GESTE AND SRI'S SUBMISSION TO THE EDPB PUBLIC CONSULTATION ON GUIDELINES 2/2023 ON TECHNICAL SCOPE OF ART. 5(3) OF EPRIVACY DIRECTIVE

Introduction. – GESTE[1] - *an organization that brings together the main publishers of online content and services, comprising 101 members, including most French media groups. Since its establishment in 1987, GESTE has been analyzing changes in publishers' economic models, providing a better understanding of the challenges of digital transformation, and contributing to the development of favorable economic, legislative, and competitive conditions* - and **SRI**[2],- *a French trade association regrouping 28 members, digital sales houses and sell-side adtech partners. The SRI and its members share their expertise and promote best practices for a responsible and sustainable digital advertising landscape. It also provides key information to understand the complexity of the digital advertising ecosystem, in particular through its report "l'Observatoire de l'e-pub"* -, welcome the EDPB's initiative to clarify the scope of Article 5(3) of ePrivacy Directive ("**ePD**") in its draft guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive.

Clear rules have better chances to be well-enforced and to ensure an effective protection of online privacy. However, GESTE and SRI wish to raise some concerns regarding the above-mentioned draft guidelines, as Article 5(3) should only be interpreted by competent authorities and with due respect for the wording of said article, as well as for the EU legislator's intentions.

This document presents GESTE and SRI's comments and concerns on these draft guidelines, and more specifically on (i) the overly broad and unfounded interpretation of the scope of Article 5(3) that they propose, and (ii) more general concerns.

(i) Concerns on the overly broad and unfounded interpretation of the scope of Article 5(3)

Relevant provisions. – Article 5(3), as amended by Directive 2009/136/CE, provides that:

> "*Member States shall ensure that the storing of information, or the gaining of access to information **already** stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".

Recitals 24 and 25 ePD specify that:

> "(*24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.*
>
> *(25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being*

[1] *Groupement des Editeurs de Contenus et Services en Ligne.*
[2] *Syndicat des Régies Internet.*

> *placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose*".

Recitals 65 and 66 of Directive 2009/136/CE further specify that:

> "*(65) Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party (spyware) poses a serious threat to the privacy of users, as do viruses. A high and equal level of protection of the private sphere of users needs to be ensured, regardless of whether unwanted spying programmes or viruses are inadvertently downloaded via electronic communications networks or are delivered and installed in software distributed on other external data storage media, such as CDs, CD-ROMs or USB keys. Member States should encourage the provision of information to end-users about available precautions, and should encourage them to take the necessary steps to protect their terminal equipment against viruses and spyware.*
>
> *(66) Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities*".

Outline. – In light of this article and these recitals, it is GESTE and SRI's opinion that the EDPB's draft guidelines should be reviewed:
- from a technical and literal perspective (**a.**),
- from a teleological legal perspective (**b.**) and
- from a practical perspective (**c.**).

a. From a technical and literal perspective

Technical operations covered. – According to the EDPB's current version of the guidelines, "*Article 5(3) ePD does not exclusively apply to cookies, but also to 'similar technologies'. However, there is no comprehensive list of the technical operations covered by Article 5(3) ePD*".

Article 5(3) does indeed not only apply to cookies, but also to "similar devices".

However, the technical operations to be covered by Article 5(3) ePD are listed comprehensively. Indeed, this article specifically targets (i) the storing of information and (ii) the gaining access to information already stored in the terminal equipment. These are "technical operations" and they are as such the only ones meant to be covered by Article 5(3).

► **The phrase on the absence of comprehensive list of technical operations covered by Article 5(3) should be removed.**

Storage of information. – The EDPB seems to consider that the information stored within the meaning of Article 5(3) can be constituted of instructions to generate specific information.

This interpretation is too broad and has no legal ground. Article 5(3) targets the storage of information and not the storage of instructions generating information. Such interpretation would lead to encompass all protocols entailing the generation of information by a terminal equipment and, as such, almost all online interactions and basic Internet protocols.

