR details the data subject rights, data controllers' responsibility, processors' obligations, security of processing, development of codes of conduct and certifications. The GDPR also details remedies, liability and penalties in case of breach of the substantive rules. - Regulation 2018/1807 on free-flow of non-personal data entrusts the Commission with the task to encourage and facilitate the development of EU codes of conduct for cloud services. - Proposed e-privacy Regulation aims to impose EU wide the requirement of user-consent for the processing of communication data. - Directive 2019/XXX on open data and Public Service Information requires Member State to harmonise their national rules on open data so that they cover research data and specific documents held by public undertakings, and that dynamic data is made available in the shortest possible timeframe after collection. The Member States' rules have to provide that access to certain specific information shall be free of charge for its users (high value datasets). - Recommendation 2018/790 on scientific information invites the Member States to ensure that scientific publications that are publicly funded, are accessible in open-access, under licensing terms that are as wide as possible. - Communication Staff Guidance on sharing private sector data provides principles and guidance on business-to-business (B2B) as well as on business-to-government (B2G) data sharing agreements.
Unification or harmonisation of national enforcement	<p>- GDPR 2016/679 details extensively the tasks of the national supervisory authorities as well as the relations between each other. Furthermore, it includes a consistency mechanism to ensure consistent application of its provisions with opinions and dispute resolution delivered by the Data Protection Board.</p>

3.4. Security

The **Directive 2016/1148 of 6 July 2016 on Network Information Security (NIS)** requires that Member States adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures in relation to cybersecurity and designate a national competent authority in the regard. The Directive also creates a cooperation group between Member States to support and facilitate strategic cooperation and the exchange of information among Member States as well as the setting up a network of Computer Security Incident Response Team (CSIRT), in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks. The Directive also requires the identification of undertakings across sectors, which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure (essential services) and ensure that these undertakings take appropriate security measures and notify serious incidents to the relevant national authority. Key digital service providers (search engines, cloud computing services and online marketplaces) must also comply with the security and notification requirements under the NIS Directive.

The **Regulation 2019/XXX for a Cybersecurity Act** has two main objectives. (i) First, the Regulation gives a permanent mandate to the European Network Information Security Agency (ENISA), including for the implementation of the NIS Directive. ENISA will contribute to stepping up both operational cooperation and crisis management across the EU. (ii) Second, the Regulation creates a framework for EU cybersecurity certificates for connected products, Internet of Things devices and critical infrastructures. Such a cybersecurity certification framework incorporates security features in the early stages of their technical design and development (security by design). It also enables their users to ascertain the level of security assurance and ensures that these security features are independently verified. The resulting certificate will be recognized in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

The **Regulation 2019/XXX establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres** establishes a competence Centre which will set up and help to coordinate the National Coordination Centres Network and the Cybersecurity Competence Community. The Centre will implement cybersecurity-related financial support from Horizon Europe and the Digital Europe Programme.

The **Commission Recommendation 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises** details the plan to be followed in case of large-scale cross-border cyber incident or crisis. It sets out the objectives and modes of cooperation between the Member States and EU Institutions in responding to such incidents and crises and explains how existing Crisis Management mechanisms can make full use of existing cybersecurity entities at EU level.

The Commission **Communication of 19 April 2016 on ICT Standardisation Priorities for the Digital Single Market**⁵³ promotes a fresh approach to standards in five domains, among which Cybersecurity.

⁵³ COM(2016)176.

It tries to ensure that all forces in Europe pull in the same direction, using standardisation as a strategic instrument to EU industrial policy. The Communication announces that it will support European standardisation organisations and other standards development organisations, European regulators as well as public-private initiatives, in the development of standards-based cybersecurity risk management guidelines for organisations and of corresponding audit guidelines for authorities or regulators with oversight responsibilities.

Table 6: EU rules regarding security

<p>EU rules facilitating cross-border trade</p>	<p>- Regulation 2019/XXX on Cybersecurity Act establishes an EU wide cybersecurity certification scheme and prohibits Member States to introduce new national cybersecurity certifications schemes for matters covered. The Act also fixes the penalties for in case of infringement of its rules.</p>
<p>Unification or harmonisation of national rules or codes of conduct</p>	<p>- Directive 2016/1148 Network Information Security harmonises national laws governing network security including the identification of operators of essential services.</p> <p>- Regulation 2019/XXX on Cybersecurity Act provides for common EU principles to govern the national strategies on the security of network and information systems, on security requirements and incident notifications, on establishment of jurisdiction, and on promoting of standardisation by Member States.</p> <p>- Guidance for the implementation of the NIS Directive promotes a common interpretation and transposition for example as regards the national Computer Security Incident Reponse Team (CSIRT) capabilities or the consistency of identification of operators of essential services.</p> <p>- Recommendation 2017/1584 on a coordinated response to large scale cybersecurity incidents proposes a common cooperation procedures between the Member States and the EU and for the transmission of information in case of a crisis (large scale cybersecurity incidents). It further provides for the adoption of a common taxonomy of crisis management categories.</p>
<p>Unification or harmonisation of national enforcement</p>	<p>- Directive 2016/1148 NIS requires Member States to designate national competent authorities and single points of contact and establishes a CSIRTs network in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation. It is composed of representatives of the EU Member States' CSIRTs and a CSIRT for EU institutions CERT-EU. The CSIRTs Network provides a forum where Member States' National CSIRTs can cooperate, exchange information and also build trust. Member States CSIRTs will improve the handling of cross-border incidents and discuss how to respond in a coordinated manner to specific incidents.</p> <p>- Regulation 2019/XXX on Cybersecurity Act entrusts ENISA with limited implementation powers in the area of cybersecurity such as steering NIS operational cooperation by actively supporting Member States' CSIRTs' cooperation or developing the future certification schemes and provide secretariat assistance to the EU cybersecurity certification group.</p> <p>- Regulation 2019/XXX on Cybersecurity Act provides for national certification supervisory authorities to be appointed by Member States in relation to European cybersecurity certification schemes and their features. The proposed Act also provides for the establishment of the European cybersecurity certification group, composed of the national certification supervisory authorities, and defines its tasks.</p>

- | | |
|--|---|
| | <ul style="list-style-type: none">- Regulation 2019/XXX establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres creates a competence Centre to manage cybersecurity-related financial support from the EU's budget and facilitate joint investment by the Union, Member States and industry.- Recommendation 2017/1584 on a coordinated response to large scale cybersecurity incidents establishes an EU cybersecurity crisis response framework to ensure cooperation, exchange of information and efficiency of all relevant actors in case of a crisis. |
|--|---|

3.5 Consumer Protection in the digital era

The **Regulation 2017/2394 of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws** (i) strengthens the minimum powers of the consumer protection authorities to cooperate in cross-border context, especially to tackle faster online practices including the powers to carry out test purchases and mystery shopping, to suspend and take down websites, to impose interim measures, to impose penalties proportionate to the cross-border dimension of the imputed practice. The Regulation also allows these authorities to accept commitments from traders.

The **Directive 2019/XXX on better enforcement and modernisation of EU consumer protection** extends the protection for consumers to free digital services exchanged against personal data. The Directive also adapts and harmonises consumer protection to specific digital issues such as the transparency for online marketplaces regarding price personalisation; paid advertising and placement, the main parameters of ranking, whether the third-party offering product or service is a trader or not, and the authenticity of consumer reviews. The Directive also strengthens the penalties for infringements⁵⁴ and sets the criteria administrative authorities or courts have to take into account when deciding whether to impose a penalty and on its level.

The **Directive 2019/XXX on digital content contracts** targets digital content and services (e.g. cloud, video and music streaming, digital television, apps, social networks and messaging apps) and covers, besides contracts in exchange of a price, contracts in exchange of the consumer's personal data.⁵⁵ Contractual clauses, which are not in line with the Directive, to the detriment of the consumer, are void, unless explicitly allowed. The Directive puts the burden of proof on the supplier of the digital content and of the conformity of the content supplied. Consumers have the right to terminate contracts and the supplier have to provide the consumer with the technical means to retrieve all the consumer's content and data produced/generated through the use of the digital content provided it has been retained by the supplier. Member States have to ensure that adequate and effective means of redress exist. Member States do not have the possibility to impose additional requirements.

The Commission **Guidance of 25 May 2016 on the implementation of the Unfair Commercial Practices Directive** (UCPD) provides guidance on the UCPD's key concepts and provisions and practical examples taken from the case-law of the Court of Justice of the European Union and from national courts and administrations on how to implement it. However, it is itself not legally binding.

⁵⁴ For instance, for widespread infringements, Member States have to provide for maximum fines that should not be set below 4% of the infringing trader's turnover in the Member State or Member States concerned)

⁵⁵ The proposal was initially not connected with the data economy, but rather with the Commission's failed attempt to introduce a Common European Sales Law, COM(2011) 635, withdrawn in late 2014.

Table 7: EU rules regarding consumer protection

Unification or harmonisation of national rules or codes of conduct	<ul style="list-style-type: none"> - Directive 2019/XXX on better enforcement and modernisation of EU consumer protection extends consumer protection to services exchanged against personal data and increase the transparency of online market places. - Directive 2019/XXX on contracts for the supply of digital content harmonises Member States' legislations regarding conformity of digital service/service with the contract, the remedies available in the case of lack of conformity and modification and termination of the contract.
Unification or harmonisation of national enforcement	<ul style="list-style-type: none"> - Regulation 2017/2394 on Consumer Protection Cooperation sets EU wide rules regarding the powers of national consumer protection authorities and for joint enforcement measures (mutual assistance mechanism) in case of cross-border infringements to consumer protection law, as well as a framework for coordinated investigations and enforcement mechanisms in case of widespread infringements to the same set of rules, exchange of information, and a framework for sweeps, i.e. concerted and simultaneous investigations on respect of EU consumer protection law.

3.6. Electronic Communications Networks and Services

Context

The EU regulatory framework that had been put in place in 2002 was revised in 2009 with the Telecoms Package, which included the Better Regulation and Citizens' Rights Directives, as well as two new Regulations to reduce mobile roaming charges and create a body of European regulators for electronic communications (BEREC). A subsequent Regulation was introduced in 2012 to further limit roaming charges. However, on year later, the European Commission still found that "(s)ome large telecommunications companies are present in several Member States; but none is present in all. For the most part mobile operators have merely a national footprint; for many fixed operators it is even more localised. Those who do operate in several Member States must work under separate rules, according to the sometimes diverging requirements and remedies of different regulators, and needing distinct authorisations in each Member State. In addition, often operators active across several Member States do not behave as truly European operators, and appear content to run their activities separately in each Member State. The market includes over one thousand fixed operators, and several hundred mobile operators, which, despite often belonging in larger groups, operate on a national basis. At the same time the sector is increasingly global in nature and depends on scale to be profitable."⁵⁶ The Commission concluded that "the sector suffers from fragmentation along national borders; a lack of regulatory consistency and predictability across the Union; unfairly high prices for specific services; and a lack of investment."⁵⁷ To address this perceived gap in the digital single market, the Commission proposed a Regulation for a Connected Continent.⁵⁸ However, the scope of the regulation as eventually adopted⁵⁹ was reduced compared to the Commission proposal, covering only net neutrality and international roaming. The remaining issues were addressed by the Commission in its September 2016 proposal for a European Electronic Communications Code.

Another issue dealt with in the Code is the perceived absence of a level playing field in the Member States following the success of Internet applications allowing to users to establish communications over broadband internet connections ('over the top' services) that can replace traditional telecommunications services provided by telecom operators. The new Code subjects the latter, in different degrees, to the same rules than the telecom operators. While the measure can be seen as promoting a level playing field in national markets, it does not necessarily contribute to the single market. Where in the past the providers of the internet applications were regulated at EU level (country of origin principle), the global operators will now be regulated and have to notify their service in each of the Member States.⁶⁰

⁵⁶ Communication from the Commission on the Telecommunications Single Market, 11.9.2013 , COM(2013) 634, p.4.

⁵⁷ *Idem*, p.5.

⁵⁸ Outlined in European Commission, COM (2013) 627 - A proposal for a regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations No 1211/2009 and No 531/2012, 2013

⁵⁹ Regulation 2015/2120, published in the Official Journal on 26 November 2015

⁶⁰ As we explained in de Streel and Hocepied (2017). See also Renda (2017).

Measures adopted

The **Regulation 2015/2120 of 25 November 2015 on the open internet access and on roaming on public mobile communications networks** forces providers of internet access services to treat all traffic equally, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. In addition, the Regulation prohibits any surcharge to the domestic retail price on international roaming customers in any Member State for calls, SMS and data provided the subscribers comply with the fair use policy. The abolition of roaming surcharges led to the following two measures: (i) the Commission Implementing Regulation 2016/2286 of 15 December 2016 on the fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges which allows roaming providers to apply 'fair use' policies to prevent permanent or abusive roaming;⁶¹ and (ii) the Regulation 2017/920 of 17 May 2017 on rules for wholesale roaming markets which caps the maximum international wholesale roaming prices that mobile operators may charge to each other in the EU.⁶²

The **Decision 2017/899 of 17 May 2017 on the use of the 470-790 MHz frequency band for mobile services** seeks the coordinated release of the 700 MHz band (694-790 MHz) under harmonised technical conditions by 30 June 2020 at the latest in all EU countries. This frequency band is particularly well-suited for ensuring the provision of broadband services in rural areas, while accommodating the specific needs of audio-visual media distribution.

The **Regulation 2017/1953 of 25 October 2017 on the promotion of internet connectivity in local communities** (also known as Wifi4EU) earmarks €95 million over a period of three years to finance the provision of fast wireless internet connections for citizens located in spaces where public services are provided, such as public administrations, libraries and hospitals.

The **Directive 2018/1972 of 11 December 2018 on the European Electronic Communications Code** brings a more consistent single market approach to spectrum policy and deliver conditions for a true single market by tackling regulatory fragmentation. These two general objectives are pursued through several specific objectives, addressing perceived specific internal market restrictions by either private players or by Member States: (i) reduced regulatory entry barriers, (ii) predictability for spectrum right holders, (iii) procedures to ensure that national regulators impose access remedies which foster the internal market, (iv) EU wide interoperability of services and mandatory standards, (v) EU wide Security of networks and services, (vi) the availability of an EU wide numbering space, (vii) lessening the fragmentation resulting from divergences between national end-user protection rules.

⁶¹ Operators may restrict the benefit of the abolition of the roaming surcharge to end users residing in the country where they have subscription or who are otherwise able to demonstrate stable links at the request of the roaming provider.

⁶² The wholesale charge shall not exceed a safeguard limit of EUR 7,70 per gigabyte of data transmitted. That maximum wholesale charge shall decrease to EUR 6,00 per gigabyte on 1 January 2018, to EUR 4,50 per gigabyte on 1 January 2019, to EUR 3,50 per gigabyte on 1 January 2020, to EUR 3,00 per gigabyte on 1 January 2021 and to EUR 2,50 per gigabyte on 1 January 2022.

The **Regulation 2018/1971 of 11 December 2018 on the Body of European Regulators of Electronic Communications (BEREC)** seeks, on the one hand, to introduce new competences granted to Body of European Regulators for Electronic Communications (BEREC) and, on the other, to streamline its functioning. This Regulation also amends the previous Regulation 2015/2120 to regulate the charges for cross-border intra EEA calls and SMS.

Table 8: EU rules regarding electronic communications networks and services

EU level rules	<ul style="list-style-type: none"> - Regulation 2015/2120 on Open Internet and international roaming and associated legal instruments regulate international roaming rates. - Regulation 2015/2120 on Open Internet, retail charges for regulated intra-EU communications and international roaming regulates the tariffs of international calls, sets up an EU numbering space and prohibits of discrimination by operators, on the basis of residence or nationality.
Unification or harmonisation of national rules or codes of conduct	<ul style="list-style-type: none"> - Regulation 2015/2120 on Open Internet, retail charges for regulated intra-EU communications and international roaming imposes common network neutrality rules across the EU . - Spectrum Decision 2017/899 sets common deadline for the coordinated release of the 700 MHz spectrum band. - Directive 2018/1972 EECC harmonises many national telecom rules and enables an EU numbering space, ensures network security, EU standards, maximum harmonization user protection as well as predictability over time for spectrum right holders.
Unification or harmonisation of national enforcement	<ul style="list-style-type: none"> - Directive 2018/1972 EECC grants power to the Commission to block national deregulation of network access when contrary to the internal market, provides that this body shall conduct an analysis of transnational end-user demand for products and services that are provided within the Union in one or more of the markets listed in the Recommendation, if it receives a reasoned request providing supporting evidence - Regulation 2018/1971 on BEREC grants new tasks to BEREC. - Directive 2018/1972 on EECC provides for out of court dispute resolution mechanism, including the obligation on Member States to enable the national regulator to act as a dispute settlement entity.

4. FUTURE POTENTIAL OF THE DIGITAL SINGLE MARKET AND POSSIBLE INITIATIVES

KEY FINDINGS

As many regulatory and non-regulatory actions have been taken during the 8th legislature, the first task is to **implement those new rules in an effective and harmonised manner** across Europe. This is particularly important because most of those EU substantive rules are implemented by national authorities. Then the **efficiency and the effectiveness of the rules and their enforcement should be evaluated**, in particular the impacts on the economy and the society.

However, evaluating the effects of the actions already adopted will not be enough given the importance of the digital technologies for the European economy and society, the rapid pace of evolution of those technologies and the increasing global competition for digital leadership. To respond to change, the **pace of reform should remain important during the forthcoming 9th legislature**.

Regarding the objectives and policy fields, we have identified **following priorities**:

- **Make the EU a technological powerhouse for the emerging and important technologies** such as AI, quantum computing, security of connected devices or data exchanges that should be designed and developed according to European values enshrined in the Treaties and the Charter of Fundamental Rights;
- Stimulate the **development of online platforms**: (i) start-ups should be stimulated by rules ensuring a level playing and access to the main capabilities for digital innovation (in particular data) and to the ecosystem of products that are used by consumers, (ii) scale-up should be stimulated by one set of rules and enforcement all over Europe, (iii) significant platforms should be subject to an increased duty of care should be imposed;
- Stimulate **e-government**: given the potential benefits of digital public services, the EU should stimulate the adoption and the diffusion of national and cross-borders e-government services as well as the adoption of digital technologies, such as blockchain, to improve public regulation.

Regarding the **policy and regulatory techniques**, we recommend the reliance of principles-based legislation that can easily adapt to fast and unpredictable technology and market evolutions **complemented with codes of conduct** agreed with all the digital players (firms, consumers associations, NGOs ...) under the auspices of EU institutions and with a close monitoring by the EU institutions. We also recommend that the **enforcement of those rules is more Europeanised** either with the continuous strengthening of the cooperation network of national regulatory authorities or with the **establishment of a EU regulator for significant platforms** as it was done some year ago for the significant banks with the creation of the Single Supervisory Mechanism within the European Central Bank. The **regulatory authorities in Europe should also size the potential of digital technologies**, such as big data or AI, to improve their operations (*RegTech*). To go further when feasible, enforcement may be automatized in the computer code as it is the case for smart contracts or privacy by design (more generally, *compliance by design*).

Those regulatory actions should be **complemented with non-regulatory initiatives**, in particular the monitoring and exchange of best practices of key digital national policies, the increasing smart use of EU funds to stimulate the deployment and the adoption of key digital networks and services and the development of the digital skills of EU workers and citizens.

