Remarks on the French draft Decree implementing Law No 2022-300 of 2 March 2022 aimed at strengthening parental control over the means of access to the Internet.

(Notification TRIS 2022/0694/F)

DIGITALEUROPE and the French alliance for digital industries (AFNUM) fully support the objective of the Law of 2 March 2022 aimed at strengthening parental control over the means of access to the Internet. Our members already provide efficient and proven parental control tools on their terminal equipment, which are used daily by millions of Europeans to prevent children from being exposed to harmful content over the Internet.

However, the draft Decree proposed by the French authorities introduces new obligations which have significant impacts on the current design of these tools, while they are not necessary nor proportionate to achieve the desired goal of the law. Therefore, these should be removed from the proposed Decree or adapted in matter that put less additional and local specific burden on economic operators, and, thereby, does not undermine the right to conduct a business in the EU, nor the free circulation of goods and services within the internal market.

1/ The general obligation to block the downloading of or access to illegal content made available on software application shops undermines the uniform application of EU law and, in particular, of the Digital Markets Act (DMA).

Article 6(4) of the DMA, read in the light of Recitals 50 and 57, specifies that, as a matter of principle, the end-user must be able to install and effectively use third-party software applications or software application shops on hardware or operating systems. The end-user's choices can only be restricted for reasons relating to the security or integrity of the terminal equipment.

However, the Draft Decree introduces a restriction in principle on downloads and access to illegal content without justifying this prohibition on grounds relating to the security and integrity of the terminal equipment.

Therefore, an obligation on terminal equipment manufacturers and operating system providers to block the downloading of or access to illegal content would be contrary to the provisions of the DMA.

2/ The bans on linking the parental control functionality with the creation of a personal account, on the communication of personal data to a distant server, and on the processing of minors' data, do not meet the objective of protecting minors.

The Draft Decree provides that a parental control device is only compliant if it can be activated, when first put into service, without the configuration of the device requiring the creation of an account on a server, except in the case of the express agreement of the adult user or when this is technically impossible[1].

[1] Draft Article R. 20-29-10-1-II of the CPCE.

In practice, the exemptions to this prohibition provided for by the Draft Decree are of limited application and will not allow designers of parental control devices to offer such a functionality and users of these devices to benefit from it.

Such a ban is not necessary to achieve the objective of protecting minors online.

In this regard, it is undeniable that a parental control device associated with the creation of an account on a server best meets the objective of protecting minors and should therefore, in principle, be implemented as soon as the parental control device is activated. In so doing, these parental control devices fully involve parents by enabling them to accompany their children and protect them, in a targeted manner, against exposure to content that may be harmful to their development.

As a parent, the adult user is free to determine the level of parental control according to the profile used. It goes without saying that the parent must be able to define, according to the age of his child and the education he wishes to give him, the type of content he can access. The restrictions in this regard cannot be the same for a 4 year old as for a 16 year old. The latter must be able, if his parents so choose, to access content not recommended for children under 10 or 12.

The creation of user profiles according to the age of the child is a practice that parents are used to and, above all, fully trust[2]. 80% of parents of children aged 8 to 9, 73% of parents of children aged 10 to 14 and 58% of parents of children aged 15 to 17 have installed a parental control system. Logically, the percentage of parents with a parental control system in place gradually decreases as children approach the age of majority[3].

Therefore, by prohibiting the association of the creation of an account with the use of a parental control device, the government is directly disregarding the freedom currently offered to parents to decide on the educational direction they wish to give to their children's education and, in so doing, is necessarily disregarding the objective of protecting minors.

Additionally, the ban on processing the data of minors and transfer of data to a server is difficult to reconcile with European Union privacy law. The GDPR and the proposed ePrivacy Regulation do not impose a blanket prohibition on the processing of children's data or personal data generally. In situations where a data controller relies on consent, the GDPR specifically contemplates the processing of children's data based on parental consent (Art. 8(1) GDPR). Additionally, processing of children's data may also occur under other legal bases under the GDPR such as for the performance of a legal obligation, or in furtherance of an identified and proportional legitimate interest. Art. 8.1(b) and (c) of the ePrivacy Regulation proposal (and the corresponding provisions from the ePrivacy Directive) also provide that the collection of information from end-users' terminal equipment is lawful when the end-user has given his or her consent or if it is necessary for providing an information society service requested by the end-user. The GDPR also does not prohibit the transfer of data to the extent requirements related to data protection are met, and it is difficult to reconcile this prohibition on the processing of children's data or on their transmission to servers with principles established under the GDPR. It is unclear what more restrictive obligations would achieve.

---

2 Parenthood put to the digital test, Observatory of parenthood & digital education, Médiamétrie, 17 January 2020.

3 The digital behavior of children, Parent and child perspectives, IFOP survey for the CNIL, February 2020.

Further, such obligations will necessarily dissuade manufacturers established in other Member States from selling terminal equipment in France, as well as operating system suppliers established in other Member States from targeting the French market. The main effect of this measure would be to prohibit, on the French market, OS that integrate a parental control device working on the basis of filters by user profile, i.e. all the major systems in place today, as well as all devices equipped with such OS. This is a clear infringement to quantitative restrictions within the meaning of Article 34 TFEU as well as the free circulation of services within the EU.

