



Prof. Dr. Eleni Kosta - Contribution to the public consultation on the Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

## Introduction

The EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive stipulate that Article 5(3) of the ePrivacy Directive applies if:

a. CRITERION A: the operations carried out relate to 'information'. It should be noted that the term used is not 'personal data', but 'information'.

b. CRITERION B: the operations carried out involve a 'terminal equipment' of a subscriber or user.

c. CRITERION C: the operations carried out are made in the context of the 'provision of publicly available electronic communications services in public communications networks'.

d. CRITERION D: the operations carried out indeed constitute a 'gaining of access' or 'storage'. Those two notions can be studied independently, as reminded in WP29 Opinion 9/2014: 'Use of the words "stored or accessed" indicates that the storage and access do not need to occur within the same communication and do not need to be performed by the same party.

The inclusion of criterion C (the operations carried out are made in the context of the 'provision of publicly available electronic communications services in public communications networks') is incorrect, as I will explain below and I would urge the EDPB to remove it from the list of Criteria on the application of Article 5(3) ePrivacy Directive.

## The 2009 amendment of Article 5(3) ePrivacy Directive

The ePrivacy Directive contains protective rules relating to the confidentiality of communications and Article 5(3) ePrivacy Directive in particular regulates the storing of information and the gaining of access to information that is already stored in the terminal equipment of users and subscribers. Article 5(3) ePrivacy Dirctive was amended in 2009 by the by the Citizens' Rights Directive<sup>1</sup>, which modified the scope of Article 5(3).

<sup>&</sup>lt;sup>1</sup> Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the





The old Article 5(3) of the 2002 ePrivacy Directive stated that:

"Member States shall ensure that **the use of electronic communications networks** to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned **is provided with clear and comprehensive information** in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and **is offered the right to refuse** such processing by the data controller. [...]"<sup>2</sup> (emphasis added)

The new Article 5(3) of the ePrivacy Directive reads as follows:

"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. [...]"<sup>3</sup> (emphasis added)

The phrase "the use of electronic communications networks to store information or to gain access to information stored"<sup>4</sup> was thus replaced by "the storing of information or the gaining of access to information already stored" in order to expand the application of Article 5(3) of the ePrivacy Directive. The Citizens' Rights Directive clarified that the storing of information or gaining access to information already stored in the terminal equipment of the user, described in Article 5(3) of the ePrivacy Directive, may range "from the legitimate [i.e. purposes] (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses)"<sup>5</sup>. Thus, the field of application of the aforementioned provision is rather broad. The amended provision covers not only unwanted spying programs or viruses which are inadvertently downloaded via electronic communications networks, but covers also hidden programs that are

protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws ("Citizens' Rights Directive") [2009] OJ L337/11 (18.12.2009).

<sup>&</sup>lt;sup>2</sup> Old Article 5(3) 2002 ePrivacy Directive.

<sup>&</sup>lt;sup>3</sup> Article 5(3) ePrivacy Directive.

<sup>&</sup>lt;sup>4</sup> Old Article 5(3) 2002 ePrivacy Directive.

<sup>&</sup>lt;sup>5</sup> Recital 66 Citizens' Rights Directive. The 2002 ePrivacy Directive also made explicit reference to "[s]o-called spyware, web bugs, hidden identifiers and other similar devices" (Recital 24), as well as "cookies" (Recital 25).





delivered and installed in software distributed on other external storage media, such as CDs, CD-ROMs, USB keys, flash drives, etc.<sup>6</sup>

According to Article 3, the ePrivacy Directive applies to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices"<sup>7</sup>. By broadening the scope of Article 5(3) beyond the use of electronic communications networks, the European legislator overreaches the scope of the ePrivacy Directive. The Article 29 Working repeatedly confirmed that Article 5(3) ePrivacy Directive is a general provision, which is applicable not only to electronic communication services but also to any other services when the respective techniques are used.<sup>8</sup> The Article 29 Working Party has specifically clarified that Article 5(3) ePrivacy Directive applies also to information society services and not only to electronic communications ones.<sup>9</sup>

