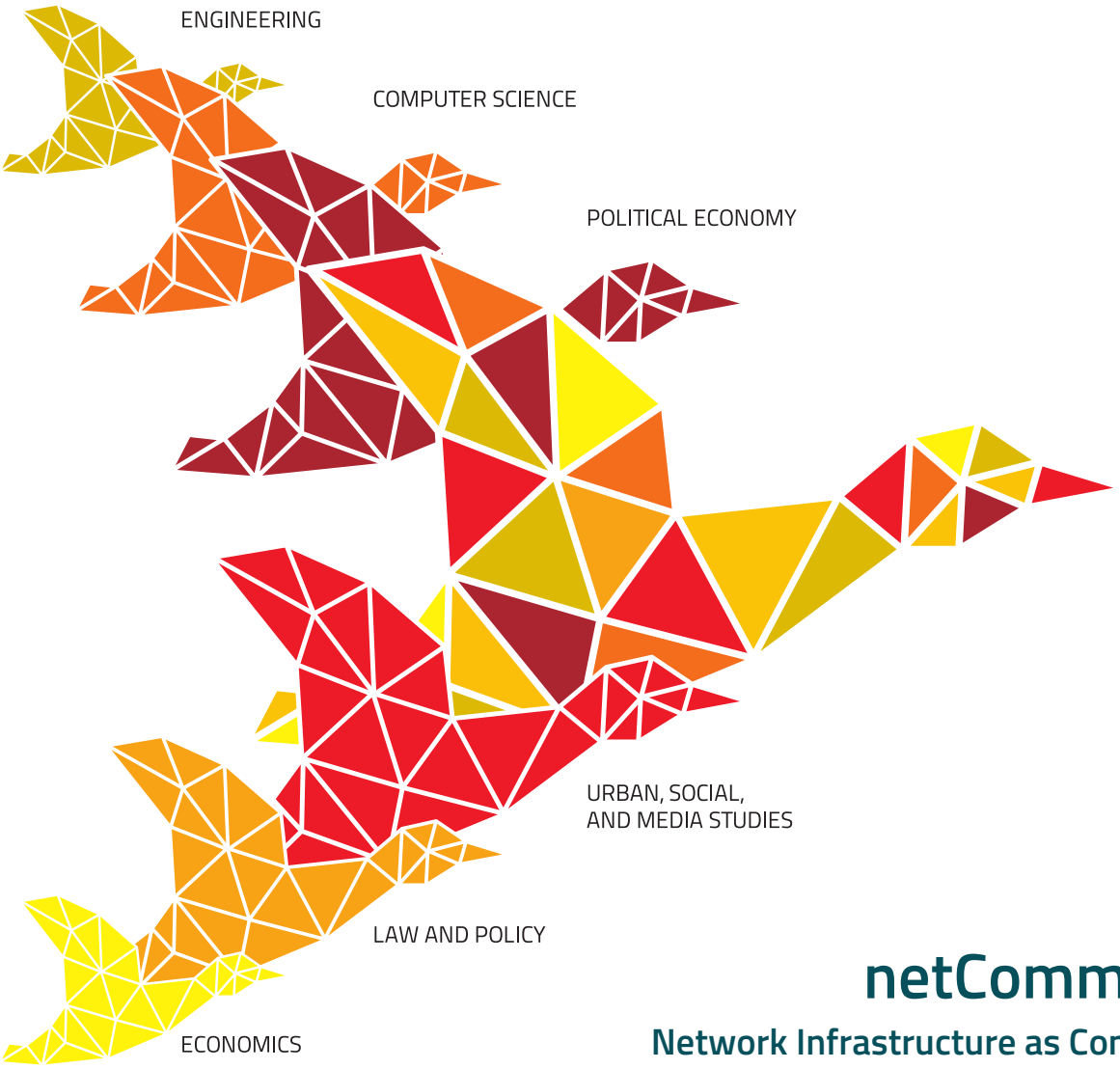


netCommons

Network Infrastructure as Commons

European legal framework for CNs (v3)

Deliverable Number D4.3
Version 1.2
August 23, 2018

netCommons.eu

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:	Virginie Aubree, UniTN
Deliverable nature:	Report (R)
Dissemination level:	Public (PU)
Contractual Delivery Date:	June 30, 2018
Actual Delivery Date	August 23, 2018
Number of pages:	126
Keywords:	community networks, legal framework
Authors:	Virginie Aubrée, UniTN Melanie Dulong de Rosnay, CNRS Federica Giovanella, UniTN Arthur Messaud, CNRS Felix Tréguer, CNRS
Peer review:	Maria Michalis, UoW Roberto Caso, UniTN Renato lo Cigno, UniTN

History of Revisions

Rev.	Date	Author	Description
v0.1	12/04/2018	Virginie Aubrée	First draft
v0.2	20/04/2018	Melanie Dulong, Felix Tréguer	review of the first draft
v0.5	5/05/2018	Virginie Aubrée	finalising chapter two on the European framework
v0.6	17/05/2018	Melanie Dulong, Felix Tréguer	review on Chapter two and five
v0.7	29/05/2018	Renato lo Cigno	review on the structure of D4.3
v0.8	6/06/2018	Melanie Dulong	work on Executive summary and conclusion
v0.9	27/06/2018	Félix Tréguer	work on introduction and conclusion, general review and formatting
v1.0	29/06/2018	Virginie Aubrée	implementation of comments from peer review
v1.1	26/07/2018	Virginie Aubrée, Mélanie Dulong de Rosnay, Félix Tréguer	added section on EU Code of Electronic Communication which had been obtained in June and general review
v1.2	20/08/2018	Virginie Aubrée, Félix Tréguer, Renato Lo Cigno	Final proofreading, impact of the work and harmonization with other deliverables

Executive summary

Community Networks are network infrastructures built by local people providing access to the global Internet and other services. Their model is based on democratic governance, infrastructure managed as commons and promotion of digital human rights. Their existence and the non-mainstream way in which they conduct their activities fall within the scope of several areas of law, all over the European Union.

As we explain in the **introduction**, this deliverable builds on legal research conducted over the past two years by the netCommons team in the context of Work Package 4. The first deliverable of the task related to the "European legal framework for CNs" focused on a description of the existing laws [1], the second one updated this mapping and emphasises the actual behaviour of CNs regarding this framework [2]. This final deliverable of this task takes over the findings of these two previous deliverables, updating and deepening them throughout more formal guidelines to respect the applicable law and will also describe various advocacy activities aimed at influencing the current legal framework.

Deliverable 4.3 is thus composed of two parts: a descriptive one, and the presentation of the active role played by netCommons, in coordination with CNs, regarding the legal framework and its interpretation.

Chapter 2 is the core of the "descriptive research". It offers a final update of the European legal framework, including current ongoing changes that were left out for further analysis in the previous two deliverables. It covers four main topics that are key to the activity of CNs: 1) civil liability, 2) data protection law, 3) data retention law, and 4) telecommunication law. This chapter highlights some important results of netCommons efforts and collaboration with Community Networks and digital rights groups, as we successfully weighed in the legislative process on the European Code of Electronic Communications over the past year. The last working (but almost final) versions of this pending legislation seen by our legal team indeed provide special rules for Community Networks. This means that in the future, the special regulatory needs of CNs will have to be taken into account by telecom policy-makers at both the EU and national levels. In this section on the applicable legal framework, we have also developed a more substantial analysis on data retention law, which the survey conducted last year proved to be a problematic issue for many CNs.

Under European law, CNs can both be regarded as 'electronic communications services' and 'electronic communications network'. They can also be regarded as providers of an 'information society service' –depending on national implementation. Moreover, since CNs usually need to replace the software included by the manufacturer in radio hardware with open software, the application of the directive on 'radio equipment' may involve legal difficulties. Indeed, its requirements might impair the possibility to modify the software included in the hardware.

Regarding civil liability, providers can be held liable only if they do not comply with specific behaviours requested of them by law. These behaviours vary depending on the different roles played by CNs, which can qualify as *mere conduit*, *caching* or *hosting* providers. For instance, hosting providers can be held liable if they do not remove an allegedly illegal piece of information when such information is notified by a third party (e.g., a user of their services). Such an obligation to remove online content is applicable to any kind of data, regardless of the source. This means that, in our case, it does not matter whether the data to be removed comes from within a CN or not, as long as it is hosted within the networks and to the extent that the CN and the persons responsible for it can take active steps to take the targeted content down. Furthermore, in the context of open WiFi networks, CNs can be held liable if they do not comply with an injunction measure requiring to prevent third parties from engaging in copyright infringement. According to the Court of Justice of the EU, such measures might involve setting up passwords so that users "are required to reveal their identity in order to obtain the required password and may not therefore act anonymously" (for details, see the *McFadden* ruling of the Court of Justice of the European Union (CJEU), described in Sec. 2.1.1).

Concerning data protection law, we give an overview of the framework of the General Data Protection Regulation (GDPR) regarding the processing of personal data, which will inform upcoming guides to be written by the team on this very issue. An analysis on data retention was added in the light of the Tele2 case law of the

Court of Justice of the European Union, where we touch on the actual application of this legal framework by and within Community Networks.

Chapter 3 provides an overview of the "actual practice" of CNs regarding these legal requirements. Here too, we update the results of the survey conducted last year for D4.2 and offer a more extensive analysis of the results. This study gathers replies of CNs from six EU countries (France, Italy, Germany, Greece, Portugal and Slovenia). It focused on five main areas: organisation, services offered, relationship with users, data protection and data retention law. About organisation, it was highlighted that most respondents are organised as an association. Yet, some of them do not have a legal form, enjoying the informal relationship allowed by this kind of structure. This idea is in line with the way decisions are taken in these structures (consensus-driven). In this regard, all respondents acknowledged the importance of a distribution of power and a horizontal approach as well as a participative and collective decision process within the community. Regarding services provided by CNs, the core of their activity is to provide an Internet access (through WiFi mostly, but sometimes through optical cables too). However, they very often offer several additional services such as hosting, e-mail or Tor node services which can imply extra subtleties in terms of civil liability.

Concerning the nature of the relationship with users, the 'informal' relationship is also favoured. The results of the survey we conducted show that most of the respondents do not use a contractual form to enter in contact with their users. However, there is a different kind of proximity built with the user since there is often a requirement to be a member of the community in order to access to the service provided. This implies a flexible and trust-based relationship with the users. Yet, it can create difficulties regarding data protection law. Besides, CNs tend to highly favour privacy in their relationship with their users.

This concern is also shown though their data retention habits, as a large part of the respondents declared that they do not retain any data. A minority of the respondents, however, retain data in compliance with their national laws. According to our analysis, these national laws are often not in compliance with European law. As for data protection law, CNs did not seem to be aware of the wide scope of the notion 'personal data' and the deliverable recommended that they anonymize data to avoid non-compliance with data processing requirements'.

We then move to more "active research" reported in two other chapters.

Chapter 4 presents specific legal guidelines so that community networks can comply with their current legal requirements. These guidelines refine those previously drafted in D4.1 and D4.2 in order to offer to CNs a clearer view on their compliance.

- Civil liability has proved to be a problem for a number of CNs, particular in Germany where Freifunk participants for years had to deal with the risk of third party infringement (people accessing the open Freifunk networks to share copyrighted works, which in turn motivated right-holders to sue people sharing their connections). In Germany, Freifunk and its allies successfully campaigned for a change in the legal framework, which is not perfect but significantly reduce the legal risk. Although our joint advocacy efforts around the European Code of Telecommunications failed to create a liability exemptions for people sharing their connections, we feel that, generally speaking, even the McFadden case law of the Court of Justice of the European Union does not entail strong legal risks for users sharing their wireless connection with their vicinity. CNs enacting special privacy and anonymity protections by running VPNs or relays for the TOR networks should also feel free to do so.
- Data protection should be a significant concern for EU CNs in the months to come, especially in light of the increased sensitivity to this issue in the wake of the implementation of the General Data Protection Regulation. To ensure the lawfulness of personal data processing, including security measures and transfer of data, anonymising and pseudonymising data as much as possible, and various strategies such as mapping existing practices related to data processing, and ad hoc processes to manage potential data leaks and inform users are urgently called for.
- Although we make these recommendations with a degree of cautiousness considering the commitment of some CNs to informal organization processes, we feel however that entering into a contract with the users of CN's services can be an interesting solution to mitigate the risks associate with the applicable liability

regime as well as the data protection framework. For the same reasons, incorporating a CNs through a non-profit legal status will also help alleviate legal risks and clarify the distribution of liability within the community, so that it can reflect on these risks and anticipate them rather than act in the context of a legal crisis.

- On data retention, CNs face a particularly thorny issue considering the legal limbo surrounding these legal obligations established across Europe to facilitate law enforcement. Given the 2014 and 2016 rulings of the Court of Justice of the EU, which invalidated obligations for indiscriminate, blanket data retention, 17 Member States are, according to our analysis, still in breach of this crucial case law. Although netCommons has helped establish a Europe-wide advocacy and litigation effort on the issue, it will probably be months, or years, before all ambiguities are finally resolved. In the meantime, we have highlighted various strategies that we have observed in the course of research, inviting CNs to choose that which they deem to be most appropriate. These strategies range from the most ”conservative” (i.e. deciding to respect national law at the expense of the right to privacy as construed by the ”Supreme Court” of the EU in its case law), to the most ”activist” (i.e. defying national law while invoking this European case-law to highlight the lack of regard of national lawmakers for EU law and fundamental rights, which bears the risk of litigation and, possibly, fines or even jail).

This part should be regarded as both transitory and complementary with the advocacy work presented in the Chapter 5, and a milestone as we move towards general guidelines with Deliverable 4.5 due for month 36 of the netCommons project.

The second part of active research is reported in Chapter 5. This chapter is complementary to D1.5 [3] and relies on its conceptual framework and its recommendations regarding advocacy. This part of the deliverable also details several actions based on litigation, advocacy or dissemination intended to create a better legal and practical framework for CNs. It provides an overview of our interactions with various CNs as well as policy-makers over these issues in the past months.

The last two chapters of the deliverable, Chapter 6 and 7 respectively, summarize the impact of the work done in Task 4.1 and draw a general conclusion on the state of the art concerning the interaction of the law with the right to digital communications and grassroot initiatives to secure this right to citizens.

Contents

List of Figures

List of Acronyms

BEREC	Body of European Regulators for Electronic Communications
BEUC	Bureau Européen des Unions de Consommateurs
BNetzA	Bundesnetzagentur
CEF	Connecting Europe Facility
CJEU	Court of Justice of the European Union
CN	Community Network
DPA	Data Protection Authority
DPO	Data Protection Officer
ECS	Electronic Communication Service
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
EECC	European Electronic Communications Code
FCC	Federal Communication Commission
FSFE	Free Software Foundation Europe
GDPR	General Data Protection Regulation
IAP	Internet Access Provider
ICT	Information and Communication Technologies
INEA	Innovation and Networks Executive Agency
ISM	Industrial Scientific Medical
ITU	Innovation and Networks Executive Agency
ITU	International Telecommunication Union
LTE-U	Long Term Evolution–Unlicensed
MEP	Member of the European Parliament
NGO	non-profit organisation
NRA	National Regulatory Authority
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PNRF	Piano Nazionale di Ripartizione delle Frequenze
RSPG	Radio Spectrum Policy Group
RSPP	Radio Spectrum Policy Programme
TFEU	Treaty on the Functioning of the European Union
TKG	Telekommunikationsgesetz
TMG	Telemediengesetzes
ToS	Terms of Service
TTE	Transport, Telecommunications and Energy

URL Universal Resource Locator
VwGO Verwaltungsgerichtsordnung

1. Introduction

This deliverable offers an overall analysis of the European legal framework for these small yet major actors of alternative Internet. Concluding Task 4, it relies on:

- the mapping of EU and relevant national law drafted in D4.1 [1];
- the results of the survey about CNs' practices and their analysis in D4.2 [1];
- the findings about advocacy from D1.5 [3];
- the final report on the governance instruments for Community Networks (CNs) D1.4 [4].

In continuation of these works, this deliverable provides synthetic guidelines for CNs to cope with legal hurdles. Aiming more generally to promote a legal framework favouring community networks, this conclusive report is also built in cooperation with WP1. In this regard, it delves into the active role played by the netCommons research team concerning advocacy.

This final year of research is divided in two parts. The first one, illustrated by the present deliverable, should be regarded as the final update of D.4.1 and D.4.2. Altogether, these 3 reports are the basis upon which the legal and policy part of a 'Best Practice guide' will be built (in D4.5 at M36), as the achievement of our research, to allow the sustainability and swarming of CNs.

A first introductory part offers a quick reminder of the findings of the two previous deliverables (D4.1 and D 4.2). It specifies the goal and structure of this report and explains choices that were done in that respect. The research activities undertaken during M25–M30 for the Task 4.1 are presented through two main parts.

Part one intends to be a descriptive actualization of the relevant legal framework for CNs. After having described the legislation applied to CNs, this part goes through the current practice of their activity. It analyses, above all, the evolution of their behaviour during these three years of research and interaction with the netCommons project. The results of the survey and interviews conducted in 2017 will be analysed afresh, in light of these new legal findings, and also with the knowledge provided by the wider survey analysis reported in D5.4 [5].

Part two details the active role played by CNs and members of the project in order to influence the existing legal framework. It is comprised of all the advocacy work for which we provided assistance to the communities. It also includes overall legal guidelines. These would be some preliminary guidelines, which will be incorporated in the final deliverable of WP4 (D4.5), the best practice guide due for M36. This part can also be regarded as a continuation of the D1.5 since it relies on its theoretical and conceptual framework. Moreover, D4.3 is in line with its strategy of 'finding a common voice' for community networks and enumerates several advocacy actions in coordination with CNs in order to promote changes in the legal framework described.

1.1. D4.1: Mapping of the legal framework

In order to map the legal requirements that community networks have to comply with, D4.1 focused on three main areas: Telecommunication law, civil liability and data protection law.

Regarding telecommunication law, D4.1 presented the cornerstone definitions of European telecom law and how those should apply to CNs. It states that CNs can both be regarded as 'electronic communications services' and 'electronic communications network'. They can also be regarded as services providers of an 'information society service' –depending on national implementation. Moreover, since CNs usually need to replace the software included by the manufacturer in radio hardware, with open software the application of the directive

on 'radio equipment' may involve legal difficulties. Indeed, its requirements might impair the possibility to modify the software included in the hardware.

Regarding civil liability, providers can be held liable only if they do not comply with specific behaviours requested of them by law. These behaviours vary depending on the different roles played by CNs, which can qualify as *mere conduit*, *caching* or *hosting* providers. For instance, hosting providers can be held liable if they do not remove an allegedly illegal piece of information when such information is notified by a third party (e.g., a user of their services). Such an obligation to remove online content is applicable to any kind of data, regardless of the source. This means that, in our case, it does not matter whether the data to be removed comes from within a CN or not, as long as it is hosted within the networks and to the extent that the CN and the persons responsible for it can take active steps to take the targeted content down.

Furthermore, in the context of open WiFi networks, CNs can be held liable if they do not comply with an injunction measure requiring to prevent third parties from engaging in copyright infringement. According to the Court of Justice of the EU, such measures might involve setting up passwords so that users "are required to reveal their identity in order to obtain the required password and may not therefore act anonymously" (for details, see the *McFadden* ruling of the CJEU, described in D4.3 Sec. 2.1.1).

Concerning data protection law, D4.1 described the whole framework of the GDPR regarding the processing of personal data.

Considering the ongoing changes initiated by the European Electronic Communications Code (EECC) –and despite our engaging in collaboration with CNs involved in policy advocacy –, telecommunication law was set aside in our analysis during the second year of research up until these changes become reliable enough to be usefully analysed (the legislative process is ending as we conclude D4.3 and an overview of the main changes is offered in this deliverable). The ambitious directive establishing this Code will aim at merging the four main existing texts on telecommunications law:

- the 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;
- the 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;
- the 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;
- the 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.

Delaying the analysis of this reform provided better hindsight to evaluate the advocacy work conducted by netCommons. This way, new provisions could be compared with the letter to EU policy-makers as well as notes and voting recommendations delivered to Member of the European Parliaments (MEPs) (see D4.2, 3.1 p.48).

Conversely, an analysis on data retention was added to D4.1 in the light of the Tele2 case law of the Court of Justice of the European Union. It then emphasised the study of the actual application of this legal framework by and within Community networks.

The first deliverable mapping the legal framework of community networks will be summarized and updated below (see, Chapter 2).

1.2. D4.2: Table of practices of CNs

The survey conducted in 2017, prepared thanks to in-depth interviews of two CNs, led to an analysis of their behaviour regarding their legal obligations.

First, interviews were conducted with two community networks with two very different governance model: a

French one very structured, and an Italian one with a more informal approach. These interviews with two polar opposite models of CN were the basis upon which a wider questionnaire was created and later circulated among CNs and their members.

Conducted with a degree of anonymisation, this study gathered replies of CNs from six EU countries (France, Italy, Germany, Greece, Portugal and Slovenia). It focused on five main areas: organisation, services offered, relationship with users, data protection and data retention law.

About organisation, it was highlighted that most respondents are organised as an association. Yet, some of them do not have a legal form, enjoying the informal relationship allowed by this kind of structure. This idea is in line with the way decisions are taken in these structures (consensus-driven). In this regard, all respondents acknowledged the importance of a distribution of power and a horizontal approach as well as a participatory and collective decision process within the community.

Regarding services provided by CNs, the core of their activity is to provide an Internet access (through WiFi mostly, but sometimes through cabled (mostly optical) networks too). Although, they very often offer several additional services such as hosting, e-mail or Tor node services which can imply extra subtleties in terms of civil liability.

Concerning the nature of the relationship with users, the 'informal' relationship is also favoured. The results show that most of the respondents do not use a contractual form to enter in contact with their users. However, there is a different kind of proximity built with the user since there is often a requirement to be a member of the community in order to access to the service provided.

This implies a flexible and trust-based relationship with the users. Yet, it can create difficulties regarding data protection law. Besides, CNs tend to highly favour privacy in their relationship with their users.

This concern is also shown though their data retention habits, as a large part of the respondents declared that they do not retain any data. A minority of the respondents, however, retain data in compliance with their national laws. According to our analysis, these national laws are often not in compliance with European law.

As for data protection law, CNs did not seem to be aware of the wide scope of the notion 'personal data' and the deliverable recommended that they anonymize data to avoid non-compliance with data processing requirements'.

2. Three years of a European Legal Framework for Community Networks

As part of the description of the European legal framework for community networks, reminders and updates in four main area appear relevant: Civil liability (Sec. 2.1), data protection law (Sec. 2.2), data retention law (Sec. 2.3) and telecommunication law (Sec. 2.4). In this perspective, we mostly study EU law and several implementations at the national level. We focussed on France, Italy, Spain, and Germany were CNs are very active.

Moreover, in these countries the framework is particularly topical, explanatory and influential.

Beside, if the case of **Greece** was less involved in this deliverable, a **dedicated workshop** was set up in July 2018 in Athens[1]. Thanks to this event we will be able to understand specific issues and stakes in this national framework and, therefore, be able to provide guidelines and targeted legal support. Moreover, we could open the dialogue with the national telecommunication regulator and directly raise its awareness on these four following issues.

2.1. Civil liability

For civil liability, this section substantially reiterated the findings of D4.1 regarding the *McFadden* case law of CJEU (Sec. 2.1.1) as well as national frameworks, along with updates as of June 2018 (Sec. 2.1.2).

2.1.1. Unresolved questions raised by the McFadden case law

As it is a **preliminary ruling**, a special procedure under the article 267 of the Treaty on the Functioning of the European Union (TFEU)[2], this case law reply to a case-oriented question and is a **very compact abstract** answer to the case presented. Moreover, as this ruling stands alone on the subject in EU law, this case still raises important issues regarding its interpretation[3].

