I. How to effectively keep users safer online?

Ever since the current directive's implementation two decades ago the possibilities of online activities for users have increased significantly. Shopping online, staying connected with friends or family, sharing, and searching for information are only a few of the activities people can easily conduct online nowadays.

With the seemingly endless possibilities that users have access to online comes an equal amount of problems regarding users' safety. From the sale, supply and promotion of illegal goods (e.g. dangerous products, counterfeits or prohibited and restricted goods, etc.) to other illegal activities, like illegal hate speech or practices infringing consumer law (e.g. scams, misleading advertising, etc.) – there are a lot of issues that need to be taken into consideration when proposing new legislation regulating online content and activities.

Hence why, we have identified main issues regarding users' safety online.

The spread of illegal activities online, including the sale of illegal and dangerous goods, has been amplified by the development of digital services, as they often facilitate widespread infringements of consumer law. Not only are products, that are not compliant with EU safety regulation, a danger to consumers, but also do they undermine a level playing field for businesses by providing unfair competitive advantage to those who do not follow the rules, as stated by Commissioner Breton.[1] To amend this issue, it is important to also focus on consumer and fundamental rights protection and online safety, by **clearly establishing consumer protection and product safety requirements** within the Digital Services Act, complementing other relevant future and/or existing legislation. With regards to product safety there have indeed been agreements between EU and platforms in the past, like the Products Safety Pledge[2], where only a few online platforms have committed themselves to the swift removal of products, not in line with product safety rules. The magazine "Which?", published by the largest consumer organisation in the UK, the Consumers' Association, regularly carries out systematic tests of product, services and suppliers. In 2019, it has been found, that in spite of prior notices and alerts unsafe products were still listed on the same platforms which have committed themselves to the swift removal of such listings.[3] This instance has shown that **voluntary actions and self-regulation by platforms have proven to be insufficient**, as those agreements allowed platforms to decide for themselves which actions they deemed necessary to take, without taking into account European as well as the Member States' national legislation. To this end, an ex-ante regulation providing **a clear set of rules and obligations for platforms and the implementation of a comprehensive notice and action mechanism is necessary**.

Apart from the sale of illegal and unsafe products online, there is also a multitude of illegal content being spread online. Given the current state of digital technologies there is plethora of possibilities on how the spread of illegal hate speech, infringements of intellectual property, child sexual abuse material, activities infringing consumer law (scams, misleading advertising, etc.) is facilitated. The **prevention of publication and the effective removal of illegal content are key for the protection of users** and consumers in Europe.

---

[1] https://www.europarl.europa.eu/resources/library/media/20191113RES66410/20191113RES66410.pdf
[2] https://ec.europa.eu/info/sites/info/files/voluntary_commitment_document_4signatures3-web.pdf
[3] https://www.which.co.uk/news/2019/10/which-investigation-prompts-100s-of-unsafe-co-alarms-to-be-removed-from-sale-do-you-have-one/

Legislation regulating illegal content should specifically target online platforms that have actual knowledge of and exert a certain degree of control over such content. Having "actual knowledge" requires a legal definition. To this end, we call for **revised definition of hosting intermediaries that clearly differentiate between active and passive hosts**, in order to prevent the abuse of liability exemptions currently set out under Article 14 of the e-Commerce Directive. We recommend considering that having a certain degree of control by, e.g. accumulating, moderating, or editing data, should be considered active hosts, and thereby excluded from liability exemptions. Additionally, a **comprehensive and transparent notice-and-action mechanism should be established**, not only facilitating effective cooperation between digital services providers and Member States' authorities, but between Member States as well and thus strengthening the country where a service is provided.

Furthermore, we call onto the Commission to **refrain from incentivising "voluntary actions" enabling self-regulation** of platforms and to rather adopt a rule of law approach. We **express scepticism regarding such "good Samaritan" provisions**[4], as non-binding agreements and recommendations have proven to be insufficient. An example would be the "Product Safety Pledge" mentioned before. Stimulating such voluntary actions strengthens the decision-making power of platforms, allowing for themselves to decide which measures they deem necessary to take, **which in turn hinders compliance and enforcement**. The Commission's initiative[5] on proposing mandatory rules for platforms to "detect report and remove" the spread of online child abuse is welcomed, but this rule of law approach should be extended to all illegal content online.