As explained in the previous section, the European Parliament, together with the other EU institutions, has been very active during its 8th legislature to stimulate the Digital Single Market. However, given the rapid pace of technological progress and market evolutions and the important issues at stake, there is no time for complacency and efforts will need to be stepped up during the forthcoming legislature.

4.1 Applying and evaluating the newly adopted rules

As many new rules have been adopted, the first challenge is to ensure that those new rules are integrated into the legal regimes of the Member States in a timely and harmonised manner. This implies that the national laws transposing EU Directives and, when needed, complementing EU Regulations should be sufficiently clear to guarantee legal certainty, respect the letter and the spirit of EU law to ensure harmonisation and alleviate any regulatory gold-plating and over-regulation. Then, those rules need to be enforced by national administrative, regulatory and judicial authorities to be effective in a manner which is effective and proportionate. The numerous network of national authorities which have been established or strengthened should help in that regard.

After some years of application, those rules and their enforcement should be evaluated⁶³ in a rigorous manner as foreseen in the Commission Better Regulation Guidelines⁶⁴ or in Muller et al. (2013). In particular, the Commission will have to assess the effectiveness, the efficiency, the relevance given the needs, the coherence with other EU interventions and the EU added value of the rules and their enforcement. On that basis, an adaptation of the existing rules and/or their enforcement may have to be proposed.

4.2. Digitalizing and deepening the single market

The application and, then, the evaluation of the newly adopted rules and their enforcement will take years and yet no time can be lost. Therefore already now, it is important to envisage the actions adopted during the 8th legislature that need to be developed and the new actions that need to be initiated during the next parliamentary term. On the basis of the expected technological evolution and their impacts, we suggest the following avenues for future actions.⁶⁵

a. From digital single market to digitised single market

As explained by Bauer (2017), some of the impediments to digital business developing and scaling up is the regulatory heterogeneity in non-digital industries. Indeed, the OECD Product Market Regulation (PMR) Index and the OECD Service Trade Restrictiveness Index show important regulatory heterogeneity between Member States for non-digital goods and services. To be sure, such heterogeneity may be justified by different national preferences or endowment but it affects the possibility of establishing and operating cross-border digital business. Moreover as new digital technologies are general-purpose technologies which permeate all the sectors of the economy and the society, it is appropriate to digitize the four freedoms and all the sectors of the single market instead of

⁶³ Many EU legal instruments have review clauses which make such evaluation by the Commission compulsory.

⁶⁴ Commission Staff Working Document of 7 July 2017, Better Regulation Guidelines, SWD(2017) 350, Chapter VI.

⁶⁵ Also McKinsey Global Institute (2018).

developing a specific strategy for digital sectors.⁶⁶ As proposed by the Lisbon Council (2018), the (digital) single market could be decoupled from the digital agenda and the First Vice-President of the Commission should be in charge of all digital files in a transversal manner while a Vice-President should be in charge of the single market including both the implementation of digital-single-market legislation and a broad overview of cross-cutting and sectoral single-market questions. In addition, as suggested by Erixon and Lamprecht (2018), this single market strategy should focus on integrating market relying of country of origin principle rather than regulating business at the EU and national levels.

b. Making Europe a technological power house and adopting an ambitious cyber-security and AI industrial policy

Before being a regulatory powerhouse, the EU should first and foremost be a technology powerhouse, its policies should stimulate the development of the emerging and important technologies for tomorrow such as quantum computing, very fast micro-processing, different AI techniques, secure data exchanges and secure Internet of Things and AI enabled tools. Europe should also ensure that those technologies are designed and developed according to its values enshrined in the Treaties and in the Charter of Fundamental Rights.⁶⁷ This requires smart innovation policies based on close dialogue between public and private bodies.

c. Regulation should accompany the development of online platforms in Europe

Online platforms are playing an increasing role in the economy and society. As explained by Bauer (2018) and Martens (2016), they are powerful engines for growth and innovation. They allow small professional users to reach out to millions of customers at very low cost, they increase customers and traders' information and, in the end, they allow the development of new and disruptive business models. However, their increasing role raise concerns on their economic, societal and political power: big platforms monopolise markets and may buy any potential disruptive innovator (Cremer et al., 2019), they capture a big share of the economic surplus they generated and value may be shifted from creators and prosumers to platforms, they disrupt labour relationship and may threaten social security systems, they influence elections and may threaten democracy as we know it. While some concerns are valid and other are exaggerated, it remains that online platforms are destabilising some of our past governance models and the State (being EU or national institutions) should adapt their policies while keeping control of the public sphere. Different actions are needed to stimulate the start-up, then the scale-up and finally ensuring a sufficient duty of care by the most significant platforms.

First, EU policies should stimulate the emergence and the take-up of new platforms, in particular in Europe and ensure that digital markets remain contestable and contested.⁶⁸

⁶⁶ This is the direction suggested by the Presidency discussion paper of 20 November 2018 on the future of Single Market, 14003/18. Also Communication of the European Commission of 21 November 2018, The Single Market in a changing world, COM(2018) 772, section 3.1.

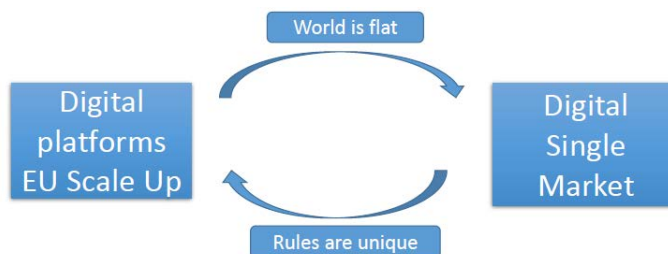
⁶⁷ For AI, see Joint Research Centre (2018); Maciejewski M. et L.C. Matos (2018).

⁶⁸ Jean Tirole, "Regulating the Disruptors", available at <https://www.livemint.com/Technology/XsgWUgy9tR4uaoME7xtIT/Regulating-the-disrupters-Jean-Tirole.html>

As explained by Dittrich (2017 and 2018), this requires smart innovation policy and regulation that ensure access to the main capabilities for digital innovation, in particular access to data,⁶⁹ skills, computing power and risky and patient capital.

Second, the EU policies should stimulate the scale-up of the digital platforms, which is one the main weaknesses of Europe compared to the US or China. There is a positive feedback loop between the single market and the platform scale up as (i) the scale-up makes the world more flat and allows business and consumers to more easily reach their counterparts all over Europe, thereby contributing to the single market while (ii) the single market rules facilitate the business operation and consumer trust all over Europe.

Figure 2: Feedback loops between platform scale-up and single market



For this feedback loop to work, online platforms should be subject to one set of rules. This can be achieved with the mutual recognition of national rules (country of origin principle) or with the full harmonisation of national rules. Those rules should then be subject to one enforcement, either at the national level in case of mutual recognition or identically in all Member State in case of full harmonisation.

Third, when an online platform has scaled up and become significant, it may raise systemic risks to the economy and society (to paraphrase what was said for the big banks, big platforms may be too big to rule). In this case, EU policies and regulation should ensure an appropriate duty of care. This implies (i) transparency on the practices vis-à-vis the regulators and the platforms customers (business and consumers), (ii) loyalty of the platform which should provide their services to the benefit of their customers and not their own and (iii) increased responsibility for a safer Internet as with power comes responsibility (Floridi et al., 2017). To do that, the e-commerce Directive could be revised or complemented to condition the liability exemption to the provision of an infrastructure facilitating the detection and the removal of illegal content by users, third parties and the platforms themselves, possibly relying on AI detection tools (de Streel, Buiten and Peitz, 2018).

d. Developing E-government everywhere at all levels

E-government is one the core of national competences and organisation. However, given the importance of public sector as an enabler for the digitization of the economy and society, EU should continue to incentivize the digitization of public service within each Member States as well as across the Member States.⁷⁰

⁶⁹ In favour of data sharing policies: OECD (2015), Gans (2018), Mayer-Schonberger and Ramge (2018). Also Lisbon Council (2019).

⁷⁰ See TNO, WIK-Consult and Rand (2013)

The measures of the e-Government Action Plan 2016-2020 and the best practices of the 2017 Tallinn Declaration on e-Government are good basis and should be developed further in the next legislature (Lisbon Council, 2018).

4.3. Smart policy and regulatory techniques

To achieve those objectives in the most effective manner, the EU should rely on the most adapted policy and regulatory techniques as explained in Muller et al. (2015).

a. Smart regulation in dynamic and uncertain environments

Given the very high rapidity and uncertainty of market evolutions, regulation should be principle-based to adapt easily to technologies and market evolutions (de Streel and Larouche, 2016). Detailed and prescriptive rules should be alleviated at all costs as they quickly outdate and miss their objectives while possibly stifling innovation. As principle-based rules often lead to uncertainty that, in turn, may increase regulatory costs and reduce regulatory effectiveness, those rules need to be complemented by soft-law instruments and codes of conducts agreed between authorities and digital players on the basis of the regulatory principles, closely monitored and adapted when necessary.⁷¹ The different codes of conducts which have been adopted to reduce some illegal or harmful content online could serve as best practices.

b. Smart enforcement in global and digital markets

It is not enough to have good rules, they need to be enforced effectively and, as shown by the recent review of the EU consumer acquis, this is often the weak point of the EU regulatory framework as rules remain enforced at the national level. As many digital markets and firms are global and the digital services of the most significant online platforms are offered across the Member States, it is key that EU rules are enforced in the same manner in all the Member States. Moreover, given the imbalance between some digital platforms and national regulatory authorities, an EU enforcement could increase the effectiveness of EU rules. Therefore, the different coordination networks between the national regulatory authorities should continue to be strengthened. Possibly an EU regulator for the significant digital platforms should be created similarly to what has been done in the financial and banking sector with the recent establishment of an EU regulator (the Single Supervisory Mechanism within the European Central Bank) for the significant banks in Europe.

In addition, regulators, as every other player in our society, should rely on digital technologies to improve their operations and, as a side-effect, improve their understanding of new technologies that they may need to regulate. Regulators could rely on big data and AI techniques to improve the detection of rules violation and/or improve the predictability of such violations (*RegTech*). Going one step further (Lessig, 2006), in some cases, the regulator could be replaced by the computer code when regulatory compliance is enshrined in the design of the digital technologies (*compliance by design*). In that case, compliance will be automated (as in smart contracts for instance), hence the role of regulator is by-passed or at least reduced. The development of RegTech and compliance by design raise a series of ethical and legal issues that will need to be addressed during the next parliamentary legislature.

⁷¹ Furman et al. (2019) also suggest the development of code of competitive conducts with the participation of stakeholders.

REFERENCES

- Bauer M. (2017), *Right Direction, Wrong Territory: Why the EU's Digital Single Market Raises Wrong Expectations*, American Enterprise Institute.
- Bauer M. (2018), *Online Platforms, Economic Integration and Europe's Rent-Seeking Society*, ECIPE Policy Brief.
- Crème J., Y.A. de Montjoye, H. Schweitzer (2019), *Competition Policy for the digital era*, Report for the European Commission
- Civic Consulting (2014), *Contribution of the Internal Market and Consumer Protection to Growth*, Study for the IMCO Committee
- de Streel A. and P. Larouche (2016), *An Integrated Regulatory Framework for Digital Networks and Services*, CERRE Policy Report.
- de Streel A. and C. Hocepiéd (2017), *Optimal regulatory model for telecommunications services in the EU*, Study for the IMCO Committee of the European Parliament.
- de Streel A., M. Buitten and M. Peitz (2018), *The Liability of Online Platforms: Should exceptionalism end?*, CERRE Policy Report, Sept. 2018
- Dittrich, P.J. (2017), *Balancing Ambition and pragmatism for the digital single market*, Jacques Delors Institute Policy Paper 204.
- Dittrich, P.J. and J. Krewer (2018), *The European answer to the digital revolution*, Jacques Delors Institute Policy Brief.
- Eberlein B. (2004), *The Institutional Dynamics of Regulation in the EU: Formal and Informal Institutions in Supranational Governance*, *14th International Conference of Europeanists*, Chicago, p.7.
- EPRS (2017), *Mapping the Cost of Non-Europe 2014-2019*, 4th edition
- Erixon F. and P. Lamprecht (2018), *The Next Steps for the Digital Single Market: From Where do We Start?*, ECIPE Policy Brief 2/2018.
- Floridi L. and M. Taddeo (2017). *The responsibility of Online Service Providers*, Springer.
- Furman J. et al. (2019), *Unlocking digital competition*, Report of the Digital Expert Panel.
- Gans J. (2018), *Enhancing Competition with Data and Identity Portability*, The Hamilton Project Policy Proposal 2018/10.
- Godel M., Harms A., Jones S., Mantovani I. (2016), *Reducing Costs and Barriers for the Businesses in the Single Market*, Study for the IMCO Committee of the European Parliament.
- Joint Research Centre (2018), *Artificial Intelligence: A European perspective*.
- Lessig L. (2006), *Code and Other Laws of the Cyberspace – Version 2.0*, Basic Book.
- Lisbon Council (2018), *Digital Europe: Next Steps*, A European Agenda for the Digital 9+.
- Lisbon Council (2019), *A Roadmap for a Fair Data Economy*, Policy Brief.
- Maciejewski M. et al. (2015), *EU Mapping: Overview of IMCO Related Legislation*, Study for the IMCO Committee.

- Maciejewski M. et L.C. Matos (2018), *EP-EUI Roundtable on Strategy for Artificial Intelligence in Europe*, Study for the IMCO Committee.
- Martens B. (2016), *An Economic Policy Perspective on Online Platforms*, *JRC Digital Economy Working Paper 2016-05*.
- Mayer-Schonberger V. and T. Ramge (2018), *Re-inventing capitalism in the age of big data*, Ed. John Murray.
- McKinsey Global Institute (2018), *European Economy: Three Pathways to rebuilding trust and sustaining momentum*, Briefing Note for Davos.
- Muller P., Conlon G., Denvani S. and Benard C. (2013), *Performance-based Policy*, Study for the IMCO Committee of the European Parliament.
- Muller P., S. Jones and L. Koch (2015), *Smart Single Market Regulation*, Study for the IMCO Committee of the European Parliament.
- Naess-Schmidt H. et al. (2012), *Simplifying and Modernising VAT in the Digital Single Market*, Study for IMCO.
- Nordemann, J.B. (2018), *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, In-Depth Analysis for the IMCO Committee of the European Parliament.
- OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publications.
- Poiares Maduro M., G. Monti and G. Coelho (2016), *The Geo-blocking proposal: Internal market, competition law and regulatory aspects*, Study for the IMCO Committee of the European Parliament.
- Renda A. (2017), *Reforming e-communications services: A critical assessment*, In-Depth analysis for the IMCO Committee of the European Parliament.
- Renda A. (2018), *The legal framework to address “fake news”: possible policy actions at the EU level*, In-Depth analysis for the IMCO Committee.
- TNO, WIK-Consult and RAND (2013), *Ubiquitous Developments of the Digital Single Market*, Study for the IMCO Committee of the European Parliament.

ANNEX LIST OF DIGITAL SINGLE MARKET LEGAL INSTRUMENTS

Digital Single Market Strategy

- **Communication** from the Commission of 6 May 2015, **A Digital Single Market Strategy for Europe**, COM(2015) 192.
- **Resolution of the European Parliament of 19 January 2016 on Towards a Digital Single Market Act, 2015/2147 (INI).**
- **Communication** from the Commission of 10 May 2017, **Mid-Term Review on the implementation of the Digital Single Market Strategy**, COM(2017) 228.
- **Communication** from the Commission of 15 May 2018, **Completing a trusted Digital Single Market for all**, COM(2018) 320.

E-commerce and online Platforms

Legislation

- **Regulation 2017/1128** of the European Parliament and of the Council of 14 June 2017 on **cross-border portability of online content** services in the internal market, O.J., L 168, 30.06.2017, p. 1.
- Council **Directive 2017/2455** of 5 December 2017 amending Directive 2006/112 and Directive 2009/132 as regards certain **value added tax** obligations for supplies of services and distance sales of good, O.J., L 348, 29.12.2017, p. 7.
- Council **Regulation 2017/2454** of 5 December 2017 amending Regulation 904/2010 on administrative cooperation and combating fraud in the field of **value added tax**, O.J., L 348, 29.12.2017, p. 1.
- Council **Implementing Regulation 2017/2459** of 5 December 2017 amending Implementing Regulation 282/2011 laying down implementing measures for Directive 2006/112/EC on the **common system of value added tax**, O.J., L 348, 29.12.2017, p. 32.
- **Regulation 2018/302** of the European Parliament and of the Council of 28 February 2018 on addressing **unjustified geo-blocking** and other forms of discrimination based on consumers' nationality, place of residence or place of establishment within the internal market and amending Regulation 2006/2004 and 2017/2394 and Directive 2009/22, O.J., L 60/l, 2.3.2018, p.1.
- **Regulation 2018/644** of the European parliament and of the Council of 18 April 2018 on **cross-border parcel delivery** services, O.J., L 112 of 2.5.2018, p. 19.
- Commission **Implementing Regulation 2018/1263** of 20 September 2018 establishing the **forms for the submission of information by parcel delivery service providers** pursuant to Regulation 2018/644 of the European Parliament and of the Council, parcel delivery service providers pursuant to Regulation (EU) 2018/644 of the European Parliament and of the Council O.J., L 238, 21.9.2018, p. 65.
- **Council Directive 2018/1713** of 6 November 2018 amending Directive 2006/112, as regards rates of **value added tax applied to books, newspapers and periodicals**, O.J., L 246 of 14.11.2018, p. 20.
- **Directive 2018/1808** of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services (**Audiovisual Media Services Directive**) in view of changing market realities, O.J., L 303 of 28.11.2018, p. 69.
- **Regulation 2019/XXX** of the European Parliament and of the Council of 19 March 2019 on the implementation and functioning of the **.eu Top Level Domain name** and amending and repealing Regulation 733/2002 and repealing Commission Regulation 874/2004, to be published in the OJ.

- **Directive 2019/XXX** of the European Parliament and of the Council on **copyright in the Digital Single market**, to be published in the OJ.
- **Directive 2019/XXX** of the European Parliament and of the Council on laying down rules on the exercise of **copyright** and related rights applicable to certain online transmissions of **broadcasting organisations** and retransmissions of television and radio programmes, to be published in the OJ.
- **Regulation 2019/XXX** of the European Parliament and of the Council on promoting **fairness and transparency for business users of online intermediation services**, to be published in the OJ.
- *Proposal of the Commission of 12 September 2018 for a **Regulation** of the European Parliament and of the Council on **preventing the dissemination of terrorist content online**, COM (2018) 640.*

Soft-Law

- **Communication** from the Commission of 2 June 2016, A **European agenda for the collaborative economy**, COM (2016) 356.
- Final report of the Commission of 10 May 2017 on the **E-commerce Sector Inquiry**, COM(2017) 229.
- Commission **Recommendation 2018/344** of 1 March 2018 on measures to effectively tackle **illegal content online**, O.J., L 63 of 6.3.2018, p. 50.

E-Government

Legislation

- **Regulation 2018/1724** of 2 October 2018 the European Parliament and the Council establishing a **single digital gateway** to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation 1024/2012, O.J. L 295 21.11.2018, p. 1.

Soft-law

- **Communication** from the Commission of 19 April 2016, **EU e-Government Action Plan 2016-2020**. Accelerating the digital transformation of government, COM (2016) 179.
- **Communication** of the Commission of 23 March 2017, **European Interoperability Framework**, COM(2017) 134.

