

LAW AND DIGITAL TECHNOLOGIES
ELECTRONIC COMMUNICATIONS

ePrivacy

Prof. Gerrit-Jan Zwenne
February 10th, 2023



1

HOME > EU DATA PROTECTION > COUNCIL OF THE EU RELEASED A (NEW) DRAFT OF THE EPRIVACY REGULATION

Council of the EU Released a (New) Draft of the ePrivacy Regulation

By Dan Cooper and Anna Oberschelp de Meneses on January 6, 2021

POSTED IN DATA PRIVACY, EU DATA PROTECTION, EUROPEAN UNION, GDPR

On January 5, 2021, the Council of the European Union released a new **draft version** of the ePrivacy Regulation, which is meant to replace the ePrivacy Directive. The European Commission approved a first draft of the ePrivacy Regulation in January 2017. The draft regulation has since then been under discussion in the Council.

On January 1, 2021, Portugal took over the presidency of the Council for six months. Ahead of the next meeting of the Council's working party responsible for the draft ePrivacy Regulation, the **Portuguese Presidency** issued a revised version of the draft regulation. This is the **14th draft version** of the ePrivacy Regulation (including the European Commission's first draft).

Once approved, the ePrivacy Regulation will set out requirements and limitations for publicly available electronic communications service providers ("service providers") processing data of, or accessing devices belonging to, natural and legal persons "who are in the [European] Union" ("end-user"). The regulation aims to safeguard the privacy of the end-users, the confidentiality of their communications, and the integrity of their devices. These requirements and limitations will apply uniformly in all EU Member States. However, EU Member States have the power to restrict the scope of these requirements and limitations where this is a "necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests."



2

Council of the European Union

Brussels, 5 January 2021
(OR. en)

5008/21

Interinstitutional File:
2017/0003(COD)

LIMITE

TELECOM 1
COMPET 1
MI 1
DATAPROTECT 1
CONSON 1
JAI 1
DIGIT 1
FREMP 1
CYBER 1
CODEC 3

NOTE

From: Presidency
To: Delegations
No. prev. doc.: 9931/20
No. Cion doc.: 5358/17
Subject: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

L INTRODUCTION

- In view of the WP TELE meeting on 7 January, Delegations will find in Annex I the Presidency proposal of the ePrivacy Regulation.
- The Presidency aims to conduct swift discussions with Member States, intending to jointly discuss articles and the relevant recitals.
- During the recent discussions in the WP TELE, it has become clear that the majority of Delegations could not support the text as it stood in doc. 9931/20. A number of them expressed their wish for more substantial changes in the proposal.

5008/21 TREE.2.B PB/vk 1
LIMITE EN

3

Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (Tecom Code)

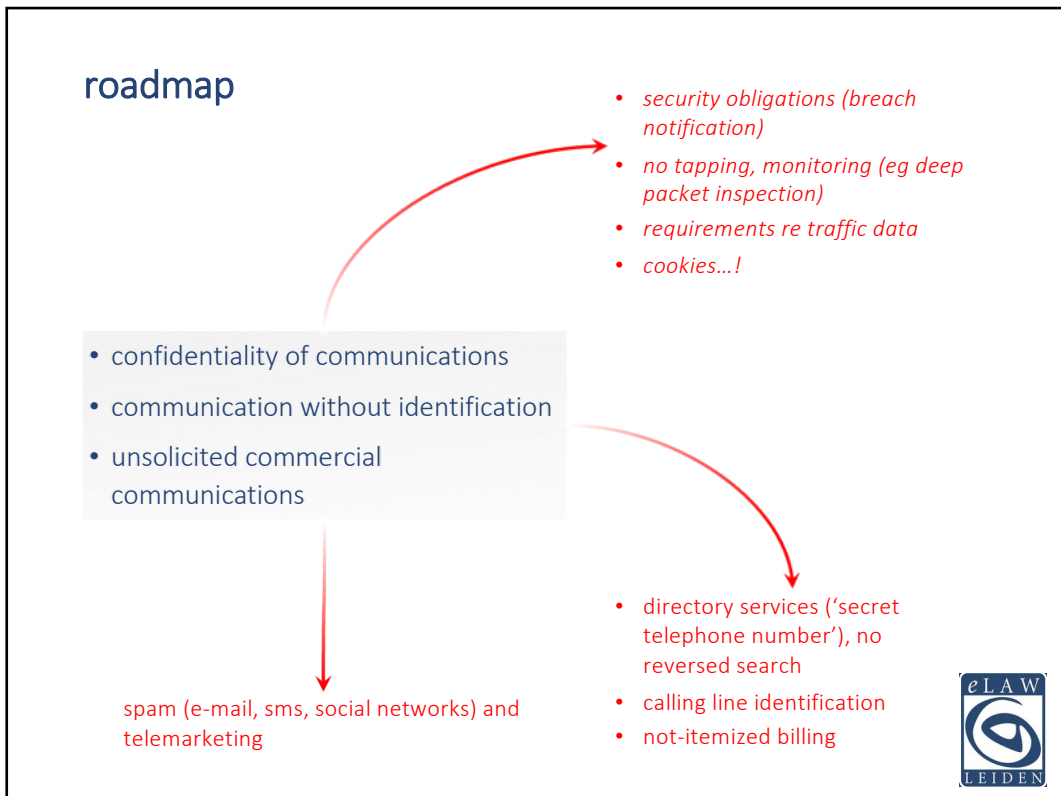
Art. 2(4)
 ‘electronic communications service’ means a service normally provided for remuneration via electronic communications networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services