Regarding harmful but not necessarily illegal content, it should be kept in mind, that **what might not be considered illegal in one Member State, might be in another**. A rule of law approach regarding the containment of harmful content should apply as well. We call onto the Commission to focus on the advertising market, where business models of platforms like Facebook and Google inadvertently reward the spread of harmful content like disinformation and fake news. Referring to the spread of disinformation and conspiracy regarding COVID-19 the Global Disinformation Index has found that practices conducted by Google, Amazon and other **digital enterprises has generated ad revenue for COVID-19 disinformation sites amounting to USD 25 million**, which not only poses harm to users and consumers but also to brand's falsely being linked with conspiracy sites, often contradicting the brand's corporate responsibility aims.[6]

This regulation shall also **apply to businesses and platforms established outside the EU** as well, providing goods, services or digital content to EU consumers. According to recital 58 of the E-Commerce Directive, current provisions do "not apply to service providers established in a third country". The scope of application of the new legislative act should oblige platforms to check whether suppliers from third countries targeting EU citizens, have set up a branch in the EU or have appointed a representative in the EU which can be held liable. To this end, platforms that fail to ensure and verify traders' compliance with these obligations shall be held accountable for damages and guarantees.

<u>Clarifying responsibilities for online platforms and other digital services</u>

[4] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648780/IPOL_STU(2020)648780_EN.pdf
[5] https://www.euractiv.com/section/digital/news/commission-to-present-mandatory-rules-for-platforms-to-detect-report-and-remove-online-abuse/
[6] https://disinformationindex.org/2020/07/why-is-ad-tech-paying-us25-million-to-covid-19-disinfo-sites/

The advancements in technology and internet and telecommunication is correlating with an increase of online activities, solutions, and applications. Especially large platforms like Google, Facebook and Amazon are particularly dominant and exert great power in a highly concentrated market. With vast amounts of users and data generated they should be obligated to bear great responsibility. To this day, platforms are still able to operate in an unregulated environment for the most part. This is particularly evident considering platforms' decisions on e.g. community standards, notice and action mechanisms, implementation of algorithms. Those have extensive influence on fundamental rights, like the freedom of expression, and society at large.

A platforms' ability to exert control over data, e.g. the distribution, moderation, and organisation of content, calls for the effective safeguarding of the general interest, fundamental rights and core values within the EU. The need of serving the public interest in users' access to information and content is evident. Furthermore, future legislation needs to increase levels of transparency and accountability to bring platforms' responsibility in line with their ability to influence opinion making and their potential to harm citizens.

Platforms should have clear responsibilities, when taking content-related decisions, to protect and support freedom of expression and information. Effective rules are not only needed when platforms take down content considered illegal, but even more so in cases where they take down legal content in general that they consider incompatible with their own terms of use and when they make decisions about the visibility of content and services through organization, ranking, recommendation.

II. Reviewing the liability regime of digital services acting as intermediaries?

With the entry into force of the e-Commerce Directive in 2000 a 'special liability regime' was introduced, which provides safe harbour to three specific types of service providers ('mere conduit', 'caching' and 'hosting')[7], which are **exempted from liability for third party content, under certain circumstances.** In Recital 42 of the e-Commerce Directive it is required that the activity of 'giving access to a communication network over which information made available by third parties is transmitted or temporarily stored (…) is of a mere, technical, automatic and passive nature.'[8]

While mere conduit providers have a strictly passive nature and caching providers are only allowed to select the data and/or the recipient of the service, hosting providers have the least amount of required passiveness. This is due to the fact, that such providers are able to select the data and recipient of the service, but most importantly are also able to modify data. Nevertheless, we consider that digital and internet technology has changed drastically and call for **revision of this liability regime, as those three types of providers no longer adequately reflect the reality** of the range of services platforms offer. To this end, we call onto the Commission to provide for a **clear distinction between 'active' and 'passive' intermediaries**, based on the control they exert over data, in terms of ranking, moderating or otherwise modifying it. Furthermore, we address the fact that platforms and service providers nowadays often a wide range of activities and possibilities online. **The current liability regime enables platform to hide behind this safe harbour and be exempted from liability**, even though only a minor part of services offered might be considered 'hosting'.