Data and Artificial Intelligence

Legislation

- **Regulation 2016/679** of the European Parliament and of the Council 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**, and repealing Directive 95/46 (**General Data Protection Regulation**), O.J., L 119, 4.5.2016, p. 1.
- **Directive 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the **processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences** or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O.J., L 119, 4.5.2016, p. 89.
- Council **Regulation 2018/1488** of 28 September 2018 establishing the **European High-Performance Computing** Joint Undertaking, O.J., L 252, 8.10.2018, p. 1.
- **Regulation 2018/1807** of the European Parliament and of the Council of 14 November 2018 on a framework for the **free flow of non-personal data** in the European Union, O.J., L 303 of 28.11.2018, p. 59.

- **Directive 2019/XXX** of the European Parliament and of the Council on **open data and the re-use of public sector information**, to be published in OJ.
- *Proposal of the Commission of 10 January 2017 for Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58 (**Regulation on Privacy and Electronic Communications**), COM(2017) 10.*

Soft-law

- **Communication** from the Commission of 19 April 2016, **ICT Standardisation Priorities for the Digital Single Market**, COM(2016) 176
- **Communication** from the Commission of 19 April 2016, **European Cloud Initiative - Building a competitive data and knowledge economy in Europe**, COM(2016) 178.
- **Communication** from the Commission of 19 April 2016, **Digitising European Industry - Reaping the full benefits of a Digital Single Market**, COM(2016) 180.
- Commission **Recommendation 2018/790** of 25 April 2018 on **access to and preservation of scientific information**, O.J. L 134, 31.5.2018, p. 12.
- Commission Staff Working Document of 25 April 2018, **Guidance on sharing private sector data in the European data economy**, SWD(2018) 125
- **Communication** from the Commission of 8 April 2019, **Building Trust in Human-Centric Artificial Intelligence**, COM(2019) 168.

Security

Legislation

- **Directive 2016/1148** of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (**Network Information Security**), O.J., L 194, 19.7.2016, p.1.
- **Regulation 2019/XXX** of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency and on Information and Communication Technology cybersecurity certification (**Cybersecurity Act**), to be published in the OJ.
- **Regulation 2019/XXX** of the European Parliament and of the Council **establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**, to be published in the OJ.

Soft-law

- Commission **Recommendation 2017/1584** of 13 September 2017 on coordinated response to **large-scale cybersecurity incidents** and crises, O.J., L 239, 19.9.2017, p. 36.
- **Communication** from the Commission of 4 October 2017, **Making the most of NIS – towards the effective implementation of Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union**, COM (2017) 476.
- **Consumer protection in the digital era**

Legislation

- **Regulation 2017/2394** of the European Parliament and of the Council of 12 December 2017 on **cooperation between national authorities** responsible for the enforcement of consumer protection laws and repealing Regulation 2006/2004, O.J., L 345, 27.12.2017, p. 1.

- **Directive 2019/XXX** of the European Parliament and of the Council as regards better **enforcement and modernisation of EU consumer protection**, to be published in the OJ.
- **Directive 2019/XXXX** of the European Parliament and of the Council on certain aspects concerning **contracts for the supply of digital content**, to be published in OJ.

Soft-law

- Commission Staff **Guidance** of 25 May 2016 on the **implementation/application of Directive 2005/29 on Unfair Commercial Practices**, SWD (2016) 163.

Electronic Communications Networks and Services

- **Regulation 2015/2120** of the European Parliament and of the Council of 25 November 2015 laying down measures concerning **open internet access and retail charges for regulated intra-EU communications** and amending Directive 2002/22 and Regulation 531/2012 on **roaming on public mobile communications networks** within the Union, O.J., L 310, 26.11.2015, p. 1, as amended by Regulation 2018/1971.
- Commission **Implementing Regulation 2016/2286** of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail **roaming surcharges** and on the application to be submitted by a roaming provider for the purposes of that assessment, O.J., L 344, 17.12.2016, p. 46.
- **Regulation 2017/920** of the European Parliament and of the Council of 17 May 2017 amending Regulation 531/2012 as regards rules for **wholesale roaming markets**, O.J., L 147, 9.6.17 p.1.
- **Decision 2017/899** of the European Parliament and of the Council of 17 May 2017 on the **use of the 470-790 MHz frequency band** in the Union, O.J., L 138, 25.5.2017, p. 131.
- **Regulation 2017/1953** of the European Parliament and of the Council of 25 October 2017 amending Regulations 1316/2013 and 283/2014 as regards the promotion of **internet connectivity in local communities**, O.J., L 286, 1.11.2017, p. 1.
- **Regulation 2018/1971** of the European Parliament and of the Council of 11 December 2018 establishing the **Body of the European Regulators for Electronic Communications**, O.J. L 321 of 17.12.2018, p.1.
- **Directive 2018/1972** of the European Parliament and of the Council of 11 December 2018 establishing the **European Electronic Communications Code**, O.J., L 321 of 17.12.2018, p. 36.

Soft-Law

- Commission Guidelines of 27 April 2018 on market analysis and the **assessment of significant market power** under the EU regulatory framework for electronic communications networks and services, O.J., C 159, 7.5.2018, p.1.

This study reviews all the rules adopted during the 8th Parliamentary legislature (2014-2019) to strengthen the Digital Single Market. On that basis, the report analyses the rights and obligations as well as the institutions and procedures created or improved in the main policy fields of the Digital Single Market (e-commerce and online platforms, e-government, data and AI, cybersecurity, consumer protection and electronic communications networks and services). Finally, the report identifies remaining gaps and possible actions for the forthcoming Parliament's legislature.

This document has been prepared for the IMCO Committee at the request of the Policy Department A of the European Parliament.

PE 638.395
IP/A/IMCO/2017-17

Print ISBN 978-92-846-4819-1 | doi: 10.2861/71422 | QA-04-19-421-EN-C
PDF ISBN 978-92-846-4818-4 | doi: 10.2861/979516 | QA-04-19-421-EN-N

Contribution to Growth: European Digital Single Market

Delivering improved rights for
European citizens and
businesses

Abstract

This study reviews all the rules adopted during the 8th Parliamentary legislature (2014-2019) to strengthen the Digital Single Market. On that basis, the report analyses the rights and obligations as well as the institutions and procedures created or improved in the main policy fields of the Digital Single Market (e-commerce and online platforms, e-government, data and AI, cybersecurity, consumer protection and electronic communications networks and services). Finally, the report identifies remaining gaps and possible actions for the forthcoming Parliament's legislature.

This document has been prepared for the IMCO Committee at the request of the Policy Department A of the European Parliament.

This document was requested by the European Parliament's Committee on the Internal Market and Consumer Protection.

AUTHORS

Prof. Dr Alexandre de STREEL, University of Namur and CERRE (Centre on Regulation in Europe)
Christian HOCEPIED, University of Namur

With the assistance of Michael LOGNOUL and Zorana ROSIC, University of Namur

ADMINISTRATOR RESPONSIBLE

Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT

Irene VERNACOTOLA

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:

Policy Department for Economic, Scientific and Quality of Life Policies

European Parliament

L-2929 - Luxembourg

Email: Poldep-Economy-Science@ep.europa.eu

Manuscript completed: May 2019

Date of publication: May 2019

© European Union, 2019

This document is available on the internet at:

<http://www.europarl.europa.eu/supporting-analyses>

DISCLAIMER AND COPYRIGHT

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

For citation purposes, the study should be referenced as: de STREEL, A., *Contribution to Growth: European Digital Single Market. Delivering improved rights for European citizens and businesses*, Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019

CONTENTS

LIST OF FIGURES	4
LIST OF TABLES	4
LIST OF ABBREVIATIONS	5
EXECUTIVE SUMMARY	6
1. INTRODUCTION	11
2. POLICY AND REGULATORY TECHNIQUES TO BUILD THE DIGITAL SINGLE MARKET	13
2.1 EU substantive rules: Unification or harmonisation of national rules	14
2.2. EU procedural rules: Unification or harmonisation of enforcement	17
2.3. Non regulatory techniques to reduce national divergences	18
3. MAIN ACHIEVEMENTS DURING THE 8TH PARLIAMENTARY LEGISLATURE	19
3.1. E-commerce and Online platforms	23
3.2. E-Government	28
3.3. Data and Artificial Intelligence	32
3.4. Security	36
3.5 Consumer Protection in the digital era	40
3.6. Electronic Communications Networks and Services	42
4. FUTURE POTENTIAL OF THE DIGITAL SINGLE MARKET AND POSSIBLE INITIATIVES	46
4.1 Applying and evaluating the newly adopted rules	47
4.2. Digitalizing and deepening the single market	47
4.3. Smart policy and regulatory techniques	50
REFERENCES	51
ANNEX LIST OF DIGITAL SINGLE MARKET LEGAL INSTRUMENTS	53

LIST OF FIGURES

Figure 1:	The Six Building blocks of the Digital Single Market	12
Figure 1:	Feedback loops between platform scale-up and single market	49

LIST OF TABLES

Table 1:	Main achievements of the 8th legislature to stimulate the Digital Single Market	9
Table 2:	List of legal instruments adopted or proposed during the 8th Legislature to build the Digital Single Market	21
Table 3:	EU rules regarding e-commerce and online platforms	26
Table 4:	EU rules regarding e-government	31
Table 5:	EU rules regarding data and AI	35
Table 6:	EU rules regarding security	37
Table 7:	EU rules regarding consumer protection	41
Table 8:	EU rules regarding electronic communications networks and services	45

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programme Interface
AVMS	Audio-Visual Media Services
BEREC	Body of European Regulators for Electronic Communications
CPC	Consumer Protection Cooperation
CSIRT	Computer Security Incident Response Team
DCD	Digital Content Directive
DESI	Digital Economy and Society Index
DSM	Digital Single Market
EECC	European Electronic Communications Code
EESSI	Electronic Exchange of Social Security Information
EIDAS	electronic IDentification, Authentication and trust Services
ENISA	European Network Information Security Agency
ERGA	European Regulators Group for Audiovisual Media Services
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
HPC	High Performance Computing
IOT	Internet of Things
NIS	Network Information Security
P2B	Platform-to-Business
PSI	Public Sector Information
RSPG	Radio Spectrum Policy Group
TLS	Internet Top Level Domain
UCPD	Unfair Commercial Practices Directive
VAT	Value Added Tax

EXECUTIVE SUMMARY

In May 2015, the European Commission launched a very ambitious agenda to strengthen the Digital Single Market (DSM) for Europe that led to a very intense activity of the European Parliament in this field during the 8th legislature (2014-2019). This Study analyses (i) the barriers eliminated or reduced by specific DSM legislative measures, (ii) the specific rights and obligations as well as the legal institutions or procedures introduced or improved by those measures and (iii) the remaining gaps and possible actions for the forthcoming Parliament's legislature. The Annex lists all the specific legislative measures adopted during the 8th legislature.

The Study is organised as follows: (i) the first section explains the policy techniques used by the EU institutions to stimulate the DSM (*how* it was achieved), (ii) the second section reviews the different measures adopted in the main building blocks of the DSM, the rights and obligation they have established and the barrier to the internal market they have removed (*what* was achieved) and (iii) the third section proposes future reforms for the next Parliamentary legislature.

1. Policy and regulatory techniques to achieve the Digital Single Market

The EU institutions may rely on **diverse policy techniques to build the Digital Single Market** and remove barriers to trade between Member States. Some techniques are regulatory and aim, on the one hand, to unify or harmonise across the EU the substantive rules and, on the other hand, to unify or harmonise the enforcement of those rules. Other techniques are non-regulatory and rely on action plans, policy benchmarking or financial support.

EU unification and harmonisation of the substantive rules can be achieved with hard law, in particular Regulations that are directly applicable or Directives that need to be transposed into national law. They can also be stimulated with the soft-law, in particular with Recommendations or Guidelines giving interpretation of existing EU laws or recommending particular approach in national laws or with Codes of conduct or Memorandum of Understanding to involve more closely stakeholders in the elaboration of the rules (participatory regulation). **In the digital field, Regulations have been used extensively** and represent a higher proportion of legislative acts than in other EU policy fields. In addition, **several Recommendations and Guidelines** have been adopted to ensure a common interpretation of those rules. Finally, multiple **Codes of conduct** were agreed by the industry to supplement or substitute the adoption of hard-law.

However, common EU rules are not enough to achieve the single market if those rules are implemented by national authorities differently across the Member States. This is why many institutional and procedural rules are needed to **unify or harmonise across the EU the enforcement mechanisms**. They should respect the constitutional and procedural autonomy of the Member States. **In the digital field, many procedural rules were adopted to improve the quality of the national enforcement agencies as well as their cooperation at the EU level**, in particular through the establishment or the strengthening of EU networks of agencies.

Next to rules, **non-regulatory actions** are also key to stimulate the single market, in particular in area where the adoption of legislation is difficult or not appropriate. In the digital field, numerous **policy action plans** were adopted to coordinate EU and national digital policies. **Benchmarking** of national digital policies to diffuse best practices across the Member States are also common. Finally, increasing amount of **EU funds** have been allocated to digital initiatives.

2. Main achievements in removing barriers in the Digital Single Market during the 8th legislature

During the 8th legislature, the European Parliament and the other EU institutions have been very active in the digital field. To review the numerous achievement, we present **the DSM measures into six building blocks**. The two first blocks relate to the digital services used by European consumers and citizens: the e-commerce and online platforms and the e-government services. The three successive blocks are horizontal and necessary to ensure the development of and the trust in private and public digital services; they relate to data and AI, security and the specific consumer protection for the digital era. Finally, the last block relates to the infrastructures on which the digital applications are provided: the electronic communications networks and services. Most of policy actions **during the 8th legislature took place for e-commerce and online platforms as well as for data and AI**.

For each building block, we analyse, as summarised in Table 1 below, how the specific DSM measures (i) **directly facilitate cross-border trade** by removing specific barriers to the single market, (ii) **unify or harmonise the national substantive rules** which indirectly ease cross-border operations and create specific rights and obligations and (iii) **unify or harmonise the enforcement** of those rules and establish legal institutions and procedures which also indirectly ease cross-border operations.

Regarding **e-commerce and online platforms**, some of the main impediments to cross-border trade have been removed or reduced with the cross-border portability of some digital content, the prohibition of unjustified geo-blocking, the simplification of VAT declaration and collection, the improvement of eu. Top Level Domain and the new copyright rules facilitating access to online TV and radio content across borders. Moreover, several national rules on the operations of online platforms have been harmonised, in particular for platforms offering audio-visual media services and intermediation services as well as platforms hosting illegal or harmful online content. To ensure effective and harmonised enforcement of those rules, ERGA - the network of national media regulators - has been strengthened.

Regarding **e-government**, which remains a national competence, the EU institutions can merely stimulate the adoption and the diffusion of best practices across the Member States as well as facilitate the interoperability between the different national public services, as for example by the setting up a single digital gateway. The EU is also leading by example by digitizing its own public services.

Regarding **data and AI**, data location requirements have been limited. Moreover, several national rules on the governance of data have been harmonised in order to ease cross-border data businesses and the movement of data across the EU while ensuring strict privacy protection and respecting EU values and fundamental rights. This is the case for personal data with the now famous General Data Protection Regulation (GDPR), for public data with the new Open Data and Public Sector Information Directive and for non-personal and non-public data where best practices for data sharing have been established. To ensure effective and harmonised enforcement of data protection rules, a new European Data Protection Board (EDBP) has been established between the national data protection authorities. In addition, a plan to stimulate AI in Europe has been coordinated between the EU and the Member States and new EU funds are being made available.

Regarding **security**, an EU cyber-security culture is emerging. New cooperation between cybersecurity agencies have been set up, ENISA will become an EU level Cybersecurity agency, a new EU Competence Centre has been set up and EU funds have been made available to strengthen network security.

Regarding **consumer protection**, an adaptation of the existing consumer acquis to the characteristics of the digital sector, in particular the lack of monetary prices and the difficulties to understand the

Table 1: Main achievements of the 8th legislature to stimulate the Digital Single Market

	E-commerce and online Platforms	E-Government	Data and AI	Security	Consumer protection in the digital era	Electronic communications networks and services
EU rules facilitating cross-border trade	<ul style="list-style-type: none"> - Cross-border portability content - Geo-blocking - VAT e-commerce - Cross-border parcel delivery - .eu top domain level - Facilitating cross-border access to online TV and radio content 	<ul style="list-style-type: none"> - Digital Single Gateway - VAT One Stop shop 	<ul style="list-style-type: none"> - Limitation of data location requirements 	<ul style="list-style-type: none"> EU cybersecurity certification 		<ul style="list-style-type: none"> - International roaming - International calls - EU numbering space
Unification or harmonisation of national rules	<ul style="list-style-type: none"> - Media services - Transparency for online platforms - Effective removal of illegal content online 	<ul style="list-style-type: none"> - Interoperability framework 	<ul style="list-style-type: none"> - Personal data: protection of privacy - Public data: openness - Private data: sharing 	<ul style="list-style-type: none"> - NIS requirements and notification 	<ul style="list-style-type: none"> - Adaptation of the consumer protection rules to the characteristics of digital economy 	<ul style="list-style-type: none"> - Adaptation of telecoms rules to stimulate investment in very high capacity infrastructures (fibre and 5G) while protection consumers - Better coordination of spectrum assignment, in particular the 700 MHz band
Unification or harmonisation of national enforcement	<ul style="list-style-type: none"> - DG COMP Sector enquiry on e-commerce - Strengthening of ERGA 		<ul style="list-style-type: none"> - Establishment of EDPB 	<ul style="list-style-type: none"> - Cooperation in large scale incidents - Network of CSIRT - Strengthening ENISA - EU Cybersecurity Industrial, Technology and Research Centre 	<ul style="list-style-type: none"> - Strengthening CPC Network 	<ul style="list-style-type: none"> - Strengthening of BEREC - Strengthening RSPG
Action plan and coordination of national strategies		<ul style="list-style-type: none"> - eGov Action Plan 	<ul style="list-style-type: none"> - Coordination of AI Strategies 			

3. Future potential of the Digital Single Market and possible initiatives for the next legislature

As many regulatory and non-regulatory actions have been taken during the 8th legislature, the first task is to **implement those new rules in an effective and harmonised manner** across Europe. This is particularly important because most of those EU substantive rules are implemented by national authorities. Then the **efficiency and the effectiveness of the rules and their enforcement should be evaluated**, in particular the impacts on the economy and the society.

However, evaluating the effects of the actions already adopted will not be enough given the importance of the digital technologies for the European economy and society, the rapid pace of evolution of those technologies and the increasing global competition for digital leadership. To respond to changes, the **pace of reform should remain important during the forthcoming 9th legislature**.

Regarding the objectives and policy fields, we have identified the following **priorities**:

- (i) **Make the EU a technological powerhouse for the emerging and important technologies** such as AI, quantum computing, security of connected devices or data exchanges that should be designed and developed according to European values enshrined in the Treaties and the Charter of Fundamental Rights;
- (ii) Stimulate the **development of online platforms**: (i) start-up should be stimulated by rules ensuring a level playing and access to the main capabilities for digital innovation (in particular data) and to the eco-system of products that are used by consumers, (ii) scale-up should be stimulated by one set of rules and enforcement all over Europe, (iii) and significant platforms should be subject to an increased duty of care;
- (iii) Stimulate **e-government**: given the potential benefits of digital public services, the EU should stimulate the adoption and the diffusion of national and cross-borders e-government services as well as the adoption of digital technologies, such as blockchain, to improve public regulation.