- ‘internet access service’ as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
- interpersonal communications service**
- services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting

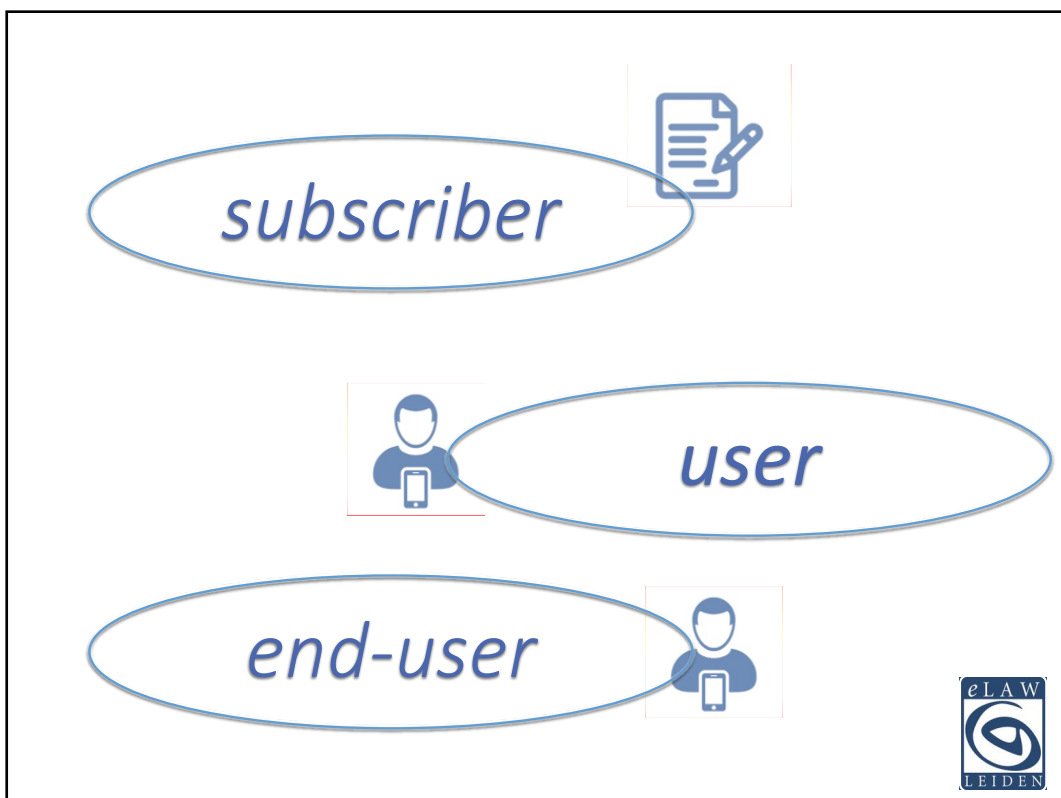
Over The Top (“OTT”) Services e.g. Whatsapp, Signal, Telegram etc. Facebook? Twitter?