[7] e-Commerce Directive [2000/31/EC], Articles 12, 13 and 14.
[8] e-Commerce Directive [2000/31/EC], Recital 42.

Caching and hosting providers are obligated to the swift removal of illegal content, but under the stipulation of having or acquiring actual knowledge of the illegality. The fact that Article 15 of the e-Commerce Directive also provides for **"no general obligation to monitor"[9] leads to the reliance on self-regulating practices by hosting providers** and platforms.

We acknowledge that there might be genuine intentions by platforms to take proactive steps for the detection and removal of illegal content, but we remind that this is only facilitated by voluntary and self-regulating acts. Those acts are incentivized by the Commission with e.g. the Code of Conduct (2016), the Communication on Tackling Illegal Content Online (2017) or the Recommendation on Measures to Effectively Tackle Illegal Content Online (2018). Especially the Commissions' communication from 2017 **promote 'good Samaritan' actions and encourages platform to undertake proactive measures**, as those do not automatically lead to the loss of safe harbour under Article 14 of the e-Commerce Directive.[10] **From such practices should be refrained in future legislation.**

The current 'special liability regime' as well as the legislator's call to voluntary actions, as main components of platform regulation, have proven unfit. **If platforms cannot properly be held liable, there is no incentive for them to comply.** Non-compliance by platforms poses a threat to effective enforcement on national and EU level, since enforcement bodies are heavily reliant on the goodwill and cooperation of platforms. We agree with the principle stated in the Draft Report by Rapporteur MEP Alex Agius Saliba "what is illegal offline is also illegal online".[11] Hence why, **we call for regulation online as offline, to ensure compliance by platform and to secure effective enforcement**.

To this end, **we argue for regulation by a network of National Enforcement Bodies (NEBs) overseen by Central Regulatory Authority on EU level**. The Central Regulatory Authority should be equipped with appropriate powers to investigate and to intervene, while NEBs should have the necessary powers to regulate externalities and other negative effects through the application and enforcement of national law.

III. What issues derive from the gatekeeper power of digital platforms?

There is no doubt, that in a highly concentrated market, with a few "winner takes it all" platforms, the influence they have on complete online ecosystems is worrying. Gatekeeper platforms act as intermediaries for other platforms and control and at times limit the access to different markets, goods and services or other groups of users. Furthermore, they generate enormous volumes of data and influence how information is transferred to users.

The control over such online ecosystems by gatekeeper platforms allows for **lock-in effects, providing users with little to no choices on alternatives**. The size of such gatekeepers and the advantage they have by benefiting from economies of scale, network effects and most of all the vast amount of generated data, allows them to **leverage their assets for entering new areas of activity and thus hinder new innovative competitors from entering** and establishing themselves in the market. This is also enabled by having the purchasing power to take over innovative start-ups, which is particularly evident in the case of large US platforms. According to findings of the study "Startup

[9] e-Commerce Directive [2000/31/EC], Article 15.
[10] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=35410&no=3
[11] Draft Report with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market [2020/2018 (INL)]

Transatlantic M&As. US vs EU" the top 15 US-based companies (including usual suspects such as Google, Facebook, and Amazon) acquire six times more start-ups than the top European companies. Google alone has acquired the same number of start-ups than the top 15 active European companies in the same period.[12]

Other companies, platforms and new market entrants are heavily reliant on the services provided by gatekeepers, e.g. search engines such as Google and Bing or advertising on sites like Amazon and Facebook. The bargaining power of those gatekeeper platforms is so strong, that they can take self-regulating decisions (e.g. their terms of service) on how, when and where third-party content is displayed or removed, facilitating the favouring of their own content. Those content-related decisions

Those unilateral decisions often facilitate not only the **takedown of illegal content but also legal content not compliant with their terms of service without a clear legal basis**. This is in contravention of Article 52 of the Charter of Fundamental Rights, which is stating that "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms."[13] **Thus, a clear legal framework is desperately needed to restrict the self-regulating practices of mentioned platforms.**

We consider that the introduction of ex-ante regulation of platforms holding a gatekeeper position is required, as they increasingly crowd out competitors and further strengthen their already dominant market position. To address any negative societal or economic effects of the gatekeeper role that large online platforms exercise over online ecosystems, we call onto the Commission to **implement dedicated regulatory rules including obligations** for such gatekeepers. To guarantee effective enforcement of dedicated rules, **a Central Regulatory Authority entrusted with the tasks of supervision and intervention should be established at EU level**.