Regarding the **policy and regulatory techniques**, we recommend the reliance of **principles-based legislation** that can easily adapt to fast and unpredictable technology and market evolutions **complemented with codes of conduct** agreed with all the digital players (firms, consumers associations, NGOs ...) under the auspices of EU institutions and with a close monitoring by the EU institutions. We also recommend that the **enforcement of those rules is more Europeanised** either with the continuous strengthening of the cooperation network of national regulatory authorities or with the **establishment of a EU regulator for significant platforms** as it was done some years ago for the significant banks with the creation of the Single Supervisory Mechanism within the European Central Bank. The **regulatory authorities in Europe should also size the potential of digital technologies**, such as big data or AI, to improve their operations (*RegTech*). To go further when feasible, enforcement may be automatized in the computer code as it is the case for smart contracts or privacy by design (more generally, *compliance by design*).

Those regulatory actions should be **complemented with non-regulatory initiatives**, in particular the monitoring and exchange of best practices of key digital national policies, the increasing smart use of EU funds to stimulate the deployment and the adoption of key digital networks and services and the development of the digital skills of EU workers and citizens.

1. INTRODUCTION

The Digital Market Strategy

On 6 May 2015, the European Commission launched its Digital Market Strategy for Europe,¹ announcing ambitious legislative steps towards a connected digital single market. The Strategy was built on three pillars:

- *Better access for consumers and businesses to online goods and services across Europe* – by removing of key differences between the online and offline worlds to break down barriers to cross-border online activity;
- *Creating the right conditions for digital networks and services to flourish* – by fostering high-speed, secure and trustworthy infrastructures and content services, through the right regulatory conditions for innovation, investment, fair competition and a level playing field; and
- *Maximising the growth potential of our European Digital Economy* – by promoting investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competitiveness as well as better public services, inclusiveness and skills.

At the same time, the Commission stressed, that these actions must “*go hand-in-hand with efforts to boost digital skills and learning across society and to facilitate the creation of innovative start-ups*” and that “*enhancing the use of digital technologies and online services should become a horizontal policy, covering all sectors of the economy and of the public sector.*”² The European Parliament welcomed this programme in a Resolution of 19 January 2016 on a Digital Single Market Act and called for ambitious actions.³

Aims of this Study

This study aims to update, for the Digital Single Market, the findings related to EU digital policies of Civic Consulting Study (2014) on the Contribution of the Internal Market and Consumer Protection to Growth. To do that this Study analyses (i) the barriers eliminated or reduced by specific DSM legislative measures adopted during the 8th legislature (2014-2019), (ii) the specific rights and obligations as well as the legal institutions or procedures introduced or strengthened by those measures and (iii) the potential future initiatives that should be elaborated and discussed during the forthcoming 9th legislature. This Study focuses on legal issues and is complemented by the companion economic study on the benefits of the European Digital Single done by Dr. Scott Marcus and his team at Bruegel.

To analyse the numerous achievement, we organise the DSM measures into six building blocks following Maciejewski (2015:19) as explained in Figure 1 below.

¹ Communication from the Commission of 6 May 2015, A Digital Single Market Strategy for Europe, COM(2015) 192. See <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market> and <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market>

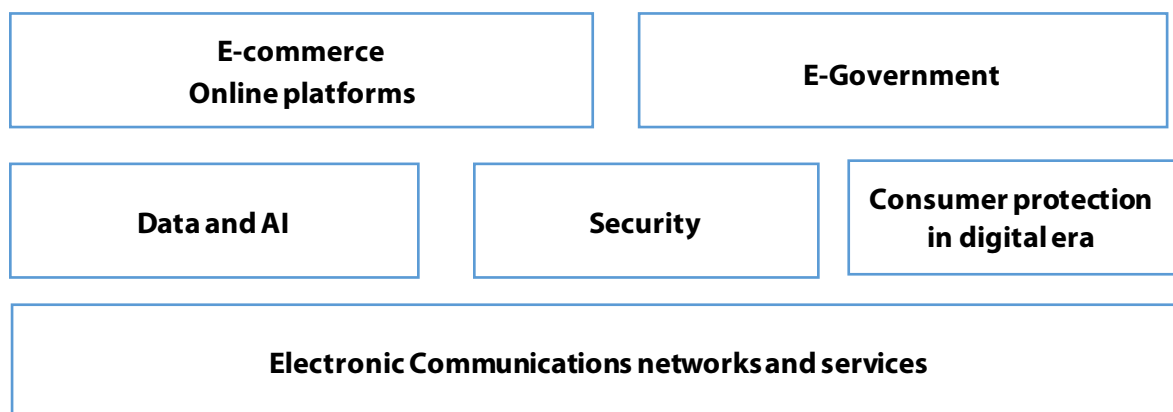
² Idem, p. 2.

³ 2015/2147 (INI).

The two first blocks relate to private and public digital applications used by European consumers and citizens: the e-commerce and online platforms and the e-government services.

The three successive blocks are horizontal and necessary to ensure the development of and the trust in private and public digital services: they relate to data and AI, security and the specific consumer protection for the digital era. Finally, the last block relates to the infrastructures on which digital applications are provided: the electronic communications networks and services.

Figure 1: The Six Building blocks of the Digital Single Market



The Study is organised as follows: After this brief introduction the first section explains the policy techniques used by the EU institutions to stimulate the DSM (*how* it was achieved). Then, the second section reviews the different measures adopted in the main building blocks of the DSM, the rights and obligation they have established and the barriers to the internal market they have removed (*what* was achieved). Finally, the third section proposes future reforms for the next Parliamentary legislature. The Annex lists all the specific legislative measures introduced during the 8th Parliamentary legislature.

2. POLICY AND REGULATORY TECHNIQUES TO BUILD THE DIGITAL SINGLE MARKET

KEY FINDINGS

The EU institutions may rely on **diverse policy techniques to build the Digital Single Market** and remove barriers to trade between Member States. Some techniques are regulatory and aim, on the one hand, to unify or harmonise across the EU the substantive rules and, on the other hand, to unify or harmonise the enforcement of those rules. Other techniques are non-regulatory and rely on action plans, policy benchmarking or financial support.

EU unification and harmonisation of the substantive rules can be achieved with hard law, in particular Regulations that are directly applicable or Directives that need to be transposed into national law. They can also be stimulated with the soft-law, in particular with Recommendations or Guidelines giving interpretation of existing EU laws or recommending particular approach in national laws or with Codes of conduct or Memorandum of Understanding to involve more closely stakeholders in the elaboration of the rules (participatory regulation). **In the digital field, Regulations have been used extensively** and represent a higher proportion of legislative acts than in other EU policy fields. In addition, **several Recommendations and Guidelines** have been adopted to ensure a common interpretation of those rules. Finally, multiple **Codes of conduct** were agreed by the industry to supplement or substitute the adoption of hard-law.

However, common EU rules are not enough to achieve the single market if those rules are implemented by national authorities differently across the Member States. This is why many institutional and procedural rules are needed to **unify or harmonise across the EU the enforcement mechanisms**. They should respect the constitutional and procedural autonomy of the Member States. **In the digital field, many procedural rules were adopted to improve the quality of the national enforcement agencies as well as their cooperation at the EU level**, in particular through the establishment or the strengthening of EU networks of agencies.

Next to rules, **non-regulatory actions** are also key to stimulate the single market, in particular in area where the adoption of legislation is difficult or not appropriate. In the digital field, numerous **policy action plans** were adopted to coordinate EU and national digital policies. **Benchmarking** of national digital policies to diffuse best practices across the Member States are also common. Finally, increasing amount of **EU funds** have been allocated to digital initiatives.

The Digital Single Market Strategy relies on different regulatory and non-regulatory techniques. Legislation appears to be, by far, the privileged approach. The 'acquis' is impressive and will still require many years to be fully implemented because implementation in practice often require periods longer than a Parliament legislature. The number of Commission Communications reflects the absence of executive powers at EU level. Instead of launching specific projects – which the Commission successfully did for example for the Electronic Exchange of Social Security Information (EESSI) – the Commission is obliged to promote best practices and general principles, without certainty of effective results. Another finding is that the Digital Single Market cannot be forced through a top down approach.

Public private partnerships, test projects and other research networks play a key role in developing applications that will give a face to the concept of digital and show its benefits.

The Commission has clearly understood this as reflected by its proposed Digital Europe programme for the period 2021-2027. More than regulation, funding is the lifeblood of digitization.

2.1 EU substantive rules: Unification or harmonisation of national rules

a. Types of EU legal instruments

Regulations are legislative acts that can directly be enforced by national courts in the EU. Regulations must be applied in their entirety across the EU. However, the use of Regulations does not suffice to achieve full harmonization of the national rules. Some provisions of Regulations may not be directly applicable and yet require further implementation measures or interpretations.⁴ **Directives** are legislative acts that set out a goal that all EU countries must achieve. Directives are binding for the Member States, but normally not for citizens and undertakings. It is up to the individual countries to devise their own laws on how to reach these goals. However, national measures transposing Directives must be of a binding character and not merely in the form of administrative practices. Some Directives do however go further than setting goals. They can require Member States to set up national regulatory authorities and give them far-reaching powers. This is the case in the telecom and postal sectors, for the broadcasting sector, data protection and, increasingly, in the area of consumer protection. **Decisions** are binding on those to whom it is addressed (e.g. an EU country or an individual company) and are directly applicable. Decisions are rarely used in the digital sector.⁵

Recommendations can, in principle, not be enforced in national courts. A Recommendation allows the EU institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed. However, national courts have considered that national authorities have not complied with obligations under national law to give reasons for their decisions when these decisions diverged from the line of action recommended by the Commission, without the national authority providing adequate justifications for its own line of action. Recommendations – which can be named ‘guidelines’ or ‘communication’ – go beyond peer pressure and naming and shaming exercises, like the Digital Economy and Society Index (DESI).⁶ Recommendations play an essential role to ensure that national policies – though autonomous – are designed with the better functioning of the EU economy in mind.⁷

⁴ For example, Article 8 GDPR determines 16 as the relevant age of consent for minors when using information society services, but allows Member States to lower the age to 13 years. Many Member States have done so. In addition, the GDPR does not encroach on the principle of procedural autonomy, and Member States legislated on the organization of their national DPA(s) and the rules of procedure to be followed by the latter. On the other hand, the GDPR empowers the European Data Protection Board (EDPB) to adopt interpretative guidelines, stressing that, despite common rules, national practices are susceptible to remain different.

⁵ An example is the 700 MHz spectrum decision 2017/899, which requires that Member States would no later than 30 June 2018, adopt and make public their national plan and schedule (‘national roadmap’), to make this frequency band available for wireless broadband electronic communications services under harmonized technical conditions.

⁶ <https://digital-agenda-data.eu/datasets/desi/indicators>

⁷ For example, the Commission sets out principles and guidance on business to business (B2B) data sharing agreements, as well as on business to government (B2G) data sharing agreements, promoting voluntary harmonisation of practices across the EU.

b. Objectives of legal instruments

More than the instrument chosen, the content and nature of the solutions chosen to tackle the remaining barriers to the digital single market matters. This content can diverge on the following aspects.

Negative and positive integration

European integration studies firstly distinguish between negative and positive integration. **Negative integration** refers to provisions in EU law (or case-law) requiring Member States to remove certain national measures, no matter how the obstacle disappear.⁸ **Positive integration** addresses the fragmentation resulting from national rules with the adoption of common rules and regulatory standards across the EU, i.e. requires the Member States to adopt specific rules or principles and not only to prohibit Member States to enact measures restricting trade.

Country of origin and country of destination

Another distinction is between, on the one hand, the home state control or country of origin principle (mutual recognition) and, on the other hand, the country of destination' principle.⁹ The country of origin principle is the cornerstone of the Services Directive,¹⁰ but the Directive excludes several services from its scope, notably financial services, transport, telecommunications network services, gambling, health and certain social services.

In the telecommunications sector, the Commission proposed in 2013 to introduce the country of origin principle for the provision of electronic communications networks and services¹¹ to remove unnecessary obstacles in the authorisation regime and in the rules applying to service provision so that an authorisation obtained in one Member State is valid in all Member States, and that operators can provide services on the basis of consistent and stable application of regulatory obligations. But the proposal was not accepted. Besides the fear of some Member States to lose the control of operators active in their jurisdictions, the main reason seems to have been that every Member State would depend on the market surveillance of its neighbours. Consequently, weaknesses in the organisation of market surveillance in one single Member State could seriously undermine the efforts taken by other Member States and creates a weak link in the chain.

The reluctance of Member States to accept the country of origin principle implies that the country of destination principle underlies most of the EU legislation governing the Digital Single Market. The AVMS Directive, the e-commerce Directive and some copyright rules constitute exceptions.

⁸ An example of such provision is Article 92 of the EEC, which prohibits any discrimination on the basis of residence or nationality by providers of electronic communications networks or services, unless such different treatment is objectively justified.

⁹ This distinction originates from the Court of Justice, when specifying the underlying principles of the free movement of goods enshrined in the TFEU (at the time EEC Treaty) in respectively Case 120/78 *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein* and Case C-267/91 and C-268/91, *Keck and Mithouard*.

¹⁰ Directive 2006/123 of 12 December 2006 on services in the internal market, OJEU L 376, 27.12.2006, p. 36.

¹¹ Article 3 of the proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627.

This fact explains largely why the voluminous acquis could not tackle yet the fragmentation of national markets remains in the EU.

Maximum and minimum harmonization

The country of destination principle is thus one of the causes of the regulatory fragmentation of the single market because Member States impose more detailed and often more onerous obligations than those listed in the EU rules (regulatory gold-plating). To deal with this unintended consequence of harmonization legislation, maximum harmonisation is becoming more common. This does not mean that EU law would replace national law and constitute a uniform law applicable to the whole EU. Member States can still regulate the sector or activity as far as they do not impose more stringent obligations as regards the issues covered explicitly by the EU instruments.

However, the success of measures aimed at maximum harmonisation may be undermined by national legislation circumventing the scheme laid down in European rules.¹² In addition, given the preference of some for a high level of protection, the maximum harmonization risks being set at a level that dissuades commercial offers and investment, bringing the contrary of the aim pursued of boosting the offer of digital services and investment in digital networks.¹³

Maximum harmonisation is a goal worth pursuing, but is not the silver bullet to bring the single market. Even in the case of maximum harmonization, there is no guarantee that the rules will be enforced identically in each Member State. Indeed, new legislation, however well-designed, cannot avoid all regulatory gaps and implementation deficits, so that the need for more detailed rule-making and coordination on a transnational basis persist. The enforcement of Union harmonisation legislation remains the Member States' competence. The Court of Justice acknowledges the principle of procedural autonomy of the Member States, meaning that the actions necessary to achieve the objectives set forward by regulations or directives continue to be carried out by Member States' civil servants, except in the areas where the EU legislation gives specified implementation powers to an EU-body. However, until now EU legislator has been reluctant to give implementation powers to EU bodies.¹⁴

¹² An example is provided by the Electronic Communications Authorization Directive which regulates the fees that Member States can ask to telecommunications operators to deploy their electronic communications networks. Local authorities in the Member States are however not precluded to impose annual taxes on network installations such as antennas as long as the 'triggering' factor of the taxes is not related to the authorization to deploy a network. In practice, it might be difficult to establish what the precise 'triggering' factor.

¹³ And deregulation by the EU is legally not straightforward to pursue in the case of shared competences. Indeed, Article 2(2) TFEU implies that the Member States may maintain (or further expand) regulation in all domains where the EU would decide to abolish regulation.

¹⁴ In addition, the case law of the EU Court of Justice does not accept the granting of a wide margin of discretion to EU regulatory bodies. See Case C-270/12, United Kingdom v Parliament and Council, [2014].

2.2. EU procedural rules: Unification or harmonisation of enforcement

The Court of Justice stressed in its case law the balance between the autonomy of national systems to enforce EU law and the imperative of effective and uniform enforcement of EU law across all Member States.¹⁵ However, the concept of effectiveness remains subjective. National patterns of regulation and governance differ, notably, with respect to the power, autonomy and resources allocated to the bodies entrusted with the enforcement of the EU in the various domains of the digital sector. For this reason, the EU has in this 'two-tiered system', sought, where politically acceptable by the Member States, to regulate the regulators that deal directly with the addressees of regulation. However, any stringent or intrusive procedures allowing the Commission to interfere with the decision-making of national regulators are doomed to be blocked by political vetoes from adversely affected member states, or seeking to avoid precedents.

An alternative route was therefore followed: establishing EU enforcement networks grouping national authorities entrusted with the implementation of the EU rules concerned.¹⁶ For example, in the framework of the reform of the Consumer Protection Cooperation (CPC) Regulation, the Commission promoted harmonized rules governing the powers of enforcement authorities and the manner in which they can cooperate. The GDPR also requires, on the one hand, stronger enforcement powers for the national DPAs, while, on the other, ensuring that the DPAs coordinate their approaches via the EDPB. The EDPB's binding dispute resolution system can even lead to harmonised decisions, even in individual cases. This procedure is, today, likely a model to follow in other domains.

Next to public enforcement, the main aim of out of court mechanism is to facilitate dispute resolution by reducing their cost and speed. Moreover, out of court dispute resolution mechanism contribute to the single market in two ways:

- Directly, in the case of on-line resolution mechanisms. The best example is the internet platform created by the European Commission for the settlement of disputes arising from e-commerce. The whole out-of-court dispute resolution processes takes place on the internet, which means that long and expensive trials are avoided and that the European consumer's trust in cross-border shopping is strengthened.
- Indirectly as European legal principles and precedents will more easily be used in such procedures than in formal court proceedings, which are often constrained by the national judicial traditions and vocabulary. For example, the creation of a uniform European insurance market has been facilitated by the application of out-of-court insurance dispute resolution through the European consumer protection regulations under Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution.

¹⁵ Referring to the third paragraph of Article 288 TFEU, the Court held: 'Although that provision leaves Member States to choose the ways and means of ensuring that the directive is implemented, that freedom does not affect the obligation imposed on all the Member States to which the directive is addressed, to adopt, in their national legal systems, all the measures necessary to ensure that the directive is fully effective, in accordance with the objective that it pursues': Case 14/83, *Sabine von Colson et Elisabeth Kamann v. Land Nordrhein-Westfalen*, , ECLI:EU:C:1984:153, point 145.

¹⁶ Commission Communication "EU Law: Better Results through Better Application", 13.12.2016, Pages 5-6.

2.3. Non regulatory techniques to reduce national divergences

Because of the limits of harmonizing or unifying rules at EU level, alternative approaches should be considered to foster the digital single market. Those can be based on EU policy plans to try to influence and possibly coordinating policy actions at the national level, monitoring and benchmarking of national policies to stimulate an exchange of best practices among the Member States or financing support with EU funds. Indeed, EU financing can be a powerful means to accelerate cross-border cooperation.¹⁷

¹⁷ For example in the area of standard setting, the Commission proposes to speed up the standard setting process in five priority domains: 5G, cloud computing, internet of things, data technologies and cybersecurity, and to co-finance the testing and experimentation of technologies to accelerate standards setting, including in relevant public-private partnerships.