Art. 2(5)
 a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service

4



5

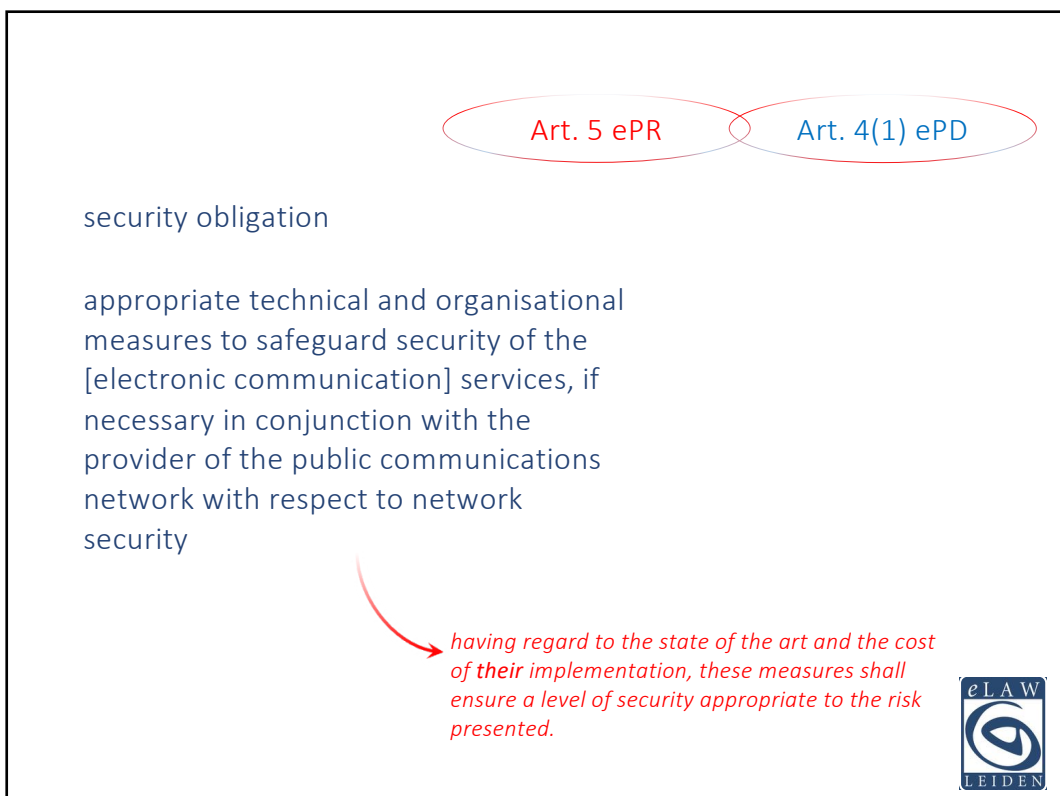


6



confidentiality of communications

7



Art. 5 ePR Art. 4(1) ePD

security obligation

appropriate technical and organisational measures to safeguard security of the [electronic communication] services, if necessary in conjunction with the provider of the public communications network with respect to network security

having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

8

Art. 33-34 GDPR

Art. 4(3) ePD

breach notification

- notify the personal data breach to the competent national authority
- also notify the subscriber or individual, if likely to adversely affect the personal data or privacy of a subscriber or individual, if the breach without undue delay

→ 24 hours? 72 hours?
what's the startingpoint?



9

breach notification to DPA

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

notification to data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.



10

authentication...?

11

“electronic communications metadata”

confidentiality of communications and traffic data

no listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned

Art. 6 EPR

Art. 5(1) ePD

deep packet inspection (“dpi”)

net neutrality debat...

spam filter..?

12

Art. 6 ePD

traffic data relating to subscribers and users must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication

with user or subscriber data may be used for the purpose of marketing electronic communications services or for the provision of value added services.