2.1.1.1. Facts of the case

On September 15, 2016, the CJEU adopted a decision in a case that could potentially affect any CN in Europe (C-484/14, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*). 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** free of charge. Access to the 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 formal 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

[1] See https://www.netcommons.eu/?q=content/new-eu-telecommunications-code-greece-and-its-effect-community-networks

[2] For a clear introduction, see https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14552&from=EN

[3] On this subject, see See: Federica Giovanella, Melanie Dulong de Rosnay. Community wireless networks, intermediary liability and the McFadden CJEU case. Communications Law, Bloomsbury, Wiley, 2017, 22 (1), pp.11-20.https://halshs.archives-ouvertes.fr/halshs-01478116/document

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[4]. 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 former German Tele-Media Act (*Telemediengesetz*).

2.1.1.2. Pre-Mc Fadden ruling: the contrary doctrine of Störerhaftung

Prior to the *Mc Fadden* case, a form of strict liability existed in Germany regarding third-party copyright infringement: the so called doctrine of *Störerhaftung*[5]. Meaning literately *"liability of the interferer"*[6], it implied that private individuals could be held liable for unlawful actions done by third-party through their unsecured WiFi connection.

However, this doctrine only concerns **injunctions**, an order from the judge to stop an infringing activity[7], and to be pronounced, they should fulfil three cumulative conditions[8]

- There shall be an **adequate causal contribution** to the activity of the infringing party;
- There must have been a **legal and factual possibility to avoid** the third party's infringement;
- The subject must have violated a reasonable **duty of care** or a duty to monitor aimed at preventing infringements.

Yet such a liability was regarded as contrary to the limitation set out for "provider of information society services" by article 12, Directive 2000/31, as described in the Mc Fadden case below.

2.1.1.3. Answer to the preliminary ruling

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?**

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=FR

[5] For a deeper analysis see D4.1 Sec. 3.3.2, p.37

[6] See Hören T., Yankova S. 2012. The liability of internet intermediaries – the German perspective, International Review of Intellectual Property and Competition Law – IIC, 501-531, and more precisely 511-518; 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, more precisely 532.

[7] Federica Giovanella and Melanie Dulong de Rosnay, Community wireless networks, intermediary liability and the Mc Fadden CJEU case, Communications Law. The Journal of Computer, Media and Telecommunications Law, Vol. 22, No 1, 2017, pp. 11-20. https://halshs.archives-ouvertes.fr/halshs-01478116

[8] 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, p. 3.

2. **What measures should a provider adopt to avoid liability for third party's intellectual property rights infringement through WiFi networks?**

2.1.1.3.1 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 TFEU ***"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 [9].

2.1.1.3.2 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 WiFi 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[10] and 2004/48[11] –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.

2.1.1.3.3 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

[9] 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, see p. 3.

[10] 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, 10–19.

[11] 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, 45–86.

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 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.

2.1.1.3.4 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.

2.1.1.4. 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[12] considered the provision to be applicable.

Even though Mr Mc Fadden did not gain any profits from the offer of WiFi 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 WiFi 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. I n 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.

[12] Opinion of the Advocate General Szpunar in the case C-484/14, Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH, par. 34-56; http://curia.europa.eu/juris/document/document.jsf?docid=190593&doclang=EN

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[13].

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 WiFi connection[14].

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[15]. The Advocate considered the obligation to make WiFi 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 WiFi would need identification and entering a password. The Advocate makes the clear example of fast-foods[16].

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[17].

2.1.1.4.1 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

[13] Husovec, Martin, Holey Cap! CJEU Drills (Yet) Another Hole in the E-Commerce Directive's Safe Harbors (September 26, 2016). Forthcoming, Journal of Intellectual Property Law & Practice (JIPLP). Available at SSRN:https://ssrn.com/abstract=2843816

[14] 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.

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

[16] 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 WiFi connections

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

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[18]. 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"[19].

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"[20]. 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[21].

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 McFadden).

Would it for a CN –or for anyone providing a gateway to the Internet– 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, which will be described below.

2.1.2. National frameworks

2.1.2.1. Germany

As foreseen in D4.1, the German scenario was influenced by the Mc Fadden decision. Indeed, the doctrine of *Störerhaftung* was dismissed by the third amendment of the Telemedia Act (*Telemediengesetzes (TMG)*) which have entered into force on October 13, 2017[22]. Its part 3, on liability (*Verantwortlichkeit*), states general principles (§7).

More precisely, its article §7 (4) provides that if a **Telemedia service of a service provider**, namely *"any natural or legal person who holds own or third party telemedia for use or provides access to the use"*[23], has been used by a user to infringe one's intellectual property rights, an injunction of blocking the use of information in order to prevent the repetition of the infringement can be demanded, provided that:

- The owner of this right has **no other means of remedying** the infringement;
- The blocking must be **reasonable and proportionate**.

Yet, it is limited to the extent that:

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

[19] 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; http://curia.europa.eu/juris/document/document.jsf?text=&docid=181465&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=554492

[20] 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.

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

[22] See the text currently in force, in German, here: https://dejure.org/gesetze/TMG

[23] See, Article 2 of this law. Available in German, here: https://dejure.org/gesetze/TMG/2.html

- **In principle**, there is **no liability** of Telemedia service providers for third-party copyright infringement, that is to say no obligation to reimburse "preliminary and extra-judicial costs[24]" in the hypothesis above-described.

Then, specific provisions frame **exceptions to this principle** concerning liability in case of transmission (*Durchleitung von Informationen*, §8), caching (*Zwischenspeicherung*, §9) and storage (*Speicherung*, §10) of information.

2.1.2.1.1 Transmission of information

Service providers are not responsible for third-party information that they transmit or provide access to in a communications network, as long as they fulfill three cumulative requirements:

- They **do not cause the transmission**,
- **The addressee** of the transmitted information **is not selected**,
- They do **not select or change** the information provided.

2.1.2.1.2 Caching of information

Service providers are not responsible for any automatic, temporary caching that is solely for the purpose of making the transmission of third-party information to other users more efficient at their request, provided that they follow five cumulative requirements:

- They do **not change the information**,
- They comply with conditions of access to the information,
- They comply with rules for updating the information set in widely recognized and used industry standards
- They do **not interfere with the permitted** use of technologies for the **collection of data on the use of information** specified in widely recognized and used industry standards,
- They **act promptly to remove or block access** to information held in accordance with this provision as soon as they have become aware that the information has been removed from the network at the original place of origin or access to it has been blocked, or a court or administrative authority has ordered the removal or blocking.

2.1.2.1.3 Storage of information

Service providers are not responsible for third-party information that they store for a user, as long as, alternatively:

- They have **no knowledge of the unlawful act or information** and, in the case of claims for damages, they are not aware of facts or circumstances from which the unlawful act or information becomes apparent, **or**
- They **have acted promptly to remove** the information or to block access to it as soon as they have gained this knowledge.

2.1.2.1.4 Application of the new version of the Telemedia Act

On March 13 2018, The Higher Regional Court of Munich (*Oberlandesgericht München*(Oberlandesgericht (OLG)) München) issues a decision[25] regarding the application of this new law – in the national case involving

[24] Free translation of §7 (4) 3. **"vor- und außergerichtlichen Kosten** für die Geltendmachung und Durchsetzung des Anspruchs"

[25] The full-text of the decision is available in German here: http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-003015?hl=true

Tobias Mc Fadden. Partly confirming the lower Court's judgement of May 2017[26], OLG München considers that the third amendment of the Telemedia Act – and thus the repeal of the Störerhaftung's doctrine – only applied for requests lodged from October 12, 2017, date of entering in force of these new provisions. Therefore, even if the German framework has been reformed, the temporal scope of the old doctrine of liability is broadly interpreted and as such was partly applied to Mc Fadden in the end.

In line with this case law, on July, 26 2018, the Federal Court (*Bundesgerichtshof*) issued an important decision – not yet available in full-text. This case-law reviews a concerning decision[27] of the Higher Regional Court of Düsseldorf (*Oberlandesgericht (OLG) Düsseldorf*).

In 2011, the claimant – a copyright owner – have sent cease-and-desist letters to the defendant – which operates several hotspots as well as Tor exit nodes. These letters demand him to take measures against the infringement of his rights on a program offered via the defendant's Internet connection through a Peer-to-Peer network. Confirming the lower Court's decision, OLG Düsseldorf considers that:

- the defendant is obliged to secure its connection by a password, following CJEU's view on the balance of fundamental rights to be adopted (§18);
- Hotspots and Tor exit nodes should not be distinguished, except in terms of security measures as blocking Peer-to-Peer software would be regarded as a reasonable measure to take for a Tor server (§26).

As the Federal Court's decision is not available yet, a proper analysis should not be provided. However, its official press-release[28] stated that part of the judgment was remanded to the Higher Regional Court, so that it could examine whether the plaintiff is entitled to demand that the defendant block information pursuant to §7 (4) TMG (mentionned above). Thus, The final decision on this case should be closely monitored in the coming months.

2.1.2.2. France

In France, Internet access subscribers shall ensure that their access is not used for the unlawful reproduction, publication or communication of copyrighted works[29]. 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**[30]. 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[31].

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).

[26] The full-text of the decision is available in German here: http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2017-N-116901?hl=true

[27] See the full-text in German: https://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2017/I_20_U_17_16_Urteil_20170316.html

[28] http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=85948&linked=pm

[29] Code de la propriété intellectuelle, article L336-3 https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000020738731&dateTexte=

[30] Code de la propriété intellectuelle, article L331-25 https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000020738173

[31] Code de la propriété intellectuelle, article R. 335-5 https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000022393991

2.1.2.3. Italy

In Italy, the analysis to be conducted shall include the three scenarios:

1. User's liability,
2. ISP's liability,
3. CN's liability.

Starting with **user's liability**, the applicable rules are those for general liability in tort (article 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 WiFi". Quite the opposite, in the last few years the policy towards WiFi 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[32]. 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[33]. 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 WiFi 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 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[34].

[32] 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.

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

[34] Giovanella F., 2015. "Liability Issues in Wireless Community Networks," Journal of European Tort Law, volume 6, number 1, 49-68, especially 54-55 and 61-63.

2.2. Data protection

This section substantially reiterated the findings of D4.1 regarding the framework and supervision of GDPR (Sec. 2.2.1) and D4.2 about the complementary proposal for the ePrivacy regulation –which was updated in light of negotiations conducted during January-June 2018 (Sec. 2.2.2).

2.2.1. The reform of the GDPR

Entering into force on May 25, 2018, the framework of the new general data protection regulation (GDPR – Regulation (EU) 2016/679) reforms numerous requirements and principles, including consent and sanctions (see, D4.1, p. 43). The GDPR will be directly applicable in all Member States and, as such, will also replace most of national data protection law.

It states a specific conceptual framework (Sec. 2.2.1.1), as well as targeted obligations (Sec. 2.2.1.2). The GDPR introduces a number of specific terms that precisely define the framework of application, and identify subjects and objects falling within the scope of this regulation[35]. In particular it is important to clearly focus the **data subject**. The data subject is "*a natural person whose personal data is processed by a controller or processor*". It is of the utmost importance, to fully understand this document and the GDPR, to keep in mind that the final goal of the entire regulation is protecting "data subjects".

2.2.1.1. Key definitions

It was highlighted in the survey conducted last year (see D4.2 or Sec. 3.2) that it was difficult for CNs to distinguish between the different form of data they are processing while providing Internet access or services to their users. Therefore, it seems appropriate to provide several cornerstone definitions, stemming from the **article 4** of this regulation. This implies to clarify data typology (Sec. 2.2.1.1.1) and players involved in processing (Sec. 2.2.1.1.2).

2.2.1.1.1 Typology of data

First, a clear distinction should be done among different kind of data.

Personal data are any information relating to an individual and which may be attributed to this individual. The scope is **very wide**[36] and **often underestimated** by communities. To be specific, it implies:

> "*any information relating to an identified or identifiable **natural person** ('data subject'); an identifiable natural person is one **who can be identified, directly or indirectly,** in particular by reference to an identifier such as a name, an identification number, location data, an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*"

Thus, data such as name, surname, dynamic and static IP address, e-mail address, phone number etc. should be regarded as personal data[37].

Conversely, **anonymous data** are any information relating to an individual, but which cannot be attributed to this individual. No legal requirement is attached to such data.

[35] All the terms are specified in the GDPR, but to disambiguate terminology in this document the glossary available at https://www.eugdpr.org/glossary-of-terms.html is sufficient.

[36] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 4; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[37] *Ibid.*

In between, **pseudonymised data** refers to "*personal data that can **no longer be attributed to a specific data subject without the use of additional information**, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*"[38].

Thus, to avoid the scope of "personal data" which implies heavy requirements, two process can be implemented: **anonymisation** or **pseudonymisation** of data (see, Sec. 4.1.2).

Moreover, special categories of personal data are addressed with specific concerns, due to their high degree of privacy requirements (for instance genetic or biometric data and data concerning health).

2.2.1.1.2 Typology of players

Numerous players are identified as being related to a processing of such data. Two mains players in terms of data protection law are the controller and the processor who are complementary.

- A **controller** is a "*natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing** of personal data*"[39].
- A **processor** means a "*natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller***".[40]

Simply put, a controller designs and plans the processing, while the processor is the one who concretely executes it.

However, a processing can involve other players called **third party**. They are any natural or legal person, public authority, agency or body apart from the data subject, controller, processor and persons *"who, **under the direct authority of the controller or processor**, are authorised to **process personal data***". It may refers, for instance, to subcontractor.

Finally, the concept of **recipient** should be emphasized. A recipient is any kind of person "*to which the **personal data are disclosed***". They can be a third party or not[41].

The application of regulatory obligations weighs differently on each corresponding player.

2.2.1.2. The framework of the GDPR

Community Networks 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 (regarding data retention legal framework, see Sec. 2.3). CNs may also provide other services, such as email or hosting services.

Each of these activities raises privacy-related issues which should be compliant with the new framework. Some of these issues are associated to all of these activities (Sec. 2.2.1.2.2) while others are specific to each of them (Sec. 2.2.1.2.1). In both cases, CNs may consider dealing with these issues through collective adjustments

[38] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 4; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en ; even though the meaning of "pseudonymisation" is discussed, see e.g., Mourby et al. "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK" https://www.sciencedirect.com/science/article/pii/S0267364918300153

[39] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 4; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[40] *Ibid.*

[41] *Ibid.*

in light of these requirements. In this regard, D4.1's analysis on decentralized network is reiterated below (Sec. 2.2.1.4).

2.2.1.2.1 General obligations: 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[42]. A processing is lawful where these cumulative requirements are fulfilled:

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

In turn, a purpose may be lawful in **three** cases.

First, a purpose is lawful if it pursues a **legitimate interest**[43]. 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 Authority (DPA) and the Court of Justice of the EU have yet to provide clear and general criteria for balancing the different interests at stake.

Second, a purpose is also lawful where data subjects **consent**[44] 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 fulfilled these cumulative requirements[45]:

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

Regarding this consent, data subjects may withdraw it at any time.

Third, five purposes are regarded as systematically lawful[46].

1. Performance of a contract with the data subject;
2. Implementation of pre-contractual measures requested by the data subject;
3. Compliance with a **legal obligation**;
4. Performance of a task carried out in the public interest;

[42] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), **Article 6**; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[43] *Ibid.*

[44] *Ibid.*

[45] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 7; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[46] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 6; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

5. Protection of the **vital interests** of any person.

Along with these general provisions and requirements for all kind of processing, specific obligations also apply.

2.2.1.2.2 Specific obligations

2.2.1.2.2.1. Security measures

Regarding security measures there are upstream (1) as well as downstream measures (2).

1. ***Preventing accidental and unlawful processing.***

   Controllers and processors shall implement appropriate technical and organisational measures to ensure an appropriate level of security[47], so 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. Here, 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 –even though appropriate measures to be implemented may vary depending on each of these activities.

2. ***Informing authorities and users in case of breach of security***.

   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 DPA within 72 hours[48] –or later if he/she 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[49]. This information shall be provided individually or, where this would involve disproportionate effort, through a public communication.

2.2.1.2.2.2. Relationship with data subjects

[47] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 32; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[48] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 33; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[49] *Ibid.*

1. ***Information of users.***

   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.

   Here, information means letting users know **how their data are processed**. The controller shall provide data subjects with the following information[50]:

   - 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[51]:

   - 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.

2. ***Rights of users (data subjects).***

   Data subjects have four main rights:

   a) **Right of access**[52] to the information already provided by the controller – as described above – and to obtain a copy of their personal data;

   b) Right to **data portability**[53] - 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);

   c) Right to **rectification**[54] of inaccurate personal data;

[50] *Ibid.*

[51] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 13; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[52] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 15; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[53] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 20; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[54] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection

d) Right to **erasure**[55] 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 lack of action and of his/her right to lodge a complaint with a DPA and to seek a judicial remedy. These requirements and procedures apply to every activity of CNs.

2.2.1.2.2.3. 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.**

2.2.1.2.2.4. Data protection Officer

In some cases, controllers and processors shall appoint an independent Data Protection Officer (DPO) who monitors compliance with the law and advises its employer[56]. 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"[57] of data subjects on a large scale. The meaning of "monitoring" remains unclear, but some of the

of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 16; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[55] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 17; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en

[56] *Ibid.*, art. 39.

[57] *Ibid.*, art. 37, 1. b).

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.**

2.2.1.2.2.5. 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[58]. The controller shall then consult its DPA where such assessment reveals a risk[59].

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"[60].

However, as CNs are offering Internet access and regular additional services –according to the survey conducted in 2017, mostly email or VPN services, see Sec. 3.2.2.1– they are not likely to be regarded as using "new technologies" or technologies resulting in some specific risks for data subjects.

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

Community networks may transfer some personal data outside the territory of the European Union in order to provide some services to their users. However, 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 five cases.

First, 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 United Kingdom has left the EU, it will probably be added to this list, since its data protection law is already similar to the EU law. Moreover, as of now, an agreement is currently being negotiated with Japan in order to find mutual adequacy[61].

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 a third-party country, like United States, 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.

[58] *Ibid*, art. 35.
[59] *Ibid*, art. 36.
[60] *Ibid*, art. 35, 1.
[61] See the joint press-release of May 31th 2018: http://europa.eu/rapid/press-release_STATEMENT-18-4021_en.htm

Therefore, adequacy decisions have little – if any – direct impact on CNs from a legal point of view. However, these decisions might go against the core values of Community Network by allowing the processing of personal data of their users by operators from countries where the legal framework is less protective in terms of privacy.

For instance, the European Commission has stated that any company located in the United States and subscribing to the "EU-U.S. Privacy Shield" is allowed to received personal data from the EU and, as such, is subject to specific obligations ensuring an adequate level of data protection. As an adequacy decision, this 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, including by French CNs, advocating that the adequacy decision of the European Commission fails to comply with the EU Charter of Fundamental Rights.

Second, aside from adequacy decisions, 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, cumulatively:

1. Ensures the protection of the transferred data and the enforceability of data subjects' rights; and
2. Has been **validated by a Data Protection Authority** or contains standard data protection clauses66 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.

Third, 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.

Fourth, 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 June 2018, none of these cases seems to apply to CNs activities.

Fifth and final, 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 DPA or containing standard clauses).

2.2.1.3. Supervision and liability under the GDPR

Each Member State provides for one or more **independent public Data Protection Authorities to monitor** the application of data protection law[62]. As mentioned above, CNs should consult the authority responsible for such monitoring in their respective State or area for any inquiry concerning their obligations.

Regarding liability, **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[63]:

- 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.

Furthermore, controllers and processors are liable for any damage a data subject has suffered as a result of an infringement of their obligations[64]. Finally, Member States law provide that judges may also impose fines or imprisonment.

2.2.1.4. Specific comments concerning decentralized networks

As pointed out thoroughly in D4.1 (Sec. 4.6) –and reiterated in this consolidated version– complying with all the above mentioned obligations 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.

2.2.1.4.1 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 (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.

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;

[62] The European Commission enumerates them here: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080
[63] GDPR, art. 83.
[64] *Ibid.*, art. 82.

- 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.

Concrete findings: *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.*

2.2.1.4.2 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.

Concrete findings: *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.

Concrete findings: *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).

Concrete findings: *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.*

2.2.2. Toward an ePrivacy regulation

As partly described in D4.2 (Sec. 2.1.4.1), on January 10, 2017 the European Commission published a proposal for an ePrivacy Regulation[65]. The Regulation will repeal and **substitute Dir. 2002/58/CE** on privacy and electronic communications. As it happened with the GDPR, the European legislator no longer proposes a directive, which should be transposed by Member States, but it rather introduces a Regulation that has direct applicability at the national level, with the clear aim of reaching a higher level of harmonisation amongst Member States. The proposal is part of the **Digital Single Market strategy**[66] of the EU and it constitutes ***lex***

[65] For an introduction see https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation; for the full-text of the proposal see https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN

[66] European Commission, "Press Release. Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions," Jan. 10 2017. http://europa.eu/rapid/press-release_IP-17-16_en.htm

specialis to the GDPR. Therefore, it will complement it as regards electronic communications data that qualify as personal data.

The proposal relies on some definition provided by the proposed European Electronic Communications Code (see below, Sec. 2.4.5, such as "electronic communications services" (art. 4(b) of the proposal) and it will apply to Over-The-Top Providers (OTT) as well.

In regard with CNs' obligations, art. 9 of the proposal clarifies that *"the definition of and conditions for consent provided for under Articles 4(11) and 7 of Regulation (EU) 2016/679/EU shall apply"*. There is therefore complete homogeneity between the two texts as for users' consent. The ePrivacy Regulation proposal also requires **consent to be the only legal basis for some specific processing** that can therefore be carried out only if and when the data subject's consent has been acquired.

Article 29 Working Party[67] has expressed its concerns and recommendation regarding this proposal[68] as well as European Data Protection Supervisor (EDPS)[69].

Indeed, as highlighted by Art. 29 WP, among the processing of data that could be subject to users' consent there is WiFi tracking. This actually depends on the circumstances and purposes of the data collection, but nonetheless the Art. 29 WP recommends anonymization. Furthermore, in the same opinion the Art. 29 WP strongly support the idea of terminal equipment and software that are by default set to offer privacy protection. The Art. 29 WP as well as the EDPS also suggest *"all public wireless internet hotspots should fall within the scope"*: this might have an impact on CNs that offer WiFi to the public at large.

Our findings in D4.2 have stopped here as this regulation was yet to be adopted –originally on May 2018. However, in June 2018, surprisingly, the debate is still ongoing and peculiarly difficult to conduct.

First, there are several **incompatibilities between GDPR and the original philosophy of ePrivacy**. For instance, the first one introduce the concept of "legitimate interest" as an alternative basis of processing whereas the second tended to focus on the consent as a unique basis for some processing.

Second, many players with **polarized opinions** are weighting on the European legislative process (Member States, Bureau Européen des Unions de Consommateurs (BEUC)[70], EDPB, EDPS, European NGOs defending digital rights[71], telecoms operators[72] ...). Thus, **privacy settings of web browsers** and the framework regarding **cookies** –and especially the issue "cookies walls"– are very thorny.

Thirdly, and above all, several Member States would like to include a **debate on data retention provisions**[73]. However, this issue is **highly controversial** and therefore extends even more the decision process.

On June 8, 2018, during the Telecommunications Council[74], it was widely acknowledged that the period of negotiations have to be extended.

In the current context, data retention has became a major issue in CNs' legal framework and, as such, it requires a dedicated analysis in this deliverable that we carry out in the following Sec. 2.3.

[67] Art. 29 WP has been the EU independent body for the analysis and development of of data protection measures since the late '90s. Article 29 Working Party ceased to exist as of 25 May 2018, and has been replaced by the European Data Protection Board (EDPB) https://edpb.europa.eu/

[68] Art. 29 Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)," Apr. 4 2017; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140

[69] EDPS, "Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)," Apr. 24 2017; https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf; EDPS exists since 2004 to monitor EU institutions and bodies' processing of personal data. To ensure that right to privacy and data protection are respected in these processing, EDPS conducts investigations, advises EU bodies and handles complaints. https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en

[70] See their position: http://www.beuc.eu/publications/beuc-x-2017-059_proposal_for_a_regulation_on_privacy_and_electronic_communications_e-privacy.pdf

[71] several open letters as well as meetings were organised by European NGOs, see for instance proposals of amendments https://www.accessnow.org/cms/assets/uploads/2017/06/ePrivacy-paper-amendments-Access-Now.pdf

[72] https://etno.eu/datas/ETNO%20Documents/ETNO%20GSMA%20Joint%20Statement%20on%20ePR%2020170621.pdf

[73] http://statewatch.org/news/2017/dec/eu-data-ret-ms-positions.htm

[74] Transport, Telecommunications and Energy (TTE) Council http://www.consilium.europa.eu/en/meetings/tte/2018/06/08/

2.3. Data retention

Introduced in D4.2 in the light of the *Tele2* ruling of the CJEU, data retention is not only a mere legal issue for community networks, but also an ethical one. Above all, the stake relies on the divergence between European (Sec. 2.3.2) and national (Sec. 2.3.3) requirements, which has led CNs to act through advocacy actions (see Sec. 5.1 below).