3. MAIN ACHIEVEMENTS DURING THE 8TH PARLIAMENTARY LEGISLATURE

KEY FINDINGS

During the 8th legislature, the European Parliament and the other EU institutions have been very active in the digital field. To review the numerous achievement, we present **the DSM measures into six building blocks**. The two first blocks relate to the digital applications used by European consumers and citizens: the e-commerce and online platforms and the e-government services. The three successive blocks are horizontal and necessary to ensure the development of and the trust in private and public digital services; they relate to data and AI, security and the specific consumer protection for the digital era. Finally, the last block relates to the infrastructures on which the digital applications are provided: the electronic communications networks and services. Most of policy actions **during the 8th legislature took place for e-commerce and online platforms as well for data and AI**.

For each building block, we analyse, as summarised in Table 1 below, how the specific DSM initiatives and measures (i) **directly facilitate cross-border trade** by removing specific barriers to the single market, (ii) **unify or harmonise the national substantive rules** which indirectly ease cross-border operations and create specific rights and obligations and (iii) **unify or harmonise the enforcement** of those rules and establish legal institutions and procedures which also indirectly ease cross-border operations.

Regarding **e-commerce and online platforms**, some of the main impediments to cross-border trade have been removed or reduced with the cross-border portability of some digital content, the prohibition of unjustified geo-blocking, the simplification of VAT declaration, the collection and the improvement of eu. Top Level Domain and the new copyright rules facilitating access to online TV and radio content across borders. Moreover, several national rules on the operations of online platforms have been harmonised, in particular for platforms offering audio-visual media services and intermediation services as well as platforms hosting illegal or harmful online content. To ensure effective and harmonised enforcement of those rules, ERGA - the network of national media regulators - has been strengthened.

Regarding **e-government**, which remains a national competence, the EU institutions can merely stimulate the adoption and the diffusion of best practices across the Member States as well as facilitate the interoperability between the different national public services, as for example by the setting up a single digital gateway. The EU is also leading by example by digitizing its own public services.

Regarding **data and AI**, data location requirements have been limited. Moreover, several national rules on the governance of data have been harmonised in order to ease cross-border data businesses and the movement of data across the EU while ensuring strict privacy protection and respecting EU values and fundamental rights. This is the case for personal data with the now famous General Data Protection Regulation (GDPR), for public data with the new Open Data and Public Sector Information Directive and for non-personal and non-public data where best practices for data sharing have been established. To ensure effective and harmonised enforcement of data protection rules, a new European Data Protection Board (EDBP) has been established between the national data protection authorities. In addition, a plan to stimulate AI in Europe has been coordinated between the EU and the Member States and new EU funds are being made available.

Regarding **security**, an EU cyber-security culture is emerging. New cooperation between cybersecurity agencies have been set up, ENISA will become an EU level Cybersecurity agency, a new EU Competence Centre has been set up and EU funds have been made available to strengthen network security.

Regarding **consumer protection**, an adaptation of the existing consumer acquis to the characteristics of the digital sector, in particular the lack of monetary prices and the difficulties to understand the functioning of algorithms, has been adopted. A strengthening of the cooperation between national consumer protection authorities has also been agreed.

Regarding **electronic communications networks and services**, rules were adopted to deal with specific cross-border issues such as international roaming calls or international calls. EU harmonised rules were reviewed in order to ease entry and spectrum use, thereby stimulating private investment and to protect consumers. The cooperation between national regulatory authorities was slightly strengthened with the reform of BEREC. More EU funds were made available to support the deployment of new fibre and 5G infrastructures.

During the 8th legislature, **digital policy has been a key priority and the EU institutions proposed, agreed or adopted many regulatory and non-regulatory actions** in several policy fields to build the digital single market. The most ambitious reforms have been achieved in the field of *e-commerce and online platforms* to stimulate the digital economy while protecting consumers as well as in the field of *data and AI* to ensure that data become a fifth internal market freedom. Then, some important reforms have been agreed in the field of *security and trust* and an EU cyber-security culture begins to emerge and other important reforms are being negotiated to adapt the *consumer protection rules* to the digital environment. Some reforms have been agreed to adapt the EU rules on *electronic communications networks and services* to the increasing needs of connectivity. Finally, the EU continues to stimulate the deployment of *e-government* in the Member States.

Table 2: List of legal instruments adopted or proposed during the 8th Legislature to build the Digital Single Market

E-commerce and online platforms	E-Government	Data and AI	Security	Consumer protection in the digital era	Electronic communications networks and services
Regulation 2017/1128 on cross-border portability of online content services	Regulation 2018/1724 establishing a Single Digital Gateway	Directive 2015/2366 Payment Services	Directive 2016/1148 on Network Information Security	Regulation 2017/2394 on Consumer Protection Cooperation	Regulation 2015/2120 on Open Internet and International Roaming
Regulation 2017/2454 and Directive 2017/2455 on VAT for e-Commerce		Regulation 2016/679 General Data Protection	Regulation 2019/XXX on EU Cybersecurity Act	Directive 2019/XXX Better enforcement and modernisation of EU consumer protection rules	Regulation 2017/920 on wholesale roaming
Regulation 2018/302 on unjustified geo-blocking		Directive 2016/680 Data Police	Regulation 2019/XXX European Cybersecurity Industrial, Technology and Research Centre	Directive 2019/XXX on contracts for the supply of digital content	Decision 2017/899 on use of 470-790 MHz frequency band
Regulation 2018/644 on cross-border parcel delivery services		Regulation 2018/1488 on European High-Performance Computing Joint Undertaking			Regulation 2017/1953 to promote Internet Connectivity in local communities (Wi-Fi4EU)
Directive 2018/1713 VAT on e-publication		Regulation 2018/1807 on free flow of non-personal data			Directive 2018/1972 on European Electronic Communications Code
Directive 2018/1808 amending Audio-Visual and Media Services		Dir. 2019/XXX on open data and the re-use of public sector information			Regulation 2018/1971 on BEREC
Regulation .2019/XXX on .eu Top Level Domain name		<i>Prop. Reg. e-privacy – (2017/1807)</i>			
Directive 2019/XXX on copyright in the Digital Single Market					
Directive 2019/XXX Copyright and					

E-commerce and online platforms	E-Government	Data and AI	Security	Consumer protection in the digital era	Electronic communications networks and services
broadcasting organisations					
Regulation 2019/XXXX P2C fairness and transparency					
<i>Prop. Reg. on terrorist content online (2018/640)</i>					
Communication on European Agenda for collaborative economy (2016/356)	Communication on EU e-Government Action Plan 2016-2020 (2016/179)	Communication on ICT Standardisation Priorities in DSM (2016/176)	Rec. 2017/1584 on coordinated response to large scale cybersecurity incidents	Guidance on the implementation UCPD (2016/163)	Guidelines on market analysis and SMP (2018)
Competition Sector Enquiry e-commerce (2017/229)	Communication on European Interoperability Framework (2017/134)	Communication on European Cloud Initiative (2016/178)	Communication on Making most of NIS Directive (2017/476)		
Recommendation 2018/344 on illegal content online		Communication on Digitising European Industry (2016/180)			
		Recommendation 2018/790 on access to and preservation of scientific information			
		Guidance on sharing private sector data (2018/125)			
		Communication on Building Trust in Human-Centric Artificial Intelligence (2019/168)			

In green: the legislative acts that have been adopted or agreed between the European Parliament and the Council

In yellow, the legislative acts that have been proposed by the Commission and are negotiated between the European Parliament and the Council

In yellow, important soft-law instruments adopted by the Commission

3.1. E-commerce and Online platforms

As part of the Commission's Digital Single Market strategy and its plan to boost e-commerce and online platforms, the Commission announced several measures to promote e-commerce in early June and late May 2016. The European Parliament adopted an important Resolution on 15 June 2017 on online platforms and the digital single market.¹⁸ Legislation was subsequently approved and soft law in the form of communications and guidelines issued.

The **Regulation 2017/1128 of 14 June 2017 on cross-border portability of online content services in the internal market** ensures that subscribers can watch paid-for online content when they are temporarily outside their country of residence. To achieve its aim without encroaching on the right of rightholders to license their works on exclusive basis per Member State, the Regulation requires providers to verify the subscriber's Member State of residence when the contract for the provision of the service is concluded and renewed. At the same time, the Regulation provides no details on the enforcement. National law and procedures apply in case of breach.

The **Directive 2017/2455 of 5 December 2017 as regards certain Value Added Tax obligations** for the supply of services and the distance sales of goods reduces the border effect on e-Commerce of the country of destination principle in the VAT system in the EU.¹⁹ The Directive introduces a sales threshold (€10,000), under which traders may continue to apply their domestic VAT rules for the online sales of goods and electronic services anywhere in the EU (home country principle) instead of the VAT of the country of destination. The Directive also introduces the home country principle as regards invoicing and record keeping so that retailers would not have to apply the different rules applicable in the Member States where consumers are located. The retailers will no longer be audited by each Member State where they make sales. Finally, the Directive removes the low value consignment relief (LVCR) for the importation of small consignments below €22 from suppliers in third countries. In the same vein, the Directive makes online selling platforms liable for the collection of VAT when acting as intermediaries for the supply of goods imported from non-EU countries when the goods have a value under €150.

Two related Regulations were also adopted: the Council Regulation 2017/2454 of 5 December 2017 on administrative cooperation and combating fraud in the field of value-added tax and the Council Implementing Regulation 2017/2459 of 5 December 2017 on the common system of value-added tax.

The **Regulation 2018/302 of 28 February 2018 on addressing unjustified geo-blocking** removes geo-blocking and other forms of discrimination based on consumers' nationality, place of residence or place of establishment within the internal market by establishing a single set of rules directly applicable throughout.²⁰ However, the Regulation does not apply to financial services, electronic communications services, transport services, audio-visual and gambling services.

¹⁸ 2016/2276 (INI)

¹⁹ As suggested by Naess-Schmidt H. et al. (2012).

²⁰ See also the Questions & Answers on the Geo-blocking Regulation in the context of e-commerce: <https://ec.europa.eu/digital-single-market/en/news/geo-blocking-regulation-questions-and-answers>. Also Poiares Maduro, Monti and Coelho (2016).

Regulation 2018/644 of 18 April 2018 on cross-border parcel delivery services improves price transparency of cross-border parcel delivery services and make the national regulatory oversight of these services more effective. The Regulation imposes a single set of obligations for all delivery services providers throughout the entire EU. On that basis, the Commission adopted the Implementing Regulation 2018/1263 of 20 September 2018 establishing the forms for the submission of information by parcel delivery service providers.

The **Council Directive 2018/1713 of 6 November 2018 on rates of value-added tax applied to books, newspapers and periodicals** complements the measures addressing the fragmentation resulting from the territorial copyright licensing, by phasing out the differences in VAT rates applicable on physical media – that often benefit from lower rates and may sometimes be reduced to 0% - and e-publications, on which the standard VAT rate (a minimum of 15%) currently applies. Decreasing the VAT on e-publications aims to foster on-line cross border sales.

The Directive 2018/1808 of 14 November 2018 adapts the Audio-visual Media Services Directive to changing market realities by extending the scope of the current Directive to video-sharing platforms providers and social media of which the provision of programmes and user-generated videos constitute an essential functionality. It also requires Member States to designate independent regulatory authorities or bodies to implement the rules of the Directive.

The **Regulation 2019/XXX of 19 March 2019 on the implementation and functioning of the .EU Top Level Domain name** aims to improve the attractiveness of the .EU top level domain. It facilitates the eligibility criteria for registration of .EU domains and allows European citizens to register the domain name independently of their place of residence. The Regulation also improves the governance of the .EU domains by setting a multi-stakeholder advisory Council. This body would be independent from the Registry.

The Directive 2019/XXX on copyright in the Digital Single Market introduces an EU-wide ancillary copyright for press publisher, reduces the liability exemption granted by the e-commerce Directive to video-sharing and other platforms,²¹ strengthens the bargaining position of authors and performers vis-à-vis online distributors and requires Member States to set up impartial bodies to facilitate licensing agreements between rights holders and video on-demand platforms.²² However, Member States remain competent to decide on conditions, such as the timing and duration of the assistance and who bears the costs. The Directive complements current EU Copyright Directive as regards possible exceptions.

The **Directive 2019/XXX on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organizations and retransmissions of television and radio programmes** extends the country of origin principle that currently applies to cross-border satellite broadcasting and retransmission of copyrighted content by cable of television and radio programmes

²¹ On that change, see Nordemann (2018).

²² For further information see Kullas and Brombach (2017).

from other Member States. The Directive aims to give broadcasters the possibility making the vast majority of their content available online in other Member States.

The **Regulation 2019/XXX on promoting fairness and transparency for business users of online intermediation services** bans certain unfair practices such as sudden or unexplained account suspensions, increases transparency regarding ranking, data collection and use and differentiated conditions, and provides for new avenues for dispute resolution such as internal compliant-handling system to assist business users and the possibility of relying on mediators.

In May 2015, the EU Commission also intervened directly in the e-commerce sector based on its competition law powers with sector inquiry complementing the Commission's legislative proposals. On 10 May 2017, the Commission published the **final report of the inquiry**.²³

Soft-law was used to foster a common approach of Member States to deal with illegal content and disinformation. Commission **Recommendation 2018/334 on measures to effectively tackle illegal content online** aims to make the detection and the removal of online illegal content more effective, in particular for terrorism content. In addition, a series of codes of conducts have been agreed by some industry players and are closely monitored with the Commission:

- (i) to reduce the online diffusion of **child sexual abuses**, multiple commitments have been taken by digital firms;²⁴
- (ii) to reduce the online diffusion of **terrorist content**, a **Multi-Stakeholders Forum** has been set up in December 2015 between the Internet platforms and the enforcement agencies;²⁵
- (iii) to reduce the diffusion of hate speech, a **Code of conduct of May 2016 on countering illegal hate speech online** has been agreed by the main IT companies (now Facebook, YouTube, Twitter, Microsoft, Instagram, Google+, Dailymotion, Snapchat and Webmedia);²⁶
- (iv) to reduce the sale of counterfeit products on the Internet, a **Memorandum of Understanding of 21 June 2016 on counterfeit products** has been concluded between some online platforms and trademark right-holders in June 2016;²⁷
- and (v) to reduce the diffusion of online fake news and disinformation, a **Code of practice of October 2018 on disinformation** has been agreed by Google, Facebook, Twitter, Mozilla and the trade associations representing the advertising sector.²⁸

²³ COM(2017) 229.

²⁴ Several initiatives were established to fight the diffusion of child sexual abuses online: a CEO Coalition in 2011: <https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kid> (last visited 26 February 2019); an ICT Coalition for Children Online in 2012: <http://www.ictcoalition.eu> (last visited 26 February 2019); and an Industry Alliance to deal with child sexual abuses in 2017: <https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online> (last visited 26 February 2019).

²⁵ An EU Internet Forum was established in 2015: Commission Press release of 3 December 2015, IP/15/6243.

²⁶ https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300

²⁷ https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en

²⁸ <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> Also Renda (2018).

Table 3: EU rules regarding e-commerce and online platforms

<p>EU rules facilitating cross-border trade</p>	<ul style="list-style-type: none"> - Regulation 2017/1128 on cross-border portability of online content introduces a temporary exception to territorial copyright licences, which is directly applicable throughout the EU. - Directive 2017/2455 on VAT for e-commerce harmonises the conditions for the application of the VAT rules for the online sales of goods and electronic services. - Regulation 2018/302 on unjustified geo-blocking prohibits traders to block access to their online interface, or redirect consumers to another version of their online interface than the one sought for by consumers, based on their nationality. This Regulation also prohibits discrimination based on nationality in relation to the application of traders' general conditions of access to specific goods or services, or the use of means of payment. - Regulation 2018/644 on cross-border parcel delivery requires parcel delivery service providers to provide their National Regulatory Authorities with their applicable tariffs each year (especially cross-border tariffs). NRAs must determine if tariffs are not unreasonably high. Consumer information by delivery service providers is also required. - Regulation 2019/XXX on.eu Top Level Domain improves EU level governance of the .eu domain name management.
<p>Unification or harmonisation of national rules or codes of conduct</p>	<ul style="list-style-type: none"> - The amending Directive 2018/1808 on Audiovisual Media Service harmonizes regulatory obligations imposed on video-sharing platforms providers and social media, in addition to those already covered by the current Directive, including as regards EU content. - Directive 2019/XXX on copyright in the Digital Single Market aims to harmonise national legislations regarding licensing practices, granting of a related right for publishers and availability of mechanisms of adjustment of contracts and dispute settlement. - Directive 2019/XXX on copyright and related rights applicable to certain online transmissions of broadcasting organisations brings similar systems for the clearance of rights by broadcasting organisations in all Member States. - Regulation 2019/XXX on P2B fairness and transparency imposes common general transparency obligations on providers of online intermediation services throughout the EU regarding their commercial terms and conditions, conditions for suspension and/or termination of their contracts, ranking methods, differentiated treatments, on the access to business or user data they provide, and on their rules for businesses on offering different conditions through other means. It also foresees the drawing up of codes of conduct by providers of online intermediation services and online search engines to contribute to the proper application of the regulation, under the impulsion of the Commission.

	<ul style="list-style-type: none"> - Proposed Regulation on preventing the dissemination of terrorist content online aims to harmonises the rules regarding the diffusion and removal of online terrorist content. - Recommendation 2018/344 on illegal content online calls upon Member States and hosting service providers to take effective, appropriate and proportionate measures to tackle illegal content online, through guidance on the mechanisms of notice and action and of proactive measures by automated means.
<p>Unification or harmonisation of national enforcement</p>	<ul style="list-style-type: none"> - Commission’s e-commerce sector inquiry investigated whether companies erected barriers affecting European cross-border e-commerce (for example, restrictions in agreements between suppliers and distributors) and prompted companies to review their commercial practices on their own initiative. - Regulation 2018/302 on geo-blocking provides for the designation in each Member State, of a body responsible for providing practical assistance to consumers in case of disputes between them and traders arising from the application of the regulation. - Amending Directive 2018/1808 on Audiovisual Media Service harmonises the guarantees of independence of media regulators throughout the EU and strengthen the status of the European Regulators Group for Audiovisual Media Services (ERGA), which was set up in 2014 to facilitate cooperation between the regulatory bodies in the EU, as provided for in the AVMS directive. - Directive 2019/XXX on copyright in the Digital Single Market provides for an alternative dispute resolution mechanism. - Regulation 2019/XXX on P2B fairness and transparency aims to require providers of online intermediation services to designate mediators through their terms and conditions to settle disputes with business users out of court. - Recommendation 2018/344 on illegal content online encourages Member States and hosting service providers to allow for the use of out of court dispute settlement mechanisms.

3.2. E-Government

Many citizens and businesses embrace the possibilities of digital technology and expect the same kind of online experience from the public sector. This is often not the case. Authorities are expected to provide user-friendly information online, digitise procedures as much as possible and make them accessible to cross-border users, re-use information provided by citizens and companies as much as possible, including in a cross-border context.