## Explaining the need for the broadening of the scope

In 2003, the Music Company Sony/BMG introduced a tool, called MediaMax, as a Digital Rights Management (DRM) system in order to limit the number of musical copies of its CDs. However, MediaMax did much more than preventing piracy and limiting the number of music copies that could be produced from a CD. When a MediaMax CD was inserted into the computer of a user, a rootkit was installed in the terminal equipment of the user, without informing him or requesting his consent for the installation.<sup>10</sup> In 2006, the U.K. National Consumer Council found that the Sony/BMG End User Licence Agreement that covered the CD software allowed Sony/BMG "to install and use 'backdoors' in the software to 'enforce their rights' without prior notice".<sup>11</sup>

The public outcry against Sony/BMG was immense and led to consumer complaints around the world. The European Commission realised that the existing legal framework on the regulation of spyware and similar devices (i.e. Article 5(3) of the 2002 ePrivacy Directive) did not cover cases as the one described above, because it was applicable only when electronic communications

<sup>&</sup>lt;sup>6</sup> Recital 65 Citizens' Rights Directive.

<sup>&</sup>lt;sup>7</sup> Article 3 ePrivacy Directive.

<sup>&</sup>lt;sup>8</sup> Article 29 Data Protection Working Party Opinion 1/2008 on data protection issues related to search engines, WP 148, 04 April 2008, repeated in Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, WP 171, 22 June 2010, p. 9 and Article 29 Data Protection Working Party , Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) , WP159, fn. 7.

<sup>&</sup>lt;sup>9</sup> Article 29 Data Protection Working Party, 'Opinion 1/2008 on data protection issues related to search engines, WP148, 04 pril 2008, p. 12.

<sup>&</sup>lt;sup>10</sup> Paniza-Fullana, Antonia, 'DRM Sony system, consumer protection and user privacy' in Mercado-Kierkegaard, S. (ed) *The first international conference on Legal, Privacy and Security Issues in IT (LSPI 2006)* (Hamburg, Germany 2006) 67-72

<sup>&</sup>lt;sup>11</sup> National Consumer Council (U.K.), 'National Consumer Council submission to The All Party Internet Group inquiry into Digital Rights Management' (06.01.2006).





networks were used. Realising the inability of the then legal framework to cope with the technological challenges, the European Commission decided to broaden the scope of Article 5(3) of the ePrivacy Directive in order to cover unwanted spying programs or viruses that "are delivered and installed in software distributed on other external storage media, such as CDs, CD-ROMs, USB keys"<sup>12</sup>. The need to adjust to the current technological challenges and to provide enhanced protection to the European citizen led to the adoption of a provision that was overreaching the scope of application of the ePrivacy Directive.

## Conclusions

For these reasons, I believe that Criterion C should be deleted from the list of Criteria that specify the application of Article 5(3) ePrivacy Directive.

A detailed explanation of the legislative evolutions that led to the change in the scope of Article 5(3) ePrivacy Directive is outlined in detail in the following publications, on which my input to the public consultation relied:

- KOSTA, E., Peeking into the cookie jar: the European approach towards the regulation of cookies, International Journal of law and information technology, 2013 21: 380-406; a pre-print version of this paper is also available here: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2675810
- DUMORTIER Jos, KOSTA Eleni, Study for the European Commission DG Communications Networks, Content & Technology on the ePrivacy Directive: assessment of transposition, effectiveness and compatibility with the proposed Data Protections Regulation, June 2015, available at <u>https://digital-strategy.ec.europa.eu/en/library/eprivacy-directiveassessment-transposition-effectiveness-and-compatibility-proposed-data</u>

<sup>&</sup>lt;sup>12</sup> Recital 65 Citizens' Rights Directive.