Yet, data retention is a highly technical topic which requires an introduction to its cornerstone definitions, both from a legal and technical point of view.

2.3.1. Technical keys and cornerstone definitions

From a legal point of view, data retention is a processing of data imposed by law to telecommunication operators and/or providers of certain communication services depending on national legal provisions (for more details about national legal frameworks, see Sec. 2.3.3).

From a technical point of view, it refers to the storage of communication data collected on this basis.

2.3.1.1. Which kind of data is retained?

The scope of this specific processing is substantially reduced to **traffic and location data**, which gather all information except the actual content of a communication. They are part of the so-called "metadata".

More precisely, it is important to distinguish:

Content of a Communication is the (user) information transmitted, which is not processed in order for the information to be transferred. CNs, as anyone else, 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 Electronic Communication Services (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.

2.3.1.2. What does "retention" refers to?

The retention of data refers exclusively to Traffic and Location Data as defined above. Content of a communication is always excluded from data retention and can be accessed only for legal interception, as clearly defined by Article 5 of the Directive 2002/58/EC. Retention refers to the **collection** and **storage** of these data without further analysis for an extended period of time to allow a **future access** by a competent authority[75]. Moreover, operators which fall within the scope of this obligation have to establish internal procedures to meet the requests made by public authorities to access the retained data, and shall keep these requests confidential.

[75] For a substantial overview of data retention in the European Union and a clear introduction to its key concepts and consequences on digital fundamental rights, see https://www.privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf

2.3.2. European framework

A quick reminder of the genesis of data retention European law seems necessary (Sec. 2.3.2.1) to properly state and understand the current framework established by the *Tele2* ruling (described in D4.2 and reiterated in Sec. 2.3.2.2).

2.3.2.1. Genesis of data retention law

In **2002**, the **ePrivacy Directive**[76] 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**[77], 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.**

Since then, most Member States have passed national laws implementing such an obligation.

In **2014**, however, the **Court of Justice** has decided, in the *Digital Rights Ireland* case law[78], 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 that 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 was 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 and a British court. They ask the CJEU whether any obligation imposed on ECSs[79] providers to retain the traffic data of all of their users may comply with the Charter as such. The Court issued one decision known as the *Tele2* case law.

2.3.2.2. *Tele2*: the current data retention standard

In continuation of the *Digital Rights Ireland* ruling mentioned above, the Grand Chamber of the Court of Justice stated the current standard of protection of rights regarding retention of communication data in joined cases *Tele2 Sverige AB v. Postoch telestyrelsen* (C-203/15), and *Secretary of State for the Home Department v. Tom Watson and others* (C-698/15). In both cases the question related to the validity of a law imposing a general obligation on providers of ECSs to retain data and the law at stake was the result of the implementation of the invalidated Directive 2006/24.

[76] 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); https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[77] 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/legalcontent/EN/TXT/?qid=1478085591034&uri=CELEX:32006L0024

[78] CJEU, 8 April 2014, *Digital Rights Ireland v Minister for Communications & others*, cases C-293/12 and C-594/12; https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&from=EN

[79] https://eur-lex.europa.eu/summary/glossary/electronic_communications_services.html

In the Swedish case, Swedish law required providers to retain all the traffic and location data of their subscribers systematically and continuously, with no exceptions. However, the telecommunications operator Tele2 Sverige advocated that in reliance with the judgement by the CJEU in the Digital Rights Ireland case it would no longer retain data as Swedish law required.

In the UK case, UK norms on data retention asked public telecommunications operator to retain all the data relating to traffic for maximum 12 months. Three UK citizens brought an action challenging these norms.

This preliminary ruling[80] concerns the **interpretation of** the Article 15(1) of Directive 2002/58/EC, the **ePrivacy directive** (see hereinabove Sec. 2.3.2.1), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union.

The Court of Justice emphasises the specific requirements regarding, first, the **collection** of data, and secondly, the **access** to these data.

As for the collection, the Grand Chamber specifies that general and indiscriminate retention of data is against EU law. On this topic, it specifies that it precludes "national legislation which, for the purpose of fighting crime, provides for **general and indiscriminate** retention of **all traffic and location data** of **all subscribers and registered users** relating to **all means of electronic communication**".

As for the access, this decision holds that data retention measures which do not respect specific requirements are inconsistent with EU law, "precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime,

[I] is not restricted **solely to fighting serious crime**,

[II] where access is not subject to **prior review by a court or an independent administrative authority**, and

[III] where there is no requirement that the data concerned should be retained **within the European Union**."

Aiming to specify one of these requirements, another preliminary ruling is pending before the Court of Justice (C-207/16). More precisely, the Spanish *Ministerio Fiscal* asked two follow-up questions:

- "*Can the sufficient seriousness of offences [...] be determined taking into account only the sentence which may be imposed in respect of the offence investigated, or is it also necessary to identify in the criminal conduct particular levels of harm to individual and/or collective legally-protected interests?*"
- "*...[W]hat should the minimum threshold be? Would [EU law requirements'] be compatible with a general provision setting a minimum of three years' imprisonment?*"

While waiting for the final decision, the Advocate general recommends, in his conclusions[81], for the Court to consider that EU law should be interpreted as meaning that "*a measure allowing the competent national authorities to have access, for purposes associated with combating criminal offences, to the identification data of users of telephone numbers activated from a specific mobile telephone during a limited period, in circumstances such as those at issue in the main proceedings, entails an interference with the fundamental rights guaranteed by that directive and by the Charter which does not attain a sufficient level of seriousness for such access to be confined to cases in which the offence concerned is of a serious nature.*"

As part of negotiations regarding the ePrivacy regulation (Sec. 2.2.2), this current framework might be updated in the coming months. The trend seems to be in favour of an extension of data retention measures, reconsidering *Tele2* and its progresses for digital rights[82]. Indeed, Member States seem very reluctant to apply this ruling considering that numerous national legal frameworks, a year and half after the Court of Justice's decision, still

[80] See, D4.3, Sec. 5.1 about this procedure.

[81] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd50da99b7af5347d38069add9d8587e56.e34KaxiLc3qMb40Rch0SaxyNbNv0?text=&docid=201707&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=965748

[82] See [http://www.statewatch.org/news/2017/dec/eu-data-ret-ms-positions.htm; https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/

fail to respect it.

2.3.3. National frameworks

Despite CJEU's judgments in Digital Rights Ireland and in Tele2 most European Member States still have data retention laws that were the implementation of Dir. 2006/24 and that, therefore, are invalid in the face of EU law[83].

In 2017 Eurojust conducted a survey to investigate current data retention regimes in EU24; in particular, the survey focused on whether Member States' laws contained restrictions related to the categories of data, to the users/subscribers or to the means of communication. The responses to the survey were grouped into three categories:

1. Most of the EU countries do not have targeted data retentions rules;
2. Germany excludes some targeted users/subscribers from the retention obligation, such as organizations or individuals that offer anonymous counseling (as per the new legislation that came into force in July 2017)[84];
3. Some countries do not have any data retention law; they used to have one but it was invalidated by their constitutional or high court following Digital Rights Ireland judgment.

No country seems to have legislation containing the specific criteria that the CJEU requested in the Tele2 judgment.

Relying on these findings of D4.2, we have updated them and choosen to focus on five illustrative Member States in which CNs are very active and which embody three reactions to this new European legal framework.

In France, Spain, and Greece (Sec. 2.3.3.1), as in most country, the *statut quo* is maintained. In Italy (Sec. 2.3.3.2) recent provisions extend the current data retention measures. In Germany (Sec. 2.3.3.3) the current national provisions were partly reviewed by two national courts.

2.3.3.1. The upholding of outdated measures

2.3.3.1.1 France

In France, the current framework substantially relies on the L. 34-1 of the postal and electronic communications Code (*code des postes et des communications électroniques* (CPCE)) and the article 6 of the *Loi pour la confiance dans l'économie numérique* (LCEN).

Article L. 34-1 state a **principle of anonymisation of metadata**[85]. It also state the exception of retention of these data. The article R. 10-13 of the same Code specifies this general provision.

Altogether, these provisions require 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;

[83] See Privacy International, "National Data Retention Laws Since the CJEU's Tele-2/Watson Judgment. A Concerning State of Play for the Right to Privacy in Europe," 2017; https://privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf

[84] See, below Sec. 2.3.3.3

[85] see article L34-1 available here: https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465770

- 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[86]. 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"[87] "any place offering to the public an access to the Internet, for free or not", is subject to this obligation[88], 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[89], 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**.

[86] 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

[87] CNIL, Internet et WiFi 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

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

[89] 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).

Besides, several institutions took position toward the *Tele2* ruling. For instance, during a conference organised by the French Supreme administrative court, the Vice-Chairman of the *Conseil d'Etat* stated its concerns regarding the "*excessively constraining*" requirements of this case law toward State members. He specifically emphasised that "*[t]his **very restrictive jurisprudence** is not in line with the more well-balanced assessment held these last years by the European Court of Human Rights*"[90].

2.3.3.1.2 Spain

The *Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*[91] (Spanish Data Retention Law) 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.

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-on 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;

[90] Free translation of "*Cette jurisprudence très restrictive s'éloigne assez nettement, me semble-t-il, de l'attitude plus équilibrée adoptée par la Cour européenne des droits de l'homme depuis plusieurs décennies.*" The official speech presented during this conference in French is available here: http://www.conseil-etat.fr/Actualites/Discours-Interventions/Le-renseignement-et-son-controle

[91] See, in spanish: http://noticias.juridicas.com/base_datos/Admin/l25-2007.html

- 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.

All these **categories of data** are exactly the **same** as in the former European Data Retention **Directive of 2006**. Besides, some of these categories are problematic, for instance it seems that e-mail providers shall retain data identifying the recipients of every email sent by their users, which is instead, technically, a Content of the Communication and not Traffic Data, as the Traffic Data includes only the identification of the e-mail service provider. It must also be noted that these categories are technically inconsistent, as for instance in web-based voice and video service, User ID and telephone number do not necessarily exist. Furthermore, the circumstances under which email services may be considered as ECSs (and their providers subject to these obligations) are unclear. Anyway, since CNs usually provide pure ECS, they should, in theory, comply with these obligations when they also provide email services.

Moreover, 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**[92]. Recommendations regarding this issue are described below in Sec. 4.1.6.

Finally, as described above (Sec. 2.3.2.2) a **preliminary ruling is pending** before the CJEU (C-207/16), mostly regarding the interpretation of "serious crime".

2.3.3.1.3 Greece

In 2011, the **Greek data retention law (Law 3917/2011)**[93] has fully transposed the former **Directive 2006/24/EC**[94] and their content is substantially identical regarding data retention obligations.

Article 5 of this law imposes a retention of **one year** for the following categories of data.

Firstly, about Data necessary to detect and identify the source of communication.

Concerning **fixed-network** and **mobile telephony**:

- the caller's telephone number
- the name and address of the subscriber or registered user

Regarding **Internet access** as well as e-mail and telephony services over the Internet:

- The user ID assigned,
- The user ID and the telephone number given in each communication entering the public telephone network
- The name and address of the user

[92] See, article 10 of the Ley 25/2007

[93] http://www.dsanet.gr/Epikairothta/Nomothesia/n3917_2011.htm

[94] 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/legalcontent/EN/TXT/?qid=1478085591034&uri=CELEX:32006L0024

- The address of the subscriber or registered user who was assigned at the time of communication an IP address user ID or telephone number

Secondly, regarding data necessary to determine the destination of the communication.

Concerning fixed-network and mobile telephony:

- The called number or numbers (the number(s) dialed), in cases where additional services such as call forwarding, the number or telephone numbers to which the call has been forwarded
- The names and addresses of subscribers or registered users

Regarding **Internet access** as well as e-mail and telephony services over the Internet:

- The name and address of the subscriber or registered user and the user ID of the recipient of the communication
- The user ID or telephone number of the internet call recipient

Thirdly, about data necessary to determine the date, time and duration of the communication.

Concerning fixed-network and mobile telephony:

- The **date and time of commencement and termination** of communication

Regarding **Internet access** as well as e-mail and telephony services over the Internet:

- The **date and time** of the Internet **log-on and log-off** based on a specific time zone
- The **dynamic or static IP address** of the Internet service provider, user identity of the subscriber or registered user
- The date and time and date and time of log-on and log-off with the e-mail or internet telephony service, based on a specific time zone

Fourthly, about data necessary to determine the type of communication.

Concerning fixed-network and mobile telephony:

- The **telephone service** used

Regarding **Internet access** as well as e-mail and telephony services over the Internet:

- The **Internet service** used

Fifthly, regarding data necessary to identify the communication equipment of users or their alleged communication equipment.

Concerning fixed-network telephony:

- Caller and caller telephone numbers

For mobile telephony:

- Caller and caller telephone numbers
- The **caller's** international mobile subscriber identity (**IMSI**)
- The **caller's** international mobile telephony equipment (**IMEI**)
- The **IMSI of the called**
- The **IMEI of the called**
- In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location code (cell ID) from which the activation took place

Regarding **Internet access** as well as e-mail and telephony services over the Internet:

- The caller's telephone number for access by telephone
- Digital subscriber line (DSL) or other end of the source of communication
- The date and time and date and time of log-on and log-off with the e-mail or internet telephony service, based on a specific time zone

Sixthly, concerning data necessary to determine the location of the mobile communication equipment.

- The position code (cell ID) at the beginning and end of the communication
- Data identifying the **location of the cells** based on location codes (cell IDs) during the time period for which the communications data is maintained.

In reliance with Article 6, all these data should be stored within Greece.

These provisions were not modified in the aftermath of CJEU's decisions. However, in August 2016, a Greek Court have lodged a request with the Court of Justice for a **preliminary ruling**[95]. Very specific, it **raises 17 questions**, including:

- *Is it compatible with Articles 7, 8 and 52(1) of the Charter that **data retained** under Directive 2006/24/EC and/or Article 15(1) of Directive 2002/58/EC **is accessed and used by the police in the course of criminal investigations in cases of urgency –in particular, in cases of crimes where offenders are apprehended in the act– without prior approval** by a judicial body [or independent administrative body] **on the basis of specific substantive and procedural requirements?***
- *Having regard to the judgment of the Court of Justice in Digital Rights Ireland and Others, paragraphs 60 and 61, and **the term "serious crime"** contained in Article 1(1) of Directive 2006/24/EC, **is that term an autonomous concept of EU law** and, if so, **what is its essential content on the basis of which a specific crime must be considered serious enough** to justify the access to and use of data retained under Directive 2006/24/EC?*

Yet, no answers will be provided as the **case C-475/16 was removed** from the Court's register without judgment due to a lack of confirmation to maintain the request from the national court[96].

2.3.3.2. A recent extension up to six years of data retention

2.3.3.2.1 Italy

In November 2017, as a transposing measure of the directive 2017/546, Italy has enacted a law extending the data retention duration up to **seventy two months** –or six years.

Indeed, the article 24 of the *Legge Europea*[97], concerning the "limits of telematic and telefonic data retention" (*Termini di conservazione dei dati di traffico telefonico e telematico*) states that:

> "*[. . .], in order to provide effective tools of investigation considering the extraordinary necessities of combating terrorism, also international, for the purpose of finding an repressing offences mentioned in the article 51, paragraph 3-quater, e 407, paragraph 2, letter a), of the criminal procedure code, the term of conservation of telephonic and online communication data retention as well as data related to unanswered calls, mentioned in the article 4-bis, paragraphs 1 and 2, of the 'decreto-legge 18 febbraio 2015, n. 7', transformed, with modifications, of the 'legge 17 aprile 2015, n. 43', is established in seventy two months, notwithstanding the provisions of the article 132, paragraphs 1 and 1-bis, of the personal data protection code, as mentioned in the 'decreto legislativo 30 giugno 2003, n. 196.*"'

Free translation based upon the original Italian text[98].

[95] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CN0475&from=FR

[96] See, in Greek: http://curia.europa.eu/juris/document/document.jsf?text=&docid=194141&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=316038

[97] Legge, 20 novembre 2017, n. 167, *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017, (GU Serie Generale n.277 del 27-11-2017)*

[98] The Italian text is available here: http://www.gazzettaufficiale.it/eli/id/2017/11/27/17G00180/sg and states: "*1. In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in*

This update is introduced in the article 132 of the Italian Personal data protection Code (*Codice in materia di protezione dei dati personali*)[99] regarding "Trafic data retention for other purposes" (*conservazione di dati di traffico per altre finalita*).

With this provision, in force since December 12, 2017, Italy is one of the countries where the data retention time frame is the most extended. Previously, there was a distinguishing in terms of duration according to the kind of data retained.

- For online communications, which substantially but not exclusively refers to Internet communications, the time limit of retention was twelve months (one year)[100].
- For telephone communications, it was twenty four months[101].
- Finally, as for missed calls, it was originally thirty days[102].

The extension is significant. Moreover, henceforth all kind of data are treated equally, notwithstanding the potential differences in terms of sensitivity of these data. Indeed, a missed call could be regarded as an information less specific and therefore less private than metadata from online communication. However, the indiscriminate duration and its substantial extension raise, all the more, the issue of compliance with all requirements of the Court of Justice. On this subject, the President of the Italian Data Protection Authority (*Il Garante per la protezione dei dati personali*) formally stated his concerns about the proportionality of this measure regarding EU jurisprudence[103]. In this context, CNs may be fined up to **50 000 €**.

No national pending case is known as of June 2018 concerning this law and its provisions, however, as part of its advocacy work, netCommons relies on these findings and those of D4.1 and D4.2 to help a local non-profit organisation (NGO) to write the Italian formal complaint (in English) to be submitted to the European Commission (see Sec. 5.1).

2.3.3.3. A judicial application of *Tele2* excluding a data retention provision

2.3.3.3.1 Germany

In 2010, the German Constitutional Court already ruled about data retention, considering legal data retention obligations, in its form at the time of the review, incompatible with the German Basic Law [104].

In late 2015, the German government introduced a new bill on the issue. This "Law introducing a retention obligation and a maximum retention duration for traffic data" (*Gesetz zur Einführung einer Speicherpflicht und*

considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196."

[99] The article 132 is available in Italian here: http://www.gazzettaufficiale.it/dettaglio/codici/datiPersonali

[100] Article 132 of the Italian Personal data protection Code 1. "*[...] per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.*"

[101] See Article 132 of the Italian Personal data protection Code 1. "*Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico conservati dal fornitore per ventiquattro mesi dalla data della comunicazione [...]*"

[102] See Article 132 of the Italian Personal data protection Code 1-bis "*I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni.*"

[103] The full-text is available in Italian here: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6651715

[104] The full text in German is available here: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html;
the official English translation is available here: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html;
and the detailed press-release (in english) here: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html

einer Höchstspeicherfrist für Verkehrsdaten, (BGBl. I 2015 S. 2218))[105] provides for much shorter storage periods. Especially, Article 2 of this law substantially modified article §113a)[106] and §113 b)[107] of *Telekommunikationsgesetz* (Telekommunikationsgesetz (TKG)).

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

- 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-on 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.

Concerning 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 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:

[105] The full text of the law is available here: https://dejure.org/BGBl/2015/BGBl._I_S._2218
[106] Available in German here: https://dejure.org/gesetze/TKG/113a.html
[107] Available in German here: https://dejure.org/gesetze/TKG/113b.html

- 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).

German CNs should have complied **with all of these new obligations not later than 1 July 2017.**

However, on June 22 2017[108], the Higher Administrative Court of North Rhine-Westphalia in Münster (*Oberverwaltungsgericht für das Land Nordrhein-Westfalen* (Oberverwaltungsgericht (OVG) Münster)) considered that, in the light of the judgement of the Court of Justice of the European Union of 21 December 2016 C-203/15 and C-698/15, some of **these requirements were not in accordance with EU law** and especially the article 15, §1 of the Directive 2002/58/EC of 12 July 2002, as well as the article 7, 8, 11 and 52 of the Charter of Fundamental rights (§36 of the decision).

The applicant, here the appellant, was a company providing internet services for business customers in Germany and in other EU Member States. In first instance, in reliance with §123 *Verwaltungsgerichtsordnung* (Verwaltungsgerichtsordnung (VwGO))[109], he asked the Administrative Court of Köln to take the temporary injunction of dismissing the new version of data retention obligation weighting on the provider (VG Köln (9 L 1009/16)[110]. This request was dismissed, and the company lodged an appeal before OVG Münster.

The Court stressed that the *Tele2* ruling specified that **a general and indiscriminate retention could not be compensated**, in terms of interference with human rights, **with the limitation of authorities' access to these data** for the purpose of fighting serious crime[111]. The Court underlined that *"In any case, this [incompatibility] is entailed from the fact that the [German] obligation to retain data does not require a link between the data to be stored and the purpose pursued by law in fighting serious crime or preventing serious threats to public safety, but indiscriminately without any personal, time or geographical limitation so that almost all users of telecommunications equipment mentioned by § 113b TKG are covered"*[112].

[108] https://www.justiz.nrw.de/nrwe/ovgs/ovg_nrw/j2017/13_B_238_17_Beschluss_20170622.html

[109] Full text of this procedural provision is available here (in German): https://www.gesetze-im-internet.de/vwgo/__123.html

[110] full text of the decision is available in German: https://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2017/9_L_1009_16_Beschluss_20170125.html

[111] See the official press-release of the OVG Münster: http://www.ovg.nrw.de/behoerde/presse/pressemitteilungen/01_archiv/2017/36_170622/index.php

[112] (§ 36 of the decision, free translation of "Dies folgt jedenfalls daraus, dass die Speicherpflicht keinen Zusammenhang zwischen

In response, *BundesNetzAgentur*(Bundesnetzagentur (BNetzA)), the federal telecommunication regulatory authority, acknowledged that this decision and its reasoning overstepped the lone scope of the case and raises a European issue.

Accordingly, until the final conclusion of a main proceedings, the BNetzA declared that it "*will refrain from orders and other measures to enforce data retention obligation*" and guarantees that "*[u]ntil then,* ***no fine proceedings will be initiated*** *against the companies failing to comply with the current requirements*"[113].

In continuation with the reasoning stated in this decision, VG Köln rendered two similar judgements[114].

Therefore, in Germany, Internet services providers as well as Community Networks, will not be penalized if they do not comply with data retention requirements for the time being. Simply put, data retention requirements seem to be frozen until a conclusive national decision.

This issue might be resolved by the *Bundesverfassungsgericht*, the German Constitutional Court, since several complaints are pending. They should be reviewed in a single decision in the coming months[115].

2.4. Telecommunication law

In this section, we are presenting an update of results from D4.1, as well as analysing national implementation schemes and their impact on CNs activities, which are completely new topics.

Topics which are further developed are:

- Spectrum regulation (Sec. 2.4.1);
- Radio equipment directive (Sec. 2.4.2);
- Network neutrality (Sec. 2.4.3).

The two new topics introduced are:

- The WiFi 4 EU Directive and the possibility of public funding for local CNs (Sec. 2.4.4), with a presentation of the procedure to be followed;
- The development and perspectives of the EECC for CNs as this very important text for which we had proposed amendments has been released in June 2018 (Sec. 2.4.5).

2.4.1. Spectrum Regulation

An issue of utmost importance for wireless CNs is the one of "spectrum availability and management". Spectrum is in fact a scarce resource that has to be carefully managed in order to allow the best and most efficient use of it. As it is well known, the electromagnetic spectrum is a continuum of electromagnetic waves, from

den auf Vorrat zu speichernden Daten und dem durch das Gesetz verfolgten Zweck der Bekämpfung schwerer Straftaten bzw. der Abwehr schwerwiegender Gefahren für die öffentliche Sicherheit verlangt, sondern unterschiedslos ohne jede personelle, zeitliche oder geographische Begrenzung nahezu sämtliche Nutzer der von § 113b TKG erfassten Telekommunikationsmittel erfasst.")

