Horizon 2020

Project title: Network Infrastructure as Commons

European Legal Framework for CNs

Deliverable number: D4.1

Version 1.0

Co-Funded by the Horizon 2020 programme of the European Union
Grant Number 688768

Project Acronym:	netCommons
Project Full Title:	Network Infrastructure as Commons.
Call:	H2020-ICT-2015
Topic:	ICT-10-2015
Type of Action:	RIA
Grant Number:	688768
Project URL:	http://netcommons.eu

Editor:	Melanie Dulong de Rosnay, CNRS Felix Tréguer, CNRS
Deliverable nature:	Report (R)
Dissemination level:	Public (PU)
Contractual Delivery Date:	December 31, 2016
Actual Delivery Date:	December 22, 2016
Number of pages:	76 excluding covers
Keywords:	Community Networks, Civil Liability, Privacy and Data Protection, Spectrum Regulation, OpenWi-Fi
Authors:	Melanie Dulong de Rosnay, CNRS Federica Giovanella, University of Trento Arthur Messaud, CNRS Felix Tréguer, CNRS
Peer review:	Roberto Caso, University of Trento Renato Lo Cigno, University of Trento Maria Michalis, University of Westminster

Executive Summary

This deliverable reviews selected relevant existing legislation and case law relevant to Community Networks. The aim is describing the current legal framework, the one in which European CNs have developed. The goal of the deliverable is to understand whether the existing laws allow the prosperity of the current CNs and of new ones, or they impair them. The report includes also some brief guidelines to cope with some hurdles that might arise from the application of civil liability laws and of personal data protection laws. This is the first version of the deliverable, which will be developed in an interactive and incremental manner with the CNs. In that sense, this report will inform WP1 forthcoming work on policy advocacy by CNs to express requirements for more appropriate legislations protecting their interest and not preventing their development.

After a first introductory part giving an overview of the legal questions that CNs face, the deliverable concentrates on three main issues: telecommunications policy, civil liability, privacy and personal data protection.

As for European telecommunications policy, the report describes in Section 2 the evolution of this policy in the last 30 years and then it illustrates what parts of EU telecommunication are applicable to CNs. Among the issues considered there are also three highly topical ones: spectrum regulation, the so-called “Radio Equipment Directive”, and net neutrality. The report explains in what terms these matters affect CNs and what measures should CNs adopt to respect the legislative framework. The deliverable also gives an account of the future developments in EU telecommunications policy with particular attention to the upcoming novelties that might be going to affect CNs.

The following Section 3 of the report focuses on civil liability issues; since there is not European legal framework for civil liability, the deliverable analysis the situation in some European countries. This part also includes a careful analysis of the Mc Fadden case delivered by the Court of Justice of the European Union on September 15, 2016, that has the potential to affect CNs and - more precisely – Wi-Fi networks.

The last of the issues, studied in Section 4, is the applicability of the European regulation for privacy and data protection to CNs. This section provides a detailed analysis of the regulation and explains what specific steps should CNs follow to deal with European directives and their national implementation.

Section 5 contains conclusions for each of the three main sections. The findings highlight how the architecture of CNs is one of the most important features to cope with legal obligations. Unfortunately, some regulation would require an increase in centralization, while some other would require more decentralization.

The deliverable will be circulated among CNs and CNs’ members to obtain feedback on the actual application of laws to their cases. The opinions, facts, visions and questions that CNs will pose will constitute the base on which the project will work to elaborate the next version of this deliverable (D4.2) due to at M24.

Contents

List of Acronyms

BEREC	Body of European Regulators for Electronic Communications
BGB	Bürgerliches Gesetzbuch (German Civil Code)
BGH	Bundesgerichthof (German Supreme Court)
CJEU	Court of Justice of the European Union
CN	Community Network
DPA	Data Protection Authority
DPO	Data Protection Officer
ECS	Electronic Communication Service
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
HADOPI	Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet (the French public authority monitoring copyright infringements on the Internet)
IAP	Internet Access Provider
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISP	Internet Service Provider
LAN	Local Area Network
NRA	National Registration Authority
OTT service	Over The Top service
TFEU	Treaty on the Functioning of the European Union
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

1 Introduction

This report provides an overview of the current legal framework for CNs. In particular, even though lawmakers have never adopted regulations specifically tailored on CNs, existing laws in different sectors do have an impact on CNs and on their chances of development.

It partially draws on the contents of D.1.2 entitled "Report on the Existing CNs and their Organization (v2)" mapping existing community networks. In addition, the deliverable is also based on the techno-legal findings of the FP7 CAPS project P2PValue (https://p2pvalue.eu/) on how "common based peer production" (CBPP) communities can be regulated.

This is the first version of the report. A second and a third version will be delivered at respectively M24 (D4.2) and M30 (D4.3). The present version introduces some initial hypothesis and some preliminary conclusions; the second version will describe the findings of the first two years of the project and will help in creating guidelines and codes of conducts for CNs, which will represent the third version of the deliverable.

Task 4.1 and its reports will be the bases for developing Task 1.3 on "Advocacy capacity-building"; mapping existing regulations and understanding how they can affect CNs is the starting point to elaborate suggestions for policy makers and to enhance advocacy capacity in CNs.

Task 4.1 is also linked to Task 4.3 "Best practices guide for CNs" that aims at drafting guidelines to allow the prosperity and diffusion of CNs; the guidelines, which will include also policy, socio-economic and technical recommendations, are meant as a way to strengthen existing CNs, to support them as commons, and to encourage the creation of new ones.

1.1 An overview of the problems

So far governments have never enacted norms specifically designed for CNs. Depending on their actual organization, CNs can be assimilated to small, non-commercial Internet Access Providers (IAPs) based on Local Area Networks (LANs) technology. While up to now national laws have not been an imperious obstacle to the creation or the activities of CNs, it can at times seriously hinder their development or create constraints that run counter to CNs' values and preferred organizational modes. As it will be discussed in further detail in the next pages, lawmakers have introduced regulations that although not thought for CNs might nonetheless have a negative impact on them.

If CNs are to grow and become sustainable alternatives to existing Internet service providers, regulators should fully take their existence into account and either take steps to encourage their growth or refrain from adopting laws that might interfere with it. The current situation, where CNs live in a legal limbo, drawing insights from contextually-related regulatory environments, already proves problematic for CNs sustainability as contingent to interpretations.

As far as the legal governance of CNs is concerned, one can distinguish internal self-regulation from external regulation. The former includes all the tools applied by CNs to govern relationships amongst its members as well as relationships between users and the network. The latter comprises the regulatory tools applied by governments that have an impact on CNs. Examples of the first category are contracts and social norms (to be further analysed in D1.2), while the second category is represented by laws implemented at local, national, and supranational levels.

As it emerges from D1.1 "Report on the Existing CNs and their Organization", CNs cannot be considered as a homogeneous category. On the contrary, while they present similar traits in their objectives, they also show significant differences in their features. Such differences need to be taken into account when studying the current legal framework for CNs, in order to understand the different effects that laws can have on different CNs depending on their status impacting their legal qualification. At the same time, these differences must be considered when framing possible policy actions and in drafting codes of conducts and guidelines. The diverse features of the CNs analysed in D1.1 are therefore taken into consideration in the next paragraphs, as laws can have a different impact on different CNs.

This deliverable develops an investigation of some specific legal issues involving CNs, namely:

a) telecommunications policy;

b) laws on privacy and personal data;

c) civil liability issues.

For each of these topics, our analysis starts from the European level, delving into details for some Member States' experiences and surveying some possible future developments.

In particular, the report discusses the European telecommunications policy (section 3) as the general framework in which any other legal questions – such as privacy and data protection (section 4) or civil liability (section. 5) – develops.

The report includes preliminary conclusions (par. 6) that take into account the next steps to be followed in the next year of the project in order to accomplish the task's objectives and provide input for task 1.2 on advocacy, titled "Improving governance: maximising the impact on CN".

1.2 Features of key European CNs

The deliverable focuses on four Community Networks, which structure and features – summarized below – involve different issues.

In Spain, **guifi.net** is a CN federating many smaller and local groups and which:

- Is run by participants who own parts of the infrastructure; can be freely joined by any volunteer or professional entities willing to participate and subscribing to the collectively drafted Network Commons License;

- Provides access to its local networks and to the Internet, but also in many cases to additional services such as Web proxies, chat, VoIP, videoconferencing, Web hosting, broadcast radio and email services;
- Collectively manages the network through transparent network and geographical maps of its nodes and a distributed network monitoring system allowing to visualize usage and identify problems or bottlenecks;
- Allows to fully automatize configuration of all nodes through collectively defined parameters;
- Is coordinated by the guifi.net Foundation which may legally represent the community, enforces the License, operates critical parts of the networks (like IP addresses and Internet transit) and owns a part of the infrastructure.

In France, **FFDN** is an umbrella organization for 28 CNs which:

- Are non-profit organizations and comply with the FFDN's Charter;
- Are registered as telecommunication operators before the French National Registration Authority (NRA);
- Usually own and manage their whole network infrastructure, collecting fees from their members and subscribers;
- Usually provide access to the Internet, sometimes only VPN services (to be used on top of a commercial subscription), and which may provide hosting services; can use mapping and network monitoring tools open to members, which may give details about subscribers' contact, billing and technical information.

In Italy, **Ninux** is a highly decentralized CN run by many independent groups and which:

- Is run by volunteers who own parts of the infrastructure; can be freely joined by any individual willing to participate and subscribing to the Ninux manifesto;
- Provides access to its networks and in some cases to the Internet, and other services such as hosting, chats or videoconferencing;
- Allows participants to freely choose the technical means through which they add a node to the network;
- Collectively manages a publicly accessible map of all the nodes and links of the network;
- Has no legal existence or representation but delegates some activities to some users, such as the management of the domain name "ninux.org" or connection to the NAMEX (neutral access point of Rome).

In Germany, **Freifunk** is a highly decentralized CN which:

- Is run by volunteers (or local not-for-profit organizations) who own parts of the infrastructure;
- May be freely joined by any individual willing to participate and subscribing to the Pico

Peering Agreement;

- Provides free and anonymous access to the Internet for all and other services such as chat, email servers and lists, radio, podcast, blogging or collaborative editing services;
- collectively takes important technical decisions during weekly and annual gatherings;
- Routes its traffic through VPN exits located in Leipzig, Dusseldorf, Sweden and Chicago;
- Publishes network maps and uses mapping tools;
- Has a reference authority, the *Förderverein Freie Netzwerke e.V.*, responsible mostly for fund raising, the operation of the main web site and other media platforms, organizing events and running advocacy campaigns;
- Has an advisory council for the community-overlapping decisions and conflicts between communities.

2 Telecommunications Policy

2.1 Telecommunications Policy in General

European Union's regulatory intervention in the field of **telecommunications** has been continuous in the last few decades. Telecommunications were one of the most important means through which it could have been (and was) possible to obtain the single market and to improve it; as a consequence, the European legislator repeatedly normed the sector (for a more detailed analysis cf. D 2.1 par. 2).

In the majority of cases, EU has introduced **Directives to harmonize Member States' regulatory approaches** on telecommunications. Opposite to European Regulations, Directives are not directly applicable in Member States; they rather need to be specifically implemented by each State that will choose the tool that best fits implementation's needs. This mechanism implies that, while the core principles must be the same in all Member States, the tools by which the principles are guaranteed can be highly diverse. This increases the differences among states' legal framework that would nonetheless exist due to national judges' interpretation.

2.1.1 The main phases of EU telecommunications policy

Three main moments characterize EU telecommunications policy (Walden, 144): the **first** moment is represented by the adoption of Directives and other regulatory tools **between 1987 and 1993**[1], with the aim of **liberalizing telecommunications**, that in many cases where still owned by States. Liberalization was however only superficial mainly due to political hurdles (Walden, 144) . Hence, a **second phase** followed[2], in which concrete **liberalization** was pursued and finally **reached** in **1998**. A **third** final **phase** realized starting from 2003, with the enter into force of **five Directives adopted in 2002**, namely:

1. the "**Framework Directive**": Directive 2002/21/EC of the European Parliament and of the

[1] Council Directive 90/387/EEC of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network provision, OJ L 192 , 24/07/1990 p. 1-9; Commission Directive 90/388/EEC of 28 June 1990 on competition in the markets for telecommunications services, OJ L 192 , 24/07/1990 p. 10-16.

[2] Council Resolution of 22 December 1994 on the principles and timetable for the liberalization of telecommunications infrastructures, OJ C 379 , 31/12/1994 p. 4-5; Commission Directive 96/19/EC of 13 March 1996 amending Directive 90/388/EEC with regard to the implementation of full competition in telecommunications markets, OJ L 74, 22.3.1996, p. 13–24; Directive 97/13/EC of the European Parliament and of the Council of 10 April 1997 on a common framework for general authorizations and individual licences in the field of telecommunications services, OJ L 117, 7.5.1997, p. 15–27; Directive 97/33/EC of the European Parliament and of the Council of 30 June 1997 on interconnection in Telecommunications with regard to ensuring universal service and interoperability through application of the principles of Open Network Provision (ONP), OJ L 199, 26.7.1997, p. 32–52; Directive 98/10/EC of the European Parliament and of the Council of 26 February 1998 on the application of open network provision (ONP) to voice telephony and on universal service for telecommunications in a competitive environment, OJ L 101, 1.4.1998, p. 24–47.

Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services[3];

2. the "**Authorization Directive**": Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services[4];
3. the "**Access and Interconnection Directive**": Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities[5];
4. the "**Universal Services and User's Rights Directive**": Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services[6];
5. the "**Directive on Privacy and Electronic Communications**": Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector[7].

These Directives constituted the "**New Regulatory Framework**", which was amended in 2009 by the **so called "Telecom Package"**, that included Regulation No 1211/2009 **establishing** the Body of European Regulators for Electronic Communications (**BEREC**)[8]. The BEREC was established to ensure that EU laws are applied consistently throughout the EU. The BEREC has mainly advisory functions (Walden, 177). In addition to the BEREC, other bodies are involved in the regulatory framework of telecommunications, including the "Radio Spectrum Committee"[9] composed of

[3] OJ L 108, 24.4.2002, p. 33–50.
[4] OJ L 108, 24.4.2002, p. 21–32.
[5] OJ L 108, 24.4.2002, p. 7–20.
[6] OJ L 108, 24.4.2002, p. 51–77. This Directive was amended by Regulation 2015/2120 of 25 November 2015, laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. Cf. par. 2.5.
[7] OJ L 201, 31.7.2002, p. 37–47.
[8] OJ L 337, 18.12.2009, p. 1–10. The package included also Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 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 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 (Text with EEA relevance), OJ L 337, 18.12.2009, p. 11–36; Directive 2009/140/EC Of The European Parliament And Of The CouncilOf 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (so called "Better regulation Directive").
[9] Art. 3, Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision), OJ L 108, 24.4.2002, p.

Member States representatives, as well as a "Radio Spectrum Policy Group"[10].

The trend to regulate any aspect of telecommunications with an all-encompassing approach is still ongoing as the **proposal for a "European Electronic Communications Code"** clearly demonstrates (see infra par. 2.6.1.).

2.1.2 Cornerstone definitions in the Telecom Package

Dir. 2002/21 introduced two cornerstone definitions:

- "**electronic communications network**" that "means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed" (art. 2, letter a);

- "**electronic communications service**" that "means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks" (art. 2, letter c).

The **Authorization Directive applies** to the authorization of **both categories**. **Electronic communications services** are qualified as being "**normally provided for remuneration**", as art. 57 Treaty on the Functioning of the European Union (TFEU) requires for an activity to be qualified as "service". However, private networks are intended to be included under the Directive, even though there is no mention of the requirement "normally provided for remuneration" (Flanagan, 305).

The Directive requires Member States to introduce a regime of "**general authorization**". The procedure to obtain the general authorization cannot be subject to explicit decision or other administrative act; more precisely: general authorization can only impose the conditions that were introduced at the European level, specifically in the Annexes of the Authorisation Directive. (art. 6).

2.1.3 Applicability of the cornerstone definitions to CNs

According to the above definitions, **CNs can possibly be considered both "electronic**

1–6.

[10] 2002/622/EC: Commission Decision of 26 July 2002 establishing a Radio Spectrum Policy Group (Text with EEA relevance), OJ L 198, 27.7.2002, p. 49–51.

communications networks" and "electronic communications services". Some of them can also be **"service providers"** under E-commerce Dir. 2000/31, while some others do not. For instance, guifi.net falls into this category, while Ninux does not, because there is no remuneration for the activities that the Italian CN carries out (for details on "service providers' liability", see par. 3.1).

E-commerce Dir. 2000/31 applies to **service providers** meant as any natural or legal person **providing an "information society service"** (article 2, letter b) that is defined as any service "within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC"[11] (article 2, letter a). Dir. 98/34 defined an information society service as a "**service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services**"[12].

To understand whether CNs can or cannot be traced back to this definition, it is necessary to consider the CJEU's case law. As recently explained also in the Mc Fadden decision (for details, see par. 3.2), the sentence "provided for remuneration" recalls the wording of Art. 60 of the Treaty on European Community (currently **art. 57 of the Treaty on The Functioning of The European Union** – TFUE)[13].

The interpretation given by the CJEU has clarified that "**remuneration**" can include **different types** of **revenue**; it does not need to be the price paid by the customer/final user, it can also be the profit coming from advertisement[14].