To begin with, the provision of a clear set of criteria to **ensure unambiguous classification and identification of gatekeepers** at EU level is required. A variety of factors are relevant, when determining characteristics of particularly large online platforms:

Firstly, the **control of access to different markets, goods and services and groups of users** as well the power of decision on how, when and where information is transferred to users, **increases dependence of third parties**, since it is hardly possible to bypass platforms holding a gatekeeper role. This in turn raises market entry barriers for competitors and has a certain **lock-in effect of users**, as this often leads to **lack of alternatives**.

Secondly, the user base (in absolute numbers as well as in terms of geographic coverage within the EU) should be considered. A **large user base generates network effects**, increasing the quality of goods and services provided by gatekeepers and thus reinforcing their position.

Lastly, the vast amounts of data and information especially large platforms are able to generate and exert control over. **Access to data** gives an advantage in terms of improving goods and services provided by writing algorithms and data mining and opens the possibility of monetisation, which is

[12] https://startupeuropepartnership.eu/wp-content/uploads/2016/09/Startup-Transatlantic-MAs_MTB-Crunchbase_2016.pdf
[13] https://www.europarl.europa.eu/charter/pdf/text_en.pdf

particularly significant for advertising companies. Furthermore, this facilitates unfair practices, e.g. by ranking, listing and recommending their own products and services before a competitor's.

To conclude, **ensuring fair competition and fostering innovation within the Digital Single Market** is vital to improve quantity as well as quality of digital services in Europe. Especially during the COVID-19 pandemic it was evident that Europe with regards to the digital economy is severely behind. Most of the times it was platforms from the US or China (e.g. Amazon and Alibaba) EU citizens had to rely on due to a lack of an "equally" large platform or alternative coming from the EU. Other reasons for this, beside the role gatekeepers play when it comes European market entrants, are a fragmented market and lack of investments in start-ups.

The current degree of legal fragmentation is an obstacle, as new platforms and companies often do not have the capabilities and resources to have sufficient knowledge of the Member States' 27 different legal specifications. Hence why, the country of origin principle allows the application of one set of rules, namely that of the country where a company is based in. An improvement would be are **more streamlined approach with and high degree of cooperation between Member States**.

Furthermore, the Commission should aim to **address the lack of investments into the European start-up scene**. There is a need to create a friendlier environment for European innovation and investments. Even though, the EU and the USA had roughly the same GDP in 2016, venture capital investments in the EU measured USD 8 billion, compared to the USD 49 billion generated in the US. As a result, EU tech start-ups are cumulatively valued at USD 240 billion, compared to the valuation at USD 675 billion and USD 1.37 trillion, for start-ups from Asia and the USA, respectively.[14]

IV. Other emerging issues and opportunities, including online advertising and smart contracts

Online advertising has changed substantially since the current e-Commerce Directive's entry into force, considering the fact that **Google's ad revenue alone has increased from USD 0.07 billion in 2001 to 134.81 billion in 2019**.[15] This amount of advertising revenue was generated via Google Ads platform, which allows advertisers to display ad, product listing and service offerings across Google's network, which includes properties, partner sites and apps, to its web users.

With the excessive amount of data generated through and for advertising purposes, **the issues of lacking transparency are arising**. We do, for example, believe that it is **not clear for users who has placed an advertisement online, who has paid for the placement, or whether the revenue generated in the EU is taxed in the EU**. Considering the increased audience reach and visibility, this is especially worrying when it comes to advertisement placements next to illegal content or potentially harmful content, e.g. disinformation campaigns. As mentioned before, business models like those of e.g. Google and Facebook facilitate advertisement placements on disinformation sites. This was particularly evident during the COVID-19 pandemic, when according to the Global Disinformation Index such **digital platforms have generated advertising revenue amounting to USD 25 million for COVID-19 disinformation sites**.[16] Not only is the spread of fake news, disinformation and conspiracies about a dangerous and contagious disease harmful for online users, but also can the

[14] https://www.entrepreneur.com/article/331489
[15] https://www.statista.com/statistics/266249/advertising-revenue-of-google/
[16] https://disinformationindex.org/2020/07/why-is-ad-tech-paying-us25-million-to-covid-19-disinfo-sites/

placement of advertisements of brands on such websites considered to be defamatory, as they wrongfully imply the support of such fake news. This depicts that it is unclear, whether e.g. Google, the brand itself or a third party facilitated the placement of the advertisement.