[113] Free translation of "*Aufgrund dieser Entscheidung und ihrer über den Einzelfall hinausgehenden Begründung sieht die Bundesnetzagentur bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der in § 113b TKG geregelten Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen ab. Bis dahin werden auch keine Bußgeldverfahren wegen einer nicht erfolgten Umsetzung gegen die verpflichteten Unternehmen eingeleitet*", press-release of BNetzA, available (in German) here: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS-node.html

[114] https://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2018/9_K_7417_17_Urteil_20180420.html and https://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2018/9_K_3859_16_Urteil_20180420.html

[115] All pending actions, n°1BvR 256/08 and the joined cases: "14. Verfassungsbeschwerden gegen Vorschriften der Strafprozessordnung (StPO) und des Telekommunikationsgesetzes (TKG) in der Fassung des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (Vorratsdatenspeicherung)."; Preview for 2018 available (in German) here: http://www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2018/vorausschau_2018.html; one of these complaint were introduced by Digitalcourage, a local NGO. This substantial complaint is available, in German, here: https://digitalcourage.de/sites/default/files/users/161/digitalcourage-verfassungsbeschwerde-gegen-vds.pdf

0 Hz (cycles per second) to visible light at hundreds of THz to potentially infinity. The portion of the spectrum usable for free space *telecommunication*[116] starts at few tens of kHz with "short" radio waves (used for military and analog radio communications), up to hundreds of MHz and GHz ("radio" waves, the most precious and used for telecommunication, including WiFi and cellular systems), to tens and hundreds of GHz ("micro" waves) that are now being explored for high speed, short range communications for their specific propagation characteristics and bandwidth availability. All together, the portion of electromagnetic spectrum useful for telecommunication is known as "radio spectrum;" although this term is technically ambiguous we will used it in this document. Competing uses and users in free space telecommunication, but also other uses as radars, probing microwaves ovens, medical use, etc. cause interference; hence spectrum is a scarce resource, and only a limited number of users can actually operate effectively within a specific portion, normally called a "*band*"[117].

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

2.4.1.1. Spectrum regulation at the international level

At an international level, a big role is played by the already mentioned 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)[118]. EU represents the Member States at the international level[119]. EU policies are developed according to the ITU regulations.

2.4.1.2. Spectrum regulation at the European level

Given the increase in the use of spectrum, European policy-makers have been discussing new strategies. The current instruments in this area are the Radio Spectrum Decision No 676/2002/EC[120], the Radio Spectrum Policy Group Decision 2002/622/EC[121] and Decision 243/2012/EU establishing a multi-annual Radio Spectrum Policy Programme (RSPP)[122].

Currently, spectrum use is granted by National Regulatory Authorities (NRAs) that shall follow the 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[123]. 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

[116] According to the International Telecommunication Union (ITU) definition a telecommunication is the act of transferring information (voice, video, data, or any other *medium*) from one point in space or time to another one using technologies based on propagating electromagnetic fields; free space telecommunication are those that do not use cables for the transmission.

[117] For further information or more technical details see the web site and publications of the ITU on spectrum management at https://www.itu.int/pub/R-REP-SM

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

[119] 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, 222

[120] 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.

[121] 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.

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

[123] See Flanagan A, 2012. Spectrum Management, in Walden I. (ed), Telecommunications Law and Regulation, Fourth Ed., Oxford: OUP, 2012, 357-396, 378

the grant of individual rights of use, 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[124].

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[125].

In 2012, EU adopted the first Radio Spectrum Policy Programme (RSPP)[126]. 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.

2.4.1.3. 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[127]. 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 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[128].

Furthermore, as many, if not most, CNs are based on WiFI, which works on Industrial Scientific Medical (ISM), non licensed bands, the regulations and management of these bands should be closely monitored. For instance, there are discussions to standardize the use of Long Term Evolution–Unlicensed (LTE-U) technologies by cellular operators in the ISM bands[129], and in the USA the Federal Communication Commission (FCC) already issued licenses to experiment with this technology[130]. Given the technological difference between LTE-U and WiFi, it is generally thought that WiFi will suffer most from this interference, while is it not clear if LTE-U technology will be available for non cellular networks controlled equipment.

[124] 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, 102

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

[126] Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multi-annual radio spectrum policy programme, OJ L 81, 21.3.2012, p. 7–17.; See Flanagan A, 2012. Spectrum Management, in Walden I. (ed), Telecommunications Law and Regulation, Fourth Ed., Oxford: OUP, 2012, 357-396, 382- 383

[127] 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, 8

[128] 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, 102

[129] See Mina Labib, Vuk Marojevic, Jeffrey H. Reed, Amir I. Zaghloul. "Extending LTE into the Unlicensed Spectrum: Technical Analysis of the Proposed Variants." https://arxiv.org/pdf/1709.04458.pdf. LTE is the technology used for most services of 4G cellular networks.

[130] See https://techcrunch.com/2017/02/22/freshly-fcc-approved-lte-u-wireless-rolls-out-on-t-mobile/?guccounter=1 and references therein.

2.4.2. Radio equipment

There are other regulatory hurdles that CNs have to face. Among them there is also the issue of the recent modifications of the legislation on ”radio equipment”. More specifically, in 2014, the European Union adopted a Directive 2014/53 on radio equipment[131], that even though was not specifically heading for CNs, it might actually 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*”[132]. 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*”[133]. 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.

2.4.3. Net Neutrality

In the last few years, net neutrality issues have been at the centre of both research and telecommunication policy arenas[134]. 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[135].

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)).

[131] 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.

[132] See https://fsfe.org/activities/radiodirective/

[133] See https://fsfe.org/activities/radiodirective/

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

[135] 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.

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 Body of European Regulators for Electronic Communications (BEREC) released specific guidelines that help to interpret the Regulation[136]. 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*"[137].

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 –rarely also Internet connection– only to a predetermined group of people; hence they cannot be considered as *"publicly available"* 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".

2.4.4. WiFi4EU: Bringing direct and targeted public support to CNs?

On October 25th, 2017, the European Parliament and the Council enacted Regulation EU No 2017/1953 ("WiFi for EU directive")[138] in order to promote the deployment of local wireless access points free of charge for their users and without discriminatory means[139].

This regulation aims to encourage this deployment through simplified planning procedures, reduced regulatory obstacles and, especially, financial support. This latter provision can be of specific interest for community networks, which advocated for **"direct and targeted public support"**, along with netCommons project in the Open Letter of March 2017[140] and during the following workshop organised in November 2017 concerning telecom regulation[141]. However, at the time of writing of this document, the specific target of financing and details on how to access them, as well as many technical details on the initiative remains unspecified, as we discuss in the sequel, probably making this initiative almost irrelevant for CNs.

2.4.4.1. Key definitions

The regulation also sets up a definition of **"local wireless access point"**, which means *"low power equipment of small size operating within a small range, using on a non-exclusive basis radio spectrum for which the conditions of availability and efficient use for that purpose are harmonised at Union level, and which allows wireless access by users to an electronic communications network."*

This regulation provides an increase of the financial envelope for the implementation of the **Connecting Europe Facility** (Connecting Europe Facility (CEF)), which is a global key EU funding instrument. It is divided in

[136] 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-netneutrality-guidelines

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

[138] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R1953&from=EN

[139] which implies that this service "*is provided without corresponding remuneration, whether by direct payment or by other types of consideration, such as commercial advertising or the provision of personal data for commercial purposes*". See REGULATION (EU) 2017/1953 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2017 amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of internet connectivity in local communities, recital 3.

[140] see D1.5, p. 34, The "Open letter to EU policy makers on community networks. (2017, March 16)" is publicly available on netCommons web site at https://netcommons.eu/?q=news/open-letter-eu-policy-makers-community-networks

[141] see https://netcommons.eu/?q=content/eu-parliament-workshop-community-networks-and-telecom-regulation

three parts: the CEF transport, CEF energy and, for digital services, CEF Telecom[142]. Altogether, they aim to promote the development of sustainable and efficiently interconnected trans-European networks through financial aids.

For the CEF telecom program, Community networks may be eligible. However, the regulation sets up specific requirements, which are explained in the next section.

2.4.4.2. Financial program for wireless connectivity in local communities

2.4.4.2.1 Theoretical framework

The financial support to local wireless access points will be offered through grants and especially **vouchers**[143]. To ensure efficiency and fairness in the allocation, the regulation states criteria of eligibility of actions involving this specific Union financial assistance. Each action in a specific territory is carried out by a public sector body, and its actual realisation could be conducted by a WiFi installation provider, such as a company or a community network.

For the public body implementing the project, requirements are[144]:

- Be capable of planning and supervising the installation, as well as ensuring for a minimum of **three years** the **financing** of operating costs, of indoor or outdoor local wireless access points in public spaces;
- Build on **high-speed broadband** connectivity **free of charge** and **without discriminatory conditions**, uses most recent and **best available equipment** and supports access to innovative digital services. In this perspective, ***discriminatory conditions*** means that the service is provided in compliance with EU law and with national law that complies with Union law, and should especially ensure ***"a fair allocation of capacity between users at peak times"***[145];
- Use the **common visual identity** to be provided by the Commission to draw attention to the fact that the Union has granted funding;
- Respect the principle of **technological neutrality** at the level of the backhaul;
- Respect the principle of the **efficient use of public funding**, as in any public procurement procedure, for instance this may imply to avoid duplicating existing similar free private or public offers, which is a delicate topic that goes beyond the scope of this document;
- Ensuring a **fair competition**.

For the WiFi installation provider, it shall:

- Be able to provide an IT system and/or access point compliant with the specific **technical requirements** set up in the funding agreement between the public sector body and the European Commission (for now it is envisaged that they should comply with 802.11ac Wave I, with Hotspot 2.0, and support of 802.1x);
- Built access points which would be able to form part of a network with a **single authentication system** that is valid across the whole Union and other free local wireless connectivity networks should be able to join the system;
- Respect the **European legal framework**, including data protection law and security measures[146], described in D4.1 and D4.2, both consolidated and updated in Sec. 2.1, Sec. 2.2 and Sec. 2.3.

These requirements call for several comments.

First, regarding the **authentication system**, most Community Networks intends to offer an Internet access free of charge, with a high level of respect to their privacy and without deterrent formalities. As such, they often

[142] https://ec.europa.eu/inea/en/connecting-europe-facility
[143] See Regulation EU No 2017/1953 recital 13 and Article 1.
[144] *Ibid.* See Article 2.
[145] *Ibid.* See Recital 4.
[146] Regulation 2017/1953, Recital 3.

reject authentication system which implies for the user to log in and give personal information (email address, suscriber ID, ...) that, in turn, CNs have to retain in reliance with national laws. Moreover, having a 'single' authentication system would imply a centralized system, which, especially in terms of data retention, may go against the core values of Community Networks[147].

Second, all **technical specifications** of the **captive portal** as well as the **equipment** are not yet settled and some will be detailed in the grant agreement signed between the beneficiaries (municipalities) and the Commission. However, as we raised the issue during netCommons plenary meeting in July 2018, most of the Information and Communication Technologies (ICT) experts present highlighted that WiFi4EU current standards –especially regarding protocols used– might be inappropriate to implement for CNs.

Yet, a compromise might be reached by allowing an alternative service management of the access point, in addition and without prejudice to the WiFi4EU system. Indeed, in this Regulation, no provision impose an exclusive use of the infrastructure built with WiFi4EU financial program. Therefore, once the access-point is built, it might be interesting to allow one or several operators to offer different offers, with different terms of services. In this hypothesis, we can envisage that each person starting to use the access-point may have a choice, while connecting, between different kind of access-point services: WiFi4EU system, an alternative without authentication or with a different authentication system operated by a CNs for instance, or even commercial offers with additional services. Such a possibility would promote competition, enhance the consumer's freedom of choice and may encourage Community Networks to take part in the WiFi4EU program.

All in all, WiFi4EU appears as centralized and tends to lack clear limitations or specifications –perhaps to be detailed in each grant agreement– which might be inconsistent with most CNs models, capabilities or values.

Public bodies should submit their project on: www.wifi4eu.eu and private sector body offering their services and wishing to be chosen by these public body should also register on this web site through a specific procedure.

2.4.4.2.2 Concrete procedure

A dedicated procedure is set up to award these vouchers. There are three steps.

1. **Registration** of public sector body.

   For the first call, a specific and exhaustive list of eligible public body was published for each Member States[148].

2. **Application** for voucher.

   Municipalities registered have to formally apply on the same web site once the application procedure is open.

3. **Selection** of public sector body.

The criteria of **selection of these public body** candidates will be the date and time of their submission of application –not registration– on a **"first-come, first-serve basis"**. However, to ensure a fair balance of funding among Member States, each country will be awarded 15 vouchers –at least for the first call. Limitations are also established, as the number of vouchers per country is limited to 8% of the first call's budget. **Each municipality** can only benefit **one voucher** during the entire duration of the initiative. Each voucher is valid for 18 months.

This deadline implies that once a municipality or public sector body have a voucher, it shall make sure that the **hot-spot starts working within 18 months** after being awarded the voucher. Within this time-frame, they can define their project and select a supplier to conduct the installation. In this respect, public sector body can freely choose to enter in contract with a **CN registered** –as long as this choice is made in accordance with European and national public procurement law.

Indeed, WiFi installation companies, and therefore possibly community networks, also have to register on the WiFi4EU portal through a dedicated section. However, they have a more flexible time-frame and can register

[147] See the Open Letter sent in May 2017 on WiFi4EU; https://www.laquadrature.net/en/wifi4eu-diversity-human-rights

[148] https://ec.europa.eu/digital-single-market/en/news/list-eligible-entities-wifi4eus-first-call

at any moment as long as they do so
inquoteat the latest when a selected municipality has contracted them as a supplier[149].

To register, CNs have to provide information regarding their organisation (Name, Official address, VAT number, IBAN, contact person, ...) and specify the geographical area which will be operated.

Initially, the first call for application was launched on 15 May. However, the Innovation and Networks Executive Agency (INEA) of the European Commission considered that "a technical error prevented applicants from applying on equal terms". Therefore, in reliance with fairness of competition procedures, it decided to cancel this call and arrange another one in Autumn 2018.

In the past months, through the Telecommons mailing list, netCommons reached out to CNs in Europe to make WiFi4EU known to them, inviting them to get closer to local authorities to push the later to apply for a grant. We have not received any feedback on this issue this far. Nevertheless, we will still give updates and inform CNs regarding the next call for participation.

2.4.5. Development and perspectives of the EECC for CNs

The European Electronic Communications Code (EECC) is a sweeping piece of legislation overhauling Telecom regulation in the EU bloc. It was introduced as a legislative proposal in September 2016 by the European Commission with the goal of merging and updating existing texts:

- The 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;
- The 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;
- The 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;
- The 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.

The policy rationale behind such legislation is to boost investment in so-called Very High Capacity networks, relying on Fiber-To-The-Home (FTTH) architectures, ensuring a equal development of EU regions and warding off a so-called "investment gap". As stressed in a EU Parliament brief on this dossier:

> "*According to an Arthur D. Little study, while new giga-networks are being deployed in large parts of Europe, they only covered some 33% of EU Member State households at the end of 2016. A study prepared for the European Commission also indicates that, without more investment, the connectivity targets are out of the reach of some EU Member States, and that the EU will fall behind compared to other regions of the world (e.g. Japan) in terms of roll-out and usage of very high capacity networks. Research by Fibre-To-The-Home Council Europe estimates that €137 billion is needed by 2025 to reach gigabit society targets with an FTTH network infrastructure.*" [6].

The original proposal of the Commission, was centered on favoring the development of European-wide operators with large financial backing, and aimed at boosting their investment by lifting pro-competitive policies to which these often-dominant actors were subject to. Non-incumbent commercial providers were of course alarmed by this approach, as were a number of policy experts who stressed that the principle of pro-competitive regulations were in fact conducive to investment[150].

[149] See https://ec.europa.eu/digital-single-market/en/faq/wifi4eu-questions-and-answers

[150] A good overview of these debates is offered in [6]. From the perspective of CNs, the Commission's original approach appeared to be an inadequate one, where these smaller non-profit and commons-based network providers continued to be seen as only playing a marginal, "filling the gap" role [7].

2.4.5.1. First reading in EU Parliament (March-October 2017)

Notwithstanding this narrow focus, the overhaul of the EU telecom rules offered a key opportunity to voice the regulatory needs of Alternative and Community Networks. This is why, with the assistance of netCommons who collaborated with La Quadrature du Net and Federation FDN through a partnership presented in D1.5, dozens of organizations from across the EU wrote an open letter in March 2017 to EU policy-makers with a list of demands [3] . Unfortunately, a few days later, the Commission's initial proposition was only made worse by the rapporteur of the text in the EU Parliament, Mrs. Pilar Del Castillo (EPP, Spain). As La Quadrature du Net explained in March 2017 in an analysis to which netCommons contributed in the context of our partnership:

> "*Opposed to the demands of European Community Networks, the Commission favoured powerful operators substantially by completely deregulating investment in the as-yet undefined new network elements. It was the same when it proposed not to regulate the structurally separated operators. The Commission also handed operators a beautiful gift by offering them individual rights to radio frequencies for 25 years while counting on the secondary frequency market to keep it all working. Once again this flies in the face of history, because today Wi-Fi, and thus free frequencies, transmit more data than all other technologies combined.*"

Community Networks and their supporters were not the only ones criticizing this report, widely seen as very favourable to large-scale telecom operators by undermining pro-competition regulatory tools. Competitive operators as well as National Regulatory Authorities were also critical of the rapporteur's stance. For each specific hurdle faced by CNs and addressed in one way or another by the code (e.g., data protection, liability of WiFi hotspot providers, unlicensed access to the radio spectrum, open access to landline networks, regulation of oligopolistic situations in local markets), we highlighted which tabled amendments could move towards the right direction, and which made the situation only worse [8]. Ahead of crucial votes in EU Parliament committees working on the code, we collaborated with La Quadrature du Net to send this brief to all the Members of Parliament voting in committee. Unfortunately, back-door negotiations between the various political groups working on this dossier led to a compromise that did not reflect the demands of CNs[9]. On October 2th, the EU Parliament adopted in first reading its version of the code. In an open letter whose drafting was coordinated by netCommons and La Quadrature du Net, we pointed out that:

> "*The worst was avoided thanks to a majority of members of the Industry, Research and Energy (ITRE) who resisted calls for a sweeping deregulation. The version adopted by the committee maintains enough room for National Regulatory Authorities (NRAs) to regulate monopolistic situations and take Community Networks (CNs) into consideration, for instance by giving them access to optical fiber networks or promoting shared and unlicensed access to the radio spectrum, which can be essential to swiftly build affordable and flexible networks.*" [9].

2.4.5.2. Trilogue negotiations (October 2017 – June 2018)

As the EU Parliament gave a mandate to key MEPs to negotiate an agreement with EU Member States on the draft code, the legislative process immediately moved to a "trilogue", a secret negotiation process where representatives of the EU Parliament, of the EU Council and of the EU Commission try to find a compromise on the text before formally amending it. Although this theoretically allows for a swifter legislative process, it also comes with much less transparency and therefore represents a strong challenge for outsiders willing to track and intervene in the policy discussion.

In this context, the joint open letter therefore closed on a call to the EU Parliament:

> "*In a policy domain that has for too long been prone to regulatory capture by private interests, we call on the Members of the European Parliament to defend the public interest by promoting pro-competition and pro-diversity policies. By resisting the pressure of European governments who seek to further entrench the power of the largest industry players over network infrastructures, our elected representatives can ensure that alternative operators and local communities have the adequate means to develop and innovate, offering forward-looking models and services to the benefit of all.*"

During the netCommons workshop held at the EU Parliament on October 17th 2018 [3][151], various participants reiterated these calls and had a fruitful exchange with some Member of the EU Parliament involved in the trilogue negotiations (in particular, Miapetra Kumpula-Natri and Julia Reda).

Over the following months, various trilogue meetings took place. Spectrum policy would prove to be one of the most-debated item under discussion. Member States, usually less inclined to promote competition in telecom markets or the further "Europeanization" of telecom policy, were often standing in opposition with the stance of the EU Parliament and the EU Commission, who acted as de facto allies when the debate came down to this overarching issue.

As of March 2018, numerous important articles were still fiercely disputed, and in particular articles 74 on co-investment, article 59.2 on the power of NRA on access to infrastructure, article 33.5 on remedies or article 61 on dominant market actors. On May 23rd, netCommons researchers and board members participated in a policy workshop at the European Parliament where it was made clear that, although the worse had been avoided, smaller actors in telecom markets –and especially non-profit entities– remained largely overlooked by the most influential policy makers [10]. A compromise was finally reached during a trilogue meeting on June 5th. Related working documents were obtained in late June 2018. As they are substantial and sophisticated, this deliverable was updated in July 2018 to complete the mapping of the European legal framework for CNs.

2.4.5.3. A rapid assessment of the compromise

The following is of course a preliminary analysis, but the latest working documents seen by netCommons as we were concluding this report lead to the following assessment.

- **Lifting administrative burdens for Community Networks** has been identified as an important issue in some Member States. As the Open Letter read: "*In Belgium for instance, the registration fee that Telecom operators must pay to the NRA is at 676 € for the first registration, plus 557 € every following year (for those whose revenues are below 1 M€, which is the case for many community networks). Even such small fees can hinder the growth of small networks that efficiently serve tens of households.*" For what appears to be the first time, and after some MEPs had suggested language to that end, trilogue delegations agreed on the following principle:

  "*Recital 48: Competent authorities should duly take into account, when attaching conditions to the general authorisation and applying administrative charges, situations where electronic communications networks or services are provided by individuals on a not-for-profit basis. In the case of electronic communications networks and services not provided to the public it is appropriate to impose fewer and lighter conditions, if any at all, than are justified for electronic communications networks and services provided to the public.*

  Recital 52 (. . .) To the extent that the general authorisation system extends to undertakings with very small market shares, such as community-based network providers, or to service providers whose business model generates very limited revenues even in case of significant market penetration in terms of volumes, Member States should assess the possibility to establish an appropriate de minimis threshold for the imposition of administrative charges."

  This is of course optional, but for what appears to be the first time, **such language create an avenue for telecoms rules especially crafted for Community Networks.** It is a significant achievement for the

[151] https://netcommons.eu/?q=content/eu-parliament-workshop-community-networks-and-telecom-regulation

advocacy efforts made by netCommons over the past couple of years.