The **applicability** of the definition of "service providers" therefore **depends on the single CN** as well as on the **national implementation** of the E-Commerce Directive. CNs that offer only free services without any remuneration, do not fit this definition. From the perspective of EU law, this might be good or not, depending on national laws, as the Mc Fadden case demonstrates. In fact, if we considered CNs to fall into the category of service providers, they would enjoy liability

[11] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations (OJ L 204 , 21/07/1998 P. 0037-0048) as amended by Directive 98/48/EC of the European Parliament and 0f the Council of 20 July 1998 (OJ L 217 , 05/08/1998 P. 0018 – 0026).

[12] The same article specifies: "For the purposes of this definition: — 'at a distance' means that the service is provided without the parties being simultaneously present, — 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means, — 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request".
Dir. 98/34 was repealed in 2015 by Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, p. 1–15. Dir. 2012/1535 includes however an identical definition of "information society service".

[13] The criterion of "remuneration" is clearly linked to the fact that the activity is part of the internal market and therefore falls within the competences of the EU.

[14] C-352/85, *Bond van Adverteerders c. Paesi Bassi*, April 26 1988, par. 16.

limitations under Dir. 2000/31. On the contrary, if CNs do not qualify as service providers but as electronic communication services, they would not be shielded from liability with the consequence that, if a country places a duty to password-protect Wi-Fi or makes a person liable for third party conduct occurred through shared connections, then not only the single individual, but the entire CN can be in a difficult position. This again depends on the legal status of the CN and, crucially, on the law of individual member states. For instance, French law imposes a duty of care on private individuals to make sure their Wi-Fi connection is not used to infringe copyright (see infra par. 3.1).

2.2 Spectrum Regulation

An issue of utmost importance for wireless CNs is the one of "spectrum management".

Spectrum is in fact a scarce resource that has to be managed in order to allow the best and most efficient use of it[15]. Electromagnetic spectrum is a continuum of electromagnetic energy waves. The segment usable for carrying data (including sound) is only the one including the "radio", "micro" and "short" waves. This waves can be constitute the "radio spectrum". Competing uses can cause interference; hence spectrum is a scarce resource, and only a limited number of users can actually operate effectively within a "band" (Flanagan, 358).

International, regional and national policymakers have made agreements on how to coordinate and allocate bands of spectrum. At a national level, governments normally use a licensing mechanism.

2.2.1 Spectrum regulation at the international level

At an international level, a big role is played by the **International Telecommunication Union** (ITU), that decides the different attribution of radio frequencies in the three Regions in which the world is divided: Region 1 (comprises Europe, Africa, the Middle East west of the Persian Gulf including Iraq, the former Soviet Union and Mongolia), Region 2 (covers the Americas, Greenland and some of the eastern Pacific Islands); Region 3 (includes most of non-former-Soviet-Union Asia, east of and including Iran, and most of Oceania)[16]. EU represents the Member States at the international level (Caggiano, 222). EU policies are developed according to the ITU regulations.

2.2.2 Spectrum regulation at the European level

Given the increase in the use of spectrum, **European** policymakers have been discussing new strategies. The current instruments in this area are the **Radio Spectrum Decision No 676/2002/EC**[17], the **Radio Spectrum Policy Group Decision 2002/622/EC**[18] and **Decision**

[15] Recital n. 24 and art. 8bis of Dir. 2009/140.

[16] Cf. "List of ITU member countries by region": http://life.itu.int/radioclub/rr/itureg.htm.

[17] Decision No 676/2002/EC of the European Parliament and of the Council of 7 March 2002 on a regulatory framework for radio spectrum policy in the European Community (Radio Spectrum Decision), OJ L 108, 24.4.2002, p. 1–6.

[18] 2002/622/EC: Commission Decision of 26 July 2002 establishing a Radio Spectrum Policy Group (Text with EEA relevance), Official Journal L 198, 27/07/2002 P. 0049 – 0051.

243/2012/EU establishing a multiannual Radio Spectrum Policy Programme (RSPP)[19].

Currently, spectrum use is granted by **National Regulatory Authorities** (NRAs) that shall follow 2002 Authorisation Directive and provide spectrum under a "general authorisation" (art. 5). **NRAs can determine the necessary limitations to spectrum** use as well as the selection **criteria** on the basis of which **grant of rights to use spectrum** is awarded (Flanagan, 378). Member States may attach some conditions to the use of spectrum; these conditions are only those listed in Part B of the Annex to Authorisation Directive. Generally speaking, whenever the risk of harmful interference is negligible, Member States should not make the use of radio frequencies subject to the grant of individual rights of us, but should provide general authorizations (art. 5(1), Dir. 2002/20). This basically means that a service provider declaration of the date in which operations start shall be sufficient (Donati, 102).

The 2002 Radio Spectrum Decision established a framework in which EU and Member States could coordinate in the management of spectrum. The aim of the Decision was to "establish a policy and legal framework in the Community in order to ensure the coordination of policy approaches and, where appropriate, harmonised conditions with regard to the availability and efficient use of the radio spectrum necessary for the establishment and functioning of the internal market in Community policy areas such as electronic communications, transport and research and development" (art. 1).

Parallel to this, a Radio Spectrum Policy Group (RSPG) adopts opinions to assist and advise the Commission. The aim is to reach a management of the spectrum that takes into account not only technical issues, but also economic, political, cultural and social ones[20].

In **2012**, EU adopted the first "**Radio Spectrum Policy Programme**" (RSPP)[21] (Flanagan, 382-383). The RSPP identifies the **harmonization of national spectrum** policy as a priority also considering its impact on the internal market for wireless technologies and services, including the Digital Agenda for Europe.

2.2.3 Spectrum regulation and CNs

Spectrum regulation clearly **affects** the development of **CNs**, especially those based only on wireless connections. Some of the existing European CNs have reported that it can be really hard to preserve the quality of their networks, because **frequency bands are saturated** (De Filippi and Treguer, 8). While theoretically CNs could ask NRAs to obtain a portion of spectrum, they cannot afford the price to be paid if frequencies are assigned through market-based mechanisms.

Dir. 2002/21 requires Member States to allow companies to transfer rights to use radio frequencies

[19] Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme Text with EEA relevance, OJ L 81, 21.3.2012, p. 7–17.

[20] Cf. https://ec.europa.eu/digital-single-market/en/radio-spectrum-policy-group-rspg.

[21] Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme, OJ L 81, 21.3.2012, p. 7–17.

to other companies (art. 9(3)). However, **spectrum management at the EU level** is **based** on some **specified radio frequencies that are aimed to specific service categories**; this **impairs** the possibility to **allocate those frequencies differently** (Donati, 102).

2.3 Radio equipment directive

There are other regulatory hurdles that CNs have to face. Among them there is also the issue of recent modifications of the legislation on "radio equipment". More specifically, in **2014**, the European Union adopted a **Directive 2014/53** on **radio equipment**[22], that even though was not specifically heading for CNs, it actually might impair their development.

CNs do usually need to **replace** the **software** included by the manufacturer **in radio hardware**, **with open software** in order to allow the creation of the CN.

Art. 3 of the **Directive requires** the construction of **radio equipment to comply with special requirements**. This might **impair the possibility to modify the software** included in the hardware. In fact, it has been highlighted by **Free Software Foundation Europe (FSFE)** that this provision "implies that device manufacturers have to check every software which can be loaded on the device regarding its compliance with applicable radio regulations (e.g. signal frequency and strength). Until now, the responsibility for the compliance rested on the users if they modified something, no matter if hardware- or software-wise"[23].

Manufactures will be considered responsible for legal compliance with the Directive (and its implementation in each Member State), thus they might decide to **protect themselves by locking down the device** they produce and sell. This has already happened in the US, where similar laws were adopted. Such a possibility would **impair CNs development** by preventing them from replacing the software.

FSFE also warned on another strategy adopted by manufacturers. As a preventive measure they have already started to install modules on their devices to check what software is loaded. This is done by installing "built-in non-free and non-removable modules disrespecting users' rights and demands to use technology which they can control"[24]. Such an approach would de facto create a spying system checking on user's behaviours, locations, and data, with a clear infringement of user's fundamental rights.

2.4 National Legislation

As mentioned, each Member State shall implement European Directives through national tools.

[22] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance, OJ L 153, 22.5.2014, p. 62–106.

[23] https://fsfe.org/activities/radiodirective/.

[24] Cf. https://fsfe.org/activities/radiodirective/.

This section the Italian regulatory framework on telecommunications applying European Directives.

Italy was taken as a case study, both because of the existence on its territory of Ninux and because of the peculiarities of their legislation.

2.4.1 Italy

Italian law on telecommunication

Italian telecommunication laws are included in the so called "**Codice delle comunicazioni elettroniche**" (Electronic Communications Code), meaning: *decreto legislativo* (d.lgs) 1.8.2003, n. 259. The Code **implemented all the European directives** on the same subject.

Only some of the norms included in the Code are actually applicable to CNs. A first question to answer is whether, in the Italian context, CNs need to register in order to be legally run.

General authorization and need for registration

Art. 104 of the Code requires **telecommunications operators to obtain a "general authorization"** (autorizzazione generale) for some activities specifically listed, even when these activities are carried out "privately". There are however some **exceptions** applicable to networks and services for private use. More in general, private networks are subject to a different authorization regime than the general one (Boso Caretta, 67).

The general authorization regime is based on the notion of "electronic communications service" given by art. 2, letter c) of European Directive 2002/21, introduced verbatim by art. 1, lett. gg), d.lgs. 259/2003: "'electronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services".

This definition implies that an **authorization is mandatory only for those services that consist of the transmission of signals via electronic communications networks, by electromagnetic means.** Services that supply only content are exempted from this authorization (Boso Caretta, 68). This definition is affected by the definition of "services normally provided for remuneration" that has been recently considered also by the Court of Justice of the European Union (CJEU) in the Mc Fadden case analysed in par. 3.2.

No authorization is needed for only wireless CNs

An electronic communication service is considered to be private when it is deployed exclusively in the interest of the person who holds the general authorization. Art. 101, par. 1, adds that those holding a general authorization for a private network can use the network only to transmit data and make activities for his/her own use; there is an explicit prohibition to carry third parties' traffic. An interpretation based solely on the wording of this article would imply that CNs are not "private networks" and that they would therefore require a number of authorizations (Bonelli, 473ff).

However, **art. 99 of the *Codice delle comunicazioni elettroniche*** considers some **activities** that are considered **"in any case free"** and that are listed in art. 105. This article includes **also "radiolan and hiperlan local networks**" that comprise also **Wi-Fi networks** based on 2.4, 5.4-5.7 GHz frequency. In case a **CN is based solely on Wi-Fi connections**, as is the case of Italian CN **Ninux.org** (D.1.1 par. 5.2), **no prior authorization to build and run the network is needed**.

Authorization required for wired connections

While Wi-Fi networks can be included among free uses, **wired connections cannot**. To a wired network a **general authorization would be needed** (art. 104). The general authorization shall be **requested** by someone (either a natural or a juridical person) based on a **template** included in the Electronic Communications Code. The applicant must provide a statement in which it declares that it will comply with some specific rules, including norms related to environmental safety, to citizens' health, and urban planning. The Code does not require the subject applying for an authorization to be a "legal entity" (e.g., association, company etc.). However, it would probably be easier for a legal entity to organize the entire process to obtain an authorization. It would also be easier to guarantee the required safety measures.

The current legal scenario in Italy is the result of the implementation of European Directives package of 2009 through *decreto legislativo* 28.5.2012, n. 70. For the time being, CNs based on wireless technology do not require prior authorizations; until CNs – Ninux.org, in particular – will not change the technology on which they are based, the current legal framework allows them to be built and run with no additional requirements.

Italian spectrum regulation

As for spectrum regulation, Italy has a "**National Plan for Band Allocation**" (Piano Nazionale di Ripartizione delle Frequenze - PNRF), which is enacted by the Minister of Economic Development. The current PNRF was introduced in 2015[25]; it shall be revised within three years from the enactment, unless big changes are meanwhile introduced by the ITU.

The aim of the PNRF is to state at a national level the attribution of spectrum to different services. It also tries to verify the efficient use of the spectrum, with the goal of freeing resources for the television sector.

The plan is the **product of ITU Radio Regulations**, including the outcomes of the World Radiocommunication Conference (WRC) that modify and update the Regulations. Clearly, the Italian plan is **also the result of European Directives and Regulations**, as well as the measures adopted by the European Conference of Postal and Telecommunications Administrations (CEPT).

The current PNRF concerns **frequencies between 0 and 3000 GHz**.

[25] It was published in Italian *Gazzetta Ufficiale* on June 23, 2015. It can be found at: http://www.sviluppoeconomico.gov.it/images/stories/documenti/radio/PNRF_27_maggio_2015.pdf.

2.5 Net Neutrality

In the last few years, net neutrality issues have been at the centre of both research and telecommunication policy arenas (Belli, De Filippi). Net neutrality is basically conceived as a non-discriminatory treatment of the traffic in the provision of Internet access. Providers can be interested in specific traffic management as it can constitute a way to optimize the transmission quality of specific categories of traffic. However, in order not to hamper human rights – notably the right to freedom of expression – the possibility for providers to "unjustifiably" discriminate traffic should be banned.

The European Union adopted in 2015 Regulation n. 2120 that includes provision aimed at protecting net neutrality. The regulation states that traffic management measures should first of all be fair and transparent, not discriminatory nor disproportionate and should not be adopted on the mere base of commercial interests, but they could be a temporary measure adopted to overcome a technical problem[26].

The Regulation itself gives only three specific exceptions that can allow a provider to discriminate traffic: The first is compliance with Union law; the second is the need to preserve the integrity and the security of the network; the third and last one is to prevent congestion of the network (art. 3(3)).

Art. 2 of the Regulation clarifies that "providers of electronic communications to the public" are those "providing public communications networks or publicly available electronic communications services" and that "internet access service" is "a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used".

The definitions applied by this Regulation are those provided by art. 2 of the Framework Directive. The BEREC released specific guidelines that help to interpret the Regulation[27]. The BEREC clarified that "Electronic communication services or networks that are offered only to a *predetermined* group of end-users could be considered to be not publicly available"[28].

Whether a CN can or not be considered within the scope of the regulation depends on the characteristics of the CN itself. Some of them, as for instance the German network Freifunk or the French FFDN, might be considered as "publicly available electronic communications services". On the contrary, others like the Italian network Ninux offer their services – even Internet connection – only to a predetermined group of people; hence they cannot be considered as "publicly available"

[26] Recital 9 and art. 3, Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.

[27] BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules, BoR (16) 127, August 2016, available at: http://berec.europa.eu/eng/news_and_publications/whats_new/3958-berec-launches-net-neutrality-guidelines.

[28] BEREC Guidelines, cit., 5. Emphasis in original.

and are not subject to the net neutrality Regulation. To the same extent, they cannot be seen as "Internet access services" as this definition implies once again the concept of "public availability".

2.6 Future Developments

In light of the deep changes occurred since the last revision of the European policies on telecommunication of 2008, **on September 14, 2016 the European Commission** adopted set of initiatives and legislative **proposals** that will change the regulatory framework for electronic communications in the next few years[29].

Three main innovations can be identified: 1) a **new Directive** introducing a "**European Electronic Communications Code**"; 2) the **modification** of the Body of European Regulators of Electronic Communications (**BEREC**); 3) the promotion of **Internet in local communities**.

2.6.1 The upcoming "European Electronic Communications Code"

The proposal for a Directive establishing the "**European Electronic Communications Code**" will **merge four existing Directives** on telecommunications: Framework Directive (Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services), Authorisation Directive (Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services), Access Directive (Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities) and Universal Service Directive (Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services).

In its "press release"[30] the EU Commission explicitly stated that the **Code will encourage** "***alternative network operators*** *who focus on smaller geographical areas and contribute to bring high quality connectivity to citizens outside cities*". Such a statement **looks promising for CNs** that undoubtedly represent alternative operators that focus on smaller geographical areas.

2.6.2 The upcoming Regulation for the promotion of Internet connectivity in local communities

In addition to these innovations for "alternative networks", local communities' connectivity will be encouraged also by means of a new regulation. The proposal for a **Regulation** of the European Parliament and of the Council amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the **promotion of Internet connectivity in local communities** introduces specific tools

[29] https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code

[30] http://europa.eu/rapid/press-release_MEMO-16-3009_en.htm?locale=en

through which it will be possible for a local administrator to obtain **funding** and **grants** to develop local networks. Grants will be provided to local administrations to purchase equipment to run Wi-Fi networks and to **cover installation costs** with the aim to **provide very high-speed Internet connections**. As the proposal itself clarifies, such connections are highly encouraged especially in centres of local public life, such as libraries or hospitals.

2.6.3 Other upcoming EU regulatory tools in the field of telecommunication

Among the upcoming novelties there is another **Regulation** that will **modify** the status, tasks, and power of the **Body of European Regulators of Electronic Communications** (BEREC). The BEREC given more power, including powers to adopt binding decisions. The Directive proposal for a European Electronic Communications Code entrusts BEREC with new tasks, which will allow a **better implementation of the regulatory** framework (Regulation proposal, 2).

2.6.4 The upcoming European Electronic Communications Code will affect spectrum regulation

The same **Code** will also affect **spectrum regulation**. This is a shared competence between the EU Commission and the Member States. The new rules will allow a **better coordination** of these two layers of regulation, due to the important cross-border implication of this issue.