The Commission presented in April 2016 its **e-Government Action Plan 2016-2020**²⁹ and the European Parliament adopted a Resolution on this Action Plan in May 2017.³⁰ The Plan contains 20 measures, of which the following three regulatory measures:

- The **Regulation 2018/1724 of 2 October 2018 establishing a single digital gateway** aims to provide access to information, procedures and assistance and problem-solving services to help citizens and businesses make the most of the single market. The gateway will allow citizens and businesses to access and carry out administrative procedures online, hence taking advantages of the single market in an easier way, which is less time-consuming and less expensive. A centralised access to all information necessary for those who want to use their rights to mobility in the EU will be provided. Member States have to create full online access to the most important and used procedures. This information should be accurate, complete, up-to-date, and available in at least two languages: that of the Member State, plus at least one other official language of the Union.
- The **Council Directive 2017/2455 of 5 December 2017 as regards certain value-added tax obligations** for supplies of services and distance sales of goods extends the single electronic mechanism for registration and payment of VAT. The Directive extends the existing OSS (also called Mini-One-Stop-Shop or MOSS), that currently applies to electronic services, to EU online sales of tangible goods and services other than electronic services as well as to online sales of goods from third countries which have an intrinsic value not exceeding €150. The MOSS in operation since January 2015 allows companies selling electronic services (telecommunications, broadcasting or electronically supplied services) to customers in more than one EU country to declare and pay all the VAT due via a web portal in their own Member State (instead of having to register for VAT in each Member State in which they have customers). VAT revenues are then transferred from the home tax administration to the relevant Member States, i.e. the home countries of the customers to which the company has sold electronic services.

Among the 20 measures of the Action Plan, some were calls upon the Member States to strengthen existing cooperation in the following domains: (i) eIDAS services including eID and eSignature; (ii) the European e-Justice Portal as a one-stop shop for information on European justice issues; (iii) the

²⁹ COM(2016) 179.

³⁰ 2016/2273 (INI).

electronic interconnection of insolvency registers, (iv) the Business Registers Interconnection System (BRIS);³¹ and (v) the deployment and take-up of the INSPIRE Directive data infrastructure.³²

Other measures consist in commitments by the Commission to coordinate or support Member States' actions: (i) a revised version of the European Interoperability Framework (EIF) and the support its take-up by national administrations;³³ (ii) the establishment of the Electronic Exchange of Social Security Information (EESSI), the IT system to support social security institutions across the EU to exchange information more rapidly and securely;³⁴ (iii) support Member States in the development of cross-border eHealth services with the establishment of the European eHealth Digital Service Infrastructure (eHDSI or eHealth DSI);³⁵ (iv) a pilot for the launch of the 'once-only' principle (TOOP) project for businesses across borders;³⁶ (v) the transition of Member States towards full e-procurement and use of contract registers;³⁷ (vi) the development of a prototype for European Catalogue of ICT standards for public procurement.³⁸

However, the 2016 e-Government Action Plan does not mention the replacement of the paper-format customs procedures with EU-wide electronic procedures to create a more efficient and modern customs environment.

³¹ The BRIS interconnects the central, commercial and companies registers (typically referred to as business registers) to create a more business-friendly legal and fiscal environment in a cross-border context. In addition, BRIS provides a single point of access via the European e-Justice Portal³¹, through which citizens, businesses and public administrations can search for information on companies and their branches opened in other Member States.

³² <https://inspire-reference.jrc.ec.europa.eu/> The objective is promoting the development of end-user applications, so as to harvest from citizens and business more efficiently the data provided through Spatial Data (INSPIRE) for EU-level policy making and implementation. The INSPIRE portal invites stakeholders to actively participate by adding to the dedicated tools and apps catalogues with entries that contribute to both the production or use of INSPIRE.

³³ COM(2017) 134. The Framework is accompanied by the Interoperability Action Plan, which outlines priorities that should support the implementation of the EIF from 2016 to 2020. 47 open ended recommendations on how to improve governance of their interoperability activities and establish cross-organisational relationships are provided in the annex to the Action plan

³⁴ In particular Regulation 987/2009 of 16 September 2009 laying down the procedure for implementing Regulation 883/2004 on the coordination of social security systems, as amended, OJ L 284, 30.10.2009, p.1. The Commission in July 2017 made the central EESSI system available. Following this, Member States have two years to finalise their national implementation of EESSI and to connect their social security institutions to the cross-border electronic exchanges. All communication between national institutions on cross-border social security files will take place through EESSI: social security institutions will exchange structured electronic documents and follow commonly agreed procedures. These documents will be routed through EESSI to the correct destination in another Member State.

³⁵ See <https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Mission>. The European Commission and the national healthcare systems provide the communication infrastructure jointly. Twelve EU Member States started exchanging patient data, backed by the Connecting Europe Facility (CEF). eHDSI shares patient summaries and e-prescriptions in a safe way across borders.

³⁶ TOOP has a budget of € 8 million funded by the Horizon 2020 programme from the European Union. The consortium is composed of participants from 21 countries. The project has the ultimate goal of promoting cross-border cooperation among authorities and offering control and transparency opportunities regarding business operations across borders.

³⁷ To date, achievements related mainly to aspects such as the prequalification of economic operators (ESPD and eCertis) and e-invoicing. Under the Connecting Europe Facility (CEF), EU funding is available to support e-invoicing activities. The Multi-Stakeholder Expert Group on e-Procurement (EXEP) provides a link between the Commission and the stakeholders in the Member States and plays an important role for a successful transition to e-procurement.

³⁸ A number of standards are available on the 'joinup' portal of the EU Commission.

The legal framework for this e-Government initiative is set in the Union Customs Code (UCC), while the implementation of the European electronic customs environment is governed by the Electronic Customs Multi-Annual Strategic Plan (MASP).³⁹

³⁹ MASP Rev. 2017 Version 1.4, 30.11.2017, taxud.a.3(2017)6498377, https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/policy_issues/e-customs_initiative/masp_strategic_plan_en.pdf

Table 4: EU rules regarding e-government

EU rules facilitating cross-border trade	<ul style="list-style-type: none"> - Package on VAT on e-commerce extends the One Stop shop procedure. - Regulation 2018/1724 on Digital Single Gateway sets common rules for centralised access to all information necessary for those who want to use their rights to mobility in the EU. - Member States must connect their social security institutions to the cross-border electronic exchanges EESSI under Regulation 987/2009 of 16 September 2009
Unification or harmonisation of national rules or codes of conduct	<ul style="list-style-type: none"> - See rules on public data explained in Table 5
Unification or harmonisation of national enforcement	<ul style="list-style-type: none"> - Interoperability Action Plan lists 47 recommendations to the Member States to improve the governance of their interoperability activities and establish cross-organisational relationships. - The Commission deployed and runs the core services platform, named "European Central Platform" (ECP) underlying the Business Registers Interconnection System (BRIS). - The Commission in July 2017 made the central EESSI system available. - The Multi-Stakeholder Expert Group on e-Procurement (EXEP) provides a link between the Commission and the stakeholders in the Member States and plays likely an important role for a successful transition to e-procurement. - Under the Interoperability solutions for public administrations, businesses and citizens (ISA) Programme, the collaborative platform 'Joinup' was created to help e-Government professionals share their experience with each other and support them to find, choose, re-use, develop and implement interoperability solutions.

3.3. Data and Artificial Intelligence

In order to foster a thriving European Data Economy, the following actions were undertaken to facilitate the cross-border flow of data in the digital single market while protecting the consumers and data subjects.

The **General Data Protection Regulation (GDPR) 2016/679** provides for a comprehensive set of rules on the processing of personal data of citizens, especially on data subjects rights and freedoms. The GDPR is, firstly, an essential means to foster consumer confidence in the data economy. Secondly, unified rules across the EU are essential for the emergence of big data with adequate critical mass in Europe, which otherwise would be hampered by diverging national requirements. In addition, the network of regulators will ensure that Data Protection Agencies coordinate their approaches in a manner compatible with the implementation of big data analytics in Europe. The **Directive 2016/680** was adopted at the same time to deal with the **processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences** or the execution of criminal penalties

The proposed **e-privacy Regulation** aims to extend the scope of application of the current ePrivacy Directive⁴⁰ to over-the-top (OTT) communication services (such as WhatsApp or Skype), require user consent for the processing of communications data and metadata and increase the level of fines for breaches.

The **Regulation 2018/1807 on the free-flow of non-personal data** requires Member States to remove legal requirements on data localisation. Restrictions on the location of data will only be allowed on grounds of public security, as defined in the Treaties and as interpreted by the EU Court of Justice. Any remaining data localisation requirements will have to be communicated to the European Commission and published online, in order to ensure compliance and transparency. In addition, the Regulation proposes self-regulation to facilitate switching cloud-service-providers for professional users.

The Council **Regulation 2018/1488 of 28 September 2018 establishing the European High-Performance Computing Joint Undertaking** (EuroHPC JU) sets up a public-private partnership to pool European resources to develop top-of-the-range exascale supercomputers for processing big data. The EuroHPC JU will (i) jointly with Participating States, buy and deploy two supercomputers in Europe that will be among the top 5 in the world and at least two other that would today rank in the global top 25 for Europe's private and public users and (ii) support research and innovation activities: developing a European supercomputing ecosystem, stimulating a technology supply industry, and making supercomputing resources in many application areas available to a large number of public and private users. The EU's financial contribution to the EuroHPC JU amounts to € 486 million.⁴¹

⁴⁰ Directive 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p.37.

⁴¹ This budget will be matched by a similar amount from the participating countries. The private members will also provide additional contributions to the value of over EUR 400 million, through participation in the Joint Undertaking's activities.

The **Directive 2019/XXX on Open Data and Public Sector Information (PSI)** reduces market entry barriers by limiting the exceptions that allow public bodies to charge for the re-use of their data more than the marginal costs; increases the availability of data by bringing new types of data into the scope of the Directive, such as data held by public undertakings in the utilities and transport sectors and research data resulting from public funding; minimises the risk of first-mover advantage, by requiring a more transparent process for the establishment of public–private data arrangements and increases business opportunities by encouraging the dissemination of dynamic data via application programming interfaces (APIs).

The Commission **Recommendation 2018/790 of 25 April 2018 on access to and preservation of scientific information** calls for open access to scientific publications resulting from publicly funded research and invites the Member States to implement clear policies in the areas of preservation and re-use of scientific information, infrastructures underpinning the system for access to, preservation, sharing and re-use of scientific information and for promoting their federation within the European Open Science Cloud (EOSC), including the drafting implementation plans and setting concrete objectives and indicators to measure progress.

Regarding data policies, the Commission adopted a series of Communications and the European Parliament adopted a series of Resolutions.

- First, the Commission **Communication of 19 April 2016 on the European Cloud Initiative - Building a competitive data and knowledge economy in Europe** announces several actions and partnerships to support the European Open Science Cloud and to kick-start the European Data Infrastructure and estimates the investments required at €4.7 billion in the period of 5 years.⁴² The European Parliament adopted a **Resolution on 10 March 2016 on a thriving data-driven economy**⁴³ and then a **Resolution on 16 February 2017 on the European Cloud Initiative**.⁴⁴
- In parallel, the Commission **Communication of 19 April 2016 on digitising European Industry - Reaping the full benefits of the Single Market** calls for strengthening the coordination role of the Public Private Partnerships (PPPs) established in H2020 so that they become real aggregation frameworks and ecosystems for digital industrial innovations, including on big data.⁴⁵ The European Parliament adopted a **Resolution on 1 June 2017 on digitising European industry**.⁴⁶
- Then, the Commission **Communication of 10 January 2017 on Building a European data economy** launches a stakeholder’s dialogue on the following issues: free flow of data; access and transfer in relation to machine-generated data; liability and safety in the context of emerging technologies; and portability of non-personal data, interoperability and standards.⁴⁷ The Communication also sets out suggestions for experimenting with common regulatory solutions in a real-life environment.

⁴² COM(2016) 178.

⁴³ 2015/2612 (RSP).

⁴⁴ 2016/2145 (INI).

⁴⁵ COM(2016) 180.

⁴⁶ 2016/2271 (INI).

⁴⁷ COM(2017) 9.

- Finally, the Commission **Communication of 25 April 2018 on a common European data space** puts forward a package of measures to foster a seamless digital area with the scale that will enable the development of new products and services based on data.⁴⁸ The Communication also recommends five key principles should be complied with in contractual Business to Business and Business to Government data sharing agreements: transparency, shared value creation, respect for each other's commercial interests, undistorted competition and minimised data lock-in.

Regarding Artificial Intelligence, the European Parliament adopted an important Resolution on 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics.⁴⁹ The Commission adopted a series of three Communications with different policy action.

- First, the Commission adopted the **Communication of 25 April 2018 on Artificial Intelligence for Europe** which establishes a three-pronged strategy: boost the EU's technological and industrial capacity and AI uptake across the economy, prepare for socio-economic changes and ensure an appropriate ethical and legal framework.⁵⁰
- Then, the Commission adopted the **Communication of 7 December 2018 on a coordinated plan on AI** to create synergies between Member States and increase joint investment with the aim to foster cross-border cooperation and mobilise all players to increase public and private investments to at least €20 billion annually over the next decade.⁵¹
- Finally, the Commission adopted the **Communication of 8 April 2019 on building trust in human-centric Artificial Intelligence** which proposes seven requirements for trustworthy AI on the basis of the Ethic Guidelines developed by the High-level expert group on AI.⁵² Those key requirements are: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability.

⁴⁸ COM(2018) 232.

⁴⁹ (2015/2103(INL))

⁵⁰ COM(2018) 237.

⁵¹ COM(2018) 795.

⁵² COM(2019) 168.

Table 5: EU rules regarding data and AI

EU rules facilitating cross-border trade	<p>- Regulation 2018/1807 on free-flow of non-personal data provides for removal of Member States' legal requirements of data localisation, except for some specific exceptions. The proposal also foresees that competent national authorities may not be refused access to data based on its location in another Member State .</p>
Unification or harmonisation of national rules or codes of conduct	<p>- GDPR 2016/679 establishes common EU rules on most aspects of the processing of personal data. The GDPR details the data subject rights, data controllers' responsibility, processors' obligations, security of processing, development of codes of conduct and certifications. The GDPR also details remedies, liability and penalties in case of breach of the substantive rules.</p> <p>- Regulation 2018/1807 on free-flow of non-personal data entrusts the Commission with the task to encourage and facilitate the development of EU codes of conduct for cloud services.</p> <p>- Proposed e-privacy Regulation aims to impose EU wide the requirement of user-consent for the processing of communication data.</p> <p>- Directive 2019/XXX on open data and Public Service Information requires Member State to harmonise their national rules on open data so that they cover research data and specific documents held by public undertakings, and that dynamic data is made available in the shortest possible timeframe after collection. The Member States' rules have to provide that access to certain specific information shall be free of charge for its users (high value datasets).</p> <p>- Recommendation 2018/790 on scientific information invites the Member States to ensure that scientific publications that are publicly funded, are accessible in open-access, under licensing terms that are as wide as possible.</p> <p>- Communication Staff Guidance on sharing private sector data provides principles and guidance on business-to-business (B2B) as well as on business-to-government (B2G) data sharing agreements.</p>
Unification or harmonisation of national enforcement	<p>- GDPR 2016/679 details extensively the tasks of the national supervisory authorities as well as the relations between each other. Furthermore, it includes a consistency mechanism to ensure consistent application of its provisions with opinions and dispute resolution delivered by the Data Protection Board.</p>

3.4. Security

The **Directive 2016/1148 of 6 July 2016 on Network Information Security (NIS)** requires that Member States adopt a national NIS strategy defining the strategic objectives and appropriate policy and regulatory measures in relation to cybersecurity and designate a national competent authority in the regard. The Directive also creates a cooperation group between Member States to support and facilitate strategic cooperation and the exchange of information among Member States as well as the setting up a network of Computer Security Incident Response Team (CSIRT), in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks. The Directive also requires the identification of undertakings across sectors, which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure (essential services) and ensure that these undertakings take appropriate security measures and notify serious incidents to the relevant national authority. Key digital service providers (search engines, cloud computing services and online marketplaces) must also comply with the security and notification requirements under the NIS Directive.

The **Regulation 2019/XXX for a Cybersecurity Act** has two main objectives. (i) First, the Regulation gives a permanent mandate to the European Network Information Security Agency (ENISA), including for the implementation of the NIS Directive. ENISA will contribute to stepping up both operational cooperation and crisis management across the EU. (ii) Second, the Regulation creates a framework for EU cybersecurity certificates for connected products, Internet of Things devices and critical infrastructures. Such a cybersecurity certification framework incorporates security features in the early stages of their technical design and development (security by design). It also enables their users to ascertain the level of security assurance and ensures that these security features are independently verified. The resulting certificate will be recognized in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

The **Regulation 2019/XXX establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres** establishes a competence Centre which will set up and help to coordinate the National Coordination Centres Network and the Cybersecurity Competence Community. The Centre will implement cybersecurity-related financial support from Horizon Europe and the Digital Europe Programme.

The **Commission Recommendation 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises** details the plan to be followed in case of large-scale cross-border cyber incident or crisis. It sets out the objectives and modes of cooperation between the Member States and EU Institutions in responding to such incidents and crises and explains how existing Crisis Management mechanisms can make full use of existing cybersecurity entities at EU level.

The Commission **Communication of 19 April 2016 on ICT Standardisation Priorities for the Digital Single Market**⁵³ promotes a fresh approach to standards in five domains, among which Cybersecurity.

⁵³ COM(2016)176.

It tries to ensure that all forces in Europe pull in the same direction, using standardisation as a strategic instrument to EU industrial policy. The Communication announces that it will support European standardisation organisations and other standards development organisations, European regulators as well as public-private initiatives, in the development of standards-based cybersecurity risk management guidelines for organisations and of corresponding audit guidelines for authorities or regulators with oversight responsibilities.

Table 6: EU rules regarding security

<p>EU rules facilitating cross-border trade</p>	<p>- Regulation 2019/XXX on Cybersecurity Act establishes an EU wide cybersecurity certification scheme and prohibits Member States to introduce new national cybersecurity certifications schemes for matters covered. The Act also fixes the penalties for in case of infringement of its rules.</p>
<p>Unification or harmonisation of national rules or codes of conduct</p>	<p>- Directive 2016/1148 Network Information Security harmonises national laws governing network security including the identification of operators of essential services.</p> <p>- Regulation 2019/XXX on Cybersecurity Act provides for common EU principles to govern the national strategies on the security of network and information systems, on security requirements and incident notifications, on establishment of jurisdiction, and on promoting of standardisation by Member States.</p> <p>- Guidance for the implementation of the NIS Directive promotes a common interpretation and transposition for example as regards the national Computer Security Incident Reponse Team (CSIRT) capabilities or the consistency of identification of operators of essential services.</p> <p>- Recommendation 2017/1584 on a coordinated response to large scale cybersecurity incidents proposes a common cooperation procedures between the Member States and the EU and for the transmission of information in case of a crisis (large scale cybersecurity incidents). It further provides for the adoption of a common taxonomy of crisis management categories.</p>
<p>Unification or harmonisation of national enforcement</p>	<p>- Directive 2016/1148 NIS requires Member States to designate national competent authorities and single points of contact and establishes a CSIRTs network in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation. It is composed of representatives of the EU Member States' CSIRTs and a CSIRT for EU institutions CERT-EU. The CSIRTs Network provides a forum where Member States' National CSIRTs can cooperate, exchange information and also build trust. Member States CSIRTs will improve the handling of cross-border incidents and discuss how to respond in a coordinated manner to specific incidents.</p> <p>- Regulation 2019/XXX on Cybersecurity Act entrusts ENISA with limited implementation powers in the area of cybersecurity such as steering NIS operational cooperation by actively supporting Member States' CSIRTs' cooperation or developing the future certification schemes and provide secretariat assistance to the EU cybersecurity certification group.</p> <p>- Regulation 2019/XXX on Cybersecurity Act provides for national certification supervisory authorities to be appointed by Member States in relation to European cybersecurity certification schemes and their features. The proposed Act also provides for the establishment of the European cybersecurity certification group, composed of the national certification supervisory authorities, and defines its tasks.</p>

- | | |
|--|---|
| | <ul style="list-style-type: none">- Regulation 2019/XXX establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres creates a competence Centre to manage cybersecurity-related financial support from the EU's budget and facilitate joint investment by the Union, Member States and industry.- Recommendation 2017/1584 on a coordinated response to large scale cybersecurity incidents establishes an EU cybersecurity crisis response framework to ensure cooperation, exchange of information and efficiency of all relevant actors in case of a crisis. |
|--|---|

3.5 Consumer Protection in the digital era

The **Regulation 2017/2394 of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws** (i) strengthens the minimum powers of the consumer protection authorities to cooperate in cross-border context, especially to tackle faster online practices including the powers to carry out test purchases and mystery shopping, to suspend and take down websites, to impose interim measures, to impose penalties proportionate to the cross-border dimension of the imputed practice. The Regulation also allows these authorities to accept commitments from traders.