- **Regulators should take Community Networks into account when fulfilling their missions**. Article 3.3.e) agreed upon in the latest trilogues posit that NRAs, Member States, BEREC and the EU Commission, in fulfilling their missions pursuant to the code, should:
  "*take due account of the variety of conditions relating to infrastructure, competition, end-user and consumers circumstances that exist in the various geographic areas within a Member State* ***including local infrastructure managed by individuals on a not-for-profit basis*** " (our emphasis).
  It remains to be seen whether "local infrastructure managed by individuals on a not-for-profit basis" covers most of existing models for Community Networks (Freifunk and Ninux surely qualifies, but what about landline infrastructures managed by the Guifi.net foundation, Broadband for the Rural North (BARN), and other incorporated non-profits like FDN?). For-profit alternative providers, however, fear that the Code will create more bureaucracies and legal conundrum which are ill-adapted to their actual resources. But overall, this too can be seen as a success for CNs.
- In the same spirit, **regulators will still be able to safeguard competition of access seekers not participating in co-investment agreements**. The notion of "regulatory holidays" favoured by incumbent operators and the EU Commission has been significantly delimited. In the latest versions we have seen of the recitals, there are still possibilities for NRAs to conduct new market analysis every three years under certain conditions (recital 166), and there is still the possibility for NRAs to engage in asymmetric regulation (i.e., more stringent regulation of dominant market players). Most crucially for alternative providers like CNs, "NRAs should also safeguard the rights of access seekers who do not participate in a given co-investment" (which will almost surely never be the case for CNs which are way too small to enter such agreements). As for co-investment, we still do not have a clear understanding of what will be the relevant scale for market delimitation for the review of dominant positions (CNs like FDN have pointed out that NRAs should assess competition for relevant localities, rather than wide administrative divisions like the national territory or specific regions).
- **NRAs will retain the ability to impose active access obligations on network owners**, when "*access to passive [network] elements would be economically inefficient or physically impracticable*" (recital 165). Another condition also provides that the NRA must find that "*absent such an intervention [imposing active access], the purpose of the access obligation would be circumvented*". This line of thinking is reflected in article 59 on "access and obligations" and article 71 on "obligations of access to, and use of, specific network facilities". This is key for CNs who often cannot meet the financial conditions to connect themselves to the existing networks of incumbents to reach out to a small number of end-users. In that case, the Open Letter argued for the need of active access to lower the interconnection cost.
- **Unlicensed access to spectrum is encouraged by new provisions**. As the Open Letter explained that to prevent congestion, new "types of frequencies should (. . .) be made available either on an unlicensed (preferred scenario) or, if not possible, based on affordable and flexible authorization schemes." Recital 113 gives the context of these efforts:
  "*Shared use of spectrum increasingly ensures its effective and efficient use by allowing several independent users or devices to access the same frequency band under various types of legal regimes so as to make additional spectrum resources available, raise usage efficiency and facilitate spectrum access for new users. Shared use can be based on general authorisations or license-exempt use allowing, under specific sharing conditions, several users to access and use the same spectrum in different geographic areas or at different moments in time.*"
- **Policy-makers and telecom providers should not hinder the right to share one's Internet connection**. The right to share one's Internet connection has been undermined by so-called "secondary liability doctrines," national copyright laws as well as dangerous interpretations of the EU Court's McFadden ruling (see above). The new European Code of Electronic Communications brings useful developments in this regard, stressing that neither policy-makers of telecom providers should "*restrict or prevent end-users from allowing reciprocally or more generally accessing to the networks of such providers by other*

end-users through radio local area networks, including on the basis of third-party initiatives which aggregate and make publicly accessible the radio local area networks of different end-users" (article 55.3). The same article also stresses that "in any event", the liability exemptions provided by "Article 12 of Directive 2000/31/EC shall apply". Open WiFi sharing is a model pioneered by CNs like Freifunk and is actually encouraged by this new provision. The latter should be used to ensure that the right to share one's connection if effectively guaranteed. In the same spirit, telecom operators' contract clauses that forbid subscribers to share their connections with others must be prohibited.

Building on this, the Code goes on:

"*Article 4.4. The Commission, taking utmost account of the opinion of the Radio Spectrum Policy Group may submit legislative proposals to the European Parliament and the Council for establishing multiannual radio spectrum policy programmes. as well as for the release of harmonised spectrum for shared and unlicensed uses.*"

Article 45.2 also provides that Member States should "*e) [promote] the shared use of radio spectrum between similar and/or different uses of spectrum,*" and "*d) ensure maximisation of radio spectrum sharing.*" Article 46.1 on the authorisation of the use of radio spectrum also provides that:

"*Member States shall facilitate the use of radio spectrum, including shared use, under general authorisations and limit the granting of individual rights or of use for radio spectrum to situations where such rights are necessary to maximise efficient use in the light of demand (. . .).*"

All in all, this reiterates the Radio Spectrum Policy Programme of 2011 as discussed in D2.2 [7]. But here again, this is a policy tools that can be built upon.

To sum up, thanks to the efforts of netCommons, regulators (EU Commission, Member Stats, NRAs) will no longer be able to ignore the special policy needs of CNs. They are now incentivized to use new and already existing regulatory tools to adapt the regulatory regime to the special needs of CNs (in particular in the context of general authorisations, administrative charges, but also spectrum and obligations regarding the sharing of passive and active existing infrastructures). This is positive first step, and a way for CNs to start a dialogue with their respective NRA to make their regulatory needs known and taken into account at the national and European levels. Regarding co-investment, as Johannes Gungl, Chair BEREC, put it in a EU Parliament workshop, "*small players are too small to engage in negotiations for co-investment from a practical point of view. If a community wants to roll out a network, they should do it (. . .) on their own.*" [10].

2.4.6. National Legislation: Focus on Italy

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

This section describes 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 its legislation.

2.4.6.1. 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.

2.4.6.2. 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[152].

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[153].

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 in the Mc Fadden case analysed in Sec. 2.1.1.

2.4.6.3. 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[154].

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 WiFi networks based on 2.4, 5.4-5.7 GHz frequency. In case a CN is based solely on WiFi connections, as is the case of Italian CN ninux.org (see D1.1 [11] Sec. 5.2), no prior authorization to build and run the network is needed.

2.4.6.4. Authorization required for wired connections

While WiFi networks can be included among free uses, wired connections cannot. To build and run 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.

[152] 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, 67

[153] 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, 68

[154] 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, 473-479

2.4.6.5. 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[155]; 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.

[155] 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

3. Actual practice by and within CNs

After the description of the legal framework that applies and affects Community Networks, Chapter 3 intends to gather their reactions and practices through interviews and a survey, in order to understand the impact of this framework on CNs. Chapter 2 and 3 are complementary as they consist in presenting legal results of D4.1 to CNs before gathering their reaction and practices through interviews and a survey conducted and analysed in 2017, and presented in D4.2. In this way, the collection of data about community networks helps to understand the impact of the legal framework analysed above on their daily activity. More precisely, it delves into the critical issue of whether CNs actually correctly understand and apply existing laws. On this topic, results of D4.2 bring a mixed and in general rather complex answer. In the perspective of the **Best Practice Guide** to be written in conclusion of Work Package 4, the analysis of the survey is particularly enlightening. Thus, we reproduce most of last year's explanation and extend the analysis with a fresh look at these results based on the evolution of the legal framework and the CNs self-consciousness, also thanks to netCommons activity.

Before presenting these results in Sec. 3.2, we introduce the methodology adopted in conducting this research in Sec. 3.1.

3.1. Methodology of the survey

Based on the interviews conducted in the first months of 2017, an online questionnaire was designed and created through *Limesurvey*[1]. The tool was chosen because it came with anonymization features, and also because it allows for best resource usage as it is the same selected for the survey of Tasks 5.2, 5.3 and 5.4.

Focused on the legal daily life of CNs, this legal survey and its findings is complementary with through the larger political economic survey presented in D5.2 [12], D5.3 [13], and D5.4 [5],

This legal survey was divided into eight main sections that aimed to investigate CNs' aspects concerning both civil liability and personal data protection. The main sections relate to:

- **Services provided** by the CN: this group of questions aimed at exploring if and what services each CN offers and whether the services are offered against payment or not;
- **Organisation** of the CN: these questions were meant to understand whether the respondent CNs have a legal form and, regardless of that, how decisions are taken;
- **Distributed wireless network**: the queries investigated how distributed CNs are both in terms of property of the routers and in terms of routers management;
- **Liability** for users' behaviour: these questions asked whether liability cases have ever occurred and in the same vein investigated whether the single CN has a form of insurance;
- **Personal data (1)**: this set of questions focused on what kind of data CNs collect (if any) from their members/users and for what purposes;
- **Personal data (2)**: following the previous set of questions, this set meant to understand if and how users'/members' personal data are stored, where and how;
- **Relationship with users**: these queries were meant to understand whether CNs enter into contract with their users/members and in which way; the questions intended to find out if and how users/members are informed of the processing of their personal data;

[1] https://www.limesurvey.org/

- **Data retention**: the final set of questions were asked to understand whether CNs comply with national law on data retention, although some national laws do not comply with the requirements of the Court of Justice of the EU.

The survey included also two specific questions: the very first question asked the name and nationality of the CN. The respondents were reassured that the name of the CN would not be disclosed; however it was made explicit that knowing the name and nationality of the network would help to understand what law should apply and it would obviously also allow to manage possible multiple responses from different members of the same community.

The very last question investigated whether the CN had ever **benefited from legal advice** (either by a lawyer or a legal researcher) and if so, how often this had happened. The question intended to address the needs of CNs for legal advice as one of the outcomes of WP4 is the creation of guidelines to help CNs to deal with legal requirements and legal issues.

The survey, whose questions, as they appeared on the survey site are reported in Appendix A for easy reference, was opened at the end of August 2017 and run until the mid of October 2017. It was advertised via e-mail to all the known CNs in Europe. The responses obtained come from 5 countries, while the interviews covered also another country, for a total of **6 different countries**.

In 2018, while developing this Deliverable, we re-analyse these results afresh. We **substantially relied on the previous findings that we confirm and deepen**. We also choose, instead of a table, to present them with **graphs** and **percentages** to allow for a clearer and more synthetic read.

3.2. Results of the survey

The aim of this survey is describing and analysing in order to understand how CNs actually deal with laws – mostly on civil liability and personal data protection. Conversely, it also study the impact of law on community networks' model.

3.2.1. Organisation

From the point of view of organization, the slight majority of respondents do not have a legal status.

3.2.1.1. Do Community networks adopt a legal form?

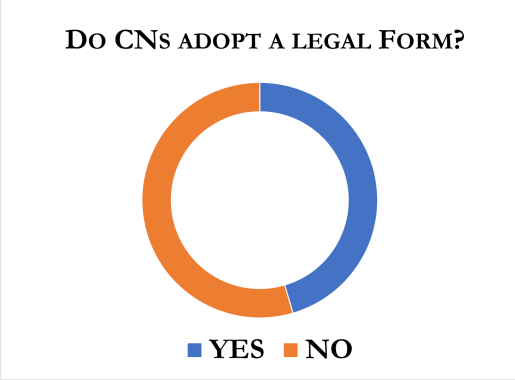


Figure 3.1.: Organisation and legal form

Although in many cases decisions are nonetheless taken at a central level, implying a sort of central organization, in 55% of interviewed CNs there is no formal entity nor any legal status, as presented in Fig. 3.1. These

CNs seems to have developed as a spontaneous group of people with no need to formalize their status. As things currently stand, probably these CNs have never felt the need nor have been obliged to undertake a process of "formalization".

Thus, only 45% of respondents do have a legal form. Mostly, they choose to be an association, as only one of the respondents is organized as a cooperative – which is a cross-over between an association and a small company. In both case, these legal forms do not have to much constraints and let CNs adopt their own kind of management and democratic process of decision (see below).

Regarding formalization as well, some respondents qualified themselves as ISP or IAP. These CNs probably asked and obtained an authorization by their National Registration Agency. This implies that the rules on intermediary liability (summarized above) need to be taken into account for these CNs.

Besides, 18% have declared that their CN is insured by an insurance company for the case of liability. Surprisingly, all of these CNs are French. Therefore, this choice may be the outcome of their specific models, where they often share server space and other infrastructures in collocation facilities which require their members to have such insurance.

3.2.1.2. What level of organizational centralisation do CNs have?

Even though their organisation is not legally formalized, in order to provide their telecommunication services and for the needs of administration, most CNs **have to** rely on core members who act as a de facto proxy for the rest of community for certain tasks. Among CNs with no formal structure, 70% do have a central entity, as shown in Fig. 3.2.

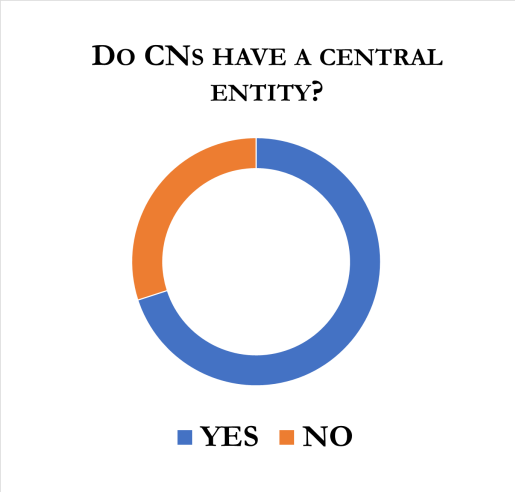


Figure 3.2.: Organisation and centralisation

To evaluate to what extent CNs are decentralized, the questions touched on the ownership and management of routers and routers as well as decision-making processes.

As for property, there is no general trend. Routers can be owned and managed by the CN or by the users; in some cases the CN owns all the routers but lets users manage them, in other cases the opposite is true.

It is interesting to notice that whenever the CN manages the routers (regardless of the ownership), the CN itself is organized as a legal entity. This might be the result of the fact that CNs organized as associations or cooperatives might have funds for managing and maintaining the network, and/or they might have stable collaborators or employees that can take care of these aspects.

3.2.1.3. How do Community networks take their decisions?

Irrespective of the ownership of the routers, it is relevant to observe that all but two of the respondents CNs place high importance on decisional processes. When asked "Where decisions are made by individual participants, how are these decisions taken?" the respondents have meaningfully answered with terms such as "collective decisions", "horizontal approach", "discussions among participants", "important/bigger decisions require plenary sessions", "participative decision-making in assemblies".

These expressions clearly suggest the importance that CNs place in member participation and are an indicator of distribution of power and commons-based governance.

3.2.2. Services offered

Regarding services provided by surveyed CNs, results show that the core activity of Community Networks is to provide Internet access through WiFi. 100% of them use a wireless technology. In addition, 30% of them also provide access through cables, usually optical fibers. Fig. 3.3 summarizes this state.

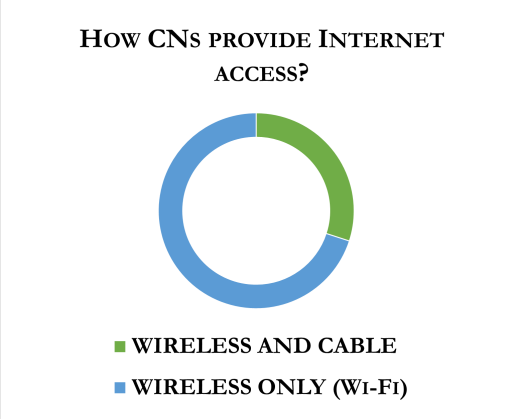


Figure 3.3.: Service offered and core activity

3.2.2.1. What additional services do CNs offer?

Aside from Internet access *per se*, Community networks tend to offer other services to their users, as sumarized in Fig. 3.4.

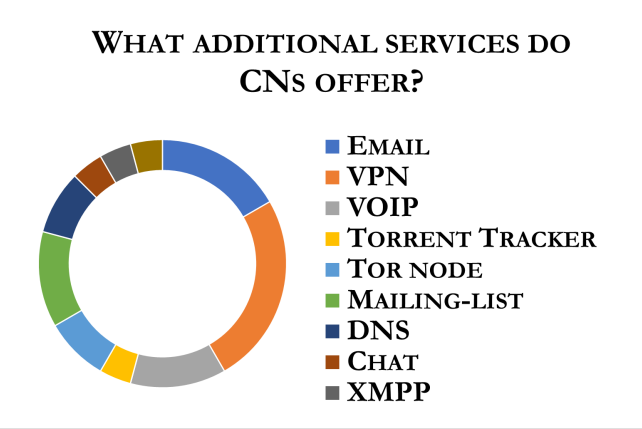


Figure 3.4.: Service offered and additional activities

CNs often offer a wide range of additional services, especially basic resources such as email or anonymity tools, including Tor nodes. Also, they provide technical resources to promote empowerment and autonomy of their users, such as DNS.

3.2.2.2. Do CNs provide Internet access free of charge?

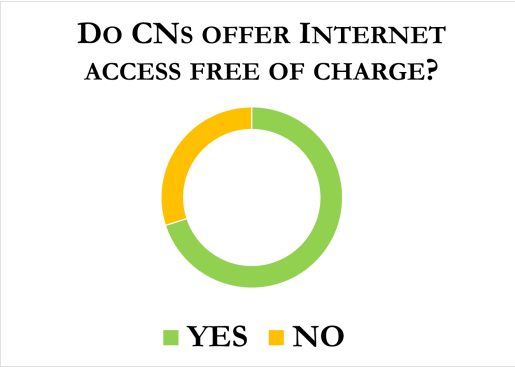


Figure 3.5.: Services offered and payment

70% of CNs surveyed declare providing Internet access for free, as shown in Fig. 3.5. Furthermore, even when CNs are actually charging their end-users, most of them make sure to *"deploy free access point in some critical areas."*

In one instance, this fee goes hand in hand with the qualification of the CN as an ISP, more precisely a non-profit ISP.

On the contrary, in another instance a CN did not qualify itself as an ISP or an Internet Access Provider (IAP); however, it is a cooperative. These characteristics are probably linked to one another.

A final remark can be made with regard to the method of offering Internet connectivity adopted by a CN in Greece. This CN can supply Internet connectivity thanks to the partnership with a local university. This synergy between the CN and the university is an interesting instance of cooperation. In addition, it represents a stimulating model that could be replicated elsewhere in the same country or in other European countries.

3.2.3. Relationship with users

Community Networks, as community-based relationship, rarely formalize a contract with their users. They often rely on an informal, flexible and trust-based relationship, as shown in Fig. 3.6.

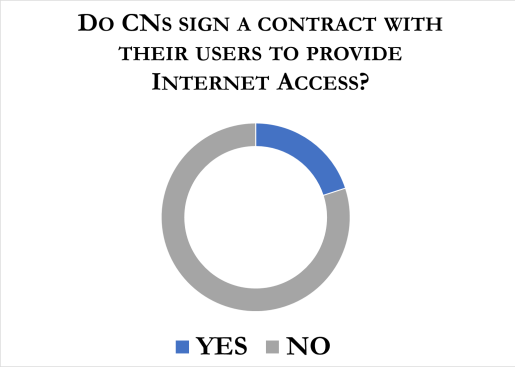


Figure 3.6.: Relationship with users and contract

Moreover, when such an agreement do exist, they often state basic ethical guidelines but sometimes also distributes obligations and liabilities for their participation in the project. However such a distribution is not often very elaborated.

A peculiar approach is the one of CN in Portugal: they require users to sign the "project user/participant agreement" that is based on the pico-peering agreement[2]. The respondent briefly describes the contents of the agreement and specifies that the agreement "*establishes basic guidelines, distributes obligations and liabilities for participation in the project and also that give each participant the possibility of determining which resources are made available to the project and how they should or can be used as long as they do not contravene mandatory clauses.*"

The most interesting part of this answer is the one where it is clarified that the agreement "distributes liabilities".

This is of utmost importance for the case of civil wrongdoing: distributing liability to users via contractual clauses could be a way to save the CN from users' wrongdoing. This is indeed the same strategy adopted by commercial providers.

Another CN answered that there is no contract with users, but it nonetheless declared that users have to sign an agreement (CN France 4). This agreement also specifies that users shall not circulate illegal content. The other CNs apparently rely on informal relationships with their users.

This approach has both positive and negative aspects. On the positive side, an informal relationship denotes trust between users and CNs as well as among users; it gives flexibility to the entire structure of the CN and it probably encourages new users to enter in the community. On the negative side, and with special reference to law, the lack of a contract means that the CN cannot dictate users' rights and duties, including the distribution of liability. In addition, it becomes more difficult to deal with data protection laws. Although many CNs stated that the policy governing data collection and processing is displayed on their websites, this might not be enough for an informed consent as required by Directive 95/46 and especially by Regulation 679/2016. This issue is one of the thorniest for CNs, as highlighted also by the answers on data processing and data retention that follow.

3.2.3.1. Do CNs provide their services regardless of social characteristics?

82% of community networks interviewed offer their services to any person. Sometimes, being a end-user of their services imply to be or become part of the community (8%).

In particular, one of the respondents states that their users need to be member of the cooperative running the CN; therefore, even though there might not be a contract detailing rights and duties of users, there is still the need for any user to take part to the cooperative. This in turn implies agreeing to the contract establishing the cooperative that usually includes also members' rights and duties. Indeed, the respondent specifically stated that paying users are also members and have a right to vote in decision making processes as well as a right to act on the network to keep it up and running (although only a small number of members do).

In some country, CNs try to rationalize their deployment and focus on a specific geographical location, letting other similar structures focus on others (9% of the respondents are doing so in their regions). But even in these cases, as detailed above, CNs often deploy free access points in *"critical places"*.

However, none of the respondents choose to provide Internet access only to a restricted group or individuals, such as unemployed or low-income individuals. It seems that Community Networks do not intend to have a "positive discrimination" or "affirmative action" policy while conducting their activities. They provide Internet services and additional services regardless of any social feature.

The last two sections of the survey concern personal data protection. Considering the answers given by the respondents, this is the area in which CNs lack most knowledge of the legal framework and of the corresponding

[2]the Pico Peering Agreement is a template of contract among CNs' participants which could provide for the delegation of their obligations, see http://www.picopeer.net/PPA-en.shtml

obligations pursuant to European and national laws.

3.2.4. Processed data

Regarding data processing, a divergence need to be highlighted between what Community Networks stated in the survey, and what they concretely report. Indeed, a **misconception of the scope of personal data** seems to be shared among several CNs. Therefore, 30% of them declare that they do process personal data of their users. However, their replies describing their processing imply that they are all dealing with personal data. Indeed, they process a wide range of personal data, from IP, MAC, e-mail and postal addresses to phone numbers and name. Fig. 3.7 summarizes the data that CNs actually process, clearly showing that they often handle personal data too.

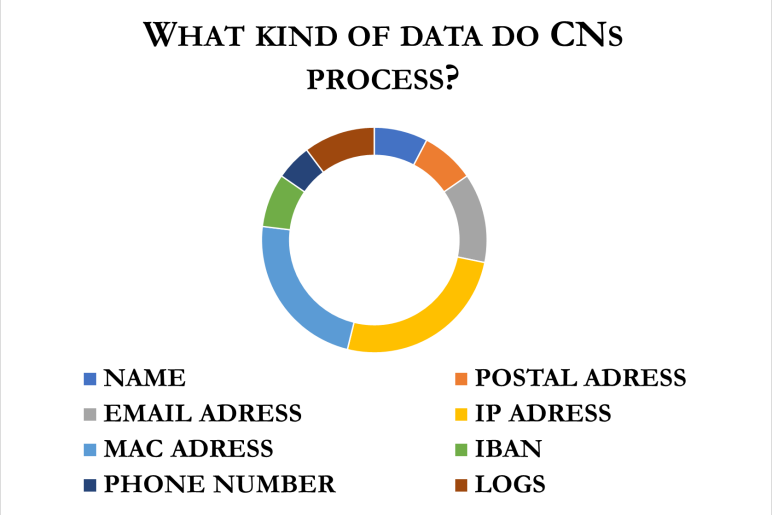


Figure 3.7.: Processed data and personal data

Although the majority of the surveyed CNs do not collect names and addresses of their users, they still somehow know and hold a lot of different information about their users. While some of this information is clearly personal data (IP addresses, bank account information, e-mail addresses), some other may also be qualified as such according to the case law of the CJEU and according to the Article 29 Data Protection Working Party.

Indeed, the Court of Justice of the EU has interpreted the definition of personal data as encompassing information that *prima facie* might not seem to be personal, but that may gain this qualification because of the processing it undergoes. The difference is that, this time, IP addresses are qualified as personal data as they are linked to an identifiable person. For instance, it means that IP addresses –and information similar to them– are personal data even when collected and stored by someone who cannot directly associate IP addresses with users' real identity if there is someone else who can be asked to associate this information. This is relevant for the answers given by the majority of the respondents to the survey since almost all of them collect IP addresses.

In two cases, IP addresses are even stored associated with users' names. Many of the respondents also process several other information that might qualify as personal, such as MAC adresses, WiFi logs, Universal Resource Locators (URLs) of accessed websites, and so on. Nobody seems to realize that a URL is a content of a communication and not Traffic Data.

Only one of the respondents seems to handle data in a way that could not be linked to the real identity. They declared: "*we do not collect anything we think is personal data about our users, we also do not know which data we collected is by which user*".

Moreover, the list of data they collect and store does not include either personal information (name, surname, ...) or IP addresses. The way this CN describes how it handles data recalls anonymous data that is not subject

to either Directive 95/46/CE41 or Regulation 679/201642.

Given that the data mentioned in CNs' responses to the survey are mainly personal data, the collection and possible storage of such information surely constitutes an act of processing personal data according to art. 4(2), Reg. 679/2016.