13

2006/24/EC

processed and stored by the provider of a public communications network or publicly available electronic communications service

4 months

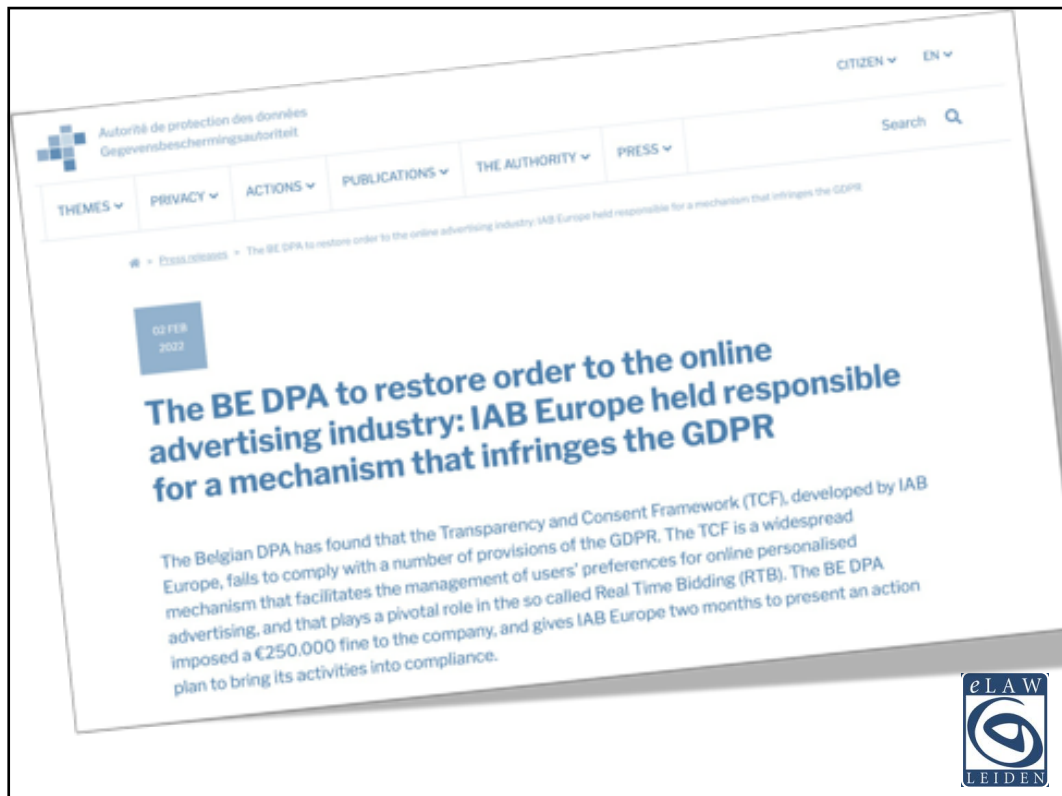
data retention obligation for the purpose of the investigation and prosecution of serious crime

Retention Directive 2006/24/EC annulled by CJEU 8 July 2014 C-293/12 and C-594/12