One of the issues that EU regulation on spectrum has always faced is that of interferences amongst different operators. This has led to the attribution of frequencies exclusively or at least mainly to specific communication services. However, **current technologies would allow flexibility of usage for the same frequencies also by different services** (Donati, 223). Hence, the EU should allow this possibility provided there is no harmful interference, leaving national regulators to work out how this can be achieved.

2.7 Conclusions

Europe should take more seriously the public interests, including the need to connect rural, remote and underdeveloped areas[31], as well as guarantee free development and innovative services.

The applicability of the current regulatory framework for electronic communication depends both on the national implementation of the European Directives, and on the features of the single CN.

The upcoming regulatory novelties might bring with them good news for CNs. Attention is paid to local connectivity: enhancing Internet connectivity also through funds and grants might be an opportunity for those CNs that are already devoted to bringing Internet connection where unavailable (as guifi.net, for instance).

Modification in spectrum regulation might be an opportunity for CNs to expand their wireless links, provided that a better coordination between the different regulatory layers will be ensured.

[31] Cf. European Parliament Resolution Towards a European policy on the radio spectrum (2006/2212(INI)), par. 33.

3 Civil Liability Issues

What is meant for "civil liability"?

"**Civil liability**" can be defined as the **liability arising from private wrongs or breach of contractual duty** and that is **not criminal** liability; in general, civil liability implies a duty to **compensate for damages**. Civil liability can for example arise when someone causes damages to someone as a consequence of a privacy breach or defamation, or in cases of intellectual property rights' damages. These are classical cases arising from the use of the Internet. The diffusion and use of CNs might entail similar cases.

Possible scenarios in case of wrongdoing

In particular, **different scenarios** can be imagined.

A **first case** is the one of the **final user**, that could be held **liable for his/her own actions**, **and** – in case s/he is the owner of a gateway node – also **for other users' conduct**.

A **second possibility**, which still related to the existence of **gateway nodes**, is that an **Internet Service Provider is liable** for actions occurring within the network.

Third, the option that the **CN itself could be responsible** for its members' illicit actions should be considered (Giovanella, 52-63).

Civil liability rules and their application are normally Member States' competence; only rarely has the EU enacted laws in the realm of civil liability. For this reason, after a first paragraph on the implication of European law for CNs' civil liability cases, national scenarios will be considered.

Civil liability and CNs peculiarities

However, the **peculiarities of CNs** as **for civil liability classical rules** should be stressed. Normally, the **first step would be to identify and sue the person** that committed the wrongful action; however, very **often** it is **impossible** to determine who the individual responsible is. Such impossibility is linked mainly to **two reasons**. The first is related to the **structure** of **CNs**: the **illicit action might be allocated to a high number of different users'** machines, which makes legally and technically problematic to define who contributed to the violation of a right (Dulong de Rosnay, 2015). The second one is the additional presence of **software** through which users **shield their identity and obtain anonymity**.

Another issue concerns the **possibility to hold the CN liable**. In case a CN has a **legal status** – such as in the case of guifi.net or FFDN (D.1.2 entitled "Report on the Existing CNs and their Organization (v2)", table 4.1), rules that concern each specific legal entity would be applicable. Usually, **the person(s) in charge of the entity** – being it an association or a foundation, where there is an entity (unlike to Ninux or Freifung) – **would be considered liable** for the wrongdoing arising from the use of the network. In any case, once again, national laws would apply.

3.1 European Legal Framework

Internet Access Providers' liability and wrongdoing committed through a gateway node

The European Union has only seldom enacted legislation on civil liability. In the context of telecommunications and civil harms, a remarkable example of attempting harmonization is the adoption of **Directive 2000/31 on "Electronic Commerce"**[32]. More in particular, **articles 12 to 15** regulate **Internet Service Providers' liability**.

Providers' liability shall be considered as it is possible for CNs to be opened to the Internet by means of a gateway. What if a **wrongful action** took place **through the gateway**? Could a provider be considered liable for the wrongful action of a user? Although national transposition of Directive 2000/31 will be applicable, it is still relevant to consider what the Directive provides.

Providers can be held liable only if they do not comply with specific behaviours requested of them by the law. Behaviours are different according to the different roles of the providers, that can qualify as mere conduit, caching or hosting providers (articles 12, 13 and 14).

Caching and hosting providers' liability in case of wrongdoing coming from the CNs

Caching and **hosting** providers' activity as described in Directive 2000/31 involves storage of information provided by a recipient of the service. Even though the way in which they store information differs greatly – as caching providers usually store data only for a limited time, while hosting ones could store it potentially forever – they can **be held liable if they do not remove the stored information when required**. Such obligation to remove the content is applicable to **any kind of data**, **regardless of the source** from which it comes. This means that, **in the case of CNs**, it does not matter whether the data to be removed come from within a CN or not: caching and hosting providers are subject to the same obligations regardless whether the information to be removed comes from the user owning the node or from any other user within or outside a CN.

Access providers' liability for wrongdoing coming from the CNs

Access providers are instead those providers that transmit information provided by a recipient of the service or provide access to a communication network. These providers normally sign a **binding contract with their customers**, in which **often** a **clause expressly forbids** the customer to share the connection. Another frequent **clause** is the one that considers the **customer liable for the damages** suffered by the provider as a consequence of a conduct that is prohibited by the contract itself.

Therefore, for the **mere fact that the customer shares his/her connection s/he will be liable for**

[32] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market), OJ L 178 , 17/07/2000 P. 0001 – 0016.

breaching the contract and – in case of damages caused by a third party's wrongdoing – s/he could also be **asked to compensate the victim** (Kern; Hale; Mac Síthigh; Robert et al.; Giovanella).

Request to ISP for customers' data in order to sue them directly

Another option would be one in which **the victim asks the intermediary to provide its customer's data, in order to sue** her/him to obtain compensation for the damages suffered. In fact, the **gateway node** could be **identified by means of its IP address**, that could, in turn, be matched to the name of the provider's customer. While this could be a way to enforce victims' rights, such as copyright or data protection, the discovery of customer's data by the provider is not certain. P**revious cases involving the enforcement of IP rights** demonstrated that this **situation is a difficult one** and that national courts have been struggling to understand whether they should order providers to reveal customers' data or not. This issue gave rise to the famous CJEU's case *Promusicae v. Telefonica*[33], in which the Court stated that Member State shall ensure proportionality when implementing European law so that a fair balance is struck between the fundamental rights at stake (in the specific case: copyright vs. right to personal data protection). The Court did not, therefore, clearly state whether national law should or should not allow providers to be ordered to disclose their clients' personal data, if requested in case of an alleged infringement.

In a subsequent case on the same subject matter – *Bonnier Audio AB et al. vs. Perfect Communication Sweden AB*[34] – the CJEU more precisely stated that Member States can introduce laws that allow an ISP in civil proceedings to be ordered to disclose its customers' information related to an IP address in case of an alleged infringement.

The possibility to **hold** the **gateway node liable** for third party's conduct is a **matter of national law**. However, the so called "Mc Fadden case" decided in September 2016 by the Court of Justice of the EU might set the stage for the creation of a new third party liability hypothesis.

3.2 The Mc Fadden Case by the Court of Justice of the EU

Facts of the case

On September 15, 2016, the **Court of Justice of the European Union** (CJEU) adopted a decision in a case that could potentially affect any CN in Europe[35].

The request for a preliminary ruling was made by the Munich Regional Court in Germany in a **process** pending **between Tobias Mc Fadden and Sony Music Entertainment Germany GmbH**.

Tobias **Mc Fadden** owns a shop where he sells and leases lighting and sound systems. Within his shop, Mr Mc Fadden **runs a wireless local area network (WLAN)** free of charge; **access** to the

[33] C-275/06, January 29, 2008.
[34] C-461/10, April 19, 2012.
[35] C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH.*

network was intentionally **open to anyone** and not protected by a password, to allow customers to use it and to draw passers-by's attention.

In September **2010**, **by means of this WLAN a musical work was made available to the public on the internet free of charge**, without the consent of the right holders. **Sony Music**, which is the producer and the right holder of that work, sent a fo**rmal notice to Mr Mc Fadden to obtain protection of its rights** on the musical work. As a response, **Mr Mc Fadden** brought an **action** to obtain a **negative declaration** (so called "negative Feststellungsklage") before the Munich Regional Court.

Sony counterclaimed **asking** for **damages compensation** on the ground of direct liability for copyright infringement. The company **also asked an injunction**, that is an order from the judge to stop Mc Fadden's allegedly infringing activities.

In January 2014, the Munich court dismissed Mr Mc Fadden's action and upheld Sony's counterclaims. Tobias **Mc Fadden** appealed the decision, arguing that he is **exempted** from liability thanks to article **12.1 of Directive 2000/31**. As seen, Directive 2000/31 introduced internet service providers' liability exemptions; in particular, article 12 deals with mere-conduit (or access) providers. More precisely, he held he is exempted by the German implementation of the Directive, namely: arts. 7 to 10 of the German Tele-Media Act (*Telemediengesetz*).

The German Doctrine of "Störerhaftung"

Consequently, **Sony claimed** that in the event that the Munich Court would not find **Mr Mc Fadden** directly liable, it should apply the so called "**Störerhaftung**" – literally: **liability of the interferer – for not having secured his wireless network**, so allowing third parties to infringe Sony's copyright.

Paragraph 97 of the German Law on Copyright (Gesetz über Urheberrecht und verwandte Schutzrechte – Urheberrechtsgesetz)[36] introduces the right for the **copyright holder to ask** for an **injunction** and for **damages** compensation in case of copyright infringement. This paragraph has been interpreted as **applicable to both direct** (Täterhaftung) **and indirect infringements** (Störerhaftung). In the latter case, a person that contributed to the infringement committed by another person, either voluntary or with a sufficient degree of causation, can be considered a *Störer*, meaning: an indirect infringer (cf. par 5.2, German legislation)[37].

The case might affect CNs' development. In fact, many CNs offer free, open Wi-Fi, exactly as Mr Mc Fadden does. At the same time, there might be the possibility to qualify CNs as Internet Service Providers: in this case, they might also be the target of the above mentioned injunctions. More in particular, the referring court asked what measures should a provider adopt in order to avoid liability (see paragraphs 3.2.3 and 3.2.4).

[36] Law of 9 September 1965 (BGBl. I, p. 1273), as amended by the Law of 1 October 2013 (BGBl. I, p. 3728).

[37] Cf. Opinion of the Advocate General Szpunar in the case C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, par. 15-16.

The questions referred to the Court of Justice of the EU

The Munich court considered plausible that the violation of Sony's rights was not committed by Mr Mc Fadden, but by another party. At the same time, the **German court** was also inclined to consider Tobias Mc Fadden liable under the Störerhaftung doctrine. However, the Court **was not sure whether the exemption provided by article 12, Directive 2000/31 was or not applicable to Mr Mc Fadden**; as if it was, he could not be considered liable at all.

In such a situation, the German court **referred the case to the CJEU** asking for the interpretation of some European Directives and asked ten different questions. For the scope and purpose of this research, the questions can be essentially reduced to two main ones:

1) Can a free WLAN operator be qualified as "provider of information society services" and therefore enjoy the liability exemptions introduced by article 12, Directive 2000/31?

2) What measures should a provider adopt to avoid liability for third party's intellectual property rights infringement through Wi-Fi networks?

3.2.1 The definition of "provider of information society services"

The first step to be done to answer this question is to interpret the definition of **"information society service" included in Directive 98/34 and recalled by Directive 2000/31**. An "information society service" is meant as any service normally provided for remuneration, by electronic means and at the individual request of a recipient of services (article 1(2) Directive 98/34). Hence, services have to be considered as "**services normally provided for remuneration**" exactly in the same vein as in article 57 TFUE.

"**Normally provide for remuneration**" does not necessarily imply that the remuneration is paid by customers or clients; it is enough if the service is supported **by advertisements or other services** sold by the same provider.

As a consequence, also Mr Mc Fadden's service can be categorized as an "information society service" for the scope and the applicability of the liability exemptions provided by article 12, Directive 2000/31.

In case a Member State, while implementing the Directive, did not include the distinction between commercial/non-commercial/free of remuneration services, this interpretation would not apply (Husovec, 3).

3.2.2 What measures should a service Wi-Fi provider apply to avoid liability for third party infringement?

The most innovative part of the **decision** and the one that is **likely to affect Wi-Fi networks and**, in turn, **CNs** development, is the one where the CJEU illustrated what measures should a provider adopt in order to avoid third party copyright infringement and subsequent indirect **liability**.

To answer this question, another one shall be made first: **is a provider enjoying liability exemptions of article 12 shielded only from damages or is s/he also shielded from injunctions?**

Directive 2000/31 must be read in conjunction with Directives 2001/29[38] and 2004/48[39] – which regulate copyright in the information society and intellectual property rights enforcement. These Directives do not preclude a court to impose on a provider, which is exempted from liability under article 12, Directive 2000/31, to be the target of an injunction. In other words, a provider can at the same time be shielded from liability but be the subject of an injunction.

The Munich court explained that it had already be ascertained that only three alternative measures could be adopted in the specific case:

1. To terminate the account
2. To password-protect the access to the network
3. To examine all communications passing through the network.

Monitoring, termination, and password protection as possible measures and how they clash with fundamental rights

The CJEU stressed the **importance of the different rights at stake** that are all contemplated by the **Charter of Fundamental Rights of the European Union**. First, copyright deserves protection, as article 17.2 of the Charter; at the same time, however, it is necessary to consider access provider's freedom to conduct a business (article 16 of the Charter), that could be compromised by the injunction requested, as well as users' freedom of information protected by article 11 of the Charter.

The Court of Justice only analysed the three measures that according to the referring court can be adopted in the case at stake:

1. The **examination of all communications passing through the network**. The CJUE easily stated that **such a measure would be in contrast with article 15 of Directive 2000/31**, that excludes the imposition on service providers of a general obligation to monitor;
2. The **termination of the account**: this solution would cause **serious infringement to the freedom to conduct a business**, although in the case at issue providing an internet connection is only a secondary activity for Mr Mc Fadden; hence it would not allow to strike a fair balance amongst the various rights;
3. The **password protection of the Internet connection**: according to the CJEU such measure could **strike a fair balance**. In fact, it would **affect** both freedom to conduct a business and users' freedom of information but **only marginally**. In particular, the Court held that this measure would not affect strongly the freedom of information of the recipient, as such

[38] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19

[39] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ L 157, 30.4.2004, p. 45–86.

connection would be only one of the many ways to access the Internet. There could be two ways to interpret the position on the password. First: password protection is acceptable because it satisfies the balance of rights; second: password protection is acceptable if and when it satisfied the balance of rights. On both cases it is arguable that password protection can effectively strike a fair balance between the rights at stake.

Need to identify users

The CJEU clarified that in any case when a provider adopts an injunction, it must ensure that the measure prevents unauthorized access to the copyrighted material, or at least it makes infringement very discouraging for Internet users.

The Court of Justice therefore held that **password protecting** a connection **can be a deterrent to copyright infringing activities**, as long as **users are required to identify** themselves to obtain the password **and do not act anonymously**.

3.2.1 The possible implication of the Mc Fadden case for CNs meant as providers

Applicability of Directive 2000/31 limitations to CNs: what elements distinguish a commercial activity from an ancillary one in absence of a remuneration?

The first question concerned the **applicability to Mr Mc Fadden's WLAN of the liability exemptions** provided by article 12 of Directive 2000/31.

Both the Court and the Advocate General Szpunar[40] **considered the provision to be applicable**. Even though Mr Mc Fadden did not gain any profits from the offer of Wi-Fi connection as it was made for free, such offer was part of his main economic activity (a shop). The network could be a way to advertise his business and to attract customers. As it **was strictly related to** Mr Mc Fadden's **main economic activity**, it has been considered as an information society service, even in spite of the fact that it was only an ancillary activity. As a part of the main activity, the Wi-Fi offer was considered as "**made for remuneration**" in spite of the lack of a direct remuneration from clients or users.

The **implication of this interpretation depends on the implementation of the Directive made by each Member State**. In fact, the decision seems to imply that unless there is remuneration, CNs would be outside the applicability of the E-Commerce Directive. Only in the case that a CN offered other services, being paid in a way or another by users, it could be considered as a service provider and enjoy the corresponding limitations on liability for third party's conduct. However, if a Member State, in implementing the Directive, did not include the distinction between commercial/non-commercial/free of remuneration services, this interpretation does not apply[41].

[40] Opinion of the Advocate General Szpunar in the case C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, par. 34-56.
[41] Cf. Husovec, 2016, 3.

Still, **if one of the gateway nodes is run by a shop owner or by a company, the person owning the node would probably enjoy the limitations provided by Directive 2000/31**. In fact, in such instances, providing an Internet connection would be an ancillary activity to the main economic one, exactly as in the case of Mr Mc Fadden.

Interestingly enough, while the case was pending before the Court of Justice the German legislator amended the law on media and communications and extended the liability exemptions for access providers to providers that offer Wi-Fi connection[42].

Risks and downsides of injunctions requiring to apply password-protection

The Court of Justice found that the **measure of password-protecting** the connection allows to reach a **fair balance** amongst the different rights at stake: it would not restrict too much the freedom to conduct a business nor the freedom of information. The Court also clarified that such a measure would be **properly applied if users were required to identify themselves** in order to obtain the password.