- ► **Article 5(3) should not be considered as covering the storage of instructions generating information.**

Gaining of access. – From a different angle, still aiming at the coverage of information generated automatically and instantaneously, the EDPB considers that Article 5(3) covers the gaining of access to such information.

However:

- the fact that the gaining of access mentioned by Article 5(3) only pertains to "information already stored in the terminal equipment" is omitted on several occasions in the draft guidelines. The word "already", added to Article 5(3) when this text was amended by Directive 2009/13/CE, is crucial to understand the notion of gaining of access and means that the information must predate the access. This especially entails the exclusion of information instantaneously generated and, as such, non-preexisting in the terminal equipment, even if, for the sole purpose of the automatic transmissions of this information, it can be ephemerally stored in RAM and cache. The mere storage in RAM and cache for the sole purpose of an automatic transmission cannot indeed suffice to consider that the information precedes this transmission.
- the use of the terminology "gaining of access" is also to be taken into account. It involves an active request to receive targeted information. It does not include passive receipt of information automatically and inevitably sent without any specific instruction targeting this information.

- ► **Article 5(3) ePD should not be considered as covering the gaining of access to information automatically transmitted without any specific instruction targeting this information.**

Tracking pixels and links. – The EDPB considers that the use of tracking pixels and links constitute storage on the users' terminal equipment, since said equipment is instructed to send back the targeted information.

However, the EDPB's interpretation regarding tracking pixels is built on the confusion made between the storage of information, covered by Article 5(3), and the storage of instructions generating information, not covered by Article 5(3) (*see* above).

Actually:

- for pixels, there is no storage of information within the meaning of Article 5(3), but only the loading of pictures through standard HTTP requests;
- for links, there is once again no storage of information within the meaning of Article 5(3), but only the loading of the resource requested by the user of the website yet again through standard HTTP requests.

There is no gaining of access to information already stored either for both mechanisms. There is only an automatic transmission of information non-preexisting in the terminal equipment without any specific instruction targeting this information.

As such, Article 5(3) is not applicable to any of them.

The fact that, during the loading, an information, which was not already stored on the equipment, is collected does not trigger the application of this Article 5(3), since this provision does not cover this

type of technical operation. GDPR however may apply and ensure, to the extent needed, the protection of the privacy of users (*see* section (ii)).

- ► **Tracking pixels and links should not be mentioned as devices covered by Article 5(3) ePD.**

Unique identifiers. – The EDPB considers that the use of unique identifiers on websites or mobiles applications triggers the application of Article 5(3), since the entity collecting it is instructing the browser to send that information, which would constitute a gaining of access within the meaning of Article 5(3).

However, this is again a too broad interpretation of Article 5(3) disregarding here the requirement of an information "already" stored in the terminal equipment.

Article 5(3) should only apply to the unique identifier mechanism when unique identifiers are stored in the terminal equipment of the user, for instance by the means of a cookie.

- ► **It should be specified that Article 5(3) applies when unique identifiers that are already stored on the terminal equipment of users are being accessed.**

b. From a teleological legal perspective

Article 1(1) ePD. – According to the EDPB, Article 1 ePD must be considered to "correctly frame the notion of gaining access".

Article 1(1) provides that:

> "*This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community*".

However, the EDPB only focuses on one part of this provision, *i.e.* the fact that the ePD is a "*privacy preserving legal instrument aiming to protect the confidentiality of communications and the integrity of services*".

GESTE and SRI regret that, by doing so, the EDPB completely disregards the second aim of the ePD, which is "*to ensure the free movement of such data and of electronic communication equipment and services in the Community*".

In fact, as the GDPR, the ePD was meant as a regulatory tool ensuring the balance between privacy and other legitimate considerations such as the free movement of data and services, both to be taken into account when interpreting the ePD.