3/ The self-certification mechanism proposed in the draft Decree relies on a modification of the European declaration of conformity, which significantly undermines the single market and European harmonization.

Beyond the complexity of the proposed mechanism, which would require a significant adaptation of the current process of proof of conformity, any modification of this mechanism, which is so fundamental to the European market, would be likely to create a precedent, thereby authorizing all the other Member States to introduce their own local variations leading to European regulatory fragmentation.

While we understand that the French authorities wish to setup a means to allow the market surveillance authority (ANFR) verifying whether terminal equipment entering the French market are compliant with the Law on parental control, there are other ways to achieve the same objective while not putting less additional burden on economic operators and also while not affecting the European declaration of conformity.

For example, a centralized online platform could be set up by the ANFR, where manufacturers could upload the list of product models that comply with the law's provisions on parental control. Such a platform would be easy and inexpensive to set up by ANFR, which already operates similar platforms for the declaration of radio frequency users. It would enable the market surveillance authority to effectively check that each product sold in France has been the subject of a self-certification. Such a mechanism would meet the market control objectives defined in the law just as much as a modification of the European conformity declaration system, and in a much more proportionate manner for manufacturers.

Additionally, the proposed mechanism would subject radio equipment to dual certification under both EU and national law, which would be contrary to the Radio Equipment Directive, which states that "*Member States shall not impede, for reasons relating to aspects covered by this Directive, the making available on the market in their territory of radio equipment which complies with this Directive*" *(Art. 9)*.

4/ The share of responsibilities between product manufacturers and operating systems providers will not comply with the upcoming General Product Safety Regulation (GPSR).

The draft Decree places the main responsibility for compliance on the terminal manufacturer, while the operating system provider is solely responsible for providing the manufacturer with a certificate of compliance.

However, the GPSR final draft considers that the developer or producer of software, such as operating systems, firmware, computer programs, applications or AI systems, should be treated as a manufacturer (recital 12). The GPSR clearly extends the definition for products to software (art. 4-1).

Therefore, discriminating the responsibilities between hardware manufactures and operating systems providers as proposed in the French draft Decree will be contrary to GPSR.

5/The general obligation to block specific content made available through software application shops lacks the safeguards and liability standards of EU law in the fight against illegal content

Under EU law, the blocking of downloads or access to illegal content online by a third party is intertwined with the search for a balance between freedom of expression, the protection of privacy, the fight against illegal content and the protection of minors.

For example, the removal of illegal content carried out by intermediary service providers is strictly regulated: it must never lead to a general obligation of monitoring or active fact-finding[4]. Even though neither terminal equipment manufacturers nor OS providers qualify as "intermediary service providers", the Draft Decree intends to require them to ensure the possibility of blocking the downloading of and access to illegal content[5], with no further safeguards or guarantees.

In comparison, the general obligation of the Draft Decree to block the downloading of or access to illegal content made available by software application, applied indefinitely to operators who are not intermediary service providers, does not apply the same standards as those set out by European legislative instruments in the fight against illegal content, in terms of guarantees to safeguard the fundamental freedoms of users.

In addition, the Draft Decree does not contemplate the scenario where the content would be incorrectly classified by the publisher or other content provider that plays an active role in providing knowledge of or control over the content uploaded, and does not provide any cascading liability to make the content provider primary responsible for such classification. Rather, under the Draft Decree, equipment manufacturers and OS providers could be held liable if the parental control system does not allow the blocking of such content, even though it was not classified as restricted to minors by the content provider[6]. This does not comply with the standards of EU law either, pursuant to which content providers remain primarily responsible.

As we have shown above, these measures infringe, or are inconsistent with, several European laws, while being unnecessary and disproportionate to reach the objective of the French law on parental control. Therefore, these should be removed from the proposed Decree or adapted in matter that put less additional burden and disproportionate efforts on economic operators, and, thereby, does not undermine the right to conduct a business in the EU, nor the free circulation of goods and services within the internal market.

---

[4] Articles 8 and 9 of the DSA.

[5] Draft Article R. 20-29-10-1-I (a) and (b) of the CPCE.

[6] See Article 6(1) of the DSA (and formerly Article 14(1) of the ecommerce Directive), read jointly with CJEU settle case-law, e.g., C-682/18 and C-683/18, 22 June 2021, paragraph 117, precluding liability for service providers insofar they do not play an active role in the content published. By contrast, the responsibility lies with the provider - e.g. the publisher classifying the content - who plays an active role in giving it knowledge or control over the content uploaded to his platform.

****

AFNUM (Alliance Française des Industries du Numérique) represents, in France, manufacturers in the consumer electronics, IT, printing, networks, photography and connected objects sectors. The economic weight of AFNUM's member companies is 35,000 direct jobs and 130,000 indirect and induced jobs in France for a turnover of 29 billion euros. AFNUM is a member of FIEEC, MEDEF and DIGITALEUROPE.

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national trade associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.