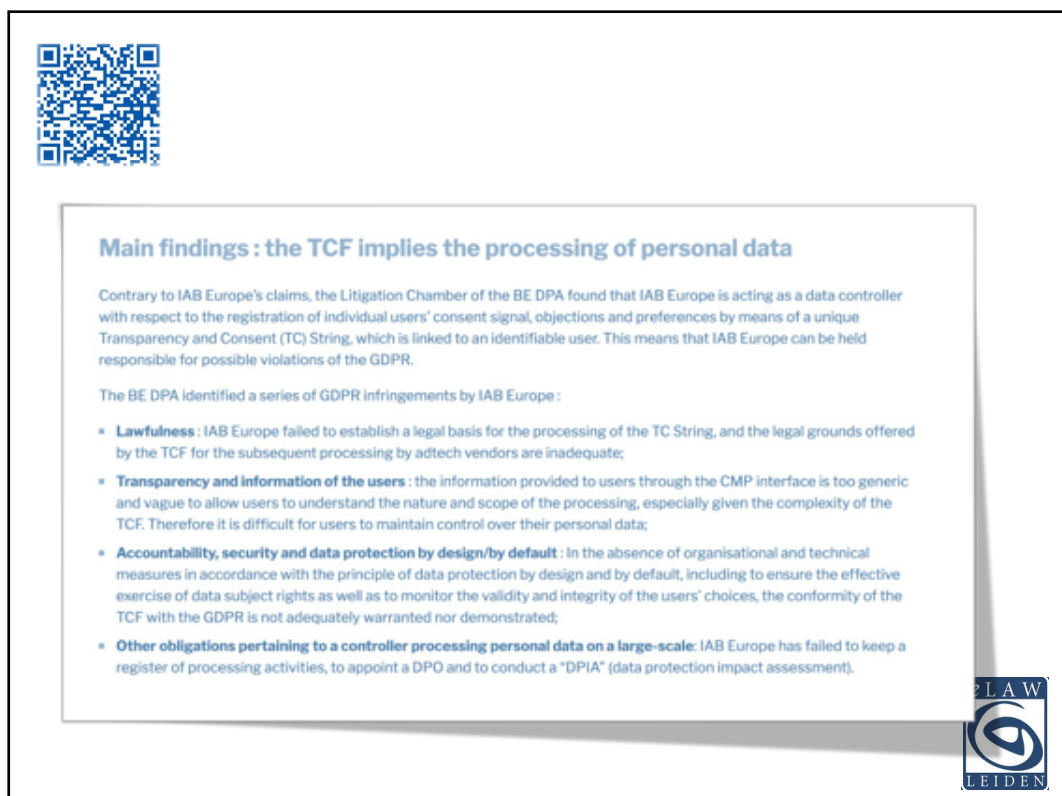
as defined in Article 1(2) of the Directive



14



15



16


Art. 8 ePR Art. 5(3) ePD

cookies! device fingerprinting, pixels etc..

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


but functional or technical cookies are allowed nevertheless

“cookies”



17

where technically possible and feasible [...] consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet.



18

Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment



19

CNIL.
To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL | Q | TW

🏠 > Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

29 June 2020

In its decision of 19 June 2020, the Council of State (Conseil d'État) essentially validated the guidelines on cookies and tracking devices adopted by the CNIL on 4 July 2019. The purpose of these guidelines was to clarify the enhanced legal

GDPR. However, the Council of State overturned the provision of the guidelines prohibiting in a general and absolute manner the practice of "cookie walls", ruling that such a prohibition could not be included in an act of soft law. The CNIL takes note of this decision and will adjust its guidelines with future recommendations to comply with it accordingly.

20

CNIL.
To protect personal data, support innovation, preserve individual liberties

MY COMPLIANCE TOOLS | DATA PROTECTION | TOPICS | THE CNIL

> Cookies and other tracking devices: the Council of State issues its decision on the CNIL guidelines

The Council of State's position on cookie walls

However, in its decision of 19 June 2020, the Council of State suppressed a paragraph in which the CNIL considered that the Internet user should not suffer major inconvenience in the event of the absence or withdrawal of consent. The CNIL considered in particular that access to a website could never be subject to the acceptance of cookies ("cookie walls").

The CNIL had followed the doctrine of the European Data Protection Board (EDPB), which brings together all the European data protection authorities, which had considered that, in order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so-called cookie walls) (Guidelines on consent under GDPR of a Member State).

The Council of State considered that by deducting this general prohibition from the GDPR, the CNIL had gone beyond what is legally possible with guidelines, which are an instrument of "soft law".

The Commission takes note of the Council of State's decision and will comply strictly with it.

21

3aa) Making access to website content provided without direct monetary payment dependent on the consent of the end-user to the storage and reading of cookies for additional purposes would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. This would normally be the case for websites providing certain services, such as those provided by public authorities. Similarly, such imbalance could exist where the end-user has only few or no alternatives to the service, and thus has no real choice as to the usage of cookies for instance in case of service providers in a dominant position.