One of the questions of the survey inquired if and how CNs supply their users/members with information related to personal data protection rights. The respondents mainly inform their users about personal data processing through the main web page of the CN, very often via a wiki.

Only very few CNs seem to offer clear information to users on their rights under data protection laws. Some CNs, in accordance with their idea that they do not collect personal data at all, do not offer any information on how data is processed and on users' rights. Only in one case the CN informs its users through the contract by which users join the network.

Consent makes the vast majority or processing activities lawful. For instance, a problem arises regarding one CN explicitly answered that sometimes it transfers data overseas. There are a number of mechanisms that govern so-called "transborder data flows", but the presence of a data subject's consent makes any of those mechanisms not relevant. As long as there is users' consent, data can be transferred in any country outside EU regardless of the level of protection offered in the country where data is transferred (art. 49, Reg. 679/2016).

The same CN also declared that they offer a cloud service. The interaction between cloud services and personal data protection law is another thorny issue. The CN does not specify whether the transfer of data overseas is linked to the cloud service or not. If so, what just described applies to cloud services as well.

If not, then data have to be handled as if stored in a database on the European Union territory. Once again, obtaining data subjects' informed consent is the first step to have a legal processing of personal data.

In addition, some CNs' activities could be qualified as Electronic Communication Services (ECS) and therefore be subject to Dir. 2002/58/CE (soon to be repealed by a new regulation mentioned above, so called ePrivacy Regulation). Despite the fact that the qualification of CNs' services as ECS is questioned, it should be noted that some other duties come from the application of this directive especially with regard to traffic data and their retention, as the next paragraphs illustrates.

3.2.5. Data retention

The answers given by CNs as for data retention provide a very interesting insight of the impact of the legal framework on them. Except for a CN that stated that as they do not collect personal data, they do not retain personal data, the other respondents can be divided into two groups: those who retain data to comply with national law and those who do not, as shown in Fig. 3.8.

Only 40% of the respondents declare retaining data to comply with legal obligations. Here, replies are directly based upon the nationality of the CN responding. Interestingly, all French CNs, the Portuguese and the Greel CNs declare being compliant, while all the German CNs and the Slovenian do not retain data.

Our first year findings highlighted that the majority of EU Member States have laws requiring providers of ECSs to retain traffic and location data for a specific period of time. At the time of the survey[3], Germany did not have data retention obligations. More precisely, even though a law existed, it was not applied as German courts have declared its invalidity(See, Sec. 2.3.3.3.1).

Hence, while the law should have started being applied from July 1st, 2017, this did not happen. This might be the reason why German CNs do not retain data. Another possible explanation is that German CNs do not consider themselves as providers of ECSs and therefore do not feel anyway obliged to retain data.

On the contrary, at first sight French CNs seem to comply with the law as they declared they retain data only to fulfill legal obligations. However, looking more closely at what data is retained, some French CNs actually fail to retain all the data requested by French law.

[3]For the updated German framework on data retention, see par. 2.3.3.3

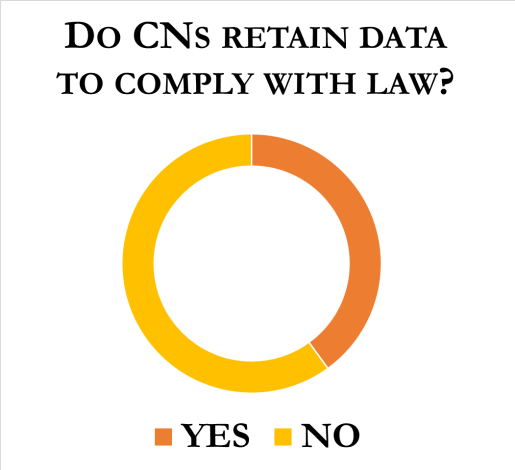


Figure 3.8.: Data retention and compliance with national law

For instance, CN France 3 does not retain data related to recipients (IP addresses consulted by a user), when conservative readings of French law would push them to do so asks[4].

3.3. Specific interviews

As a preliminary study in order to design the survey four interviews were conducted with Community Networks. These answers, already described in D4.2, let to refine the above-mentioned findings.

Each community is unique and has its own way of managing a network. Therefore, such interviews do not cover the wide range of Community Networks' behaviour and philosophy. However, we focused on four of them, two from France and two from Italy, with different characteristics:

- one very tiny and discrete;
- one very structured and almost professionalized;
- one very informal and highly-decentralized;
- one rather in between those categories (size, publicity, formal/informal, and level of decentralization).

This way, we aimed to have a holistic and refined perspective of the practice of legal requirements by and within Community Networks and also pinpoint the impact of these obligations on CNs.

As for **civil liability**, three out of four CNs are organized as associations. This means that national laws would apply in case a civil wrongdoing happened. Normally, this entails that the president of the association will be responsible and liable for these wrongdoings. In the case of an Italian CN, also other people in charge of the association's obligations might be held liable, in case the wrongdoing happened as a consequence of their actions (for instance, a leakage of information is due to the lack of update of a software and the update was to be carried out by a specific person within the association).

In the meantime, however, users –who are also members of the associations– sign a contract in which they bear the civil liability for wrongdoing committed by themselves or someone else using their login/password.

They also commit themselves not to use P2P software, in order not to impair shared resources. One Italian CN offers Internet to its subscribers; however it is not an IAP from a legal point of view. Hence, it cannot enjoy the liability limitations offered by art. 12, Dir. 2000/31 and its Italian correspondent art. 14, d.lgs. 70/2003.

The opposite is true for the two French CNs that qualify as IAP and therefore can enjoy the liability limitations introduced by EU law.

[4] See D4.1, Sec. 4.5.10.

In the case of an Italian CN, there is no legal entity behind the community; the community seems to be highly decentralized and with no person in charge of it. This would probably mean that in case of wrongful action no one could be held liable, unless everyone could be considered as a contributor to the wrongdoing.

There is however the issue of shared connections. Although in the Italian context there is no liability for WiFi sharing, the gateway user (that is, the user sharing their connection) might be contractually liable towards their IAP in case the contract forbids sharing the connection.

75% of CN interviewed ask their users to sign Terms of Service (ToS) in which they also agree to the **processing of personal data**. However, the information given to users is sometimes incomplete; for instance, in both French CNs the ToS do not specify all the kind of processing that are actually carried out.

In the case of one Italian CN, the information that the users have to sign is outdated, as it refers to a law (L. 31.12.1996, n. 675) that was repealed and substituted many years ago. In addition, no attention is paid to "sensitive data", although it could be part of what is stored, for instance through the hosting service.

The French CNs collect and retain personal data for billing purposes. In the case of this same Italian CN, data is also retained as a database of the association.

Often, users can modify their data: for instance, in another Italian CN they can ask modification at any time and every year they are asked to confirm whether the information stored by the CN are still accurate.

In the two French CNs users can access a personal page where they can modify their information. All of the four interviewed CNs retain technical data to allow for maintenance; the data is retained to allow for security.

In addition, 75% of CNs interviewed retain log data to comply with the national laws. In particular, the French CNs retain data for 1 year; the Italian one retains data for 6 months. This is in partial contrast with our findings of the first year, as according to the Italian legislation in force, data should be retained for 1 year.

The same three CNs also monitor and retain some data in order to understand whether there are violation of the ToS, for instance whether there is P2P traffic.

3.4. Overall analysis of the survey: Impact of the legal framework on CNs

CNs and compliance: growing concerns and interests about legal resources

The very last question of the survey investigated whether CNs are supported and advised in their activities by legal experts. While many of the respondents have never benefited from the advice of a lawyer, **some of them clearly stated that they needed to rely on a lawyer more than once** in the CN lifetime. In one case, the respondent underlines that the CN **has been looking for a *pro-bono* lawyer for a long time**. Thus, first the apparent lack of attention of many CNs to legal details is not due to negligence, but to the utter difficulty in accessing legal advice and finding a way in this maze of rules and regulations.

These answers highlight the need for CN to have clear guidance in the field of law: as seen and demonstrated in D4.1, the current legal framework for CNs is far from clear both in terms of civil liability and of personal data protection. Legal uncertainties do impair the growth and prosperity of CNs, and they seem to be well-aware of it. For this reason, clear guidelines would be a valuable tool for community networks and their sustainability.

Henceforth, to offer perspectives of growth for communities, such preliminary legal guidelines will be defined (Chapter 4), while in the future, advocacy work might help change the legal framework in a more welcoming one (Chapter 5).

4. General guidelines regarding the legal framework

This chapter is divided in two parts. The first one gives general recommendations in reliance with the European framework, whereas the second one aims to deliver a tailored approach based on national law.

4.1. European framework

Six main guidelines relying on the work and findings of Task 4.1 have emerged and are represented here as separate Sections. Each section contains a sharp ”short recommendation” and it is then developed with explanations, legal references and additional reasoning as needed. The goal is to settle preliminary recommendations that can be shared with CNs and, for each, a general approach to be refined during Task 4.3 and reported in Deliverable 4.5 ”Best Practices Guide for CNs” at M36.

4.1.1. Adopting a legal form

4.1.1.1. Short recommendation

We recommend that Community networks adopt a suitable legal form to conduct their activity –association, cooperative, foundation or other non-profit organisation form, depending on what their national laws offer.

4.1.1.2. References and legal reasoning

Insofar as CNs determine the means and purpose of the processing of users' data, they qualify as data controller under art. 4(7) of the GDPR. When a Community Network is organized as an association or cooperative, there is a legal entity and therefore there are no issue in determining who the data controller is, being it a natural or legal person. On the contrary, when the CN does not have any specific legal form, it becomes more difficult to understand who is the controller, and liability might bear only on private individuals participating in running the network. Thus, to mitigate legal risks and share liability, it is more suitable to adopt a legal form.

4.1.1.3. Further comments: toward a forced professionalization process of CNs?

Community Networks manage a commons infrastructure for telecommunication build by the community for the said community. However, the legal framework, by identifying them as Internet Service Providers or Internet Access providers considers them as players which should be highly regulated and therefore can impose many obligations on them.

Yet, complying with these –sometimes heavy– requirements tends to shape the organisation of people conducting these activities. Unfortunately, this trend can clash with the core values of CNs, which instead promotes a decentralized, horizontal and often very informal approach of management of infrastructure (see Sec. 3.2.3).

While waiting for advocacy work to alleviate some of their regulatory burdens, a balance between mitigating legal risks and maintaining their original model should be found. For instance, while having an insurance, as some of the French CNs, may be useful, this additional protection is not mandatory. Furthermore, several legal forms imply minor constraints and do not necessarily clash with the alternative process of decision often adopted among CNs. In France for instance, being an association do not seem to impair it and Community Networks often adopt this legal form.

4.1.2. Anonymising processed data and inform users

4.1.2.1. Short recommendation

Aside from technical or legal requirements, we recommend to anonymize as much as possible the data processed. At the same time, we recommend to emphasize the information of users and state in a clear and plain language, the purpose for data processing for which consent is requested.

4.1.2.2. References and legal reasoning

The scope of the GDPR and data protection's principles does not apply to anonymous data –namely "*information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*"[1]. Simply put, as long as they **cannot be attributed to any individual, by anyone, in any circumstance** data is not personal. Thus, anonymizing data would be a good practice to reduce legal risks. As underlined in the results of the survey, it is encouraging to note that some CN seem to achieve this goal[2]. They declared: "*we do not collect anything we think is personal data about our users, **we also do not know which data we collected is by which user***"[3].

However, **truly anonymous data are rare** and if they can be attributed in a way to a specific data subject, they can be regarded as personal data and fall within the scope of the GDPR. Therefore, it would be safer for CNs to also take into account obligations regarding informed consent and transparency[4].

Any CN should provide its users/members with information about their rights with regard to their personal data processing. In particular, the information provided through the web page of the CN should comply with the requirements introduced by art. 12, Reg. 679/2016: Information should be provided "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*". Any CN should provide its users with such information before processing data.

4.1.2.3. Further comments: the scope of personal data

As previously underlined, Community Networks tends to **underestimate the scope of personal data** and, as a consequence, obligations weighting on them in terms of data protection. In this perspective, it would be safer for CN to consider that every piece of data processed is likely to be regarded as personal. To help them understand the scope of this legal concept, a concrete and exhaustive list of these sensitive information will be written down and disseminated among CNs together with Deliverable 4.5 "Best Practices Guide for CNs".

4.1.3. Signing a contract with their users

4.1.3.1. Short recommendation

We recommend that Community networks sign a contract with their user when offering to provide a service –either Internet access or additional services.

4.1.3.2. References and legal reasoning

Signing a contract with users seems an appropriate measure to avoid legal risks.

[1] GDPR, mentioned above, (26).
[2] Regarding anonymisation, see Art. 29 Working Party, "Opinion 05/2014 on Anonymisation Techniques", Apr. 10 2014.
[3] See, Sec. 3.2.4
[4] On this subject, Art. 29 WP published guidelines regarding consent which will be a reliable basis to draft more specific guidelines in the upcoming Best Practice Guide; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Concerning data protection law, the GDPR states that a lawful processing of personal data –which CNs have to do in order to provide their services– requires a *legitimate interest*, *consent* or *contract*[5]. Of all these legal basis for personal data processing, the more reliable is the contractualisation of a data processor's relationship with their user. Indeed, the extent of the legitimate interest is difficult to evaluate with certainty.

Such an agreement could help establish a transparent relationship between a CN and its members and users. It could also contain provisions in order to distribute liability.

4.1.3.3. Further comments: contractualisation, informal relationship and empowerment of users

When they provide their services, CNs originally tend to have a **trust-based** and informal relationship[6] with their users. Thus, contractualisation may be difficult to implement for CNs which often have a more informal behaviour and flexible relationship with end-users. However, signing a contract with users may also be in line with others values strongly upheld by Community Networks. Indeed, such an agreement could contain information and, as such, promote understanding and empowerment of users.

4.1.4. Using a dedicated communication tool with users for security measure information

4.1.4.1. Short recommendation

Community Networks should set a dedicated communication tool that its participants may use to notify dangerous security breaches to the whole community. Then, in case of a security breach, they should notify the said breach within 72 hours.

4.1.4.2. References and legal reasoning

The GDPR emphasizes informing end-users of measures adopted regarding security. Controllers and processors shall implement appropriate technical and organisational measures to ensure an appropriate level of security to avoid personal data breach –namely, that personal data are not accidentally or unlawfully lost, altered, disclosed or accessed in a manner likely to result in a risk for the data subjects, in reliance with the scope of 'personal data breach' stated in GDPR, Article 4.

Moreover, if such a personal data breach occurs, the controller shall notify the security breach to the competent DPA within 72 hours –or later if it can explain why this deadline could not be met[7].

As a consequence, since CNs shall comply with this obligation for all of their activities it would be more efficient to implement cross-activities procedures in order to promptly react to any security breach. For instance, setting a dedicated communication tool that its participants may use to notify breaches to the community and inform users would be an appropriate measure to comply with GDPR.

It must be noted that all of this refers only to cases where the security breach imply with high probability the loss of personal data that is managed by the CN, it does not apply to (much more common) security attacks to the infrastructure, non successful intrusion attempts, denial of service attacks, intrusions into single accounts, and so on and so forth.

4.1.4.3. Further comments: fostering communication and information within each community

This measure could be regarded as a pooling of resources and participate to a common management of risks of security breach. This logic seems perfectly in line with the community-based model of CNs as well as their management of networks as a common good. Moreover, such a global information tool could also be a

[5] See, GDPR art. 6.
[6] See results of the survey conducted in 2017, detailed in D4.2 Sec. 3.2.3
[7] GDPR, Article 33.

great opportunity to emphasizes interaction, integration and engagement of users within the community –as an incentive for users to play a more active role in CNs. It could also widen the scope of information available for users and therefore foster digital literacy, awareness and understanding regarding the concerning topic of networks' security.

4.1.5. Clearly distributing obligations and corresponding liability

4.1.5.1. Short recommendation

A general recommendation for CNs would be to distribute as much as possible obligations and liabilities among members of the community and make sure that this distribution is clear for all involved parties. However, this general view call several comments and further clarification.

4.1.5.2. Recommendations, references and legal reasoning

In terms of liability, two different situation should be distinguished.

First, liability concerning **unlawful information** or content. In reliance with the McFadden case law (Sec. 2.1.1) and specific national provisions (Sec. 2.1.2), CNs should enjoy the liability exemptions introduced by Directive 2000/31, but at the same time they might be the target of injunctions to secure their connection (such as password-protect it).

Second, liability concerning the whole management of the network as a physical infrastructure able to generate physical damages. As a network is composed of different parts, those can be under the control of a **CN or its central entity**, a **user** or a **third party** –and imply therefore a different outcome regarding liability.

In each situation, choices has to be made between autonomisation of users, mutualisation of risks –with an insurance,– or decentralisation of obligations and responsibility –with a dedicated agreement.

When there is a legal 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.

Further information on this topic will be provided in the D4.5 "Best Practices Guide for CNs" in order to establish a suitable and clear distribution of liability, including a **template of terms of use**.

4.1.6. Being cautious with data retention

The issue of data retention is a **thorny** one, which could not be abstracted in a short recommendation. It requires a deeper analysis as CNs are in different position depending on their country. Moreover, their practice in this regard could be seen as part of an advocacy action that should be clearly explained as we discuss in the following.

4.1.6.1. Recommendations, references and legal reasoning

According to the **Precedence principle**[8], EU law has precedence over *any* national law. This implies that if a national rule is contrary to a European provision, the binding force of this **Member State's rule** is regarded as **suspended**[9].

[8] Court of Justice of the European Community, 15 July 1964, *Flaminio Costa v E.N.E.L*, Case 6/64, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:61964CJ0006&from=EN; for a clear introduction to the principle: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14548&from=FR

[9] Court of Justice of the European Community, 15 July 1964, *Flaminio Costa v E.N.E.L*, Case 6/64

As a consequence, on the principle, CNs should comply with the *European* legal framework. Regarding data retention, this refers to the *Tele2* case law[10].

To be specific, in light of this decision, national laws should not provide for:

1. **Indiscriminate and general collection** of data;
2. Access for an objective wider than **fighting serious crime**;
3. Without a **prior review by a court** or an independent administrative authority; **or**
4. Without an obligation of retention of these data **within the European Union**.

Indeed, several national frameworks were declared inconsistent with EU law or unconstitutional by local judges. In some of them, laws were repealed (e.g. Netherlands[11], Slovakia[12]...). In other countries, laws were set aside and operators which did not retain data as prescribed by their national laws were not sanctioned[13].

However, in most of them, there is no clear legal answer to whether national laws should still be in force. In accordance with EU criteria, high doubts of compliance could be raised regarding:

- The German legal framework, which had been declared inconsistent with EU law by a national court[14];
- The Spanish legal framework, in which categories of data that shall be retained are exactly the same as in the European Data Retention Directive of 2006 (invalidated);
- The Greek legal framework, in which categories of data that shall be retained are exactly the same as in the European Data Retention Directive of 2006 (invalidated);
- The French legal framework, which could be regarded as providing indiscriminate collection;
- The Italian legal framework, which could be regarded as providing indiscriminate collection during a disproportionate amount of time.

Therefore, where a country has such a national statute in breach of EU case law, CNs could theoretically be free not to comply with the national law. Yet, in all of these legal frameworks **serious fines exist** for Community Network that do not comply with data retention obligations (see Sec. 2.3.3). Therefore, a legal risk does exist for them.

As blanket data retention obligations goes against the core values of CNs, as expressed for instance in the Open Letter to EU policy-makers, they often tend to refuse to comply with such national provisions (60% of the CNs respondents of the 2017 survey are in this situation). Thus, several hypothesis should be considered:

1. If CNs want to reduce legal risk, they could strictly comply with national law –except when a public statement provided expressly that no fine proceedings would be started against non compliant providers (e.g., as in Germany, see Sec. 2.3.3.3). However, over-compliance also generates legal risks for CNs. Indeed, if a CN has a data retention system exceeding its legal framework –e.g., in terms of scope of data or duration of retention– this activity could be regarded as an **unlawful processing** since this additional retention would no longer be "*necessary for compliance with a legal obligation to which the controller is subject*"[15].
2. If CNs want to comply with practical requirements while avoiding over-compliance issues, a compromise could be reached. They could reduce the scope of data retained to the one that is *actually* demanded by public authority while conducting their investigations: IP addresses and suscriber ID. This would not respect the letter of the law, and therefore implies theoretical legal risks. However, such data would be

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62015CJ0203&from=FR; For an analysis see of this case, see Sec. 2.3.2.2

[11] [https://edri.org/dutch-data-retention-law-struck-down-for-now/]

[12] https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/

[13] See, for instance, three German decisions (OVG Münster 13 B 238/17 ; VG Köln 9 K 7417/17 and 9 K 3859/16) all described in Sec. 2.3.3.3

[14] See, Sec. 2.3.3.3

[15] GDPR, art. 7, (c).

enough to comply with most requests of access –which are very rare in the experience of Community Networks.

3. If CNs want to actively take part of the advocacy against blanket data retention they could choose to ignore data retention provisions. However, they should keep in mind that this choice come with a legal risk, as they could be prosecuted by national authorities. To mitigate this risk, if they are sanctioned, they still have the possibility to challenge this decision before national courts, arguing that the obligation is inconsistent with EU law and so is the fine applied to them. In this regard, this deliverable as well as D4.1 and D4.2 provides a wide range of comparative law material between and include a complete description of the current European requirements. Relying on social bonds created with the netCommons research team and Telecommons mailing list's members, they would be able to find legal support in such a thorny situation.

In any case, in order to defend their view of digital human rights and to clear an ambiguous legal framework, they could take part in other advocacy actions in order to solve this uneasy situation. Advocacy actions that we will describe in Chapter 5, and which precisely focus this year on fighting blanket data retention all over Europe (see Sec. 5.1) and voicing common concerns regarding ePrivacy Directive's ongoing negotiations.

4.2. National Frameworks

To offer more specific recommendation to CNs, we focused on two national frameworks: - France through general short practical guides; - Italy through an individualised support.

4.2.1. Short practical guides for communities and their allies

The research on advocacy conducted with the D1.5 pointed out that legal analysis should be disseminated through the release of written briefs that can educate CNs participants and the public at large, especially regarding policy developments affecting the life of a CN. Aiming to fulfill that goal, two practical guides have drafted in cooperation with FFDN, a French community networks and La Quadrature du Net, an NGO defending digital rights with which we already worked (see, D1.5, Sec. 3.3.3 p. 33)

4.2.1.1. French practical guide for CNs and organisations providing an open access to the Internet

The first guide aimed to offer clear and synthetic guidelines for organisations providing an open access to the Internet (such as CNs, CN members, but also libraries or Internet cafes). It explains, in French, what are their legal obligations with respect to data retention, data processing and Net neutrality (see Appendix B).

Emphasizing the specificity of data retention obligations, this guide answers to the following issues:

1. Which websites can be blocked?
2. Which data can be collected?
3. Which data must be retained?

These guidelines were presented to the French associations of librarians during their annual congress on Monday January 29, 2018 at the *'Bibliothèques des langues orientales'*, in Paris.

This publication advertisement and was relayed in a legal newspapers which has a wide publicity among public bodies, especially at the local level: *"La Gazette des Communes"*[16].

It was also presented on the netCommons website[17], on the CNRS website[18], on the website of La Quadrature

[16] See, http://www.lagazettedescommunes.com/548375/neutralite-du-net-et-donnees-collectees-quels-sont-les-droits-et-devoirs-des-bibliotheques/

[17] https://netcommons.eu/?q=content/french-pratical-guide-cns-and-organisations-providing-open-access-internet

[18] http://www.cil.cnrs.fr/CIL/spip.php?article3035

du net[19] and on other library websites or digital educational websites[20]. We have had several informal reports from French CNs that they had also sent the guide to local librarians or city officials to convince them to not spy on their users communication or require undue authentication.

These blogposts and articles are mostly in French since the scope of the guide is focused on French access providers. However, having this reduced scope can ensure the relevance of the guide for the targeted communities. Indeed, these local initiatives are often more targeted to their needs and accessible for them. This first release also served as a testbase for other guides regarding French law and the more general legal guidelines of D4.5, which will be based on European law.