Advocate General Szpunar had however reached a **different solution**[43]. The Advocate considered the **obligation to make Wi-Fi secure** to **hamper the business model** of those offering Internet connection as an additional service to the main ones. As **securing the network** might be **costly**, some people running these businesses might decide not to make such investments. The other side of the coin is that **consumers might stop using the connection** offered by a shop or a restaurant because the use of the Wi-Fi would need identification and entering a password. The Advocate makes the clear example of fast-foods[44].

In addition, only if users' personal data is stored together with the IP numbers and the external ports through which the users have established the connection, it would be possible to trace back the infringement to a that specific user. Therefore, imposing to put a password on the network **entails also the retention of users' data.**

Usually these obligations are imposed only on commercial ISPs. To **impose** the same **obligations** on **people offering connection as an ancillary activity** would be – in the words of Advocate Szpunar – **disproportionate**. More generally, the Advocate made clear that imposing to password protect free Wi-Fi would mean a **disadvantage for the entire society**, as such technology offers great potential for innovation[45].

---

[42] Zweites Gesetz zur Änderung des Telemediengesetzes, 21 July 2016, Bundesgesetzblatt, I. 2016 Nr. 36. The amendment added a new paragraph into Section 8 of the Telemedia Act.

[43] Opinion of the Advocate General Szpunar in the case C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, par. 134-150.

[44] Opinion of the Advocate General Szpunar in the case C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, par. 138-139. Indeed, it is well-known that many people spend time in fast-foods in order to use their free Wi-Fi connections.

[45] Opinion of the Advocate General Szpunar in the case C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, par. 148-149.

Password-protection does not strike a fair balance between rights in case of CNs

In **CNs password-protecting** the Internet connection might **not strike a fair balance** between the rights at stake: unlike Mr Mc Fadden's WLAN case, in CNs the home access to the Internet is mostly achieved through the connection offered by the CNs.

Furthermore, it depends also on the way in which the password protection is implemented: in some instances, no effort and no control from the provider is required: the end user can enter any information without verification; in some other instances, verification and data retention (as suggested by the CJEU) would be required. In this latter case, **password protection** would mean a huge **burden imposed on the CNs**.

The applicability of the decision will depend on the scope of national definitions of intermediaries and economic operators

The consequences of the decision on CNs might be strong or not also depending on the national legal framework.

The decision concerns injunctions introduced by article 8.3 of Directive 2001/29 and article 11 of Directive 2004/48 that are addressed only to "intermediaries". Given that no definition for "intermediary" exists in the mentioned directives, the interpretation made by the CJEU shall be considered. The Court has always dealt with "intermediaries" that were economic operators, such as access providers[46]. In a recent decision (so called "Tommy Hilfiger case") the Court stated that "[f]or an economic operator to fall within the classification of 'intermediary' within the meaning of those provisions, it must be established that it provides a service capable of being used by one or more other persons in order to infringe one or more intellectual property rights, but it is not necessary that it maintains a specific relationship with that or those persons"[47].

To be classified as **intermediary under arts. 8.3, Directive 2001/29 and 11, Directive 2004/48** a provider "must be established that it provides a **service capable of being used by one or more other persons in order to infringe one or more intellectual property rights**, but it is not necessary that it maintains a specific relationship with that or those persons"[48]. Furthermore, there is no need that the intermediary proposed services other than the one used by the third party to infringe property rights: it is enough that the provider offers services capable of being used by a third party to commit the wrongdoing[49].

---

[46] C-577/07, February 19, 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH*, par. 43-46.

[47] C-494/15, July 7, 2016, *Tommy Hilfiger Licensing LLC at al. v. Delta Center a.s.*, par. 23, recalling C-314/12, 27 March 27, 2014, *UPC Telekabel Wien GmbH v. Constantin Film Verleinh GmbH and Wega Filmproduktionsgesellschaft mbH*, par. 33-36.

[48] C-314/12, March 27, 2014, *Telekabel Wien GmbH v. Constantin Film Verleih GmbH e Wega Filmproduktionsgesellschaft mbH*, pars, paragraphs 32 and 35; see also C-494/15, July 7, 2016, *Tommy Hilfiger Licensing LLC, at al. v. Delta Center a.s.*, par. 23.

[49] *Tommy Hilfiger Licensing LLC, at al. v. Delta Center a.s.*, par. 24-25.

Following the interpretation of the CJEU, the Mc Fadden judgement applies certainly to those who provide an Internet connection as a main activity, as well as to those providing it as an ancillary activity to their main economic one (exactly as Mr Mc Fadden).

Would it **for a CN** – or for a gateway node – be **better to qualify as a provider**, and to **enjoy liability exemptions but** also to undergo its counterparts, including **possible injunction**?

The **qualification of CNs as intermediary is uncertain** due to different factors: first, due to the non-profit but at the same time non-ancillary nature of their activity; second, due to the architectural settings of mesh networks, that make each individual node an intermediary in the technical sense, but not in the economic sense.

Directive 2000/31 was conceived as to be applicable to businesses rather than private individuals. Would it anyway apply to CNs? This **depends on national law**.

Interpretation according to German, French and Italian laws

When a CNs' gateway node is run by an economic operator and is open to the public, this node could be ordered to password protect its Wi-Fi connection. In such cases, the owner of the node will undergo both a positive and a negative effect descending from the Mc Fadden decision: the positive effect is the liability exemption under article 12, Directive 2000/31; the negative one is that the owner could be the target of an injunction.

If the **node owner is a private individual**, it is not clear whether injunctions ordering to password-protect a connection could or not be granted against a private person. Given that the CJEU's judgement does not clarify this issue, **national legislation has to be considered**.

Obviously, each Member State implemented EU Directives, however the way in which the implementation was made can vary. It must be clarified whether the notion "intermediary" has been construed to encompass also private persons. If this was the case, then private individuals could be subject to injunctions to stop third party's infringement.

As for **Germany**, considering the case law above briefly recalled, there should be **no doubts on the applicability of injunctions also on private people**. This interpretation has been applied by German courts for many years, taking the infringer of physical property as an analogy.

Similar conclusions can be reach for the **French system**: the **gateway cannot enjoy liability exemptions**, as it is run by a **private** person. **However**, the owner could be the **target of injunctions**. This would mean that there would be two negative effects on the same subject: not enjoy liability exemptions plus be the target of injunctions.

In the **Italian** context, someone can be held liable for a third party conduct only when a specific provision exists. Currently **no provision considers a single private individual liable for the wrongdoing of another** made through the connection. In addition, a single individual **cannot be**

the target of the injunctions introduced with the implementation of EU Directives[50]. CNs and their gateway nodes are in a better position if they do not qualify as intermediaries in the meaning of the Mc Fadden decision.

A possible solution for CNs that want to promote open Wi-Fi, and an option to circumvent the inconvenience of the effect of "Mc Fadden injunction imposing passwords", could be to create a separate additional entity (association) subscribing to a CN ISP and sharing Wi-Fi. If they would receive an injunction, the operation could be transferred to a new legal entity (which wouldn't be subject to the password restriction).

The **Mc Fadden judgement could undermine CNs development**: if the gateway node user has to bear the damages caused by someone else and/or the costs and burden of an injunction, this could be a strong deterrent for the opening of the network to the Internet.

ISPs have been chosen as accountable entities also due to their "deep-pockets": CNs have neither the structure nor the economic capacity to face burdensome injunctions. The way European telecommunications policy has been built is indeed based only on commercial entities (cf. D 2.1, par. 2), including the entire system of providers' liability.

3.2.2 The impact of the Mc Fadden decision on the structural design of CNs

Could CNs – in case they run open Wi-Fi nodes – modify some of their features in order to avoid the negative consequences of the Mc Fadden judgment? In other words, can the decision affect the shaping and the sustainability of ecology of CNs as alternative, peer to peer, commons-based solution to provide a service? Which dimensions are likely to be affected? Should CNs take pre-emptive measures to avoid negative consequences, or would a modification of the design be so disruptive that it would signify the end of open CNs?

This analysis is based on a previous categorisation of peer production platforms according to their level of (de)centralisation applied to five dimensions (Dulong de Rosnay, Musiani, 194-196):

1. ownership of means of production;
2. technical architectural design;
3. socio-economic organization and governance of work patterns;
4. rights and responsibility of the peer-produced resource;
5. value of the output.

Some of these features might be affected by the Mc Fadden's decision or might affect the way the Mc Fadden's decision is applicable to CNs.

The **ownership of the means of production** can be understood as the **existence of a legal person**

[50] Article 156 and 163, L. 22 April 1941, n. 633 on copyright.

with a status. The **absence** of a legal representative poses **additional constraints** to the difficulties which had been identified by the Advocate General.

The **economic structure of the arrangement to benefit** from Wi-Fi can be variable and it is a matter of importance since the existence of a payment is mentioned in the decision **as a criterion to know whether the E-Commerce directive applies**. Policies will oscillate from the absence of a fee to subscriptions at different levels for different categories of members, also depending of their involvement in the CN. It would be difficult to assess whether voluntary in-kind contribution (as manager of a node, as rooftop care-taker, as community officer reaching out to new audiences, as drafter of user documentation) would be assimilated to a professional role.

The **governance decisions** on possible changes to bring to selected features of a CN can be taken by a board, by nodes, or in the case of a decentralised organisation, be impossible as they should be implemented by all nodes which will not necessarily agree and cannot technically be forced to.

They include possible modifications to the other dimensions of the CN: the fee policy, the legal structuration, the technical design, or Terms of Use, when they exist, and whether CN could or should amend their promises or exclusion of service.

Would **liability disclaimers** for possible wrongdoings by users **be sufficient** to relieve the other members from liability? Or, to draw a parallel with hotels, we wonder whether asking users to not commit copyright infringement, or other private wrongs, before they sign up would be considered a sufficient measure.

Finally, the most crucial aspect of the decision likely **to affect CNs** is the reflection on the **implementation of the three measures identified**: password instead of keeping the network open, registration of user information, and data retention obligation.

CNs will have to **evaluate the cost of implementing such measures,** in case one of them become compulsory to avoid liability. They **may be too expensive or too difficult** to implement, and compliance **may signify the death of the CNs**, if too many individual nodes choose to close, jeopardising the technical viability of the local network.

One possible **recommendation would be to make or to maintain a network as distributed as possible**, and even more than they currently are. Indeed, previous research on some CNs demonstrate that they might not be as decentralized as they would like to be (Maccari; Crabu, Giovanella, Maccari, Magaudda). In some cases, many nodes are actually owned by a single person, who is also the one that manages and keeps the network running. These are called "**critical nodes**" and **reflect a more general trend on the re-centralisation of the web**. If a node opened to the Internet is also a critical node for the functioning of the entire CN, the imposition of an injunction or the request for damages to the owner might hamper not only the functioning of the node, but the functioning of the entire CN.

This means that not only should the technical structure of the CN be highly distributed, but also the

ownership of the nodes should be distributed, in order to also distribute the governance and the risks.

3.3 National Legislation

3.3.1 France

In **France**, **Internet access subscribers** shall **ensure** that their **access is not used for the unlawful reproduction, publication or communication of copyrighted works**[51]. Specifically, such an obligation means that **subscribers shall ensure that their Wi-Fi connection is secured** by means of passwords in order to prevent potential infringers to access Internet through it.

If a subscriber **fails to secure** its connection, **he/she cannot be held liable** for third party's infringement. However, the **HADOPI** (the public authority monitoring copyright infringements on the Internet) **may send him/her an email ordering him/her to do so**[52]. If, during the **following six months, the subscriber is found not to have secured its connection yet**, the HADOPI may send him/her a **formal letter ordering to do so, again**. Finally, since 2010, if the subscriber is found, again, not to have comply with this obligation during the following year, **judges may fine him/her up to 1 500 €, or up to 7 500 € in case the subscriber is a legal person**[53].

As of October 2016, 1 200 cases have been brought before judges on this basis. Among these cases, the HADOPI only revealed that **68 people have been convicted**[54].

As regards CNs' activities, such an obligation may be an issue where CN's individual participants intend to offer access to the network through their personal connection to the Internet subscribed from an Internet access provider (which may be the CN or another provider).

3.3.2 Germany

Germany represents an interesting case, as it is one of the few European countries where **private individuals have been held liable for third party's wrongful actions made through an unsecured Wi-Fi**. In fact, as seen, Germany is the country where the relevant Mc Fadden case originated.

Even though no specific provision exists that introduces liability for third party's conduct for the case of unsecured Wi-Fi, the *Bundesgerichthof* (BGH – the German Supreme Court) has applied analogically § 1004 of the German Civil Code (BGB) that offers injunctive relief against infringement of property to cases of infringement of intellectual property rights (Busch, 3; Hören,

[51] *Code de la propriété intellectuelle*, article L336-3
[52] *Code de la propriété intellectuelle*, article L331-25
[53] *Code de la propriété intellectuelle*, article R335-5
[54] NextInpact, *Hadopi : 34 classements sans suite et 78 rappels à la loi connus*, 10 October 2016; http://www.nextinpact.com/news/101695-hadopi-34-classements-sans-suite-et-78-rappels-a-loi-connus.htm

Yankova, 504; 510). This is the so called **doctrine of "Störerhaftung"**, meaning "liability of the interferer" (Hören, Yankova, 511-518; Kur, 532).

This liability is a form of strict liability, but **limited to injunctions**, that is: limited to measures that aim at stopping the infringing activity or at preventing it for the future (Kur, 533). These injunctions can be granted only when **three conditions are satisfied**: 1. there shall be an **adequate causal contribution** to the activity of the infringing party; 2. there must have been a **legal and factual possibility to avoid the third party's infringement**; and 3. the subject must **have violated a reasonable duty of care or a duty to monitor aimed at preventing infringements** (Busch, 3).

Clearly, as in any other Member State, as a consequence of the implementation of Directive 2000/31, **intermediaries** do enjoy the **limitation liability** above briefly described, which are laid down in **arts. 7 to 10 of the German Tele-Media Act** (*Telemediengesetz*) (Hören, Yankova, 501).

As mentioned, the BGH has held individuals liable for unsecured Wi-Fi, both in private networks and in commercial networks.

In the **case** "**Sommer unseres Lebens**"[55] the **BGH** considered a **private owner of an unprotected Wi-Fi network to be liable** for copyright infringement committed by an unidentified person. The owner of the network should have protected it with safety measures to prevent the misuse of third parties. The suitability of the measures should be assessed considering the technical standards applicable when the modem was installed. The fact that the owner had not replaced the password set by the producer of the router was enough for the Court to hold the owner liable for the violation of a specific duty of care (Busch, 4). In addition, **once the owner has secured the Wi-Fi, there is no duty to update the safeguards to the latest standards** (Hören, Yankova, 516). Other courts took a different approach and held that the password set by the producer was a sufficient protection[56]. In the case "Sommer unseres Lebens" the BGH did not even consider the application of the liability exemption introduced by Directive 2000/31. Similar reasoning has been applied by the BGH also in cases where the owner of a Wi-Fi network had provided access to members of her family, who misused the network and infringed copyright (Busch, 5; Hören, Yankova, 516-517).

A partially different approach is adopted with regard to **commercially used open wireless networks**. In particular, differences exist between the case of networks accessible only by users known by name (as in hotels) and networks accessible by unknown users.

For instance, the Court of Frankfurt am Mein held that a **hotel owner** is not responsible for **copyright infringement committed by an unidentified individual**, when the **network** was

[55] Bundesgerichthof, Judgment of 12.05.2010, Sommer unseres Lebens.

[56] Landgericht Frankfurt am Main, Judgment of 14 June 2013, MMR 2013, 605; Amtsgericht Hamburg, Judgment of 9 January 2015, BeckRS 2015, 08939 , as reported in Busch, 2015, 5.

protected with industry standard encryption technology[57]. In a case involving an owner of a holiday apartment, the same court considered the owner not liable as he proved that he had instructed his guests not to use the Wi-Fi network for illicit actions[58].

In another case, the district court of Hamburg applied the liability limitation of the Tele Media Act to the wireless network operated by the owner of a hotel[59].

Hence, basically, **when a provider of a commercial network can know the users** by name, password protection **or instructions to users** are **enough** to shield her from liability (Busch, 6).

In cases where users are unknown, Courts have adopted fluctuating decisions. In a lawsuit involving an **Internet café**, the **Regional Court of Hamburg** held that the owner was **liable** since he had **not blocked the ports** that were used by unknown clients to share copyrighted files[60].

Very interesting for this project is a case decided in 2014 by the district court of Berlin-Charlottenburg and **involving Freifunk**, the main German CN. The Court ruled out the liability of the operator of the Freifunk Wi-Fi hotspot under the doctrine of Störerhaftung. It means that the Freifunk Wi-Fi hotpot operator could not be held liable for third party illicit actions. Interestingly, the Court discussed whether the network operator had violated a duty of care and it stressed the importance not to impair the business of "free radio". More precisely, the Court stated that **imposing the owner to block certain ports or DNS or to instruct all the users would place on the owner an excessive burden**. The Court also stressed the importance of "free radio" operators and the need to protect them, avoiding the dangers coming from the imposition a duty to register user or to block certain ports or domain main servers[61].

The **German** scenario will be at least partially influenced by the Mc Fadden decision. However, it is fascinating to note that while the case was pending before the Court of Justice the German legislator **amended** the **Tele Media Act and extended the liability exemptions for access providers to providers that offer Wi-Fi connection**[62].

3.3.3 Italy

The analysis to be conducted shall include the three scenarios above listed: user's liability; CN's liability; ISP's liability.