22

Article 8

Protection of end-users' terminal equipment information stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such equipment

1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:

(g1) it is necessary for a purpose other than that for which the information have been collected under this Regulation. Where it is not based on the end-user's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 11 the person using processing and storage capabilities or collecting information processed by or emitted by or stored in the end-users' terminal equipment shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the electronic communications data are initially collected, take into account, inter alia:

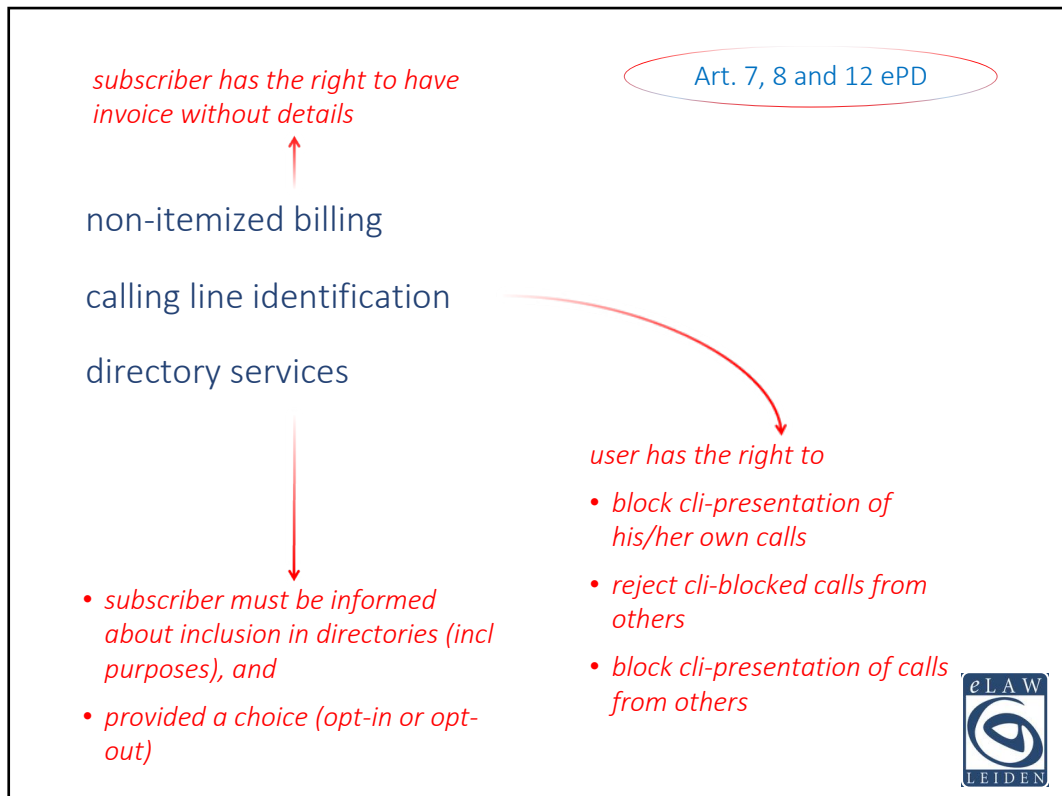


23

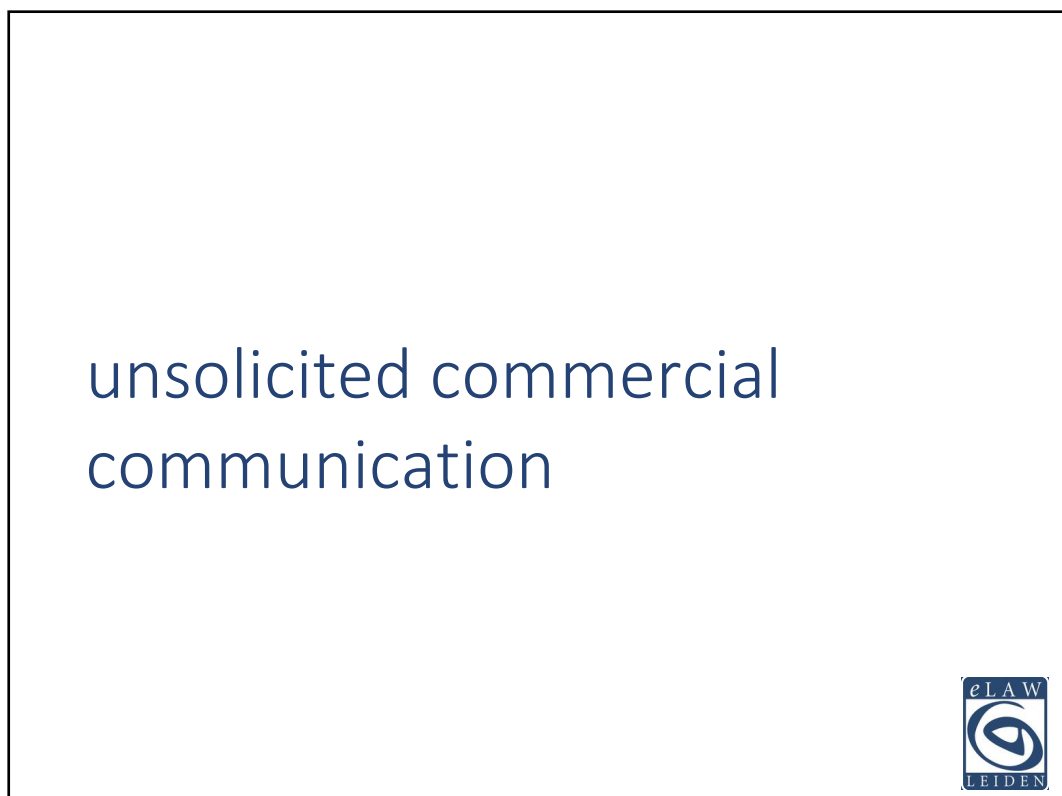
communication without
identification



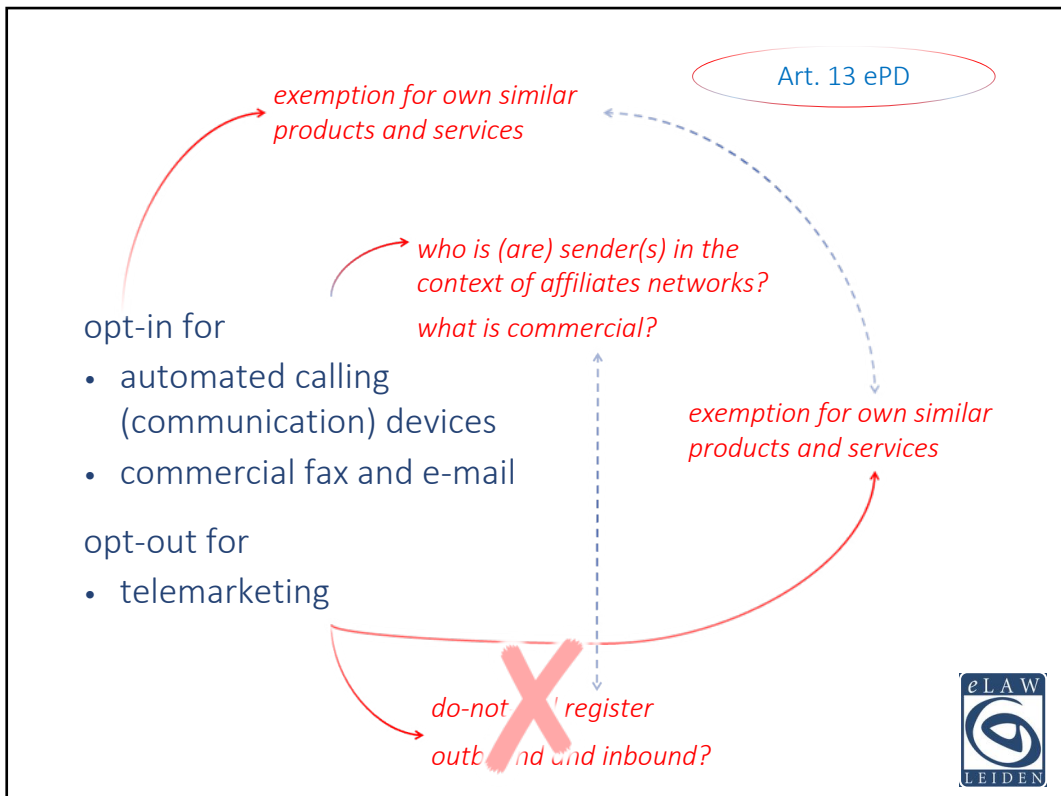
24



25




26



27

questions?

g.j.zwenne@law.leidenuniv.nl



28