4.2.1.2. French practical guide for CNs and organisations providing hosting services

In continuation with the first practical guide, a second specific study was launched for hosting services. Substantially, it offers legal guidelines to address data retention divergent obligations –between EU and national law. To achieve this goal, this synthetic guide summarizes the French framework and the European one. After doing so, it offers a concrete guideline of setting aside the national law, inconsistent with EU requirements. Relying on the precedent principle and taking into account high sanction fees included in the GDPR, it recommends to comply with EU law and encourage to adopt a limited duration of retention in accordance with technical constraints. The guide will also touch on liability issues.

This guide is also aimed for Community Networks and their allies, and as such, was made in cooperation with local CNs as well as alternative hosting providers sharing their values regarding human digital right, including Privacy and freedom of expression which may be impaired by a disproportionate data retention system.

It is currently being drafted, and it should be published in September 2018.

4.2.1.3. French practical guide for CNs providing Internet access

Another guide which we will be writing over the last semester of the netCommons project is on data processing and the data protection framework as it applies to entities providing Internet access. This guide will also touch on the issues of liability.

4.2.2. Legal Advice to an Italian CN

In the fall of 2017 the Italian community ninux asked for advice on some legal issues related to the Italian "Codice delle Comunicazioni Elettroniche" (decreto legislativo (d.lgs.) 1.8.2003, n. 259, implementing the EU Directives on the telecommunications sector).

More precisely, the request came from the "island" of the Calabria region and contained some very detailed requests of interpretation of the mentioned *Codice*. In particular, the CN wanted to have a clear picture of what authorization is needed to run a CN and the differences between an authorization for a private and for a public network.

In addition, the CN asked what possible interaction and collaboration there could be between a CN and a commercial ISP and how to regulate this possible relationship. Questions and answers, exchanged via e-mail in Italian, are included Appendix C for the sake of completeness and easy reference, as they were already reported in D4.2 Annex 7.

[19] https://www.laquadrature.net/fr/guide_internet_libre_acces

[20] http://www.bibliofrance.org/index.php/ressources/politiques-publiques-culture-livres-internet/514-internet-en-libre-acces-guide-juridique-pour-les-bibliothecaires;
http://fill-livrelecture.org/internet-en-libre-acces-un-guide-juridique-pour-les-bibliotheques/;
http://bbf.enssib.fr/le-fil-du-bbf/internet-en-libre-acces-guide-juridique-pour-les-bibliothecaires-07-02-2018;
http://www.lr2l.fr/actualites/guide-juridique-pour-les-bibliotheques-internet-en-libre-acces.html

After having described the legal framework applying to CNs (Chapter 2), we then have confronted it to their compliant, non-compliant or alternative practices (Chapter 3). To offer perspectives of growth for communities, legal guidelines have been defined (Chapter 4). However, these recommendations are transitory, while waiting for the achievement of the long-term objective: promoting a legal framework more welcoming through advocacy actions, which is the subject of the following Chapter 5.

5. Advocacy support for CNs

This chapter focuses on advocacy actions undertaken and illustrates the impact of CNs and netCommons on policy-makers with regards to the legal framework as described in Chapter 2. It should be regarded as complementary with D1.5 [3] and relies on its conceptual framework.

5.1. A European targeted advocacy action: Focus on #STOPdataRetention

The initiative stems from a litigation group in France, named "the Exegetes"[1], which works closely with French CNs and NGOs defending digital rights, in particular La Quadrature du Net. They made a first call for a joint action in November 2017. Such an initiative was clearly in line with the previous open letter coordinated by netCommons, as well as the advocacy work presented during the workshop with Members of the European Parliament organised in October 2017. More precisely, it deepened one of the key points of the open letter presenting our findings and recommendation to EU policy makers: *"abrogating blanket data retention"*. At the same time, three members of the netCommons project are also involved in La Quadrature du Net and this litigation group. Since these three organisation have a common purpose of advocacy regarding digital rights, this project was conducted in reliance with common resources.

Thus, netCommons decided to participate actively as part of its research and advocacy work. We substantially relied on regular mailing list diffusion and one-to-one mail in order to help this wide coordination (Sec. 5.1.1), but also used other relays to extend the initiative (Sec. 5.1.2).

5.1.1. Organising a joint action against data retention in the EU

This project relies on an observation: a wide part of Member States' legislation on data retention does not comply with EU law requirements regarding fundamental rights. Indeed, since EU Court of Justice's decisions, *Digital Rights Ireland* in 2014 and all the more since *Tele2* in 2016, it is clearly stated that general and indiscriminate collection of data is precluded. However, most of member States did not take action to repeal or adapt their legislation after the first ruling of the CJEU, nor after the second one.

Confronting this collective inertia, several isolated national litigation were launched before national courts. Few of them succeed[2] and some are still pending[3]. However, proceedings take a lot of time (in France, almost 3 years in the above-mentioned case). Furthermore, several authorities as well as Member States clearly expressed their reluctance toward CJEU's rulings, in the context of negotiating the new ePrivacy regulation.

In this context, this new advocacy project involving litigation aimed to to fulfil two goals:

1. Clarifying a divergent framework between national and EU laws;
2. Deepening the advocacy to policy-makers to reach a fair balance between criminal investigation and digital human rights regarding data retention measure.

As an alternative to regular national and isolated litigation, this action intended to join forces and coordinate at the European level, by coordinating individual actions.

First, a Community Network, an organisation, or an individual should lodge an individual complaint with the European Commission to point out national provisions regarding data retention that do not respect *Tele2*'s

[1] https://exegetes.eu.org/en/

[2] See Sec. 2.3.3.3.1, in Germany (OVG Münster 13 B 238/17 ; VG Köln 9 K 7417/17 and 9 K 3859/16)

[3] See Sec. 2.3.3.1.1, in France (Conseil d'Etat, req. n°393099

requirements –and therefore the precedence principle[4] of EU law.

Such a complaint would be lodged in the context of the procedure of failure to comply with EU law, pursuant to the article 258 of Treaty[5],

To put it simply, within the following **12 months**, the European Commission will assess the complaint submitted and aim to **decide whether to initiate a formal infringement procedure against the country** in question[6].

The concrete purpose has been to encourage as much as possible CNs and NGOs to submit such a complaint, in order to raise awareness of the European Commission's Taxation and Customs Union Directorate General, which, in its own definition is the "*guardian of Treaties and secondary legislation*"[7], on the widespread inconsistency of national data retention laws, so that they can take formal countermeasures.

Second, we co-draft a joint open letter to explain our strategy, highlight the coordinated aspect of the action and express our common concerns regarding non-targeted data retention in terms of human digital rights.

Relying on advocacy resources built thanks to our last open letter to EU policy-makers, we first contacted the *'Telecommons list'* –created in 2017 at the occasion of this action. Then we relied on other mailing list, including European Digital Rights (EDRi)[8] data retention list, from which we had many replies. The advocacy initiative was presented with the invitation letter reported in Fig. 5.1.

Thanks to the work of Task 4.1, we have helped several NGOs and CNs to draft their complaints –especially for Spain and Italy. However, numerous organisations write their complaint on their own and after two months of coordination and preparation we launched the action on June 25, 2018.

Regarding the complaints, as of June 25, 2018 NGOs and CNs have sent complaint from 11 Member States:

1. France
2. Italy
3. Spain
4. Sweden
5. Portugal
6. Belgium
7. Germany
8. United Kingdom
9. Poland
10. Ireland
11. Czech Republic

As for the open letter, 62 NGOs and Community Networks –such as Freifunk in Germany, Sarantaporo in Greece, WirelessPt in Portug al, FFDN, FDN, Aquilenet, Franciliens.net, SCANI, FAI Maison, Tetaneutral, ILOTH, Illyse, Rézine, Igwan.net, Touraine Data Network in France, Neutrinet in Belgium, APS Progetto Wireco Ciminna in Italy, but also beyond Europe with Network Bogota in Colombia (South America).

However, since the launching several organisations reach out to us in order to join the letter as supporters and the list, as of June 28, is getting wider.

Indeed, thanks to resources of La Quadrature du Net and the Exegetes, a dedicated web site named "stop data retention"[9] as well as a communication campaign untitled **STOPdataRetention** was launched through Twitter[10] and Mastodon. It was also relayed by journalists, including Next Impact in France[11].

[4] See Sec. 4.1.6.1

[5] "***If the Commission considers that a Member State has failed to fulfill an obligation under the Treaties****, it shall deliver a* ***reasoned opinion on the matter*** *after giving the State concerned the opportunity to submit its observations. If the State concerned does not comply with the opinion within the period laid down by the Commission, the latter* ***may bring the matter before the Court of Justice*** *of the European Union.", available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12008E258&from=EN*

[6] https://ec.europa.eu/info/about-european-commission/contact/problems-and-complaints/how-make-complaint-eu-level/submit-complaint_en#what-does-the-european-commission-do-with-your-complaint

[7] See its own presentation and the legal basis for its operation on its web site: https://ec.europa.eu/taxation_customs/infringements/general-information_en

[8] EDRi is an international non-profit association (AISBL) under Belgium law granted by decree Nr7/CDLF/14.853/S of 12 February 2003 and registered in Brussels (n° BE0866.466.752). EDRi is registered in the EU Register of Interest Representatives under the number 16311905144-06. See https://edri.org/ for further information

[9] http://stopdataretention.eu/

[10] https://twitter.com/hashtag/stopdataretention

[11] https://www.nextinpact.com/news/106775-62-associations-sattaquent-a-retention-donnees-connexion-en-europe.htm;

I am writing to you on behalf of a group of organisations and community networks litigating against surveillance and other digital rights issues in France (La Quadrature du Net and Federation FDN). Our aim is to unite throughout Europe against data retention of communications data, and to demand that the EU Court of Justice's rulings are applied (Digital Rights Ireland in 2014, and Tele2 in 2016). Our action implies:

1. ***Many individual formal complaint*** *to the European Commission (pursuant to Article 258 of the Treaty on the Functioning of the European Union) which can be sent by an individual or a NGO. It would be great to have at least two complaints by country. One in English, and one in the language of your country. This kind of complaint is very light and very different from regular litigation. After filing it, you will not be requested to do some work, or make yourself available to receive inquiries or any other related responsibilities. The European Commission will choose to investigate (or not . . .) on its own.*

2. *A* ***joint open letter*** *to the European Commission on data retention in the EU explaining clearly what we advocate for. This open letter could be signed by organisations, academics and members of parliament. You are all very welcome.*

3. *A* ***press release*** *to be broadcast through as many media as you could in your country. We are writing one in english. You could use it or draft one more to your liking.*

All documents would be sent at the same time: ***25 June 2018****.*
Depending on your energy and time, you can either just sign the open letter, which will help by giving more weight to it, sign an individual complaint already written for your country Or you can also write yourself an individual complaint.
If you do want to sign the open letter please write your name, or the name of your NGO at the end of this pad: [A specific URL was given].
If you want to draft a complaint, there is a standard form very easy to fill in. We have already draft ours in France. You can take a look at it here: [A specific URL wad given]
If you need help to prepare it, do not hesitate to ask. However, please don't submit it until this is finalized, as we want to make this a coordinated effort.
We are looking for one contact point in each country to reach out other NGOs or academics to join the action and contact local journalists to broadcast the press release. Please tell us if you want to join!
We are really looking forward to working together with you on this!
Thank you for reading this very long email,
Best,
Virginie, for the University of Trento and the netCommons project.

Figure 5.1.: Text of the invitation letter to join the advocacy action to harmonize national legislation to the EU law.

The goal of the stop data retention web site is gathering all complaints sent from NGOs and CNs throughout Europe and encourage citizen to read them, by introducing key concepts and stakes. Eventually, it also calls for citizen to play an active role and also send their own complaint by using the template available for their country.

A specific joint press release was drafted for this purpose, and published through many media[12]. Its text is

http://www.liberation.fr/planete/2018/06/25/conservation-des-donnees-par-les-operateurs-telecoms-62-associations-saisissent-la-commission-europe_1661842

[12] See for instance, NGO defending Community Network such as Common Networks: http://www.commonsnetwork.org/news/urgent-

reported in Fig. 5.2.

Massive claims against unlawful data retention
On June 25, 2018, sixty-two NGOs, community networks, academics and activists are sending a joint open letter to the European Commission, along with various complaints against EU Member States' policy on blanket data retention.
What is at stake?
"Blanket data retention" refers to the obligation for telecommunication providers (telephone and Internet services) to retain traffic data (numbers called, IP addresses, location data, identity . . .) of all of their users for several months or years (depending on each national law). Such retention applies to every user, including people who are not suspected of any crime or wrongdoing.
Seventeen States within the European Union provide for such blanket data retention.
How is it inconsistent with European Union law?
The Court of justice of the European Union clearly ruled that such general and indiscriminate retention of data was contrary to the right to privacy, protection of personal data as well as freedom of speech and information – all of which are protected by the EU Charter of fundamental rights.
In the Court's view, such mass surveillance measures are not acceptable.
What is our goal?
European law is not only more favourable for our rights and freedoms: It also trumps over national laws.. We want it to be enforced so that the 17 Member States currently in breach of EU law have to change their policies.
To this end, we are sending several complaints to the European Commission. This way, we invite the Commission to investigate and, eventually, to bring these States before the Court of Justice. This way, each of them can be sanctioned for its violation of EU law. To introduce our action, we are attaching to these complaints a joint open letter supported by more than 60 signatories in 19 Member States, which will also be sent to the European Commission.
How can you help?
You too can send your own complaint to the European Commission! You just need to put your contact information into the template for your country and send it at this address: SG-PLAINTES@ec.europa.eu . Doing so is not risky and is free. This complaint procedure is accessible to all.

Figure 5.2.: Text of the joint press release drafted for the distributed advocacy action against blanked data retention.

5.1.2. Relaying a coordinated action

To broaden the scope of participants advertisement of this initiative was conducted in different circles: with policy makers and especially Members of the European Parliament (Sec. 5.1.2.1) and also activists defending digital rights at large (Sec. 5.1.2.2).

5.1.2.1. Meeting with policy-makers

Type: Legal Workshop

Title: "the Future of Data Retention and Targeted Criminal Investigations"

Date: April 12, 2018

letter-to-the-european-commission-to-stop-illegal-data-retention/

Place: Brussels, Belgium

Organizers: Jan Philipp ALBRECHT, Greens/EFA

Actors: 35 participants

- Non profit organisations defending digital rights (60%);
- Members of the European Parliament and their assistants (20%);
- Academics (11%);
- Lawyers (6%);
- Members from a national DPA (3%).

Official purpose: The official purpose of the meeting was to share experience and legal information about data retention national laws – in light with european requirements in terms of fundamental rights – in order for MEPs and civil society at large to coordinate. In the original invitation, this official purpose was presented as follows:

> The CJEU has in recent years issued important judgements on both telecommunications data retention (Digital Rights Ireland and Tele2/Watson) and the retention of travellers' data (PNR EU-Canada). Still, many Member States have data retention laws, and even on EU level, similar initiatives such as Entry/Exit keep getting majorities. The issue is again discussed by the Council of Ministers, and the EU Commission might present a new approach in 2018. We need to develop a strategy on how to address this.
>
> Also, there are related discussions going on about other intrusive measures such as **interoperability of EU police** and border databases, access to electronic evidence, and upload filters, which all will move towards political decisions on EU level soon.
>
> The conference aims to provide a **strategic workshop with NGOs** and other allies on how **to prevent any new data retention on EU level, how to fight it on national level, and how to deal with the demands of Member States regarding other measures**. The aim is to align Greens' and NGOs' strategies. The event is a follow-up to similar meetings organised by Greens/EFA in the EP in recent years.

Planning and scope: The meeting was divided in two parts. The first one focussed on data retention per se, and the second one broaden the debate on digital Privacy and Copyright concerns.

15:00-15:15: *Welcome and Introduction*

15:15-16:45:*Recent developments around data retention*

- Short input(s)
- Tour de table
- Discussion on strategic approaches and how to coordinate

16:45-18:15: *Discussion on related developments*

- e-Evidence
- Interoperability
- Upload-Filters

18:15-18:30: *Closing remarks and follow-up*

Results and perspective for netCommons:

First, the timing as well as the purpose of this meeting seems very appropriate for us to advertise our advocacy projects. Especially, we have shared the french project that we were actively supporting to very different kind of public (academics, general NGOs, MEPs, . . .) .

Second, we had also shared legal information from our researches, and especially concerning data retention (a topic emphasized in D4.3). Sharing national litigation experience (about Germany and France especially) was really helpful since natives were there to add their policy context and several legal references.

Third, as they are directly part of the process of retention, CNs had specific ethical and technical concerns about data retention, as expressed in the last open letter. We presented the current practice of data retention by Community networks, as described in D4.2, and highlighted their peculiar perspective about the legal framework.

Publicity:

The meeting was very private. No public invitation was published. Yet, it was documented in the netCommons website[13].

5.1.2.2. Meeting with activists

5.1.2.2.1 Informative and cooperative event: The Battle of the Mesh in Germany

This year, the "Wireless Battle of the Mesh"[14] and the "Wireless Community Weekend"[15] have joined forces and realized a new event, called "Mesh is in the air"[16], merging both events in Berlin.

The Battle of the Mesh is the historical meeting of all European Community Networks, in 2018 it is the 11th edition whereas The Wireless Community Weekend is the annual meeting of the FreiFunk German wireless community. "Mesh is in the air" has been a productive event advancing the field of wireless mesh networking and fostering the development of grass-roots community networks, but also promotes digital rights movement, empowerment of people through technical skills and understanding and a free and open civil society. It is the best occasion to meet all the practitioners, developers, and maintainers of CNs around Europe.

Thus, for netCommons it was a very appropriate event where to showcase the results of the project[17]. Several members gave a talk or intervene during debates, to share with communities all the results, gather feedback and involve them in the experimental activities –the netCommons team was also at the event in the first and second year of the project, in 2016-2017[18].

More precisely, a talk was given by Leonardo Maccari, abstracting "Two Years of the netCommons.eu Project" and cross-perspectives were offered by Panayotis Antoniadis on "Community Network Special Interest Group – ISOC" as well as on "Current challenges in the city and possible synergies with CNs"[19].

Furthermore, several legal issues pinpointed as concerns in our open letter to policy makers as well as in D4.1 and D4.2 were presented by activists. Thus, we could share and discuss our findings about the radio equipment directive, but above all we invite communities and theirs allies to join our ongoing collaborative action about data retention in the EU, and use media to extend this advertisement[20].

5.1.2.2.2 Community-based event: General Assembly of the Federation FDN in France

The General Assembly of Fédération FDN (FFDN), the French federation of Community Networks[21], is a yearly event gathering more than thirty legal persons and about 3000 natural persons. In 2018, seventy people

[13] https://netcommons.eu/?q=content/data-retention-and-telecommunication-providers-new-eu-parliament-meeting
[14] https://www.battlemesh.org/
[15] https://freifunk.net/en/blog/2018/03/mesh-is-in-the-air/
[16] https://www.wireless-meshup.org/doku.php
[17] https://netcommons.eu/?q=content/netcommons-endorses-and-supports-mesh-air
[18] https://twitter.com/netCommonsEU/status/994956350206685186
[19] For the exhaustive schedule, see https://www.wireless-meshup.org/doku.php
[20] https://twitter.com/netCommonsEU/status/994956350206685186
[21] created in 2011, see their web site (in English) https://www.ffdn.org/en

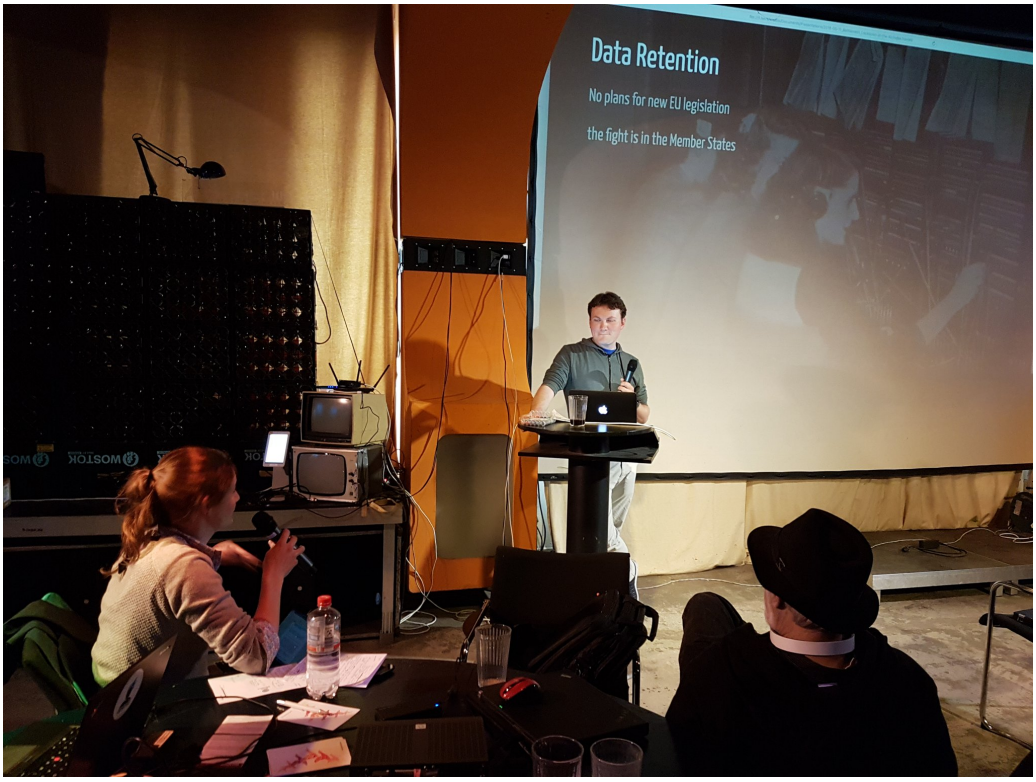


Figure 5.3.: Virginie invites #CommunityNetworks to join forces against #DataRetention in Europe @battlemesh. If interested please contact@exegetes.eu.org @lesExegetes #wbmv11 @FreakkaerF

gathered to discuss and take decision about governance. This year, it takes place in an old castle in a rural district one hour south of the city of Toulouse, in France.

Regarding governance, one key focus this year was on inclusion, with the goal of making FFDN's member organizations more welcoming for women, non-whites and disabled persons. As underlined in another report netCommons released last year on governance, this has been long-running concern at FFDN and this year, participants decided to launch a new working group to tackle these structural challenges.

Another focus of the discussions on governance was how to fund the growing joint actions taking place within the federation, and how to build financial solidarity between member organizations. One challenge in this regard is to account for the diversity of financial situations among them while preserving local autonomy and equal representation at the federal level.

One last point on governance: We witnessed a growing willingness on the part of many participants to start focusing again on growing existing organizations and seeding new ones across France. A working group has been set up to start developing a new strategy for this purpose of dissemination.

On the technical front, the three-day event was extremely fruitful as well. On the first day, a small team worked on sharing the castle's WiFi network with a circus troop established down the hill and deprived of any Internet access. To that end, the castle's own WiFi network –connected to an ADSL access in a nearby village through a radio link– was expanded thanks to a new antenna installed on the castle's roof. Other workshops focused on starting new development efforts of the "Internet Cube", a device allowing for self-hosting functionality –thanks to the Yunohost operating system– and channeling Internet traffic to a CN's VPN services.

Finally, and most important in light of WP4, we had many fruitful interactions on the legal front. We gave an update of our work on legal guidelines for data retention obligations and data protection. Several participants gave us very positive feedbacks on our French guide on legal aspects of open access points (see, Sec. 4.2.1), and in particular the fact that the guide was already helping local public authorities and libraries resist pressure to

implement illegal surveillance measures and better protect the rights of Internet users. During this meeting, as we introduced, was also an opportunity to share the coordinated project on data retention that we are supporting as a concrete depiction of this recommendation.

5.2. Advocacy capacity-building

During FFDN's 2018 General Assembly, we also discussed the findings of D1.5 on how to develop advocacy capacities to influence regulation in the interest of CNs. As we stressed in that deliverable:

> "*Building internal skills might be enough to engage in policy-making in front of local authorities, which of course can be key in providing CNs with the legitimacy and resources to scale up their projects locally. But at the national and European level, effectively* ***engaging in sustained political advocacy will require creating better coordination between communities***" (See D1.5, Sec. 4.2.3).