- ► **The European goal of ensuring the free movement of data, electronic communication equipment and services within the Community should be better taken into account in the draft guidelines.**

Working documents on ePD and Directive 2009/136/CE. – The study of the working documents from the European Commission, the European Parliament, and the Council of European Union on ePD and Directive 2009/136/CE are very enlightening with regard to these institutions' intentions when adopting both of these texts.

These documents all show without a doubt that the intended target of Article 5(3) was definitely:
- cookies and software, such as spywares (and not mechanisms such as pixels, tracking URLs or unique identifiers);
- and the active "introduction" or "entering" into the terminal equipment to store or retrieve information (and not the passive reception of such information).

For instance:

- the Working Party of Telecommunication of the Council of European Union states when studying the amendment introducing Article 5(3) (originally 5(2a)) that: "*Control of cookies and spyware (Article 5(2a), recitals 24 and 25) European Parliament amendment 26 proposes requiring the prior, explicit consent of the subscriber or user (opt-in) to any introduction of information into his/her terminal equipment. In the Commission's view, while this amendment introduces positive new features, its scope needs to be clarified. To that end and in the light of the discussions, the Presidency suggests: – two new recitals(24) and (25) to clarify the different treatment reserved, on the one hand, for "cookie" devices which are used for legitimate purposes and on condition that the user is clearly and fully informed and has right of refusal, and on the other, spyware devices which by their very nature do not inform the user and should therefore be prohibited; – adjusting accordingly the text of the new Article 5 (2a) proposed by the European Parliament*"[3];
- the European Commission refers to the strengthening of "*provisions on protection against spyware and placing of cookies on users' devices*" in its opinion dated 29 July 2009 on the European Parliament's amendments to the Council's Common Position[4].

► **The EU legislator never intended to target mechanisms such as pixels, tracking URLs or the use of unique identifiers regardless of their way of collection, nor the sole passive reception of information automatically transmitted.**

Working documents of ePrivacy Regulation. – The study of the working documents from the European Commission, the European Parliament, and the Council of European Union on the future ePrivacy regulation are also very interesting as they shed a light on these institutions' interpretation of the current scope of Article 5(3).

Especially, it must be highlighted that, in its impact assessment accompanying the proposal for a ePrivacy regulation, the European Commission states that "*the rule is at the same time over-inclusive as it also applies to non-intrusive practices (e.g. first party analytics), and under-inclusive, **as it does not address new tracking techniques (e.g. device fingerprinting)***"[5].

It should incidentally be mentioned that, by stating this, the European Commission disavows WP29's preexisting position on said fingerprinting. This is a perfect example of why the opinions of different sources, especially the ones at the genesis of ePD, should be sought by the EDPB (*see* section (ii)).

c. From a practical perspective

Major negative consequences without much added value in terms of online privacy. – Under the current version of the guidelines, all interaction online with a terminal equipment would be covered by Article 5(3) (*see above*).

This would lead to an overly broad application of Article 5(3) consent requirement and to a huge increase of consent requests.

Even in situation where there could have been room for discussion on the application on one of the exemptions of Article 5(3), numerous stakeholders will likely choose to seek consents every time they interact with a terminal equipment in order to mitigate as much as possible the risk of a complaint or a litigation.

This would also entail the potential paralysis of numerous legitimate and essential activities, especially for the economy in place for websites and applications.

[3] https://data.consilium.europa.eu/doc/document/ST-14163-2001-INIT/en/pdf%20/. See also the WP Telecommunications referring again to « 'cookies' and spywares » (« *Finally, on the basis of a European Parliament amendment, the Council clarified in its draft Directive what treatment should be reserved for "cookies" and spyware, in particular the conditions for the legitimate use of these devices, in compliance with Directive 95/46/EC* » – https://ec.europa.eu/commission/presscorner/detail/en/PRES_01_448).

[4] https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2009/0421/COM_COM(2009)0421_EN.pdf.

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5358_2017_ADD_1 (page 5). Also in the same document: « *Privacy and confidentiality of terminal equipment, including in respect of online tracking, are protected only when there is a storing of information, or an access to information already stored, into the users' terminal equipment. Any other interferences carried out by other technical means (e.g. certain forms of device fingerprinting) are as a rule not covered*" (pages 20-21).