Another issue is the rather sensitive topic of political or campaign advertising. We consider political advertising to be any analogous or digital display of advertising, used for the purpose of directly or indirectly appealing for votes or for financial or other support in any election campaign.

In September 2018, then-President Jean-Claude Juncker has presented a set of measures for securing free and fair European selections in view of the elections held in May 2019. This included a recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation. The Commission urged Member States to ensure greater transparency in online political advertisement, e.g. **allowing citizens to clearly recognize paid political ads, the amount money spent on the ad, its source and why it was targeted at them**.[17]

Technically, there is no uniform voting system for this election, as each Member State is free to choose its' own system, subject to certain restrictions.[18] Nevertheless, there has been an instance in the past year, where self-regulating measures introduced by Facebook would have severely impacted the elections to the European Parliament. Facebook, however, implemented a new policy on cross-border political advertising, which required each political institutions and parties to register one representative in each Member State across the EU-28 bloc to allow political advertising, e.g. the call for voters' participation. Guy Verhofstadt, leader of the liberal ALDE party, stated that this was "killing the idea of European democracy".[19] After a backlash from European institutions and EU political groups, Facebook ultimately revised their measures. The Commission's report on the 2019 election to the European Parliament has recognised efforts by the likes of Google, Facebook and Twitter to increase transparency of political ads, increase integrity of their services and to detect and close down on manipulative activities. Ultimately, they **failed to provide for a searchable database on political advertisements, or if they did such ad libraries where incomplete**. Furthermore, platforms **did not provide easy access to relevant bodies, like Member States' authorities** for oversight and analysis purposes.[20] Once again, such **voluntary actions of goodwill by online platforms have proven to be insufficient**.

Another issue emerging with the advancements in digital and online technology, especially in the fields of blockchain technology, are so-called **'smart contracts'**. In theory, 'smart contracts' are equal to conventional contracts with the sole difference that the entire information is stored digitally in a blockchain. In short, it is a transaction protocol, which automatically executes, controls or documents legally relevant events or actions according to the terms of the contract.[21] On the one hand, this shows great potential to profoundly change private law transactions, on the other hand, the **ability of the current law system to cope with automated contractual agreements is in question**. In our opinion there is **no sufficient legal certainty regarding smart contracts**. Since smart contracts are automatically executed and legally binding, and due to nature of blockchain technology are neither reversible, nor changeable, the question for clarity on liability for damage caused in the operation of such contracts arises. Additionally, there is **neither legislation that sets minimum standards nor recognition for the validity of smart contracts across the EU-27** bloc. With regards to smart

[17] https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681
[18] https://www.europarl.europa.eu/factsheets/en/sheet/21/the-european-parliament-electoral-procedures
[19] https://www.ft.com/content/0dab95ba-5156-11e9-b401-8d9ef1626294
[20] https://ec.europa.eu/info/sites/info/files/com_2020_252_en_0.pdf
[21] https://eublockchainforum.eu/video/educational/smart-contracts-simply-explained

contracts, **we recommend that the regulation of smart contracts and blockchain technology should not fall within the scope of the Digital Services Act** and be addressed in a separate legislative process.

V. How to address challenges around the situation of self-employed individuals offering services through online platforms?

Not only have the types of services offered online changed with the technological improvements in the digital age, but also the types of how those are provided. Analogous to the distortion of boundaries between producers and consumers arises the **question of boundaries between independent and dependent work, which differs in the access to certain rights**.

Increasingly individuals (so-called platform workers) are offering services (e.g. ride-hailing, food delivery, microtasks, etc.) online via hosting platforms in exchange for payment. Flexible employment opportunities like these often lead to a **false sense of self-employment, called 'dependent contracting', and precarious working conditions**. Dependent contracting describes the situation of a worker who, though not an employee of a company, is in a position of economic dependence on, and under an obligation to perform duties for, that company. This is the main reasons for precarious working conditions. **This applies to questions of minimum wage, working hours and other conditions**, e.g. in some cases equipment necessary for work is to be provided by the platform worker, not by the platform.