Starting with **user's liability**, the applicable rules are those for **general liability in tort** (article

[57] Landgericht Frankfurt am Main, Judgment of 18 August 2010, MMR 2011, 401.
[58] Landgericht Frankfurt am Main, Judgment of 28 June 2013, GRUR-RR 2013, 507.
[59] Amtsgericht Hamburg, Judgment of 10 June 2014, CR 2014, 536.
[60] Landgericht Hamburg, Decision of 25 November 2010, MMR 2011, 475.
[61] Amtsgericht Charlottenburg, Judgment of 17 December 2014, CR 2015, 192 as reported by Busch, 2015, 7.
[62] Zweites Gesetz zur Änderung des Telemediengesetzes, 21 July 2016, Bundesgesetzblatt, I. 2016 Nr. 36. The amendment added a new paragraph into Section 8 of the Telemedia Act.

2043 Italian Civil Code). However, as already stressed, when the user that allegedly committed the wrongdoing cannot be identified, no possibility is left for enforcing the violated rights.

A different situation would occur in case the wrongdoing was perpetrated through the **gateway**, as the gateway user could be identifiable by means of his/her IP address. However, in the Italian legal system **someone can be held liable for a third party conduct only if a specific provision exists**. This is for instance the case of providers' liability regulated by *decreto legislativo* 9 April 2003, n. 70, implementing Directive 2000/31.

Currently, no general rule considers a person liable for a third party action. In addition, contrary to what happens on other countries, **Italy does not punish "open Wi-Fi"**. Quite the opposite, in the last few years the policy towards Wi-Fi and users' identification have gone from a rigid to a softer approach.

In 2005, as a response to the terrorist attacks occurred in other countries in the previous years, the Government introduced the requirement of users' identification for any Internet point, being it wired or wireless[63]. The validity of these provisions, meant as being temporary, was extended many times, until the end of 2011. As it was not further extended, obligations to identify users do not exist anymore.

In addition, in 2013, the Government enacted another decree that clearly stated that Internet access through Wi-Fi does not require user's identification[64]. Furthermore, **when providing Internet connection is not the main activity of the person who offers it, the general authorization normally required by the Codice delle Comunicazioni Elettroniche does not apply**.

Considering that CNs do not run Wi-Fi Internet connection as their main activity, they do not need to identify people, nor to obtain a general authorization. Furthermore, a user that shares his/her connection is not liable for third party conducts. Clearly, in case the contract signed with the provider prohibits connection sharing, the user will be held liable for breach of contract. But currently this is the only existing cause of action.

As for the liability of the provider, European rules would apply. Decreto legislativo 70/2003 implemented Directive 2000/31 almost verbatim. The current interpretation of the issue by Italian courts on the liability of access providers does not differ from the European one. In addition, the Mc Fadden case decided by the CJEU will allow a coherent interpretation of article 12 of the Directive (and article 14 of the transposing decree).

Finally, the **liability of the CN** shall be considered. To held the CN liable for a wrongdoing happening within it **there should first of all be a way to consider the CN as a single entity**. This

[63] The so called "Pisani Decree": decreto legge 27 July 2005, n. 144; converted, with amendments, in legge 31 July 2005, n. 155. See also the Ministerial Decree 16 August 2005, n. 1902.

[64] Article 10, decreto legge 21 June 2013, n. 69 converted, with amendments, in legge 9 August 2013, n. 98, so called "Decreto del fare".

could be the case for a CN run and managed by an association or a foundation. In such a case, the association could be liable for the wrongdoings that can be traced back to the network.

In case there is no entity "behind" the CN, there is **no way to sue the network**. The only remaining option is to **sue all the people** that were involved in the wrongdoing for concurring in producing the same damage. However, it might be **impossible** to find which nodes participated in the wrongdoing and, besides that, it might also be very hard to identify the real person behind each node (Giovanella, 54-55; 61-63).

3.3.4 Conclusions

The current legal framework is different in different Member States:

- French HADOPI law introduced an obligation to monitor one's own Wi-Fi connection in order to avoid copyright infringement;
- German case law applied existing rules analogically, in order to hold a private person liable for third-party copyright infringement occurred through their unsecured Wi-Fi connection;
- Italy does not currently have any specific provision that introduced this liability, not has the case law applied existing rules analogically. Therefore, while the Italian system currently seems the most favourable in terms of open Wi-Fi and liability, it remains to be seen what are the consequences of the Mc Fadden case in each of the considered countries.

3.4 Brief guidelines to cope with liability issues

As a general recommendation for any CN under the point of view of **liability**, the **network should be as distributed as possible**.

In fact, when a node is a critical one (meaning: a node to which a very high number of nodes are linked) the possible liability actions against this node's owner might greatly affect the entire network. This is **especially true** in those countries (as **Germany** and **France**) where private people **can be held liable for not securing their Wi-Fi** and so allowing someone else to infringe copyright. In addition, when a network is distributed, it becomes difficult to find the person liable for a wrongdoing.

When there exists an **entity governing** the network, the entity **should ensure that each user is aware of the possible implications in terms of liability**. Entities – such as associations or foundations – might be held liable according to the national rules that regulate the activity of this entity. For instance, very often the president of an association is the person accountable for the wrongdoings of an association.

A possible way to alleviate the negative effects of an unknown person onto the association or foundation would be to purchase **insurance**.

When there is an entity, the use of licenses might be a way both to inform users and to limit the

CNs' liability: exactly as commercial providers do, **CNs can impose specific obligations on their users, interrupt service** and/or **ask for damages** when users do not comply with these obligations. This is for instance one of the clauses included in the FONN Licence adopted by Guifi.net.

Depending on the scope of national definitions of intermediaries and economic operators, some **CNs might also qualify as Internet Access Providers** under Directive 2000/31 (cf. par. 3.2.3). In these cases, they enjoy the **liability exemptions** introduced by Directive 2000/31, but at the same time they might be the target of **injunctions**. In case the injunction was to password-protect the network, this could badly hamper the functioning of the network.

For those CNs that are not formally ISPs, the idea of transforming themselves into providers might be considered. Besides the fees to be paid, the regulative framework seems to be better defined. On the one hand this might bring some limitations in terms of bureaucracy or fees to be paid, on the other hand the responsibility of the entity would be clearer. In fact, ISPs enjoy the liability limitations introduced by Directive 2000/3; although access providers might be the target of injunctions (such as password-protection), the framework of providers' liability has been built also by an increasing number of judgements that have clarified the role of providers and its boundaries.

4 Data Protection and Privacy

Community networks (CNs) process different types of data in different ways. Their core activity is to provide access to their network and to transmit communications over it. Such an activity may require them to store some data, as imposed by law. Then, CNs may also provide other services, such as email or hosting services.

Each of these activities raises privacy-related issues. Some of these issues are associated to all of these activities (part 4.1) while others are specific to each of them (part 4.2). In both cases, CNs may consider dealing with these issues through collective adjustments, especially as regards decentralized networks (part 4.3).

In principle, CNs are subject to data protection law for any of their activities involving the processing of their users' data. Data protection (whose framework is described in part 4.1.1) imposes general (part 4.1.2) and specific (part 4.1.3) obligations on CNs. Compliance with such obligations is subject to supervision and can entail penalties (part 4.1.4).

4.1 Legal framework

4.1.1 Applicable law: the GDPR

Data protection law has been strongly harmonized throughout the whole European Union (EU) since the late 90s, thanks to the 1995 European Directive on data protection, which has been transposed into national law by all EU Member States. This Directive will be repealed and replaced by the new **General Data Protection Regulation** (GDPR - Regulation (EU) 2016/679) from **25 may 2018** onward. The GDPR will be directly applicable in all Member State and, as such, will also replace most of national data protection law.

The GDPR provides merely a few major improvements in comparison with the 1995 Directive as well as numerous clarifications and harmonisations. Accordingly, and for the sake of simplification, privacy-related issues regarding CNs will mainly be discussed here in the light of the GDPR (and comments on the currently applicable law will be made where necessary).

4.1.2 Definitions: the key terms of data protection

Personal data are any information relating to an individual and which may be attributed to this individual.

Anonymous data are any information relating to an individual but which may not be attributed to this individual. Such data are not protected by law.

> *Since the distinction between personal and anonymous data determines the scope of the protected data, it is the subject of a complex and ongoing debate. A simple example may help to*

> *clarify this distinction.*
>
> *A file lists the dates of birth of all the inhabitants of a city, without associating these dates with any more information. Such dates cannot be attributed to any individual inhabitant: they are anonymous data. However, if this file associates the dates with the residents' address, these dates and addresses would likely be personal data. Indeed, it would be easy to find who they are relating to since two people born the same day rarely live at the same address.*
>
> *Broadly speaking, the likeliness that a set of seemingly anonymous data actually contains personal data increases with the number and precision of the gathered data.*
>
> *As regard CNs' activities, network addresses, content and meta-data of communications absolutely qualify as personal data if they can be associated with other information in order to be attributed to someone. As such, except where specific measures are taken to keep data anonymous, it is advised to consider that any data relating to the users or participants of CNs' services are personal data.*

Data subjects are the individuals whose personal data are processed. As regards CNs' activities, the data subjects are the users of their services and, in some cases, the participants of CNs.

Processing relates to any operation performed on data, whether or not by automated means, such as the collection, storage, use, modification, transmission, disclosure or destruction of data. Almost all of CNs' activities imply the processing of some data.

A **controller** is a person who decides to process personal data, according to the **purpose** and **means** it chooses. A controller may process data on its own or ask another person (called a **processor**) to process them on its behalf. CNs and/or their participants are controllers in most of their activities but might be mere processors in some cases, as discussed later.

4.2 Main obligation: lawfulness of the processing through legitimate interest, consent or contract

The first and most important obligation imposed on controllers is to ensure the lawfulness of their processing.

Processing is lawful where:

- It pursues a **lawful purpose**; and
- It is **strictly limited** to this purpose (no personal data are processed except for this purpose).

A purpose may be lawful in three cases.

Firstly, a purpose is lawful if it pursues a **legitimate interest**. Here, an interest means any interest of the controller, a third party or the public at large. Such interest is said to be legitimate if it is **not overridden by the own interests of the data subjects**.

Thus, the lawfulness of such a purpose depends on the **balance between these different interests**. It is up to the controller to assess this balance and to take the risk of pursuing this purpose. Unfortunately, national Data Protection Authorities (DPAs) and the Court of Justice of the EU (CJEU) have yet to provide clear and general criteria for balancing the different interests at stake.

Secondly, a purpose is also lawful where data subjects **consent** to it, whether this purpose pursues a legitimate interest or not. As such, obtaining consent from data subjects may be a convenient way to avoid the risk of relying on a legitimate interest.

In order to be valid, consent must be:

- **Explicit** (given by a statement or by a clear affirmative action);
- **Informed** (the controller should have provided data subjects with complete information, as described below);
- **Freely given** (the controller does not make the consent a condition to the provision of a service, except if such consent is necessary for such provision); and
- **Specific** to the purpose of the processing.

Data subjects may withdraw their consent at any time.

Thirdly, **five purposes** are **systematically lawful**:

- Performance of a contract with the data subject;
- Implementation of pre-contractual measures requested by the data subject;
- Compliance with a legal obligation;
- Performance of a task carried out in the public interest;
- Protection of the vital interests of any person.

> *The lawfulness of the processing carried out by CNs will be discussed with each of their specific activities. However, a general recommendation can be made already. Considering that the lawfulness of processing based on legitimate interest can never be certain,* **it is advised to rely on** *another legal basis (such as* **consent or contract***)* **wherever practicable**. *Furthermore, systematically relying on consent or contracts would ensure the empowerment of users - in compliance with the political principles defended by most CNs.*

4.3 Specific obligations

4.3.1 Security measures: preventing accidental and unlawful processing

Controllers and processors shall implement appropriate **technical and organisational measures** to ensure an appropriate level of security -- that personal data are not **accidentally or unlawfully lost, altered, disclosed or accessed**.

This appropriate level of security depends on:

- The nature, scope, context and purposes of processing;
- The likelihood of a security breach and its consequences for data subjects;
- The state of the art and the costs of implementing security measures;
- The GDPR provides two broad examples of measures that may be appropriate:
- Encryption; and
- Pseudonymisation, ensuring that the processed data can only be attributed to a specific individual with the use of additional data which are kept separately.

CNs shall comply with this obligation for all of their activities (the appropriate measures to be implemented may vary depending on each of these activities).

4.3.2 Security breach: informing authorities and users

If personal data are accidentally or unlawfully lost, altered, disclosed or accessed in a manner likely to result in a **risk for the data subjects**, the controller shall **notify the security breach** to the competent Data Protection Authority (DPA) **within 72 hours** (or later if it can explain why this deadline could not be met).

This notification shall describe:

- The nature and likely consequences of the breach;
- The nature and approximate number of personal data and data subjects concerned (where applicable);
- The measures taken (such as the encryption or pseudonymisation of the data) or proposed to be taken (such as changing accounts' passwords) to address the breach or to mitigate its effects;
- A contact point where more information can be obtained.

If the breach is likely to result in a **high risk for the data subjects**, the controller shall **provide data subjects with the same information** and without undue delay (or as soon as the DPA requires so). This information shall be provided individually or, where this would involve disproportionate effort, through a public communication.

CNs shall comply with this obligation for all of their activities. Thus, they are advised to implement appropriate and cross-activities procedures in order to promptly react to any security breach. For instance, CNs may set a dedicated communication tool that its participants may use to notify breaches to the community and inform users.

> *Until the GDPR enters into force on 25 may 2018, the scope of this obligation still varies from State to State. According to the Directive 2002/58 (ePrivacy Directive), it is currently imposed on all electronic communications service providers throughout the whole EU. However, some national laws impose it on other kinds of controllers. Thus, CNs may fall within this scope depending on their activities and applicable law. Fortunately, the GDPR will harmonize the complex current situation by extending this obligation to every controller.*

4.3.3 Relationship with data subjects

The data subjects of the processing carried out by CNs are their users and, in some cases, their participants. These data subjects must have access to complete information about the processing and be able to exercise their rights.

Information: letting users know how their data are processed.

The controller shall provide data subjects with the following information:

- The **identity and contact details** of the controller;
- The **purposes** of the processing;
- The **legal basis** of the processing (the specific legitimate interest pursued, data subject's consent or another basis);
- The **recipients** (or categories of recipients) of the personal data, if any;
- The **period** for which the data will be stored (or criteria used to determine that period);
- The **data subjects' rights** and their right to withdraw their consent (if any) and to lodge a complaint with a DPA;
- Whether personal data are being **transferred outside the EU** (as described below).

Where personal data are **directly collected from the data subjects** (such as in most of CNs' activities), this information shall be provided at the same time of this collection.

Where personal data are **collected from another source**, this information shall be provided:

- Within a reasonable period (at the latest within one month); or
- At the time of the first communication to that data subject (if the data are to be used for such communication); or
- At the time of the first disclosure of the personal data to another recipient (if such a disclosure is envisaged).

In these three cases, the controller shall also inform the data subjects of the nature and the source of these data.

4.3.4 Rights: empowering users

Data subjects have four main rights:

- **Right of access** to the information already provided by the controller (as described above) and to obtain a copy of their personal data;
- **Right to data portability** - to request the transfer of their personal data to another controller where the processing of these data are carried out by automated means and are based on their consent or on a contract (this right typically involves the transfer of an email or social network account);
- **Right to rectification** of inaccurate personal data;
- **Right to erasure** of their personal data which are no longer (or have never been) processed lawfully (as, for instance, where their processing is no longer necessary or where consent has been withdrawn) and to **oppose** to such processing.

The controller shall charge **no fees** for the exercise of these rights. It may only facilitate it. However, it does not have to take any action where it cannot identify the data subject making a request (but may request additional information to confirm his/her identity).

The controller shall inform the data subject of the action taken at his/her request without undue delay (at the latest within a period of **one month**, extended by two months where necessary and where the data subject has been promptly informed of such an extension of the delay). If the controller does not take action, it shall inform the data subject without delay (at the latest within one month) of the reasons for his absence of action and of his/her right to lodge a complaint with a DPA and to seek a judicial remedy.

For any of their activities, CNs are advised to set up appropriate procedures to comply with data subjects' requests.

4.3.5 Paperwork

The controller shall maintain a record of its processing, containing the following information:

- The **identity and contact details** of the controller;
- The **purposes** of the processing;
- The categories of **personal data and data subjects**;
- The envisaged **time limits for erasure** of the different categories of data;
- The categories of **recipients** of the personal data;
- A general description of the **security measures** implemented.

Processors shall maintain a record too, providing:

- The identity and contact details of both the processor and the controller;
- The categories of personal data;
- A general description of the security measures implemented.

Controllers and processors do not have to maintain such records regarding "occasional" processing (as this notion is yet to be clarified, it is advised to consider that none of the CNs' activities imply "occasional" processing).

> *Until the GDPR enters into force on 25 may 2018 and according to the law of each Member State, controllers shall notify such records to their DPA prior to the processing of personal data. This notification obligation may vary depending on the applicable national law. Under the GDPR, these records shall only be made available to DPAs on request – and do not have to be notified any more.*

4.3.6 Data protection officer: an internal supervision

In some cases, controllers and processors shall appoint an independent Data Protection Officer (DPO) who monitors compliance with the law and advises its employer (once a DPO has been appointed, his/her contact details shall be published and communicated to the DPA).