For instance, since users will be able to refuse all interaction with their equipment, this will impede the possibility to accurately measure the audience of the advertisements shown on websites and applications (personalised or not) and, as a result, to correctly redistribute the revenues arising from these advertisements.

As another example, tracking pixels inserted in emails are essentially use to assess the emails recipients' interest in their contents in order to avoid sending contents that do not interest the recipients. It is a precious tool to fight against spam. If tracking pixels' use was to become very difficult, or even impossible (as it would be very challenging to seek consent), this would lead to the inability for the senders of newsletters to improve them and, consequently, to the sending of less and less relevant contents.

- **The application of the EDPB's guidelines, in their current version, would exacerbate even more the consent fatigue that is presently being highly criticized on all sides, whilst, against the grain, remedies to this fatigue, including reducing the number of consents, are being actively sought, including by the European Commission with its Cookie Pledge Initiative. An over-inclusive consent requirement would be totally counterproductive.**

  It would also lead to significant costs on many businesses, major changes to the current economy of the Internet, a drastic reduction of accessible websites or applications relying on advertisement revenues to finance their activities and a massive increase of distribution of irrelevant contents on websites, applications and newsletters, all of this without in the end much added value in terms of online privacy.

The GDPR solution. – The EDPB express some concerns regarding the privacy of individuals, which should be better protected online through a broader interpretation of the scope of Article 5(3) ePD.

In addition to the fact that the existence of systematic privacy issues is questionable, GESTE and SRI do not believe that the best solution to address these concerns is to overstretch a *lex specialis*, which has to be interpreted restrictively and has been deemed by numerous stakeholders, including the European Commission as unfit and as lacking "*the necessary flexibility to support technical uses that do not present substantial threat for users' privacy*"[6].

In fact, it is GESTE and SRI's opinion that a better suited solution lies with the *lex generalis, i.e.* GDPR, also applicable in most of the use cases considered by the EDPB and whose application is considered as successful by the EDPB itself in its very recent contribution to the European Commission's report on the application of GDPR.

Indeed, in many of the use cases mentioned by the EDPB, personal data would be processed. This would trigger the application of the GDPR.

When this is required to protect the privacy of users, the application of the GDPR could result in the requirement of a consent, alongside the provision of detailed information on the data processing. More precisely, consent could be required when no other legal basis under Article 6 GDPR is applicable, especially the legal basis of the legitimate interests which must be put aside when the interests, rights and freedoms of the data subjects, including privacy, prevail over these legitimate interests, but can be an accurate legal basis for several practices mentioned in the draft guidelines.

This Article 6 and, more broadly, all the provisions of GDPR already protect the privacy of individuals, while ensuring the necessary balance between the right to privacy and the other interests, rights and freedoms in presence.

- **Thus, the privacy-preserving goal can be achieved with GDPR without stretching the meaning of ePD and disregarding the EU legislator's intentions.**

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5358_2017_ADD_1 (page 12).

GDPR is indeed an effective, and even probably better adjusted, tool to regulate what is not within the technical scope of Article 5(3) ePD, without entailing any lowering of the protection of online privacy.

(ii) General concerns

Concerns on the prerogatives and competence of the EDPB regarding ePD. – In its draft guidelines, the EDPB intends to address an alleged "circumvention" of the legal obligations provided by Article 5(3).

If such "circumvention" happens to be possible for the mechanisms and operations described by the EDPB in these guidelines, this is because such legal obligations should normally not apply pursuant to the current version of Article 5(3) (*see* section (i)).

De lege ferenda, the EDPB may regret this state of play, consider the ePD to be riddled of flaws and shortcomings or outdated and express some concerns to the EU legislator (even though the existence of privacy issues is questionable for some of the practices addressed in the draft guidelines). However, such considerations should not allow the EDPB, *de lege lata,* to reform the ePD, which is the role of the EU legislator, nor should it allow the EDPB to bypass the ongoing legislative process on the future ePrivacy Regulation within which the very same issues as the ones identified in the draft guidelines will be addressed.