In general platforms workers are considered to be self-employed.[22] This arises the issue of e.g. social protection. Usually for employees, the contributions for social protection are shared between the employee and the employer. Self-employed individuals are **responsible for the full contribution** on their own. This results in **many platform workers not being able to access certain strands of social protection**, e.g. unemployment insurance.

A prominent example for the situation of self-employed individuals offering services through online platforms are in the field of delivery and transport services. In February, financial police conducted a raid of an Amazon distribution hub in Austria, suspecting fictitious companies and illicit work. Examination covered 36 delivery firms and 174 employees – in 49 cases there have been violations against labour law and one fictitious company "employing" 20 workers was detected.[23] In such cases companies often cannot be held accountable, arguing that they online hosted product listings on their website, having no part in terms of what kind of products are listed and how distribution is facilitated. This allowed them to hide behind the aforementioned liability regime for hosting providers.

During the COVID-19 pandemic it has been particularly evident that in such parcel distribution hubs and meat processing businesses, standard with regards to workers health and working conditions are insufficient. With the current legal provisions, companies could establish other companies, sub-contracting workers from the newly established ones and hereby **splitting and minimizing liability or eliminating it completely**. Practices as these should neither be enabled, nor allowed.

---

[22] https://www.eurofound.europa.eu/mk/data/platform-economy/dossiers/employment-status

[23] https://noe.orf.at/stories/3035248/ (German only)

It is evident that individuals providing services online face more worrying issues than those providing services in the "traditional" economy. For employees in the online segment, **there is no sufficient legislative framework, providing them with legal certainty**, while in the offline economy there is. This gap benefits online platforms since they are not forced to comply with minimum standards and leads to a disadvantage for the traditional economy.

We have identified solutions regarding issues with employment status, wage and working hours.

For **better transparency and insight into the work organisation of platforms** a proof of employment should exist and be based on the presumption that a relationship is existent with a dependent employee. Furthermore, it should be **clarified that employee protection and collective agreements and minimum wage regulations apply**. This means, that platforms are responsible for the payment of wage tax, social security contributions and other wage-related charges. To extend their responsibility, there should be **information obligation for platforms** towards authorities and social security institutions. Additionally, platforms should be obligated to inform on duties they have towards their worker and clearly communicate what rights they have, as they often are unaware of their rights. In case of actual self-employment, remuneration must not be below minimum wages or rates laid down in collective bargaining agreements for the same or similar activities of employed workers. Especially with relevance to ride-hailing and delivery services (e.g. food delivery), standby times and search times should count toward active working time.

Collective bargaining and collective agreements in all areas are indispensable for both the online as well as traditional economy. They provide job security, planning on a secure basis, give legal certainty and are overall an important driver for fairer competition, in which individuals can no longer benefit at the expense of workers and other companies. Especially, **large digital companies are exploiting legislative gaps in EU legislation and hereby distorting competition** and further strengthen their already dominant market power. There is an expected growth of digital services in the online economy, hence why an **appropriate, legislative regulation is a priority**. It is a question of protection against dismissal, minimum wages, occupational health, and safety and working time regulations. Without an appropriate regulatory framework, the social security system can be severely impaired. Any future legislation must protect the growing number of platform workers.

VI. What governance for reinforcing the Single Market for digital services?

Since the e-Commerce Directive's entry into force 20 years ago the potential of digital services has increased significantly. Digital services and **platforms are continuously changing their business models** to adapt to recent economic, technological and societal changes. The European framework regulating those services within the EU has not. Especially during the COVID-19 crisis it was evident that people around the world were more and more reliant on a multitude of online services, be it ordering goods from online marketplaces, staying connected with friends and family via social media sites, continuing work with home office solutions or streaming multimedia content. Not only is it the dependence of citizens around the world on platforms – especially large non-European players like Facebook, Amazon, Alibaba etc. –, but also is it the notable control over vast amount of data they generate, that indicate the responsibility those platforms should bear towards society.