A DPO shall notably be appointed where the "core activities" of a controller/processor consist of processing operations which require "regular and systematic monitoring" of data subjects on a large scale. The meaning of "monitoring" remains unclear, but some of the CNs' activities may imply such kind of processing (as, for instance, the management of their network in some specific cases). However, the "core activities" of CNs is the transmission of communications, which does not require "regular and systematic monitoring" of data subjects. Accordingly, **it seems that CNs do not have to appoint a DPO**.

> *This obligation will enter into force with the GDPR on 25 May 2018.*

4.3.7 Impact assessment: assessing dangerous processing

The controller shall carry out an impact assessment of any envisaged processing which is likely to result in a **high risk to the rights and freedoms of natural persons**. The controller shall then consult its DPA where such assessment reveals a risk.

DPAs may publish lists of the types of processing requiring or not an impact assessment, but the GDPR already specifies that particular attention should be paid to the use of "new technologies". As some CNs' infrastructure may be uncommon, they might be considered using "new technologies" or technologies resulting in some specific risks for data subjects. Accordingly, CNs may consult their DPA in order to clarify this point.

> *This obligation will enter into force with the GDPR on 25 may 2018.*

4.3.8 Transfers of personal data outside the EU: to safe countries, through appropriate contracts or with users' consent

CNs may transfer some personal data outside the territory of the European Union. Typically, Freifunk routes a part of its traffic to a VPN exit located in the USA. Since it is more difficult to enforce European law outside of the borders of the EU Member States, the GDPR limits the lawfulness of such transfers to four cases.

Firstly, personal data can be transferred to **any country** the European Commission has found to **ensure an adequate level of data protection**. Currently, nine territories benefit from such an **adequacy decision**:

- Argentina;
- Canada;
- Switzerland;
- Israel;
- Uruguay;
- New-Zealand;
- Andorra;
- Faroe Islands;
- The British Crown dependencies (the Isle of Man and the Bailiwicks of Jersey and Guernsey).

Once the UK will have left the EU, it will probably be added to this list, since its data protection law is already similar to the EU law.

> *Even if CNs may transfer data to such countries, these transfers remain usual processing which shall have their own a legal basis. For instance, a controller cannot transfer personal data to Argentina if this transfer does not pursue a legitimate interest, is not necessary for the execution of a contract with the data subject and/or has not been accepted by the data subject. Thus, it is advised that CNs* **obtain the consent of their users for transfers to such countries** *in any case, in order to comply with their political values.*

Furthermore, the European Commission has recently decided that any company located in the **United States** and subscribing to the "**EU-U.S. Privacy Shield**" is subject to specific obligations ensuring an **adequate level of data protection**[65]. The Privacy Shield is a framework providing for a set of obligations and review mechanisms intending to ensure a higher level of data protection than the one ensured by US law. Any company may freely subscribe to it and, then, import personal data from the EU. However, the actual level of protection provided by this framework is widely criticized since it allows USA's intelligence services to access these imported data with few safeguards as regards data protection. Complaints have already been lodged before the General Court of the EU, stating that the adequacy decision of the European Commission fails to comply with the EU Charter of Fundamental Rights. Thus, it is highly recommended that CNs intending to transfer data to the USA **refrain from relying on the Privacy Shield** until EU judges have expressed their definitive decision.

[65] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield;

Secondly, personal data can be transferred outside the EU if they are transferred with **appropriate safeguards**. Typically, this is the case where the controller/processor exporting the data and the controller/processor importing them have entered into a contract which:

- Ensures the protection of the transferred data and the enforceability of data subjects' rights; and
- Has been **validated by a Data Protection Authority** or contains **standard data protection clauses**[66] adopted by the European Commission.

> *CNs may rely on such contracts. For instance, Freifunk may enter with the person running its VPN exit in the USA into one of the model contract provided by the European Commission. However, CNs may want to* **let their users decide** *whether their data can be transfer to the USA and* **refrain from relying on another legal basis than their consent**.

Thirdly, personal data can be transferred where **users have consented to it**. If CNs choose to rely on users' consent, they **shall not deny access** to their services to users not consenting to such transfers (unless these transfers are effectively necessary for the provision of these services).

> *Even if CNs rely on consent (which is advised), they can also implement the appropriate safeguards described above in order to ensure the highest protection of the personal data of their users.*

Fourthly, personal data may be transferred where it is necessary for:

- The performance of a contract between the data subject and the controller;
- The implementation of pre-contractual measures taken at the data subject's request;
- The conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
- Important reasons of public interest;
- The establishment, exercise or defence of legal claims; or
- The protection of the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Or where the transfer:

- Is made from a public register; or
- Is not repetitive, concerns only a limited number of data subjects and is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject.

> *As of today, none of these cases seem to apply to CNs activities.*

[66] The European Commission has issued model contracts for the transfer of personal data to third countries, accessible here: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

Finally, in any case, before transferring any data, CNs shall **specifically inform users**:

- About the intended transfers;
- About the importing country;
- Whether this country benefits from an adequacy decision;
- Whether the transfers are made within appropriate safeguards (a contract approved by a Data Protection Authority or containing standard clauses).

4.4 Supervision and liability

Data protection authorities

Each Member State provides for one or more independent public Data Protection Authorities (DPAs) to monitor the application of data protection law[67].

CNs should consult the authority responsible for such monitoring in their respective State or area for any inquiry concerning their obligations.

Liability: fines up to 20 million EUR

DPAs may impose a fine up to **20 000 000 EUR** (or, in the case of an undertaking and if this sum is higher, up to 4 % of their annual turnover) on controllers or processors where:

- Personal data have been **unlawfully processed**;
- Data subjects have not been properly **informed** or their legitimate **requests** have not been complied with;
- The **instructions of a DPA** have not been complied with.

A fine up to **10 000 000 EUR** (or 2% of the turnover) may also be imposed for the breach of an obligation related to **security of paperworks**.

> *Until the GDPR enters into force, such fines are limited to much lower amount (2,448,000 € in Italy, 600,000 € in Spain, 500,000 £ in the United-Kingdom, 300,000 € in Germany and 150,000 € in France)*

Furthermore, controllers and processors are **liable for any damage** a data subject has suffered as a result of an infringement of their obligations. Finally, Member States law provide that judges may also impose **fines or imprisonment**.

[67] The European Commission lists them here: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

4.5 Specific issues concerning each activity

Specific issues concern the transmission of communications (part 4.2.1), the processing subsequent to this transmission (part 4.2.2), other services CNs may want to provide (part 4.2.3) and processing imposed by law (part 4.2.4).

4.5.1 Transmission of communications

The core activity of CNs is to provide access to their network and to transmit electronic communications from and/or to points of their networks. This activity is addressed in this part irrespective of the content of these communications, the protocol used for their transmission or whether these networks are connected to other networks such as the Internet.

Definitions: the legal meaning of the transmission of a communication

Transmitting electronic communications for the public is legally called an **electronic communication service** (ECS).

Both the **content** of a communication and the information necessary for its transmission (legally called **traffic data**) are **personal data** if they can be attributed to the sender and/or receiver of this communication. As CNs can broadly be regarded as able to attribute such data, they should consider them to be personal data in all circumstances. Thus, CNs are **controllers** of the processing required to transmit communications over their network.

> *At first sight, it may be unclear whether the controller of such processing is the person who transmits the communication (the ECS provider) or the person who sends it (the sender). Indeed, the person who decides that a communication should be transmitted and for what purpose is the sender; thus, this person should be regarded as the controller. However, the technical processing required to transmit electronic communications over a network may be regarded as too complex for users to have any effective control over it.*

> *In order to dispel such a doubt, the 1995 European Directive on data protection suggests*[68] *to divide the transmission of a communication into two separate processing. On the one hand, "in respect of the personal data contained in the message", the controller is the sender. On the other hand, "in respect of the processing of the additional personal data necessary for" the transmission, the controller is the ECS provider.*

> *Thus, a transmission has two controllers and CNs are only liable for the processing of data which are not contained in the message (meta-data). However, this distinction has few practical consequences for CNs, which can broadly be regarded as controllers of the whole transmission.*

[68] Recital 47 of the directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Obligations: interactions with the users

The lawfulness of the transmission of a communication does not seem to be problematic. Users sending a communication explicitly consent to the processing necessary for its transmission by doing so. Correspondingly, in most of cases, the transmission of a communication to its receiver pursues the legitimate interest of this receiver.

However, it may be more reliable to obtain users' consent once and for all through a **general agreement** that users would be required to enter into **prior to accessing the network**. Furthermore, such a prior agreement would be a convenient way to provide users with the necessary information (which shall be provided at the latest at the same time of the first processing) and to obtain consent for other activities of the CNs or to comply with other CNs' obligations.

Firstly, such an agreement would state that users allow the CN to send, receive or otherwise transmit electronic communication on their behalf and to carry out any other processing of personal data required for that purpose.

Then, within this agreement or otherwise (but prior to transmitting any communication in any case), CNs shall **inform their users**:

- About the CN's identity and contact details;
- That the purpose of the envisaged processing is the transmission of electronic communications;
- That the legal basis of this processing is the general agreement (or, where a CN chooses not to rely on such an agreement: senders' consent and receivers' legitimate interest to receive communications);
- That the recipients of the communications and their associated data are the final receiver of the communication and any operator of a network through which the communications should be conveyed;
- That the processed personal data are erased as soon as they are no longer needed for the purpose(s) users have consented to, unless otherwise required by law (as described below);
- About the rights of data subjects;
- Whether the personal data are transferred outside the EU.

In addition, CNs shall maintain a **record** of this processing and make such record available on request of their DPA. Finally, they shall implement appropriate **security measures** to prevent any accidental or unlawful loss, alteration, disclosure or access to the processed data and implement appropriate procedures in order to promptly react to any s**ecurity breach** or **data subject's request**.

Processing subsequent the transmission of communications

CNs may want to reuse the data processed during the transmission of communications for other purposes (for instance, for managing the network). Such reuses are subjects to specific obligations

provided in 2002 by the ePrivacy Directive[69] regarding telecommunication activities. This directive has been consistently implemented by all of the studied Member States (Germany[70], Spain[71], Italy[72], United-Kingdom[73] and France[74]) with almost no difference.

Definitions: the reusable data

Content of a communication is the information transmitted and which is not processed in order for the communication to be transmitted. CNs should regard contents as **personal data** in all circumstances since they can usually attribute them to the sender or receiver of a communication. As regards content, these senders and receivers are the **data subjects**.

Traffic data are data processed for the transmission of a communication on a telecommunication network (or for billing purposes, where the service is not free).

Location data are data processed on telecommunication networks or by ECSs providers, indicating the geographic position of the terminal equipment of a user.

As regards CNs' activities, the processing of traffic and location data may be related, for instance, to the management of their network (such as the listing or the mapping of the nodes, access points and users of the network) or to research purposes. Thus, these traffic and location data may be related to the **users** of a CN as well as to its **participants** who are running nodes and access points of the network. They both may be **data subjects**.

Finally, processing of traffic and location data which have been **fully anonymised** (which cannot be attributed to any individual, by anyone, in any circumstance) are not subject to any restriction, since such data are not personal data. The data discussed below are those which have not been anonymised – which are **personal data**.

> *The obligations described in this part are only imposed on providers of electronic communication networks or electronic communication services (ECSs). European law75*

[69] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), articles 5, 6 & 9;
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219&qid=1477575994553

[70] Telekommunikationsgesetz, §§ 96-98; http://gesetze-im-internet.de/tkg_2004/index.html

[71] Ley 9/2014, de 9 de mayo, de Telecomunicaciones, artículo 48;
https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950#a48

[72] Codice in materia di protezione dei dati personali, articoli 123 e 126;
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248

[73] Privacy and Electronic Communications (EC Directive) Regulations 2003, articles 7, 8 & 14;
http://www.legislation.gov.uk/uksi/2003/2426/contents/made

[74] Code des postes et des communications électroniques, article L. 34-1;
https://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=F0335039760986A35681C10DBEF39F4C.tpdjo16v_1?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465770&dateTexte=&categorieLien=cid

defines an ECS as "a service normally provided for remuneration". This definition is unclear: it may cover any entity which usually provides its service for remuneration (such as commercial Internet access providers) or any entity which provide services usually provided by others for remuneration (such as Internet access, which is not usually provided for free). The first of these interpretations suggests that CNs providing access to their network (or any other service) without any direct or indirect remuneration cannot be regarded as providing ECSs and are not subject to the obligations described in this particle However, as such an interpretation is highly uncertain, it is advised that every CN regards itself as providing services "normally provided for remuneration".

Lawfulness of processing: strictly limited processing

Traffic data may always be lawfully processed for **two specific purposes**:

- in order to bill users (where access to the network is not free);
- For interconnection payments.

In these two cases, CNs do not have to obtain any consent, but they can only retain traffic data up to the end of the period during which the bill may lawfully be challenged or payment pursued (as provided by national law).

German[76] and Italian[77] laws on telecommunications specify that traffic data may be stored up to six months (or longer if a claim is lodged with judicial authorities). The German law specifies that this period starts after the invoice has been sent. In other studied Member States, laws on telecommunications do not provide such specifications (which should be found in national contractual law).

Furthermore, German[78] and French[79] law add another purpose, specifying that traffic data may be processed without obtaining consent in order to ensure the security of the network. French law specifies[80] that, for that purpose in particular, only the following data may be processed and shall be deleted after three months:

- *the data identifying the source of the communication;*
- *the date, time and duration of each communication;*

[75] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), article 2, c); http://eur-lex.europa.eu/eli/dir/2002/21/oj

[76] Telekommunikationsgesetz, § 97, (3)

[77] Codice in materia di protezione dei dati personali, article 123, 2

[78] Telekommunikationsgesetz, § 88, (3)

[79] Code des postes et des communications électroniques, article L. 34-1, IV

[80] Code des postes et des communications électroniques, article R. 10-14, IV

- *the technical data of each communication;*
- *the supplementary services used or required, and the providers of such services;*
- *The data identifying the receiver(s) of the communication.*

In any other case, where CNs intend to process contents, traffic data or location data for any other purpose, they shall **systematically obtain the prior consent of their users and/or participants** to this specific purpose. CNs cannot rely on any legitimate interest here.

Users' consent may be obtained through the **general agreement** described above. However, CNs **shall not refuse access to their network** to users refusing to consent to processing which are not necessary for the mere transmission of their communications. Otherwise, such consent would not be freely given and, thus, would not be valid. For instance, if a CN intends to publish a map of the equipment of its users, it cannot refuse access to its network to a user refusing to be on such a map.

Participants' consent may be obtained by any mean. Here, their participation to the network may be denied if they refuse to consent to processing necessary for the community to effectively run the network.

Users and/or participants shall be able to withdraw their consent at any time.

> *German[81] and Italian[82] laws specify that, where location data are processed, users shall have the possibility, using a simple means and free of charge, of requesting to temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.*

Other obligations

Prior content, traffic or location data being processed for any other purposes than transmission, CNs shall provide their users and/or participants with **complete information**. This information may be provided within the general agreement described above.

As regards each processing, users and/or participants shall be informed:

- About the CN's identity and contact details;
- About the purpose of the processing;
- That the legal basis of this processing is the law (for billing or interconnection payments or, in Germany and France, for security measures) or their consent;
- About the categories of data processed;
- About the recipients of the data, if any;

[81] Telekommunikationsgesetz, § 98, (2)

[82] Codice in materia di protezione dei dati personali, article 126, 3

- That the processed personal data are erased as soon as they are no longer needed for the purposes they have consented to (the CN shall specify this period or the criteria used to determine it), unless otherwise required by law.
- About their rights as data subjects;
- Whether the personal data are transferred outside the EU.

In addition, CNs shall maintain a **record** of these processing, implement appropriate **security measures** to prevent any accidental or unlawful loss, alteration, disclosure or access to the processed data and implement appropriate procedures in order to promptly react to any **security breach** or **data subject's request**.

4.5.2 Other services: email, hosting, VoIP, chat, VPN...

CNs may want to provide other services than providing access to their communication network. These services may include email, hosting, voice, chat or VPN services, for instance.

4.5.3 Processing necessary for the provision of the services: lawful as any other processing

The processing necessary for the mere provision of such services does not raise specific legal issues: CNs must comply with their general obligations as data controllers.

Firstly, they must ensure that each processing pursues a lawful purpose, whether users have **consented** to it or such a purpose is necessary for the execution of **contracts** with users or pursues the **legitimate interest** of the CN or its users.

Then, prior each processing, CNs shall provide users with **complete information**. Finally, they shall maintain **records**, implement appropriate **security measures** and appropriate procedures in order to promptly react to any **security breach** or **data subject's request**.

4.5.4 Processing subsequent to the provision of the services: strictly limited for ECSs

Once again, specific issues arise if a CN wants to reuse for another purpose data it has processed for the provision of its services. The issue is whether the service initially provided is an **electronic communication service** (ECS) – transmitting electronic communications for the public – or not.

If a service is an ECS, the data processed for its provision are **traffic data** and cannot be reused without the **consent of users** (as stated above). If it is not, the data processed for its provision may be reused without obtaining such consents but by relying on another legal basis, such as the **legitimate interest** of the CN or its users.

Some services are clearly not ECSs, such as **hosting services** or the **provision of information** or the **offering of goods and services** on-line, which does not consist of the transmission of communications for their users. CNs may reuse data processed for the provision of such services by relying on their users' consent or on a legitimate interest. Other services are clearly ECSs, such as

providing access to a network and transmitting communication over this network (as described above).

In other cases, unfortunately, determining whether a service is an ECS may be **highly uncertain**. Neither the ePrivacy Directive nor national laws provides for practical criteria for determining it, this question being left to national authorities and judges.