The **Directive 2019/XXX on better enforcement and modernisation of EU consumer protection** extends the protection for consumers to free digital services exchanged against personal data. The Directive also adapts and harmonises consumer protection to specific digital issues such as the transparency for online marketplaces regarding price personalisation; paid advertising and placement, the main parameters of ranking, whether the third-party offering product or service is a trader or not, and the authenticity of consumer reviews. The Directive also strengthens the penalties for infringements⁵⁴ and sets the criteria administrative authorities or courts have to take into account when deciding whether to impose a penalty and on its level.

The **Directive 2019/XXX on digital content contracts** targets digital content and services (e.g. cloud, video and music streaming, digital television, apps, social networks and messaging apps) and covers, besides contracts in exchange of a price, contracts in exchange of the consumer's personal data.⁵⁵ Contractual clauses, which are not in line with the Directive, to the detriment of the consumer, are void, unless explicitly allowed. The Directive puts the burden of proof on the supplier of the digital content and of the conformity of the content supplied. Consumers have the right to terminate contracts and the supplier have to provide the consumer with the technical means to retrieve all the consumer's content and data produced/generated through the use of the digital content provided it has been retained by the supplier. Member States have to ensure that adequate and effective means of redress exist. Member States do not have the possibility to impose additional requirements.

The Commission **Guidance of 25 May 2016 on the implementation of the Unfair Commercial Practices Directive** (UCPD) provides guidance on the UCPD's key concepts and provisions and practical examples taken from the case-law of the Court of Justice of the European Union and from national courts and administrations on how to implement it. However, it is itself not legally binding.

⁵⁴ For instance, for widespread infringements, Member States have to provide for maximum fines that should not be set below 4% of the infringing trader's turnover in the Member State or Member States concerned)

⁵⁵ The proposal was initially not connected with the data economy, but rather with the Commission's failed attempt to introduce a Common European Sales Law, COM(2011) 635, withdrawn in late 2014.

Table 7: EU rules regarding consumer protection

Unification or harmonisation of national rules or codes of conduct	<ul style="list-style-type: none"> - Directive 2019/XXX on better enforcement and modernisation of EU consumer protection extends consumer protection to services exchanged against personal data and increase the transparency of online market places. - Directive 2019/XXX on contracts for the supply of digital content harmonises Member States' legislations regarding conformity of digital service/service with the contract, the remedies available in the case of lack of conformity and modification and termination of the contract.
Unification or harmonisation of national enforcement	<ul style="list-style-type: none"> - Regulation 2017/2394 on Consumer Protection Cooperation sets EU wide rules regarding the powers of national consumer protection authorities and for joint enforcement measures (mutual assistance mechanism) in case of cross-border infringements to consumer protection law, as well as a framework for coordinated investigations and enforcement mechanisms in case of widespread infringements to the same set of rules, exchange of information, and a framework for sweeps, i.e. concerted and simultaneous investigations on respect of EU consumer protection law.

3.6. Electronic Communications Networks and Services

Context

The EU regulatory framework that had been put in place in 2002 was revised in 2009 with the Telecoms Package, which included the Better Regulation and Citizens' Rights Directives, as well as two new Regulations to reduce mobile roaming charges and create a body of European regulators for electronic communications (BEREC). A subsequent Regulation was introduced in 2012 to further limit roaming charges. However, on year later, the European Commission still found that "(s)ome large telecommunications companies are present in several Member States; but none is present in all. For the most part mobile operators have merely a national footprint; for many fixed operators it is even more localised. Those who do operate in several Member States must work under separate rules, according to the sometimes diverging requirements and remedies of different regulators, and needing distinct authorisations in each Member State. In addition, often operators active across several Member States do not behave as truly European operators, and appear content to run their activities separately in each Member State. The market includes over one thousand fixed operators, and several hundred mobile operators, which, despite often belonging in larger groups, operate on a national basis. At the same time the sector is increasingly global in nature and depends on scale to be profitable."⁵⁶ The Commission concluded that "the sector suffers from fragmentation along national borders; a lack of regulatory consistency and predictability across the Union; unfairly high prices for specific services; and a lack of investment."⁵⁷ To address this perceived gap in the digital single market, the Commission proposed a Regulation for a Connected Continent.⁵⁸ However, the scope of the regulation as eventually adopted⁵⁹ was reduced compared to the Commission proposal, covering only net neutrality and international roaming. The remaining issues were addressed by the Commission in its September 2016 proposal for a European Electronic Communications Code.

Another issue dealt with in the Code is the perceived absence of a level playing field in the Member States following the success of Internet applications allowing to users to establish communications over broadband internet connections ('over the top' services) that can replace traditional telecommunications services provided by telecom operators. The new Code subjects the latter, in different degrees, to the same rules than the telecom operators. While the measure can be seen as promoting a level playing field in national markets, it does not necessarily contribute to the single market. Where in the past the providers of the internet applications were regulated at EU level (country of origin principle), the global operators will now be regulated and have to notify their service in each of the Member States.⁶⁰

⁵⁶ Communication from the Commission on the Telecommunications Single Market, 11.9.2013, COM(2013) 634, p.4.

⁵⁷ Idem, p.5.

⁵⁸ Outlined in European Commission, COM (2013) 627 - A proposal for a regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations No 1211/2009 and No 531/2012, 2013

⁵⁹ Regulation 2015/2120, published in the Official Journal on 26 November 2015

⁶⁰ As we explained in de Streel and Hoceped (2017). See also Renda (2017).

Measures adopted

The **Regulation 2015/2120 of 25 November 2015 on the open internet access and on roaming on public mobile communications networks** forces providers of internet access services to treat all traffic equally, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. In addition, the Regulation prohibits any surcharge to the domestic retail price on international roaming customers in any Member State for calls, SMS and data provided the subscribers comply with the fair use policy. The abolition of roaming surcharges led to the following two measures: (i) the Commission Implementing Regulation 2016/2286 of 15 December 2016 on the fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges which allows roaming providers to apply 'fair use' policies to prevent permanent or abusive roaming;⁶¹ and (ii) the Regulation 2017/920 of 17 May 2017 on rules for wholesale roaming markets which caps the maximum international wholesale roaming prices that mobile operators may charge to each other in the EU.⁶²

The **Decision 2017/899 of 17 May 2017 on the use of the 470-790 MHz frequency band for mobile services** seeks the coordinated release of the 700 MHz band (694-790 MHz) under harmonised technical conditions by 30 June 2020 at the latest in all EU countries. This frequency band is particularly well-suited for ensuring the provision of broadband services in rural areas, while accommodating the specific needs of audio-visual media distribution.

The **Regulation 2017/1953 of 25 October 2017 on the promotion of internet connectivity in local communities** (also known as Wifi4EU) earmarks €95 million over a period of three years to finance the provision of fast wireless internet connections for citizens located in spaces where public services are provided, such as public administrations, libraries and hospitals.

The **Directive 2018/1972 of 11 December 2018 on the European Electronic Communications Code** brings a more consistent single market approach to spectrum policy and deliver conditions for a true single market by tackling regulatory fragmentation. These two general objectives are pursued through several specific objectives, addressing perceived specific internal market restrictions by either private players or by Member States: (i) reduced regulatory entry barriers, (ii) predictability for spectrum right holders, (iii) procedures to ensure that national regulators impose access remedies which foster the internal market, (iv) EU wide interoperability of services and mandatory standards, (v) EU wide Security of networks and services, (vi) the availability of an EU wide numbering space, (vii) lessening the fragmentation resulting from divergences between national end-user protection rules.

⁶¹ Operators may restrict the benefit of the abolition of the roaming surcharge to end users residing in the country where they have subscription or who are otherwise able to demonstrate stable links at the request of the roaming provider.

⁶² The wholesale charge shall not exceed a safeguard limit of EUR 7,70 per gigabyte of data transmitted. That maximum wholesale charge shall decrease to EUR 6,00 per gigabyte on 1 January 2018, to EUR 4,50 per gigabyte on 1 January 2019, to EUR 3,50 per gigabyte on 1 January 2020, to EUR 3,00 per gigabyte on 1 January 2021 and to EUR 2,50 per gigabyte on 1 January 2022.

The **Regulation 2018/1971 of 11 December 2018 on the Body of European Regulators of Electronic Communications (BEREC)** seeks, on the one hand, to introduce new competences granted to Body of European Regulators for Electronic Communications (BEREC) and, on the other, to streamline its functioning. This Regulation also amends the previous Regulation 2015/2120 to regulate the charges for cross-border intra EEA calls and SMS.

Table 8: EU rules regarding electronic communications networks and services

EU level rules	<ul style="list-style-type: none"> - Regulation 2015/2120 on Open Internet and international roaming and associated legal instruments regulate international roaming rates. - Regulation 2015/2120 on Open Internet, retail charges for regulated intra-EU communications and international roaming regulates the tariffs of international calls, sets up an EU numbering space and prohibits of discrimination by operators, on the basis of residence or nationality.
Unification or harmonisation of national rules or codes of conduct	<ul style="list-style-type: none"> - Regulation 2015/2120 on Open Internet, retail charges for regulated intra-EU communications and international roaming imposes common network neutrality rules across the EU . - Spectrum Decision 2017/899 sets common deadline for the coordinated release of the 700 MHz spectrum band. - Directive 2018/1972 EECC harmonises many national telecom rules and enables an EU numbering space, ensures network security, EU standards, maximum harmonization user protection as well as predictability over time for spectrum right holders.
Unification or harmonisation of national enforcement	<ul style="list-style-type: none"> - Directive 2018/1972 EECC grants power to the Commission to block national deregulation of network access when contrary to the internal market, provides that this body shall conduct an analysis of transnational end-user demand for products and services that are provided within the Union in one or more of the markets listed in the Recommendation, if it receives a reasoned request providing supporting evidence - Regulation 2018/1971 on BEREC grants new tasks to BEREC. - Directive 2018/1972 on EECC provides for out of court dispute resolution mechanism, including the obligation on Member States to enable the national regulator to act as a dispute settlement entity.

4. FUTURE POTENTIAL OF THE DIGITAL SINGLE MARKET AND POSSIBLE INITIATIVES

KEY FINDINGS

As many regulatory and non-regulatory actions have been taken during the 8th legislature, the first task is to **implement those new rules in an effective and harmonised manner** across Europe. This is particularly important because most of those EU substantive rules are implemented by national authorities. Then the **efficiency and the effectiveness of the rules and their enforcement should be evaluated**, in particular the impacts on the economy and the society.

However, evaluating the effects of the actions already adopted will not be enough given the importance of the digital technologies for the European economy and society, the rapid pace of evolution of those technologies and the increasing global competition for digital leadership. To respond to change, the **pace of reform should remain important during the forthcoming 9th legislature**.

Regarding the objectives and policy fields, we have identified **following priorities**:

- **Make the EU a technological powerhouse for the emerging and important technologies** such as AI, quantum computing, security of connected devices or data exchanges that should be designed and developed according to European values enshrined in the Treaties and the Charter of Fundamental Rights;

- Stimulate the **development of online platforms**: (i) start-ups should be stimulated by rules ensuring a level playing and access to the main capabilities for digital innovation (in particular data) and to the ecosystem of products that are used by consumers, (ii) scale-up should be stimulated by one set of rules and enforcement all over Europe, (iii) significant platforms should be subject to an increased duty of care should be imposed;

- Stimulate **e-government**: given the potential benefits of digital public services, the EU should stimulate the adoption and the diffusion of national and cross-borders e-government services as well as the adoption of digital technologies, such as blockchain, to improve public regulation.

Regarding the **policy and regulatory techniques**, we recommend the reliance of principles-based legislation that can easily adapt to fast and unpredictable technology and market evolutions **complemented with codes of conduct** agreed with all the digital players (firms, consumers associations, NGOs ...) under the auspices of EU institutions and with a close monitoring by the EU institutions. We also recommend that the **enforcement of those rules is more Europeanised** either with the continuous strengthening of the cooperation network of national regulatory authorities or with the **establishment of a EU regulator for significant platforms** as it was done some year ago for the significant banks with the creation of the Single Supervisory Mechanism within the European Central Bank. The **regulatory authorities in Europe should also size the potential of digital technologies**, such as big data or AI, to improve their operations (*RegTech*). To go further when feasible, enforcement may be automatized in the computer code as it is the case for smart contracts or privacy by design (more generally, *compliance by design*).

Those regulatory actions should be **complemented with non-regulatory initiatives**, in particular the monitoring and exchange of best practices of key digital national policies, the increasing smart use of EU funds to stimulate the deployment and the adoption of key digital networks and services and the development of the digital skills of EU workers and citizens.

As explained in the previous section, the European Parliament, together with the other EU institutions, has been very active during its 8th legislature to stimulate the Digital Single Market. However, given the rapid pace of technological progress and market evolutions and the important issues at stake, there is no time for complacency and efforts will need to be stepped up during the forthcoming legislature.

4.1 Applying and evaluating the newly adopted rules

As many new rules have been adopted, the first challenge is to ensure that those new rules are integrated into the legal regimes of the Member States in a timely and harmonised manner. This implies that the national laws transposing EU Directives and, when needed, complementing EU Regulations should be sufficiently clear to guarantee legal certainty, respect the letter and the spirit of EU law to ensure harmonisation and alleviate any regulatory gold-plating and over-regulation. Then, those rules need to be enforced by national administrative, regulatory and judicial authorities to be effective in a manner which is effective and proportionate. The numerous network of national authorities which have been established or strengthened should help in that regard.

After some years of application, those rules and their enforcement should be evaluated⁶³ in a rigorous manner as foreseen in the Commission Better Regulation Guidelines⁶⁴ or in Muller et al. (2013). In particular, the Commission will have to assess the effectiveness, the efficiency, the relevance given the needs, the coherence with other EU interventions and the EU added value of the rules and their enforcement. On that basis, an adaptation of the existing rules and/or their enforcement may have to be proposed.

4.2. Digitalizing and deepening the single market

The application and, then, the evaluation of the newly adopted rules and their enforcement will take years and yet no time can be lost. Therefore already now, it is important to envisage the actions adopted during the 8th legislature that need to be developed and the new actions that need to be initiated during the next parliamentary term. On the basis of the expected technological evolution and their impacts, we suggest the following avenues for future actions.⁶⁵

a. From digital single market to digitised single market

As explained by Bauer (2017), some of the impediments to digital business developing and scaling up is the regulatory heterogeneity in non-digital industries. Indeed, the OECD Product Market Regulation (PMR) Index and the OECD Service Trade Restrictiveness Index show important regulatory heterogeneity between Member States for non-digital goods and services. To be sure, such heterogeneity may be justified by different national preferences or endowment but it affects the possibility of establishing and operating cross-border digital business. Moreover as new digital technologies are general-purpose technologies which permeate all the sectors of the economy and the society, it is appropriate to digitize the four freedoms and all the sectors of the single market instead of

⁶³ Many EU legal instruments have review clauses which make such evaluation by the Commission compulsory.

⁶⁴ Commission Staff Working Document of 7 July 2017, Better Regulation Guidelines, SWD(2017) 350, Chapter VI.

⁶⁵ Also McKinsey Global Institute (2018).

developing a specific strategy for digital sectors.⁶⁶ As proposed by the Lisbon Council (2018), the (digital) single market could be decoupled from the digital agenda and the First Vice-President of the Commission should be in charge of all digital files in a transversal manner while a Vice-President should be in charge of the single market including both the implementation of digital-single-market legislation and a broad overview of cross-cutting and sectoral single-market questions. In addition, as suggested by Erixon and Lamprecht (2018), this single market strategy should focus on integrating market relying of country of origin principle rather than regulating business at the EU and national levels.

b. Making Europe a technological power house and adopting an ambitious cyber-security and AI industrial policy

Before being a regulatory powerhouse, the EU should first and foremost be a technology powerhouse, its policies should stimulate the development of the emerging and important technologies for tomorrow such as quantum computing, very fast micro-processing, different AI techniques, secure data exchanges and secure Internet of Things and AI enabled tools. Europe should also ensure that those technologies are designed and developed according to its values enshrined in the Treaties and in the Charter of Fundamental Rights.⁶⁷ This requires smart innovation policies based on close dialogue between public and private bodies.

c. Regulation should accompany the development of online platforms in Europe

Online platforms are playing an increasing role in the economy and society. As explained by Bauer (2018) and Martens (2016), they are powerful engines for growth and innovation. They allow small professional users to reach out to millions of customers at very low cost, they increase customers and traders' information and, in the end, they allow the development of new and disruptive business models. However, their increasing role raise concerns on their economic, societal and political power: big platforms monopolise markets and may buy any potential disruptive innovator (Cremer et al., 2019), they capture a big share of the economic surplus they generated and value may be shifted from creators and prosumers to platforms, they disrupt labour relationship and may threaten social security systems, they influence elections and may threaten democracy as we know it. While some concerns are valid and other are exaggerated, it remains that online platforms are destabilising some of our past governance models and the State (being EU or national institutions) should adapt their policies while keeping control of the public sphere. Different actions are needed to stimulate the start-up, then the scale-up and finally ensuring a sufficient duty of care by the most significant platforms.

First, EU policies should stimulate the emergence and the take-up of new platforms, in particular in Europe and ensure that digital markets remain contestable and contested.⁶⁸

⁶⁶ This is the direction suggested by the Presidency discussion paper of 20 November 2018 on the future of Single Market, 14003/18. Also Communication of the European Commission of 21 November 2018, The Single Market in a changing world, COM(2018) 772, section 3.1.

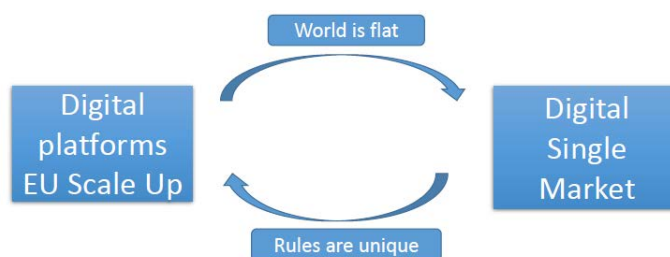
⁶⁷ For AI, see Joint Research Centre (2018); Maciejewski M. et L.C. Matos (2018).

⁶⁸ Jean Tirole, "Regulating the Disruptors", available at <https://www.livemint.com/Technology/XsgWUgy9tR4uaoME7xtlTI/Regulating-the-disrupters-Jean-Tirole.html>

As explained by Dittrich (2017 and 2018), this requires smart innovation policy and regulation that ensure access to the main capabilities for digital innovation, in particular access to data,⁶⁹ skills, computing power and risky and patient capital.