So far, the EU has been heavily reliant on forms of self-regulation, when platforms agreed to terms and marketed those agreements as voluntary acts of cooperation. An example for this would be the deal struck between the European Commission with four large short-term rental platforms in March earlier this year.[24] In this "landmark agreement (…) on data sharing" those accommodation rental providers agreed to share "reliable data". As it turned out, the quality of data agreed upon, does not fulfil the necessary requirements for law enforcement by public administrations. The **lack of an adequate regulation on EU level** can be amended with the involvement of Member States' administrations in the negotiations of agreements and the consideration of their respective needs, which in turn would lead to less legal fragmentation across all Member States.

The current degree of legal fragmentation might be considered an obstacle when it comes to innovation opportunities and the depth of the Single Market for digital services, as new platforms and companies often do not have the capabilities and resources to have sufficient knowledge of the Member States' 27 different legal specifications. Hence why, the country of origin principle allows the application of one set of rules, namely that of the country where a company is based in. This principle is considered to be an important driver for digital innovation in the EU – especially for start-ups and SMEs –, but taking a closer look at the digital economy, **out of the 15 largest digital firms, not one is European**.[25] The fact that the European market is overwhelmingly dominated by large digital firms like GAFAM (Google, Amazon, Facebook, Apple, Microsoft) from the United States and Chinese stakeholders like BATX (Baidu, Alibaba, Tencent and Xiaomi) is worrying.[26] Considering that there is a lack of European players being able to compete in this highly concentrated market, and merely a multitude of small enterprises, we call onto the Commission to generate an environment, that allows for especially European SMEs to compete. To this end, **we suggest the implementation of thresholds regulating larger platforms in a stricter way than small ones, since as gatekeepers they should bear responsibility towards the market and society at large.** If small platforms must meet the same obligations as large platforms like Facebook and Google, the environment is be considered hostile for driving European innovation.

We acknowledge that the country of origin principle and its advantages for European start-ups and SMEs is vital for the recovery of the European economy and the restart of economic activities in the EU. Nevertheless, digital companies more often than not misuse it to **opt for those Member States where conditions are optimal for them in terms of regulations, taxation or the entire legal system**. The high concentration of headquarters of leading market players – Apple, Twitter, Google, Facebook or Airbnb, to name a few – in Ireland must not be ignored, since it "places practical and political burden on a small Member State".[27] **Negative consequences for the effective fulfillment of public tasks are the results.** Although there is an obligation for Member States to cooperate set in place in the current e-Commerce Directive, the **enforcement procedure is overly bureaucratic and hardly results in satisfying outcomes**, as the conflict between the city of Vienna and Airbnb has shown. The dispute started in 2017, when the city of Vienna requested the platform to comply with applicable Austrian legislation (Austrian Federal Tax Code) and to provide anonymised data of Airbnb hosts, and has been at a standstill since.

---

[24] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_194

[25] https://www.weforum.org/agenda/2019/03/europe-is-no-longer-an-innovation-leader-heres-how-it-can-get-ahead/

[26] https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf

[27] https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648780/IPOL_STU(2020)648780_EN.pdf

Effective and robust cooperation between the country of origin and the **country of destination is vital for the preservation of the safeguard of public interests** and the protection of EU citizens. This can be achieved by strengthening the country of destination in terms of digital companies complying with the public interest in the Member State operating in. In case of conflict between these two principles the **national provisions of the Member State in which the service provider offers its services should apply**. The aforementioned unequal distribution of headquarters across the EU and the excessive burden Irelands National Enforcement Bodies (NEBs) have to bear, **calls for network of NEBs coordinated and monitored by an European Central Regulatory Authority**, provided with necessary powers to settle disputes between Member States and to enforce law in a comprehensive, swift and transparent manner. This network of NEBs should also be entrusted with the supervision of providers established in third countries offering services to EU citizens.

Furthermore, we emphasise that **the country of origin principle – albeit it a cornerstone of the Single Market – is nothing indisputable**. It arises from a multitude of factors, which allows it to be adapted in specific cases. Hence why there are areas defined in the current e-Commerce Directive, where a deviation from this principle is possible and additionally areas where the e-Commerce Directive does not apply at all. We consider that, especially with regard to protection of public interests, the **areas allowing such deviations should be extended to better reflect national and regional issues within the public sector** and to provide it with the necessary tools to safeguard its reasonable interests.