As the Body of European Regulators for Electronic Communications (BEREC) explained[83], nearly all national authorities consider that **voice services** are ECSs if they offer the possibility to make outgoing calls to the publicly available telephone service. Correspondingly, they do not consider as ECSs the voice services which do not offer such a possibility. Furthermore, most Member States do not consider **email and instant messaging services** as ECSs either, with a potential major exception in Germany.

> *The BEREC relates that "in Germany the Administrative Court of Cologne addressed the question whether Gmail qualifies as ECS. In its ruling of 11 November 2015 it found that even if Google uses no telecommunication infrastructure of its own for the signal transfer, but rather the existing infrastructure of the "open internet", the signals necessary for the transfer of emails via Gmail has to be, over all, attributed to the email service of Google. The Court therefore classified the OTT communication service Gmail as "telecommunication service" in the sense of the German Telecommunication Act. However, the ruling has been appealed and therefore there is no final judgment yet.*"

However, one potential interpretation is also that some **services provided together with an ECS are always ECSs too**. Typically, an email service provided by an Internet access provider may be an ECS (even if it would not be an ECS if provided by others). As CNs' core activity is to provide access to their network, some of the other services they provide may be regarded as ECSs as well.

The ePrivacy Directive (which specifies the ECSs' obligations) is currently being reviewed by the European Commission, which intends to **clarify the scope of ECSs** by extending its application to so-called "over the top" (OTT) services such as email or voice services (provided by anyone).

However, until the scope of ECSs is clarified, CNs are strongly advised not to rely on legitimate interest in order to re-use personal data already processed for another service. This actually may not be a practical issue since they are advised to **rely on their users' consent for whatever processing** they carry out.

[83] BEREC, report on OTT services, January 2016, p. 20;
http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5751-berec-report-on-ott-services_0.pdf

Finally, CNs shall, as usual, prior to each processing, provide users with **complete information**, maintain **records**, implement appropriate **security measures** and appropriate procedures in order to promptly react to any **security breach** or **data subject's request**.

4.5.5 Processing imposed by law: data retention

The main processing imposed by national laws on CNs is the retention of traffic data processed by providing ECSs to the public. Before describing these obligations, some general comments should be made.

In most of the studied Member States, the scope of data that shall be retained may be as uncertain as the scope of ECSs (free and e-mail services are typical examples of that). Furthermore, in some States (Italy, France and potentially United-Kingdom), ECSs providers are required to store the traffic data processed for each transmission of a communication: in some contexts, the meaning of a "communication" may not be clear. For instance, should the transmission of any packet on the network be considered as a communication, and the related traffic data be stored? It would seem unreasonable, but the legislation fails to tackle this question clearly. Thus, unfortunately, in some cases, little practical and reliable advice can be provided.

Finally, in all of the studied Member States, in addition to the obligation to retain data, CNs shall establish internal procedures to meet the requests made by public authorities to access the retained data or to intercept communication on their network, and shall keep these requests confidential.

4.5.6 European Union law

In 2002, the **ePrivacy Directive** allowed Member States to adopt legislative measures providing for the retention of communications' content, traffic or location data for a limited period when such retention is necessary to safeguard "*national security, defence or public security or for the prevention, investigation, detection or prosecution of criminal offences or of unauthorised use of the electronic communication system*".

In 2006, the European Union has passed the **Data Retention Directive**[84], providing that Member States shall ensure that some traffic and location data (and the related data necessary to identify users) processed by providers of ECSs or public communication networks are retained for a period between six months and two years.

[84] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC; http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478085591034&uri=CELEX:32006L0024

Since then, most Member States have passed national laws implementing such an obligation. In 2014, however, the European Court of Justice has decided[85] that the 2006 Directive was entailing "a wide-ranging and particularly serious interference" with the fundamental rights to privacy and data protection, "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary" according to the Charter of Fundamental Rights of the European Union. Thus, **this Directive was invalided**.

The invalidation of a European Directive does not systematically imply that the national legislations which have implemented it shall be repealed. Thus, while some Member States have repealed their data retention legislation in response to the CJEU's ruling, others have maintained it, amended it or passed new legislation. However, it is still **uncertain whether these remaining national legislations are complying with European Union law**.

In order to resolve this issue, **two preliminary questions** have been lodged before the CJEU by a Swedish[86] and a British[87] court. They ask the CJEU whether any obligation imposed on ECSs providers to retain the traffic data of all of their users may comply with the Charter as such. Then, if it does, they ask the CJEU to define the specific circumstances under which such an obligation may be imposed (which authorities may access the retained data, for what period the data may be retained and what security measures shall be implemented).

These two cases have been heard together by the CJEU on 12 April 2016. **The CJEU has yet to give its answer**, which will definitely impact the national legislation of all Member States. Until then, CNs must comply with their current national legislation.

4.5.7 German law

On 2 March 2010, Germany's constitutional court struck down the previous German Data Retention Act, stating that it was violating users' privacy by requiring the broad collection and storage of data from all users during six months. On October 2015, Germany passed a **new Data Retention Act**[88] providing, inter alia, for much shorter storage periods. German CNs shall comply with these new obligations not later than **1 July 2017.**

As regards **Internet access** services, the following information must be retained during **ten weeks**, for each access to the Internet:

[85] CJEU, 8 April 2014, Digital Rights Ireland v Minister for Communications & others, cases C-293/12 and C-594/12; http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=37513

[86] Request for a preliminary ruling from the Kammarrätten i Stockholm (Sweden) lodged on 4 May 2015 — Tele2 Sverige AB v Post- och telestyrelsen, Case C-203/15; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CN0203

[87] Reference for a preliminary ruling from Court of Appeal (England & Wales) (Civil Division) made on 28 December 2015 — Secretary of State for the Home Department v David Davis, Tom Watson, Peter Brice, Geoffrey Lewis, Case C-698/15; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CN0698

[88] Vorratsdatenspeicherung, adding §§ 113a - 113g to the Telekommunikationsgesetz

- The IP address allocated to the user;
- The identification of the port through which Internet is accessed, as well as an allocated user ID;
- The date and time (indicating the time zone) of the log-in and log-off of the Internet access service under the allocated IP address.

As regards **telephone** services, the following information must be retained during **ten weeks**, for each communication (including unanswered and unsuccessful calls):

- The phone number or another identifier (concerning Internet telephony: IP addresses and other allocated identifiers) of the calling and called parties;
- The date and time of the start and end of the communication (or, concerning text messages, of the sending and receipt of the message), indicating the time zone;
- The service used (where the telephone service allows to use different services);
- Concerning mobile telephony, the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the calling and called parties;
- In the case of pre-paid mobile telephony services, the date and time of the initial activation of the service, indicating the time zone.

As regards **mobile telephony** or **mobile access to the Internet**, the following pieces of information must be retained during **four weeks**, for each communication or access:

- The ID of the radio cells used by the calling and called parties at the beginning of the connection or used by the Internet user at the beginning of the access;
- Data from which the geographic location and the main radiation directions of the radio antennas supplying the respective radio cells result.

These obligations shall not result in the retention of the content of communications, information about websites accessed or data processed by e-mail services.

German CNs shall only retain the data they are processing by providing access to the Internet or telephone services. However, if some data should be retained according to these obligations but are not processed by a CN, this CN shall:

- Ensure that such data are retained by someone else;
- Inform the Bundesnetzagentur (the federal network agency) immediately, at its request, of who is storing these data.

As regards telephone services, CNs shall only retain data concerning unanswered or unsuccessful calls if they already process such data for another purpose – thus, they never have to ensure that these data are retained by someone else.

Furthermore, the retained data shall be:

- Stored in Germany;

- Stored in such a way that requests from the authorized authorities can be answered without delay;
- Erased at the latest within a week after the expiry of the mandatory storage periods.

German CNs shall ensure that all data are protected against unauthorized access and implement the following technical and organizational measures, at least:

- A particularly secure encryption method;
- A storage device separate from usual processing;
- A data processing system decoupled from internet and highly protected against access from the internet;
- Restricting access to the data processing facilities to individuals specially authorized;
- Requiring the participation of at least two authorized persons in accessing data.

For each access to the retained data, CNs shall log during one year (and no more):

- The time of access,
- The persons accessing the data,
- The purpose and type of access.

German CNs not complying with these obligations may be fined up to **500.000 €.**

Finally, anyone who commercially provides ECSs shall collect, store and keep up to date the following information (even if it is not necessary for the provision of the services):

- The phone number or another identifier of the connexion provided;
- The name and address of the owner of the connection (and, in the case of an individual, his/her date of birth);
- Concerning fixed connections, the address of the connection;
- In case a mobile phone is provided, the device number of this phone;
- The date of commencement of the contract.

CNs not complying with this obligation may be fined up to **300.000 €** (or 100.000 € if they only fail to keep up to date the required information).

4.5.8 Spanish law

The Spanish Data Retention Law[89] requires the providers of ECSs and public communications networks to retain the categories of data listed below during **one year**, as long as these data are processed for the provision of these services and do not reveal the content of the communications. Specific regulations may also extend or reduce the retention period up to two years or to a minimum of six month for specific categories of data.

[89] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; http://noticias.juridicas.com/base_datos/Admin/l25-2007.html

Concerning **Internet access, Internet e-mail and Internet telephony**:

- The IP address, telephone number and/or user ID allocated to the originator of the communication and his/her name and address;
- The date and time of the log-in and log-off of the service, based on a certain time zone;
- The digital subscriber line (DSL) or other end point of the originator of the communication;
- The calling telephone number for dial-up access.

Furthermore, concerning **Internet e-mail and Internet telephony** only:

- The user ID or telephone number of the intended recipient or recipients of the communication and their name and address;
- The Internet service used.

Concerning **fixed and mobile telephony** (including unanswered calls and unsuccessful calls because of a network management intervention):

- The telephone number, name and address of the calling and called parties (and any numbers to which the call may be routed);
- The date and time of the start and end of the communication;
- The telephone service used: call type (voice, voice messages, conferencing, data), supplementary services (call forwarding or transfer) and messaging services (short message, enhanced media or multimedia).

Furthermore, concerning **mobile telephony** only:

- The International Mobile Subscriber Identity (IMSI) of the calling and called parties;
- The International Mobile Equipment Identity (IMEI) of the calling and called parties;
- The location label (Cell ID) at the start of the communication;
- Data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained;
- In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated.

> *The categories of data that shall be retained under Spanish law are exactly the same as in the former European Data Retention Directive of 2006. Some of these categories are problematic: it seems that email providers shall retain data identifying the recipients of every email sent by their users. However, the circumstances under which email services may be considered as ECSs (and their providers subject to these obligations) are unclear. Anyway, as stated above, since CNs usually provide pure ECS, they should comply with these obligations where they also provide email services.*

Anyone not complying with these obligations may be fined up to **20.000.000 €** where no data are retained at all or up to **2.000.000 €** where data are not properly retained.

4.5.9 Italian law

The Italian Data Protection Code[90] requires **ECSs** providers to retain the traffic data they process for **one year** as from the date of the communication. The contents of communications shall not be retained.

The Italian Data Protection Authority has specified[91] that "owners and managers of public establishments and/or private clubs of any kind [...] that make Internet wireless access points available to the public" are not subject to these obligations. Italian CNs providing access to their network through access points owned and managed by individual participants may benefit from this exception as regards traffic data processed by this individual (but not as regards traffic data subsequently processed by other nodes of the network).

> *In 2005, Italy passed a regulation[92] imposing on anyone offering access to the Internet to the public via WIFI an obligation to collect data identifying users. This obligation was deleted in 2010[93].*

As for **telephone services** providers, they shall retain the telephone traffic data they process for **two years** as from the date of the communication. The data related to **unsuccessful calls** that are processed on a provisional basis by the providers of ECSs or of a public communications network shall be retained for **thirty days**.

The Minister for Home Affairs or a person delegated by him/her may **order** providers to retain Internet traffic data, except for contents data, for a period of ninety days, which can be extended up to six months. This order shall be kept confidential along with any activities performed accordingly.

CNs shall lay down technical mechanisms to **regularly destroy** the data after expiry of the mandatory retention period.

By way of derogation from these requirements, Italy has passed a new legislation on 20 February 2015 providing for derogative *Urgent Measures for the Fight Against Terrorism*[94]. It provides that

[90] Codice in materia di protezione dei dati personali, article 132;

[91] Garante per la protezione dei dati personali, Security In Telephone And Internet Traffic Data - 17 January 2008 [1502599] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1502599

[92] Decreto-legge 27 luglio 2005, n. 144, article 7; http://www.camera.it/parlam/leggi/05155l.htm#decreto

[93] Decreto-legge 21 giugno 2013, n. 69, article 10 http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-08-20&atto.codiceRedazionale=13A07086&elenco30giorni=false

[94] Decree-Law No. 7 of February 18, 2015, Urgent Measures for the Fight Against Terrorism, Including International Terrorism, as well as Extension of the International Missions of the Armed Forces and Police, Cooperation Initiatives

telephone and Internet traffic data processed **as from 21 April 2015** shall be **retained until 30 June 2017.**

> *The initial legislation provided that traffic data shall only be retained until 31 December 2016. This date has been postponed until 30 June 2017 by the Law No. 21 of 25 February 2016. Thus, Italian CNs must be aware that this date may be postponed again in the near future.*

Failure to retain the data, or retaining incomplete data, may be punished by an administrative fine ranging from **10,000 € to 50,000 €**, which may increase up to three times as much on account of the offender's economic conditions. If the allocated IP address does not allow a subscriber or user to be identified uniquely, an administrative fine ranging from 5,000 € to 50,000 € may be imposed, which may be increased up to three times as much on account of the offender's economic conditions.

4.5.10 French law

French law[95] requires providers of electronic communication **networks** and of **ECSs** to retain during **one year** the following traffic data if they already process them:

- The data identifying the user of the service;
- The date, time and duration of each communication;
- The technical data of each communication;
- The supplementary services used or required, and the providers of such services;
- The data identifying the receiver(s) of the communication;
- Concerning telephone service, the data identifying the source and the location of the communication.

These obligations shall not result in the retention of the content of communications or of the accessed information.

> *The French Telecommunication Authority does not regard as an ECS provider someone providing access to the Internet without obtaining any direct or indirect remuneration[96]. However, the law specifies that any entity providing access to the Internet for free "in the context of a professional activity" (such as hostels or pubs) is also subject to the obligation to retain data. Thus, it would seem that an individual providing access to Internet is not subject to this obligation if he/she is not doing so in the context of a business. Unfortunately, the French Data Protection Authority stated that any "entity"[97] or "any place offering to the public an*

for the Development and Support of Reconstruction Processes, and Participation in Initiatives of International Organizations for the Consolidation of Peace and Stabilization Processes.

[95] Code des postes et des communications électroniques, articles L34-1, R10-13

[96] ARCEP, Étude sur le périmètre de la notion d'opérateur de communications électroniques, juin 2011, p. 42; http://www.arcep.fr/uploads/tx_gspublication/etude-Hogan-Analysys-juin2011.pdf

[97] CNIL, Internet et Wi-Fi en libre accès : bilan des contrôles de la CNIL, 22 décembre 2014; https://www.cnil.fr/fr/internet-et-Wi-Fi-en-libre-acces-bilan-des-controles-de-la-cnil-0

> *access to the Internet, for free or not," is subject to this obligation*[98]*, without specifically excluding from this scope individuals not running any business. Thus, it is* **highly uncertain** *whether French individuals providing access to the Internet to the public for free* **are subject to this obligation or not**.

Furthermore, French law imposes an **additional obligation on Internet access** providers[99], which shall retain during **one year**, for each access to the Internet:

- The identifier of the connection;
- The identifier allocated to the subscriber;
- The date and time of the start and end of the access;
- The identifier of the equipment used for the access;
- The technical characteristics of the subscriber's line.

> *The law imposes this specific obligation on "entities which activity is to provide access" to the Internet. Thus, entities which main activity is not to provide such an access may be excluded from the scope of this obligation. Furthermore, the retained data relate to "subscribers", which implies a contractual relationship of some kind. In the same way, the French Data Protection Authority does not specify that hostels, pubs or cybercafés are subject to this specific obligation whereas it does indicate that they shall comply with the broader obligation imposed on ECSs providers (as stated above). Accordingly, individual participants of CNs may be regarded as excluded from the specific obligation imposed on Internet access providers.*

Then, another additional obligation is imposed on **hosting services** providers which shall retain during **one year** after the creation, modification or deletion of any hosted content:

- the time and date of the connection;
- the identifier provided by the user, if any;
- the connection ID;
- the protocols used for the connection to the service and the creation/modification of the content;
- the identifier allocated to the content;
- Whether the content has been created, modified or deleted.

[98] CNIL, Conservation des données de trafic: hot-spots Wi-Fi, cybercafés, employeurs, quelles obligations ?, 28 septembre 2010; https://www.cnil.fr/fr/conservation-des-donnees-de-trafic-hot-spots-Wi-Fi-cybercafes-employeurs-quelles-obligations

[99] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, article 6; https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=F0335039760986A35681C10DBEF39F4C.tpdjo16v_1?cidTexte=JORFTEXT000000801164&idArticle=LEGIARTI000006421546&dateTexte=&categorieLien=cid; Décret no 2011-219 du 25 février 2011; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013

> *This obligation is clearly imposed on both professionals and non-professionals, providing this service for free or not.*

Finally, Internet access and hosting services providers shall retain during **one year** the following data if they usually collect them:

- The name, postal and email addresses, phone number, user names, password (and any information required to check or change it) provided by users who have entered into a contract with the provider or created an account;
- Where users have paid for entering into the contract or creating an account, for each payment: the payment method, its reference, the amount and the time and date of the payment.