Second, the EU policies should stimulate the scale-up of the digital platforms, which is one of the main weaknesses of Europe compared to the US or China. There is a positive feedback loop between the single market and the platform scale up as (i) the scale-up makes the world more flat and allows business and consumers to more easily reach their counterparts all over Europe, thereby contributing to the single market while (ii) the single market rules facilitate the business operation and consumer trust all over Europe.

Figure 2: Feedback loops between platform scale-up and single market



For this feedback loop to work, online platforms should be subject to one set of rules. This can be achieved with the mutual recognition of national rules (country of origin principle) or with the full harmonisation of national rules. Those rules should then be subject to one enforcement, either at the national level in case of mutual recognition or identically in all Member State in case of full harmonisation.

Third, when an online platform has scaled up and become significant, it may raise systemic risks to the economy and society (to paraphrase what was said for the big banks, big platforms may be too big to rule). In this case, EU policies and regulation should ensure an appropriate duty of care. This implies (i) transparency on the practices vis-à-vis the regulators and the platforms customers (business and consumers), (ii) loyalty of the platform which should provide their services to the benefit of their customers and not their own and (iii) increased responsibility for a safer Internet as with power comes responsibility (Floridi et al., 2017). To do that, the e-commerce Directive could be revised or complemented to condition the liability exemption to the provision of an infrastructure facilitating the detection and the removal of illegal content by users, third parties and the platforms themselves, possibly relying on AI detection tools (de Streel, Buiten and Peitz, 2018).

d. Developing E-government everywhere at all levels

E-government is one of the core of national competences and organisation. However, given the importance of public sector as an enabler for the digitization of the economy and society, EU should continue to incentivize the digitization of public service within each Member States as well as across the Member States.⁷⁰

⁶⁹ In favour of data sharing policies: OECD (2015), Gans (2018), Mayer-Schonberger and Ramge (2018). Also Lisbon Council (2019).

⁷⁰ See TNO, WIK-Consult and Rand (2013)

The measures of the e-Government Action Plan 2016-2020 and the best practices of the 2017 Tallinn Declaration on e-Government are good basis and should be developed further in the next legislature (Lisbon Council, 2018).

4.3. Smart policy and regulatory techniques

To achieve those objectives in the most effective manner, the EU should rely on the most adapted policy and regulatory techniques as explained in Muller et al. (2015).

a. Smart regulation in dynamic and uncertain environments

Given the very high rapidity and uncertainty of market evolutions, regulation should be principle-based to adapt easily to technologies and market evolutions (de Streel and Larouche, 2016). Detailed and prescriptive rules should be alleviated at all costs as they quickly outdate and miss their objectives while possibly stifling innovation. As principle-based rules often lead to uncertainty that, in turn, may increase regulatory costs and reduce regulatory effectiveness, those rules need to be complemented by soft-law instruments and codes of conducts agreed between authorities and digital players on the basis of the regulatory principles, closely monitored and adapted when necessary.⁷¹ The different codes of conducts which have been adopted to reduce some illegal or harmful content online could serve as best practices.

b. Smart enforcement in global and digital markets

It is not enough to have good rules, they need to be enforced effectively and, as shown by the recent review of the EU consumer acquis, this is often the weak point of the EU regulatory framework as rules remain enforced at the national level. As many digital markets and firms are global and the digital services of the most significant online platforms are offered across the Member States, it is key that EU rules are enforced in the same manner in all the Member States. Moreover, given the imbalance between some digital platforms and national regulatory authorities, an EU enforcement could increase the effectiveness of EU rules. Therefore, the different coordination networks between the national regulatory authorities should continue to be strengthened. Possibly an EU regulator for the significant digital platforms should be created similarly to what has been done in the financial and banking sector with the recent establishment of an EU regulator (the Single Supervisory Mechanism within the European Central Bank) for the significant banks in Europe.

In addition, regulators, as every other player in our society, should rely on digital technologies to improve their operations and, as a side-effect, improve their understanding of new technologies that they may need to regulate. Regulators could rely on big data and AI techniques to improve the detection of rules violation and/or improve the predictability of such violations (*RegTech*). Going one step further (Lessig, 2006), in some cases, the regulator could be replaced by the computer code when regulatory compliance is enshrined in the design of the digital technologies (*compliance by design*). In that case, compliance will be automated (as in smart contracts for instance), hence the role of regulator is by-passed or at least reduced. The development of RegTech and compliance by design raise a series of ethical and legal issues that will need to be addressed during the next parliamentary legislature.

⁷¹ Furman et al. (2019) also suggest the development of code of competitive conducts with the participation of stakeholders.

REFERENCES

- Bauer M. (2017), *Right Direction, Wrong Territory: Why the EU's Digital Single Market Raises Wrong Expectations*, American Enterprise Institute.
- Bauer M. (2018), *Online Platforms, Economic Integration and Europe's Rent-Seeking Society*, ECIPE Policy Brief.
- Crème J., Y.A. de Montjoye, H. Schweitzer (2019), *Competition Policy for the digital era*, Report for the European Commission
- Civic Consulting (2014), *Contribution of the Internal Market and Consumer Protection to Growth*, Study for the IMCO Committee
- de Streel A. and P. Larouche (2016), *An Integrated Regulatory Framework for Digital Networks and Services*, CERRE Policy Report.
- de Streel A. and C. Hocepiéd (2017), *Optimal regulatory model for telecommunications services in the EU*, Study for the IMCO Committee of the European Parliament.
- de Streel A., M. Buitten and M. Peitz (2018), *The Liability of Online Platforms: Should exceptionalism end?*, CERRE Policy Report, Sept. 2018
- Dittrich, P.J. (2017), *Balancing Ambition and pragmatism for the digital single market*, Jacques Delors Institute Policy Paper 204.
- Dittrich, P.J. and J. Krewer (2018), *The European answer to the digital revolution*, Jacques Delors Institute Policy Brief.
- Eberlein B. (2004), *The Institutional Dynamics of Regulation in the EU: Formal and Informal Institutions in Supranational Governance*, 14th International Conference of Europeanists, Chicago, p.7.
- EPRS (2017), *Mapping the Cost of Non-Europe 2014-2019*, 4th edition
- Erixon F. and P. Lamprecht (2018), *The Next Steps for the Digital Single Market: From Where do We Start?*, ECIPE Policy Brief 2/2018.
- Floridi L. and M. Taddeo (2017). *The responsibility of Online Service Providers*, Springer.
- Furman J. et al. (2019), *Unlocking digital competition*, Report of the Digital Expert Panel.
- Gans J. (2018), *Enhancing Competition with Data and Identity Portability*, The Hamilton Project Policy Proposal 2018/10.
- Godel M., Harms A., Jones S., Mantovani I. (2016), *Reducing Costs and Barriers for the Businesses in the Single Market*, Study for the IMCO Committee of the European Parliament.
- Joint Research Centre (2018), *Artificial Intelligence: A European perspective*.
- Lessig L. (2006), *Code and Other Laws of the Cyberspace – Version 2.0*, Basic Book.
- Lisbon Council (2018), *Digital Europe: Next Steps*, A European Agenda for the Digital 9+.
- Lisbon Council (2019), *A Roadmap for a Fair Data Economy*, Policy Brief.
- Maciejewski M. et al. (2015), *EU Mapping: Overview of IMCO Related Legislation*, Study for the IMCO Committee.

-
- Maciejewski M. et L.C. Matos (2018), *EP-EUI Roundtable on Strategy for Artificial Intelligence in Europe*, Study for the IMCO Committee.
 - Martens B. (2016), *An Economic Policy Perspective on Online Platforms*, *JRC Digital Economy Working Paper 2016-05*.
 - Mayer-Schonberger V. and T. Ramge (2018), *Re-inventing capitalism in the age of big data*, Ed. John Murray.
 - McKinsey Global Institute (2018), *European Economy: Three Pathways to rebuilding trust and sustaining momentum*, Briefing Note for Davos.
 - Muller P., Conlon G., Denvani S. and Benard C. (2013), *Performance-based Policy*, Study for the IMCO Committee of the European Parliament.
 - Muller P., S. Jones and L. Koch (2015), *Smart Single Market Regulation*, Study for the IMCO Committee of the European Parliament.
 - Naess-Schmidt H. et al. (2012), *Simplifying and Modernising VAT in the Digital Single Market*, Study for IMCO.
 - Nordemann, J.B. (2018), *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, In-Depth Analysis for the IMCO Committee of the European Parliament.
 - OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publications.
 - Poiares Maduro M., G. Monti and G. Coelho (2016), *The Geo-blocking proposal: Internal market, competition law and regulatory aspects*, Study for the IMCO Committee of the European Parliament.
 - Renda A. (2017), *Reforming e-communications services: A critical assessment*, In-Depth analysis for the IMCO Committee of the European Parliament.
 - Renda A. (2018), *The legal framework to address “fake news”: possible policy actions at the EU level*, In-Depth analysis for the IMCO Committee.
 - TNO, WIK-Consult and RAND (2013), *Ubiquitous Developments of the Digital Single Market*, Study for the IMCO Committee of the European Parliament.

ANNEX LIST OF DIGITAL SINGLE MARKET LEGAL INSTRUMENTS

Digital Single Market Strategy

- **Communication** from the Commission of 6 May 2015, **A Digital Single Market Strategy for Europe**, COM(2015) 192.
- **Resolution of the European Parliament of 19 January 2016 on Towards a Digital Single Market Act, 2015/2147 (INI).**
- **Communication** from the Commission of 10 May 2017, **Mid-Term Review on the implementation of the Digital Single Market Strategy**, COM(2017) 228.
- **Communication** from the Commission of 15 May 2018, **Completing a trusted Digital Single Market for all**, COM(2018) 320.

E-commerce and online Platforms

Legislation

- **Regulation 2017/1128** of the European Parliament and of the Council of 14 June 2017 on **cross-border portability of online content** services in the internal market, O.J., L 168, 30.06.2017, p. 1.
- Council **Directive 2017/2455** of 5 December 2017 amending Directive 2006/112 and Directive 2009/132 as regards certain **value added tax** obligations for supplies of services and distance sales of good, O.J., L 348, 29.12.2017, p. 7.
- Council **Regulation 2017/2454** of 5 December 2017 amending Regulation 904/2010 on administrative cooperation and combating fraud in the field of **value added tax**, O.J., L 348, 29.12.2017, p. 1.
- Council **Implementing Regulation 2017/2459** of 5 December 2017 amending Implementing Regulation 282/2011 laying down implementing measures for Directive 2006/112/EC on the **common system of value added tax**, O.J., L 348, 29.12.2017, p. 32.
- **Regulation 2018/302** of the European Parliament and of the Council of 28 February 2018 on addressing **unjustified geo-blocking** and other forms of discrimination based on consumers' nationality, place of residence or place of establishment within the internal market and amending Regulation 2006/2004 and 2017/2394 and Directive 2009/22, O.J., L 60/I, 2.3.2018, p.1.
- **Regulation 2018/644** of the European parliament and of the Council of 18 April 2018 on **cross-border parcel delivery** services, O.J., L 112 of 2.5.2018, p. 19.
- Commission **Implementing Regulation 2018/1263** of 20 September 2018 establishing the **forms for the submission of information by parcel delivery service providers** pursuant to Regulation 2018/644 of the European Parliament and of the Council, parcel delivery service providers pursuant to Regulation (EU) 2018/644 of the European Parliament and of the Council O.J., L 238, 21.9.2018, p. 65.
- **Council Directive 2018/1713** of 6 November 2018 amending Directive 2006/112, as regards rates of **value added tax applied to books, newspapers and periodicals**, O.J., L 246 of 14.11.2018, p. 20.
- **Directive 2018/1808** of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audio-visual media services (**Audiovisual Media Services Directive**) in view of changing market realities, O.J., L 303 of 28.11.2018, p. 69.
- **Regulation 2019/XXX** of the European Parliament and of the Council of 19 March 2019 on the implementation and functioning of the **.eu Top Level Domain name** and amending and repealing Regulation 733/2002 and repealing Commission Regulation 874/2004, to be published in the OJ.

- **Directive 2019/XXX** of the European Parliament and of the Council on **copyright in the Digital Single market**, to be published in the OJ.
- **Directive 2019/XXX** of the European Parliament and of the Council on laying down rules on the exercise of **copyright** and related rights applicable to certain online transmissions of **broadcasting organisations** and retransmissions of television and radio programmes, to be published in the OJ.
- **Regulation 2019/XXX** of the European Parliament and of the Council on promoting **fairness and transparency for business users of online intermediation services**, to be published in the OJ.
- *Proposal of the Commission of 12 September 2018 for a **Regulation** of the European Parliament and of the Council on **preventing the dissemination of terrorist content online**, COM (2018) 640.*

Soft-Law

- **Communication** from the Commission of 2 June 2016, A **European agenda for the collaborative economy**, COM (2016) 356.
- Final report of the Commission of 10 May 2017 on the **E-commerce Sector Inquiry**, COM(2017) 229.
- Commission **Recommendation 2018/344** of 1 March 2018 on measures to effectively tackle **illegal content online**, O.J., L 63 of 6.3.2018, p. 50.

E-Government

Legislation

- **Regulation 2018/1724** of 2 October 2018 the European Parliament and the Council establishing a **single digital gateway** to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation 1024/2012, O.J. L 295 21.11.2018, p. 1.

Soft-law

- **Communication** from the Commission of 19 April 2016, **EU e-Government Action Plan 2016-2020**. Accelerating the digital transformation of government, COM (2016) 179.
- **Communication** of the Commission of 23 March 2017, **European Interoperability Framework**, COM(2017) 134.

Data and Artificial Intelligence

Legislation

- **Regulation 2016/679** of the European Parliament and of the Council 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**, and repealing Directive 95/46 (**General Data Protection Regulation**), O.J., L 119, 4.5.2016, p. 1.
- **Directive 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the **processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences** or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O.J., L 119, 4.5.2016, p. 89.
- Council **Regulation 2018/1488** of 28 September 2018 establishing the **European High-Performance Computing** Joint Undertaking, O.J., L 252, 8.10.2018, p. 1.
- **Regulation 2018/1807** of the European Parliament and of the Council of 14 November 2018 on a framework for the **free flow of non-personal data** in the European Union, O.J., L 303 of 28.11.2018, p. 59.

- **Directive 2019/XXX** of the European Parliament and of the Council on **open data and the re-use of public sector information**, to be published in OJ.
- *Proposal of the Commission of 10 January 2017 for Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58 (**Regulation on Privacy and Electronic Communications**), COM(2017) 10.*

Soft-law

- **Communication** from the Commission of 19 April 2016, **ICT Standardisation Priorities for the Digital Single Market**, COM(2016) 176
- **Communication** from the Commission of 19 April 2016, **European Cloud Initiative** - Building a competitive data and knowledge economy in Europe, COM(2016) 178.
- **Communication** from the Commission of 19 April 2016, **Digitising European Industry** - Reaping the full benefits of a Digital Single Market, COM(2016) 180.
- Commission **Recommendation 2018/790** of 25 April 2018 on **access to and preservation of scientific information**, O.J. L 134, 31.5.2018, p. 12.
- Commission Staff Working Document of 25 April 2018, **Guidance on sharing private sector data in the European data economy**, SWD(2018) 125
- **Communication** from the Commission of 8 April 2019, **Building Trust in Human-Centric Artificial Intelligence**, COM(2019) 168.

Security

Legislation

- **Directive 2016/1148** of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (**Network Information Security**), O.J., L 194, 19.7.2016, p.1.
- **Regulation 2019/XXX** of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency and on Information and Communication Technology cybersecurity certification (**Cybersecurity Act**), to be published in the OJ.
- **Regulation 2019/XXX** of the European Parliament and of the Council **establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**, to be published in the OJ.

Soft-law

- Commission **Recommendation 2017/1584** of 13 September 2017 on coordinated response to **large-scale cybersecurity incidents** and crises, O.J., L 239, 19.9.2017, p. 36.
- **Communication** from the Commission of 4 October 2017, **Making the most of NIS** – towards the effective implementation of Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, COM (2017) 476.
- **Consumer protection in the digital era**

Legislation

- **Regulation 2017/2394** of the European Parliament and of the Council of 12 December 2017 on **cooperation between national authorities** responsible for the enforcement of consumer protection laws and repealing Regulation 2006/2004, O.J., L 345, 27.12.2017, p. 1.

- **Directive 2019/XXX** of the European Parliament and of the Council as regards better **enforcement and modernisation of EU consumer protection**, to be published in the OJ.
- **Directive 2019/XXXX** of the European Parliament and of the Council on certain aspects concerning **contracts for the supply of digital content**, to be published in OJ.

Soft-law

- Commission Staff **Guidance** of 25 May 2016 on the **implementation/application of Directive 2005/29 on Unfair Commercial Practices**, SWD (2016) 163.

Electronic Communications Networks and Services

- **Regulation 2015/2120** of the European Parliament and of the Council of 25 November 2015 laying down measures concerning **open internet access and retail charges for regulated intra-EU communications** and amending Directive 2002/22 and Regulation 531/2012 on **roaming on public mobile communications networks** within the Union, O.J., L 310, 26.11.2015, p. 1, as amended by Regulation 2018/1971.
- Commission **Implementing Regulation 2016/2286** of 15 December 2016 laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail **roaming surcharges** and on the application to be submitted by a roaming provider for the purposes of that assessment, O.J., L 344, 17.12.2016, p. 46.
- **Regulation 2017/920** of the European Parliament and of the Council of 17 May 2017 amending Regulation 531/2012 as regards rules for **wholesale roaming markets**, O.J., L 147, 9.6.17 p.1.
- **Decision 2017/899** of the European Parliament and of the Council of 17 May 2017 on the **use of the 470-790 MHz frequency band** in the Union, O.J., L 138, 25.5.2017, p. 131.
- **Regulation 2017/1953** of the European Parliament and of the Council of 25 October 2017 amending Regulations 1316/2013 and 283/2014 as regards the promotion of **internet connectivity in local communities**, O.J., L 286, 1.11.2017, p. 1.
- **Regulation 2018/1971** of the European Parliament and of the Council of 11 December 2018 establishing the **Body of the European Regulators for Electronic Communications**, O.J. L 321 of 17.12.2018, p.1.
- **Directive 2018/1972** of the European Parliament and of the Council of 11 December 2018 establishing the **European Electronic Communications Code**, O.J., L 321 of 17.12.2018, p.36.

Soft-Law

- Commission Guidelines of 27 April 2018 on market analysis and the **assessment of significant market power** under the EU regulatory framework for electronic communications networks and services, O.J., C 159, 7.5.2018, p.1.

This study reviews all the rules adopted during the 8th Parliamentary legislature (2014-2019) to strengthen the Digital Single Market. On that basis, the report analyses the rights and obligations as well as the institutions and procedures created or improved in the main policy fields of the Digital Single Market (e-commerce and online platforms, e-government, data and AI, cybersecurity, consumer protection and electronic communications networks and services). Finally, the report identifies remaining gaps and possible actions for the forthcoming Parliament's legislature. This document has been prepared for the IMCO Committee at the request of the Policy Department A of the European Parliament.

PE 638.395
IP/A/IMCO/2017-17

Print ISBN 978-92-846-4819-1 | doi: 10.2861/71422 | QA-04-19-421-EN-C
PDF ISBN 978-92-846-4818-4 | doi: 10.2861/979516 | QA-04-19-421-EN-N