- **The draft guidelines, in their current version, lead to a wide and new extension of the technical scope of Article 5(3) that is not supported by either a technical and literal approach of the text or a teleological one (*see* section (i)) and, as such, cannot be considered as positive law.**

  As a result, by adopting this version of the guidelines, the EDPB would exceed its competence which is limited, regarding guidelines, to the interpretation of such positive law.

Furthermore, the EDPB's competence to issue guidelines on ePD is also questionable.

Article 15(3) ePD provides that its predecessor, the WP29, can carry out, with regard to matters covered by ePD (namely the protection of fundamental rights and freedoms and of legitimate interests in the electronic communications sector), the tasks that were laid down in Article 30 Directive 95/46/CE repealed and replaced by GDPR.

Pursuant to Article 94 GDPR, all reference to WP29 are to be read as references to the EPDB. However, EPDB's missions with regard to ePD were not clarified in the GDPR, including at Article 70 listing the EDPB's tasks.

- **The possibility for the EDPB to issue guidelines on ePD matters is questionable. The EDPB is probably only entitled to issue opinions or recommendations on these matters as intended initially by ePD referring to Article 30 Directive 95/46/CE.**

Concerns on the representativity of the EDPB regarding ePD. – Pursuant to Article 15 ePD, Member States were left with the choice to designate the authority in charge of enforcing the ePD rules at national level. This led to the designation of different supervisory authorities in charge of various missions, essentially authorities in charge of enforcing GDPR or authorities regulating telecommunications.

As for the EDPB, pursuant to Article 68 GDPR, it is only composed of supervisory authorities of the Member States in charge of enforcing GDPR and of the European Data Protection Supervisor. Consequently, it does not include all the authorities that are in charge of enforcing Article 5(3) ePD.

Despite of this fact, the EDPB intends to provide guidelines on how to interpret Article 5(3), without consulting all the authorities in charge of enforcing it.

- **The lack of representativity of the EDPB with regard to the enforcement of Article 5(3) could lead to the adoption of guidelines that will likely not reflect the doctrine of all authorities in charge of this enforcement.**

  This would call into question their legitimacy and relevancy and will probably allow the persistence of different interpretations and inconsistencies on the EU territory.

Concerns on the lack of supporting sources. – Such conclusions are aggravated by the lack of different sources supporting the EDPB's new and very broad interpretation of Article 5(3).

Indeed, if the EDPB indicates on several occasions that clarifications on the technical scope of Article 5(3) have already been made clear, for instance with regard to device fingerprinting, these clarifications actually emanate from its predecessor, WP29, not from national judges or ECJ or other external sources.

GESTE and SRI regret that, except on very rare topics, the EDPB's position is not supported by any other sources, whereas numerous entities, institutional, doctrinal, and jurisdictional, took an interest to Article 5(3) and its application (*see* examples mentioned above).

- **The EDPB's guidelines should be supported by other opinions than its own. The opinion of institutional, doctrinal, and jurisdictional sources, studying and applying Article 5(3), should be considered.**

Concerns on the lack of completeness. – The draft guidelines are meant to cover the technical scope of Article 5(3), but only pertain to the technical operations allegedly covered by this article without analysing the cases where such technical operations would be exempted from the rules that it provides.

Yet, the EDPB considers adopting in these guidelines an unprecedented overly broad interpretation of this technical scope. Such interpretation would lead to a theoretical application of Article 5(3) and its prior consent requirement to every interaction with the terminal equipment of a user, such as the mere loading of a website page (*see* section (i)).

- **To prevent the seeking of consent for every interaction online with a terminal equipment, it is of paramount importance that the draft guidelines also address the scope of Article 5(3)'s exemptions. To let this task to each national authority will lead to inconsistencies on the EU territory.**