Anyone not complying with these obligations may be sentenced up to **one year in prison** and fined up to **75,000 €** (or 375,000 € for legal persons).

4.5.11 British law

The United-Kingdom has initially implemented the Data Retention Directive in 2007[100] and 2009[101] by allowing the Secretary of State to require any public communication provider to retain all traffic data it processes during one year.

In response to the invalidation of the European Directive in 2014 by the CJEU, a new legislation[102] has been hastily passed, replacing the previous regulations and intending to add the safeguards required by the CJEU's ruling. This new legislation provides, inter alia, that the retention notices issued by the Secretary of State must specify the categories of data that shall be retained and the length of this retention (which cannot exceed 12 months, but can be shorter).

This new legislation has been challenged before the High Court of Justice which stated[103], in July 2015, that it failed to provide clear and precise rules for ensuring that the stored data could only be accessed in cases involving serious offences and did not give courts or an independent body control over who gets to access the data. Thus, the High Court decided that the new data retention obligation had to be disapplied by 31 March 2016, as it was incompatible with the ruling of the CJEU. Then, the government appealed to the Court of Appeal which has made a preliminary reference to the CJEU (as stated above).

[100] The Data Retention (EC Directive) Regulations 2007; http://www.legislation.gov.uk/uksi/2007/2199

[101] The Data Retention (EC Directive) Regulations 2009: http://www.legislation.gov.uk/uksi/2009/859

[102] Data Retention and Investigatory Powers Act 2014; http://www.legislation.gov.uk/ukpga/2014/27

[103] England and Wales High Court (Administrative Court), 17/07/2015, David Davis & cie.v. the Secretary of State for the Home Department, Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014; http://www.bailii.org/ew/cases/EWHC/Admin/2015/2092.html

In response to the High Court's ruling, the Government has proposed a new Bill in November 2015[104] intending to add more safeguards. Again, this Bill allows the Secretary of State to order any telecommunication services provider to retain some specific data up to twelve month after their collection. The Bill specifies that the notion of "telecommunication services" has here a broad meaning and that any "*Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition*". Such a broad definition clarifies a situation which is still unclear in other Member States.

> *In autumn 2016, the Government has issued a Draft Code of Practice on Communications Data[105] which provides for many useful clarifications, including the following:*
>
> *"The definition of a telecommunications operator" (the subject of retention notices) "also includes application and website providers but only insofar as they provide a telecommunication service. For example an online market place may be a telecommunications operator as it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service."*

Finally, the Bill gives a new massive power to the Secretary of State, which may order Internet access providers to store the list of all services (such as websites or web applications) accessed by their users during one year.

The Bill should be enacted by the end of 2016. British CNs will have to comply with the specific (or general) retention notices the Secretary of State will issue on this basis.

4.6 Specific issues concerning decentralized networks

Complying with all the obligations described above may be particularly difficult where **the infrastructure of a CN is owned and/or run by several participants** (individuals or legal entities) not acting under the direct authority of the CN as employees.

In this part, "CNs" may be regarded both as wide CNs such as guifi.net, Ninux or Freifunk or as the local sub-groups of these wide CNs running their own part of the network.

4.6.1 Centralized decision-making: contracts between the central entity and the participants

If a CN has a legal existence and acts as a central authority deciding what services are provided and through what technical means, and if the participants merely carry out processing on its behalf

[104] Draft Investigatory Powers Bill, November 2015; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

[105] *Draft Code of Practice on Communications Data*, Autumn 2016; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557862/IP_Bill_-_Draft_CD_code_of_practice.pdf

(whether they own and/or run part of the infrastructure or not), the **CN is the controller and the participants are mere processors**.

In this case, most of the data protection obligations are imposed on the CN. Participants shall only comply with their processors' obligations (security measures and records). The **CN is liable for the failure of any participant** to comply with its processor's obligations.

As regards **data retention**, obligations are imposed on anyone who actually processes data and falls within the scope of the law: that can be both the CN and its participants. However, where they are subject to this obligation, participants may transfer the collected data to the CN in order for this latter to store them and answer authorities' requests.

Finally, the GDPR requests the CN (the controller) to enter into a **contract with each participant** (the processor), indicating the subject-matter, duration, nature and purpose of each processing carried out by the participant, as well as the type of personal data and categories of data subjects, and providing that the participant shall:

- Process the personal data only on documented instructions from the CN (unless required to do so by law);
- Implement all appropriate security measures and assist the CN in case of a security breach;
- Assist the CN in answering data subjects' requests;
- After the end of the processing, delete or return all the personal data to the CN (at the choice of the CN) and deletes existing copies (unless law requires storage of the personal data);
- Assist the CN in demonstrating compliance with its obligations;
- Not engage a sub-processor without prior authorisation of the CN;
- Where the participant authorises someone under its authority to process data, ensure that this person have committed him/herself to confidentiality.

> *In France, CNs members of* **FFDN** *are usually legal entities which own the whole infrastructure of their network. Their participants may own a part of its infrastructure and/or manage the network on behalf of the CN, according to its instructions. In this case, these participants are processors, must comply with their obligations and enter into a contract witch the CN, as described above. This only applies to independent participants: employees of a CN are not processors and are not subject to any specific obligation but only to their employment contract.*

4.6.2 Decentralized decision-making: contracts between participants

If the purpose and means of the processing carried out for the provision of services are not decided by a single entity but by the participants of the CN, **these participants are the controllers** (if the CN has a legal existence, it may also be one of these participants).

In this case, in theory, each participant shall:

- Obtain users' consent for each service provided through the part of the infrastructure it manages;
- Provide user with the information related to this service;
- Maintain records concerning this service;
- Implement appropriate security measures and appropriate procedures in order to promptly react to any security breach;
- Answer data subject's requests;
- Comply with data retention obligations.

However, participants may decide to make agreements with each other in order to **delegate some of their obligations**:

- To some **specific participant**: for instance, participants who are in direct contact with the users (such as those offering access to the network) would have to inform users about the processing carried out by other participants; and/or
- To a **central legal entity**, or several entities: for instance, the central entity would maintain records about each processing and be the main interlocutor with the Data Protection Authority; it may monitor the security of the whole network and implement the appropriate procedures in order to react to security breach; it may also be a single point of contact for data subjects).

Participants may also collectively draft a **consent form** and an **information notice** which can be directly provided by the participants to end-users.

> *In Germany, Italy and Spain, the purposes and means of the services provided by* **Freifunk, Ninux and guifi.net** *are not decided by a single entity but by their participants, who are the controllers of the processing implied by these services. Each of these participants shall comply with its own obligations but may delegate some of them to other participants or to central entities, as described above.*

> *Currently, participants of these three CNs shall already subscribe to some kind of a contract (the Pico Peering Agreement, the Ninux Manifesto or the Network Commons License) which could also provide for the delegation of their obligations. Furthermore, Freifunk and guifi.net already have some kind of a central entity (the Forderverein Freie Netzwerke e.V. and the guifi.net Foundation) to which participants may potentially delegate some obligations. Finally, participants of these three CNs may also delegate some obligations to more local entities.*

> *It is advised that participants of these three CNs delegate their obligations related to consent and information to participants who are in direct contact with users (usually participants providing access to the network). It is also advised to centralize some obligations to local entities or to a single entity: obligations to keep records, to react to security breach and to answer the requests of data subjects and DPAs.*

Finally, in some cases, determining the respective obligations of the participants is not an option but an obligation. Indeed, the GDPR provides that, where several controllers **determine together the purpose and means of processing**, they shall be regarded as **joint controllers** and shall determine their respective responsibilities by means of an arrangement between them. If they do not, each of them may be **liable for the failure of any other participant** to comply with its obligations.

Participants usually determine collectively the services they intend to provide and their technical implementation (especially where these services are provided in the same area and to the same public). In this case, these participants are joint controllers and have to determine which of them shall comply with each of their respective obligations. If they do not want to delegate any obligation, they still have to pass agreements which explicitly state so.

> *The cases in which participants of* **Freifunk, Ninux** *and* **guifi.net** *are joint controllers are* **not always clear**. *In some cases, participants of a local community actually decide together all the purposes and technical means of the services they provide locally: these participants are certainly joint controllers as regards these local services. On a wider scale, some technical issues may be addressed and solved collectively by all the participants of a CN, belonging to different local communities. Thus, different communities may provide the same service through the same technical means. However, it is unclear whether the services provided by these communities form a single service (in which case all the participants of the CN would be joint controllers of this single service) or are distinct from each other (in which case participants of each local community would only be liable for the service locally provided by their community).*

> *This uncertainty may be solved through contracts explicitly determining the respective responsibilities of each participant or community (for instance, participants may agree that each of them is only responsible for the obligations implied by the services locally provided by its community). Furthermore, since it is advised that participants delegate some of their obligations through contracts in any case, knowing whether they are joint controllers or not may not be a practical issue.*

This obligation to enter into mutual agreements only applies as regards data protection but, as regards **data retention**, each participant remains individually liable for compliance with its own obligations (the notion of joint controller does not apply here).

> *Participants may still enter into a contract with a central entity: this contract would provide that participants collect the required data and directly transfer them to the central entity, which would be responsible for their storage and for answering authorities' requests. However, centralizing such data may raise security issues. CNs should adopt the more secure solution according to the technical expertise of their participants. No general advice can be provided here.*

4.6.3 Security issues: warning users about the openness of the network

If a CN allows anyone to participate in the provision of its service, it must specifically inform its users about the **security risks** posed by such a possibility. Indeed, **malicious participants may want to intercept users' communications** or otherwise monitor their activities by participating in the services. This is the case for Freifunk, Ninux and guifi.net.

4.7 Conclusions

As described above, strictly complying with data protection law may **require some degree of centralization**. Otherwise, complying with all of their obligations may be an excessive burden for individual participants. However, such a centralization collides with **CNs' ideal of decentralization** and with the **recommendations made for the issues related to liability**.

Accordingly, **CNs are welcome to express** how they interpret and comply with their data protection obligations in **a more practical and creative way** than the strict legal analysis provided above.

In the same way, as already stated, clear and reliable guidelines on **data retention** cannot be provided: there are still **too many legal uncertainties**. This is particularly unfortunate since these obligations are the complete opposite of the values promoted by CNs. Thus, CNs are also welcome to **express how they already comply** with these obligations – whose legal meaning may surely be clarified by their practical and spontaneous implementation by privacy advocates.

5 Overall conclusions

The current European legal framework for CNs is composed by a number of different provisions, that often do not allow a clear interpretation.

This report has analysed mainly three different issues: telecommunication policies; civil liability issues; privacy and data protection.

The current **regulatory framework for electronic communications** is applied differently depending both on the national implementation of the European Directives, and on the features of the single CN. The **upcoming regulatory novelties** might bring **big changes** in the existing scenario. This is especially important for what concerns connectivity in rural and underdeveloped areas, as well as for spectrum regulation and management.

While waiting for the new Electronic Communications Code to come, one of the **next steps** that the project should do is to **understand if and how the current framework is applied in each Member State to CNs and how CNs do actually cope with the obligations** arising from this regulation.

As for liability, a general recommendation for any CN under the point of view of **liability**, the **network should be as distributed as possible**. When there is an **entity governing** the network, the entity **should ensure that each user is aware of the possible implications in terms of liability**. Entities – such as associations or foundations – might be held liable according to the national rules.

When there is an entity, the use of licenses might be a way both to inform users and to limit the CNs' liability: **CNs might want to impose specific obligations on their users, interrupt service** and/or **ask for damages** when users do not comply with these obligations.

Depending on the scope of national definitions of intermediaries and economic operators, some **CNs might also qualify as Internet Access Providers** under Directive 2000/31 (cf. par. 3.2.3). In these cases, they enjoy the **liability exemptions** introduced by Directive 2000/31, but at the same time they might be the target of **injunctions**. In case the injunction was to password-protect the network, this could badly hamper the functioning of the network.

As for liability, **CNs' experience** would be invaluable to understand how law is applied. This document mainly includes a reading of the existing laws, with only a few references to **actual cases**. Field research to obtain **information directly from CNs** on their daily problems in dealing with liability will be the next step **to improve our analysis. CNs' tactics** already applied **to protect themselves** from liability are important to understand whether technical and/or legal solutions might make CNs more robust and if such solutions might be applied to other CNs in order to make them stronger too.

Finally, as for **privacy and data protection**, the report illustrates how **many different obligations** are imposed on CNs to comply with the European framework. Unfortunately, to better cope with these obligations, a **centralized architecture** would be **desirable**. However, many aspects are going to change with the introduction of the **General Data Protection Regulation**, entering into force in 2018. CNs should **get ready for the new regulation**. In order to better understand how CNs have up to now dealt with these issues, a next step will be to **investigate if CNs have adopted specific measures**, either technical or legal, to deal with privacy and personal data protection **and what measures** have they adopted. Their feedback will be the bases on which the Task will work, to improve our understanding of CNs and of laws applicability on these networks.

Indeed, the purpose of this deliverable is specifically to outline legal hurdles which, strictly interpreted, may conflict with CNs' activities and ideals. The purpose of the next version of this deliverable will be, according to CNs' feedback, to balance these conflicting interests in a practicable and reasonable manner.

6 Bibliography

Belli L., De Filippi P. (eds.). 2016. Net Neutrality Compendium. Human Rights, Free Competition and the Future of the Internet, Springer: Berlin

Boso Caretta A., 2010. La disciplina del regime autorizzatorio. Le misure di armonizzazione, in Bassan F. (ed.), Diritto delle comunicazioni elettroniche, Giuffrè: Milan, 2010, 55-86

Bonelli F.. 2004. Uso privato ed uso aperto al pubblico di «reti alternative» di telecomunicazioni (article 101), in Clarich M., Cartei G.F. (eds), Il codice delle comunicazioni elettroniche, Giuffrè: Milan, 469-479

Busch C. 2015. Secondary Liability for Open Wireless Networks in Germany: Balancing Regulation and Innovation in the Digital Economy, ssrn.com, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728350.

Caggiano G.. 2010. La riforma del regime delle radiofrequenze nel quadro delle comunicazioni elettroniche, in Bassan F. (ed.), Diritto delle comunicazioni elettroniche, Giuffrè: Milan, 203-236

De Filippi P., Bourcier D., 2016. "Three-Strikes" Response to Copyright Infringement: The Case of HADOPI," in: F. Musiani, D.L. Cogburn, L. DeNardis, N.S. Levison (editors), The Turn to Infrastructure in Internet Governance. London: Palgrave-Macmillan, 2016, pp. 125-152.

De Filippi P., Treguer F., 2015. "Expanding the Internet Commons: The Subversive Potential of Wireless Community Networks," Journal of Peer Production, volume 6, 1-11

Dulong de Rosnay M., 2015. "Peer-to-peer as a Design Principle for Law: Distribute the Law," Journal of Peer Production, volume 6, 1–9.

Flanagan A.. 2012. Authorization and Licensing, in Walden I. (ed), Telecommunications Law and Regulation, Fourth Ed., Oxford: OUP, 277-356.

Flanagan A, 2012. Spectrum Management, in Walden I. (ed), Telecommunications Law and Regulation, Fourth Ed., Oxford: OUP, 2012, 357-396.

Giovanella F., 2015. "Liability Issues in Wireless Community Networks," Journal of European Tort Law, volume 6, number 1, 49-68

Giovanella F., Dulong de Rosnay M.. 2017 (forthcoming). "Community Wireless Networks, Intermediary Liability and the Mc Fadden Court of Justice of the EU case", Communications Law.

Hale R.V., 2005. "Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet," Santa Clara Computer & High Technology L.J., volume 21, number 3, 543-559

Hören T., Yankova S. 2012. The liability of internet intermediaries – the German perspective, International Review of Intellectual Property and Competition Law - IIC, 501-531

Husovec M, 2016. Holey Cap! CJEU Drills (Yet) Another Hole in the E-Commerce Directive's Safe Harbors, JIPLP (forthcoming), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843816

Kern B.D., 2004. "Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law," Santa Clara Computer & High Technology L.J., volume 21, number 1, 101-162

Kur A. 2014. Secondary Liability for Trademark Infringement on the Internet: The Situation in Germany and Throughout the EU, Columbia Journal of Law and the Arts, 525-540

Mac Síthigh D., 2009. "Law In The Last Mile: Sharing Internet Access Through Wifi", SCRIPTed, volume 6, number 2, 355-376

Donati F.. 2009. La riforma della disciplina comunitaria in materia di gestione dello spettro radio, in Morbidelli G., Donati F. (eds.), La nuova disciplina delle comunicazioni elettroniche, Torino: Giappichelli, 101-116

Robert R., Manulis M., De Villenfagne F., Leroy D., Jost J., Koeune F., Ker C., Dinant J., Poullet Y, Bonaventure O., and Quisquater J., 2008. "WiFi Roaming: Legal Implications and Security Constraints," International Journal of Law and Information Technology, volume 16, number 3, 205-241

Walden I., 2012. European Union Communications Law, in Walden I. (ed), Telecommunications Law and Regulation, Fourth Ed., Oxford: OUP

The netCommons project

December 22, 2016

netCommons-D4.1-1.0

Horizon 2020