Now, the federation's General Assembly was very receptive to the idea and we are expecting new proposals and initiatives on how best to coordinate European networks in the coming weeks or months.

6. Impact of the work

Closing Task 4.1, this deliverable –written through M24-M30, with an extension in M31 to account for important events in July 2018– has a direct impact on CNs by improving the understanding of their legal obligations, sensitizing EU policy-makers to CNs' legal hurdles while participating to their advocacy-capacity building. During these seven months, we have:

- Described the current European legal framework applied to Community Networks;
- Detailed several national frameworks implementing EU law with provisions that may have a direct impact on CNs;
- Underlined existing legal hurdles that may impair the development of Community Networks;
- Given preliminary recommendation to CNs in order to cope with these difficulties regarding data protection, data retention, telecommunication law and civil liability for which we will in the next terms propose a template;
- Co-written a specific Open Letter deepening the Open Letter written by Task 1.3 aiming to raise general awareness on CNs legal sustainability issues;
- Co-written with CNs specific claims, as part of an advocacy action regarding data retention obligations;
- Co-written a practical guide for organisation providing an open access to the Internet in reliance with French law and worked on a next one concerning hosting providers;
- Given ongoing legal support to CNs for strategic litigation and advocacy action in France (FFDN and FDN), including hurdles faced in the fibre market;
- Prepared a workshop organized on July, 9 2018 in Athens;
- Opened the dialogue with a national regulator in Greece;
- Taken part in a legal workshop in the European Parliament regarding data retention obligation and initiated a collaboration with NGOs, MEPs and academics on April 12, 2018;
- Discussed legal policy recommendation in a workshop organized by netCommons in London with the national regulator on May 15, 2018;
- Analysed the last version of the EECC, which we have swayed as some of our proposals were adopted, which will be good for CNs sustainability.

7. Conclusion

This deliverable has offered a final update of the European legal framework, including ongoing legislative changes that were set aside in the first two deliverables. Altogether, the three incremental deliverables D4.1, D4.2 and D4.3 are the basis upon which the legal and policy part of a D4.5 'Best Practices Guide for CNs' will be built between M30 and M36. This final achievement of our research will support the legal and overall sustainability and swarming of CNs.

Having studied EU and relevant national laws allowed the production of a mapping of legal requirements CNs have to respect or to implement in the areas of liability, telecommunications law, data protection, and data retention. Interacting with the CNs through a survey about their practices further contributed to our analysis and helped us identify gaps and needs. The latter have been, and are being, addressed in two ways. First, through the development of applicable legal guidelines to cope with legal hurdles. Second, through policy advocacy for reform towards legal sustainability and the recognition of special regulatory needs, also in line with methods and topics where progress towards desired changes was identified in D1.5. In this respect, our efforts have been met with successes: Working documents suggest that the future legal regulatory framework will require regulators to draft rules especially designed for CNs.

In this deliverable, we also conducted an analysis of CNs' changing practices since the beginning of the project and the interaction with the netCommons team. Then, Chapter 3 of the deliverable provided an overview of the current practice of the activity of CNs regarding these legal requirements. It intends to be an update and offers a more extensive analysis of the results of the survey conducted last year, and focuses on the same issues: organization, services offered, relationship with users, data protection and data retention law.

In light of these findings, we produced in Chapter 4 general guidelines in the actual practice areas of CNs (organization, services offered, relationship with users, data protection and data retention law), balancing between legal requirements and CNs political ethos (maintaining privacy in their relationship with their users and a horizontal distribution of power as a participatory and collective decision process within the community).

This guidelines, summarized here, are of course transitory, pending the conclusion of D.4.5.

- Civil liability has proved to be a problem for a number of CNs, particular in Germany where Freifunk participants for years had to deal with the risk of third party infringement (people accessing the open Freifunk networks to share copyrighted works, which in turn motivated right-holders to sue people sharing their connections). In Germany, Freifunk and its allies successfully campaigned for a change in the legal framework, which is not perfect but significantly reduce the legal risk. Although our joint advocacy efforts around the European Code of Telecommunications failed to create a liability exemptions for people sharing their connections, we feel that, generally speaking, even the McFadden case law of the Court of Justice of the European Union does not entail strong legal risks for users sharing their wireless connection with their vicinity. CNs enacting special privacy and anonymity protections by running relays for the Tor networks should also be free to do so.
- Data protection should be a significant concern for EU CNs in the month to come, especially in light of the increased sensitivity to this issues in the wake of the implementation of the General Data Protection Regulation. To ensure the lawfulness of personal data processing, including security measures and transfer of data, anonymising and pseudonymising data as much as possible, and various strategies such as mapping existing practices related to data processing, and ad-hoc processes to manage potential data leaks and inform users are urgently called for.
- Although we make these recommendations with a degree of cautiousness considering the commitment of some CNs to informal organization processes, we feel however that entering into a contract with the users

of CN's services can be an interesting solution to mitigate the risks associate with the applicable liability regime as well as the data protection framework. For the same reasons, incorporating a CNs through a non-profit legal status will also help alleviate legal risks and clarify the distribution of liability within the community, so that it can reflect on these risks and anticipate them rather than act in the context of a legal crisis.

- On data retention, CNs face a particularly thorny issue considering the legal limbo surrounding these legal obligations established across Europe to facilitate law enforcement. Given the 2014 and 2016 rulings of the Court of Justice of the EU, which invalidated obligations for indiscriminate, blanket data retention, 17 Member States are, according to our analysis, still in breach of this crucial case law. Although netCommons has helped establish a Europe-wide advocacy and litigation effort on the issue, it will probably be months, or years, before all ambiguities are finally resolved. In the meantime, we have highlighted various strategies that we have observed in the course of research, inviting CNs to choose that which they deem to be most appropriate. These strategies range from the most "conservative" (i.e., decide to abide national law at the expense of the right to privacy as construed by the "Supreme Court" of the EU in its case law), to the most "activist" (i.e., defying national law while invoking this European case-law to highlight the lack of regard of national lawmakers for EU law and fundamental rights, which bears the risk of litigation and, possibly, fines or even jail).

In Chapter 5, we point to efforts between netCommons members and CNs in order to influence the existing legal framework, which is comprised of all the recent advocacy work for which we provided assistance to the communities. After the organisation of a workshop for the reform of the European Code of Communications and the drafting of notes for Members of the EU Parliament during year 2 of the project in 2017, the active role played by CNs and members of the project translated into:

- Participation to another workshop at the European Parliament, on data retention on 11 April 2018;
- Co-organisation of a litigation campaign, Stop Data Retention, undersigned by over 60 CNs and digital rights organisations;
- Seminar at UNESCO, leading to an inclusion of CNs needs in the recommendations of Internet Universality Indicators, which potentially will invite States to progressively adjust telecom policy to facilitate the development of CNs (and in this respect usefully complements some of the provisions inserted in the draft European Code of Electronic Communication);
- Participation to a workshop on the ongoing reform of telecom policy held in Brussels on May 23th.

To summarise, the continuation of the mapping of EU and relevant national law drafted in D4.1, the results of the survey about CNs' practices and their analysis in D4.2, the findings about advocacy delivered in D1.5, this deliverable builds on the work of various Work Packages to serve as a basis to provide synthetic guidelines for CNs to cope with legal hurdles.

Aiming more generally to promote a legal framework favouring Community Networks, this report concludes our exploration into the legal world of CNs. In this regard, it delved into the active role played by the netCommons research team concerning advocacy, and addresses the sustainability of such efforts after the end of the project with the building of a community –which we call "Telecommons" after the dedicated mailing-list– to continue such efforts and promote a more supportive legal environment at the local, national, European and even global levels.

In terms of future advocacy and dissemination work until the end of the project, netCommons legal team will focus on capacity-building so that our three-year long efforts can provide a sustainable basis for the European CN movement to take off and better coordinate for campaigning, engaging with policy-makers and activists, litigation and cause lawyering. To this end, and besides the 'Best Practices Guide for CNs' which will conclude WP4, we will:

- Contribute to starting a debate about the European coordination of the movement (see D1.5);
- Follow-up on the "Stop Data Retention" campaign and litigation;

- Assist FFDN in devising a campaign and litigation strategy to get access to publicly-funded Fiber-Optic regional networks, taking inspiration from what Guifi has done on the issue;
- Write two new practical guides on the legal obligations of CNs offering hosting services and Internet access, focusing on the legal framework regarding civil liability and data protection;
- Offer a template of terms of use for CNs in reliance with our preliminary recommendations.

Bibliography

[1] M. Dulong de Rosnay, F. Giovanella, A. Messaud, and F. Tréguer, "European Legal Framework for CNs," netCommons Deliverable D4.1, Dec. 2016. http://netcommons.eu/?q=content/european-legal-framework-cns-v1

[2] F. Giovanella, M. Dulong de Rosnay, A. Messaud, and F. Tréguer, "European Legal Framework for CNs (v2)," netCommons Deliverable D4.2, Jan. 2018. https://netcommons.eu/?q=content/european-legal-framework-cns-v2

[3] F. Tréguer and M. Dulong de Rosnay, "Advocacy Guidelines," netCommons Deliverable D1.5, Jan. 2018. https://netcommons.eu/?q=content/advocacy-guidelines

[4] L. Navarro, A. Lertsinsrubtavee, V. Chryssos, C. Rey-Moreno, S. Luca de Tena, C. Conder, L. Annison, E. Huerta, F. Tréguer, L. Maccari, and R. Srivastava, "Report on the Governance Instruments and their Application to CNs (v2)," netCommons Deliverable D1.4, Jan. 2018. https://netcommons.eu/?q=content/report-governance-instruments-and-their-application-cns-v2

[5] D. Boucas, M. Michalis, and L. Ghiro, "Alternative Internet's Political Economy Survey Analysis and Interpretation of Data," netCommons Deliverable D5.4, Aug. 2018. https://www.netcommons.eu/?q=content/alternative-internets-political-economy

[6] T. Madiega, "EU electronic communications code and co-investment: Taking stock of the policy discussion," European Parliamentary Research Service, Tech. Rep. PE 614.693, Feb. 2018. http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614693/EPRS_BRI(2018)614693_EN.pdf

[7] C. Fuchs, M. Michalis, and D. Boucas, "The Multiple Aspects of Politics of Sustainability in Community Networks: Definitions, Challenges, and Countermeasures (v2)," netCommons Deliverable D2.2, Jan. 2017. http://netcommons.eu/?q=content/multiple-aspects-politics-and-sustainability-cns-definitions-challenges-and-countermeasure-0

[8] "Notes on European Electronic Communications Code before decisive votes in European Parliament," netCommons, Tech. Rep., Jun. 2018. https://netcommons.eu/?q=content/notes-european-electronic-communications-code-decisive-votes-european-parliament

[9] "EU Telecom Package: courage over details," Mar. 2017. https://www.laquadrature.net/en/EU_Telecom_Package_courage_over_details

[10] "Economic landscape under the new Telecommunications Code," European Parliament, Brussels, May 2018. https://www.greens-efa.eu/en/article/event/economic-landscape-under-the-new-telecommunications-code/

[11] L. Navarro, R. Baig, F. Freitag, E. Dimogerontakis, F. Treguer, M. Dulong de Rosnay, L. Maccari, P. Micholia, and P. Antoniadis, "Report on the Existing CNs and their Organization (v1)," netCommons Deliverable D1.1, June 2016. http://netcommons.eu/?q=content/report-existing-cns-and-their-organization-v1

[12] D. Boucas and M. Michalis, "Alternative Internet Survey Plan," netCommons Deliverable D5.2, Mar. 2017. https://netcommons.eu/?q=content/alternative-internet-survey-plan

[13] ——, "Alternative Internet Survey Implementation," netCommons Deliverable D5.3, June 2017. https://www.netcommons.eu/?q=content/alternative-internet-survey-implementation

A. Annex 1

This annex reports the questionnaire we asked CNs member and/or representative through e-mail lists to fill in order to understand what is the level of understanding of the legal framework where CNs operate, as well as to collect information on how the legal framework is applied in each CN. We report it here for completeness as it was already documented in D4.2.

We are aware that some of the questions may involve sensitive issues, for instance with regard to activities which might be illegal in your own country. To avoid exposing your CN to negative consequences, we will anonymise each questionnaire once received it. In addition, in our report based on the questionnaire, we will not mention specifically what CN the answers refer to.

Answers to the questionnaire will be stored on data centres protected with strong authentication measures.

Please consider that while answering this questionnaire you consent to share your answers with netCommons researchers that will treat your information according to the ethical standards of research and protect it as just explained.

Section A: CN nationality

A1. **What is the name of the CN you take part in and in which country does it operate?** ***(please note that we will not share this information, but it is very important for us to understand what laws should be applicable)***

Section B: Services provided by your CN

B1. **How is your CN providing access to its network?**

through cables ☐

Wi-Fi ☐

other: ☐

other:

B2. **Is access to the network provided against payment?**

yes ☐

no ☐

it depends (explain): ☐

it depends (explain):

B3. **Is access to the network only provided to a restricted group of individuals?**

Examples: members of an association, low-income individuals, adults?

no ☐

yes (explain): ☐

yes (explain):

B4. **Is the network connected to the Internet?**

yes ☐

no ☐

it depends: ☐

it depends:

B5. **Does your CN provide other services?**

If your CN offers one or more of the services below, please indicate in the box if the service is provided against payment and/or only to a restricted group of individuals.

no other services are offered ☐

email ☐

chat ☐

VoIP ☐

VPN ☐

DNS ☐

torrent tracker ☐

mailing list ☐

Tor node ☐

hosting (webpage, website, cloud, virtual machine...) ☐

other: ☐

Section C: Organization of your CN

C1. Is a legal entity playing a central role within your CN?

no ☐

yes (explain how it is organized; example: as an association, foundation or co-operative): ☐

yes (explain how it is organized; example: as an association, foundation or co-operative):

C2. Who is actually providing services to the users?

a central entity (acting through its employees or members) ☐

external individual participants (not acting on behalf on the central entity) ☐

a mix of both (explain if necessary): ☐

a mix of both (explain if necessary):

C3. Where services are provided by individual participants, what is the role of the central entity?

C4. Who is deciding which services are provided by the CN?

the central entity (by a vote of its members, for instance) ☐

individual participants ☐

it depends (explain if necessary): ☐

it depends (explain if necessary):

C5. Who is defining the technical implementation of the services?

the central entity ☐

individual participants ☐

it depends (explain if necessary): ☐

it depends (explain if necessary):

C6. Where decisions are made by individual participants, how are these decisions taken?

Examples: through a collective and horizontal process or independently by each participant

C7. Where decisions are made by individual participants, how are these decisions taken?

Examples: through a collective and horizontal process or independently by each participant

C8. **Where individual participants provide services, do they have to enter into any kind of agreement with each other and/or with a legal entity?**

If so, how does this agreement distribute obligations and liabilities among them?

C9. **Where individual participants provide services, do they have to enter into any kind of agreement with each other and/or with a legal entity?**

If so, how does this agreement distribute obligations and liabilities among them?

Section D: Decentralized wireless network

D1. **Is your CN runnig a network of wireless relays managed by individual participants (not acting on behalf of a central legal entity)?**

- ☐ yes
- ☐ no

D2. **Who does legally own the relays?**

- ☐ a central entity
- ☐ each participant
- ☐ it depends:

it depends:

D3. Who is technically managing the relays?

a central entity (acting through its members, for instance) ☐

each paticipitant ☐

it depends: ☐

it depends:

D4. Is running a relay limited in any way?

Examples: by joining an association or entering into a contract?

In the latter case, describe the content of this contract.

Section E: Liability for users' behavior

E1. Do CN members use anonymity software?

no ☐

yes (describe which one; examples: Tor, encryption...): ☐

yes (describe which one; examples: Tor, encryption...):

E2. **Has it ever occurred in your CN that someone was sued for some wrongdoing?**

Examples: for defamation or copyright infringement

no ☐

yes (explain): ☐

yes (explain):

E3. **Has your CN a form of insurance?**

Examples: real insurance or a 'self-organized'-internal one?

no ☐

yes (which one?): ☐

yes (which one?):

Section F: Personal data (1)

For each category listed below, indicate the kind of data collected by your CN about its users.

For each kind of data, indicate the purpose(s) for which they are collected and used.

Examples: email addresses are collected in order to contact users in case of security issues and to send them newsletters; MAC addresses are collected in order to provide and maintain access to the network.

Where the purpose of collecting data is to comply with a legal obligation, describe the nature and basis of this obligation.

Example: the name of users accessing the network is collected in order to "protect" the network from unlawful activities, as provided by a specific law.

F1. Data that may allow the identification of users.

Examples: name, postal and email addresses, birth date

F2. Data that have been assigned by the CN to users.

Examples: IP address, phone number, user ID

F3. Data relating to the characteristics of the device through which the service is accessed.

Examples: MAC address, IMSI

F4. **Data relating to the characteristics of the line through which the service is accessed.**

Examples: lines ID, postal address

F5. **Data that may indicate the time and duration of access to a service.**

Example: DHCP operations

F6. **Data relating to the location where the service is accessed.**

Examples: relays ID, postal address

F7. **Data that may allow the identification of the recipients of communications or of the content accessed.**

Example: email address and phone number of recipients; URLs of accessed websites

F8. **Banking information.**

Example: IBAN

F9. **Data about the individuals participating in a decentralized wireless network.**

Examples: contact information, location and technical characteristics of their relay

Section G: Personal data (2)

G1. **Among the data you have listed on the previous page, which kind of data are associated together, kept separately or anonymised?**

Explain how it is done.

Example: IP addresses are associated with users' names in a central database; location data are anonymised.

G2. **Which kind of data is disclosed to third parties and for what purpose?**

Example: the postal address of users is disclosed to third party operators for interconnection matters

G3. **Is your CN transferring data outside the European Union?**

Example: through a VPN

no ☐

yes (to which countries and for what purpose?): ☐

yes (to which countries and for what purpose?):

G4. **Is your CN monitoring in any way how users are using the services?**

Examples: for payment or security issues.

If the answer to the question is yes, please explain in which way and for what purposes.

yes ☐

no ☐

G5. **What services is your CN monitoring, how and for what purpose?**

Section H: Relationship with users

H1. **Does your CN enter into a contract or any kind of agreement with each of its users?**

yes ☐

no ☐

H2. **Describe the content of such agreement.**

H3. **What kind of information is your CN providing its users with as regards the collect and use of personal data?**

Examples: they are informed that their name is associated with their IP address or that their postal address is disclosed to third party operators

H4. **How are users provided with such information?**

Example: on a website, within a contract

H5. **How can users access their personal data and ask for their rectification or erasure?**

Example: on a "user page" of your CN's website

H6.	**If any, what kind of personal data is your CN refraining from collecting or using without the consent of users?** **How is this consent given?**
H7.	**As regards decentralized wireless network managed by individual participants:** **How are participants informed of the use of their personal data? How may they access and modify their personal data? When is their consent required?**

Section I: Security

I1.	**Technically, how and where are the personal data processed by your CN stored?**
I2.	**What measure has your CN implemented in order to protect the data?** ***Examples: personal data can only be accessed by a limited number of individuals and each access is logged***

I3. If any kind of security breach has ever affected your CN:

describe it was it notified to authorities and users?

Section J: Data retention

J1. Is your CN retaining data in order to comply with national law?

yes ☐

no ☐

J2. Indicate which categories of data are retained and for how long.

J3. Where and by whom are the data retained?

J4. If public authorities have ever requested your CN to give them access to such data:

how many times? what categories of data were requiered and for what purposes? was your CN able to comply?

Section K: Legal advice

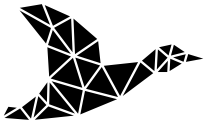
K1. Does your CN benefit from legal advice (i.e. from advice by a lawyer or a legal researcher)?

- ☐ No, it has never occured
- ☐ Yes, it occurs often (once a month or more)
- ☐ Yes, it occures sometimes (some times a year)
- ☐ Yes, it has occured a few times (once a year or once/twice in the CN's lifetime)
- ☐ I do not know

Thank you for your answers!

B. Annex 2

We report here the original French version of the practical synthetic guidelines for organisations providing an open access to the Internet (such as CNs, CN members, but also libraries or Internet cafes). It explains what are their legal obligations with respect to data retention, data processing and Net neutrality as summarized in Sec. 4.2.1.1.



netCommons.eu

Internet en libre accès

obligations en matière de vie privée et de liberté de communication

À jour en date du 29 janvier 2018

Ce guide juridique s'adresse aux organisations qui, en France, fournissent un accès à Internet de façon ouverte (par Wi-Fi, hot-spot, par câble ou sur postes fixes) : locaux associatifs, bibliothèques, centres d'information, résidences collectives, universités, bars, hôtels, magasins, cybercafés, etc.

Ce guide tente de répondre à trois questions qui se posent à elles en matière de vie privée et de liberté de communication :

– Quels sites peuvent-elles bloquer ?
– Quelles informations peuvent-elles collecter sur les personnes utilisant le service ?
– Quelles informations doivent-elles obligatoirement conserver ?

Ce guide ne s'adresse ni aux organisations qui fournissent un accès sur abonnement, ni aux individus qui partagent leur accès à Internet (dans le cadre d'une sous-location, par exemple), ni aux organisations qui fournissent un accès à un réseau fermé (un intranet).

A. Quels sites peuvent être bloqués ?

Neutralité du Net

Les organisations concernées par ce guide sont tenus de respecter la **neutralité du Net**[1], qui leur interdit de réaliser toute « restriction » quant aux « contenus consultés ou diffusés » par les utilisateurs. Par exception, la neutralité du Net permet le blocage de deux types de contenus :

– ceux qui mettent en danger la **sécurité** du service ou du terminal des personnes qui l'utilisent ;
– ceux dont le blocage est **exigé par la loi**.

Une organisation qui ne respecterait pas la neutralité du Net (en bloquant un site n'entrant pas dans une des exceptions) encourrait une **amende** égale à 3% de son chiffre d'affaire ou, s'il n'a pas d'activité commerciale, à **150 000 €**[2].

Blocage exigé par la loi

S'agissant du blocage exigé par la loi, il ne peut résulter que d'une décision judiciaire ou administrative visant des contenus précis : aucune loi n'impose aux organisations de bloquer des contenus sans décision individualisée.

De plus, certaines lois qui limitent habituellement la circulation de l'information ne s'imposent pas à ces organisations.

En premier lieu, la loi **HADOPI** exige de surveiller son accès à Internet pour éviter qu'il ne serve à commettre des actes de contrefaçon[3]. Or, cette loi **ne s'impose qu'aux utilisateurs et utilisatrices** finales qui bénéficient de l'accès et non aux personnes qui le fournissent. En effet, en droit, « les personnes dont l'activité est d'offrir un accès [à Internet] ne sont pas soumises à [...] une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites »[4].

En deuxième lieu, constitue un délit le fait de mettre à disposition de **personnes mineures** des contenus « à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine »[5]. Néanmoins, la loi prévoit aussi que la responsabilité (civile ou pénale) des personnes qui fournissent un « accès à un réseau de communications électroniques » ne peut être engagée à raison des contenus qu'elles diffusent[6]. Elles ne sont donc pas concernés par ce délit et, ainsi, **ne sont pas tenues de bloquer** les contenus concernés.

À la place, ces organisations doivent informer leurs utilisateurs et utilisatrices « de l'existence de moyens techniques permettant de restreindre l'accès » à certains sites (des logiciels de filtrage) et leur proposer un de ces moyens à utiliser[7], notamment pour protéger les mineurs. De plus, lorsqu'une organisation met des **postes fixes** à disposition du public, son activité dépasse la simple fourniture d'accès à Internet et nous lui conseillons donc d'y installer un filtre et/ou d'exiger la présence d'un adulte afin de protéger les mineurs.

Exception

La neutralité du Net ne s'impose qu'aux personnes qui offrent un accès à Internet « au public » (qui, en droit, sont alors qualifiées d'opérateurs[8]). Ceci exclut les personnes qui n'offrent cet accès qu'à un **« groupe d'utilisateurs prédéfini »**[9]. Cette notion est encore floue, et nous proposons de l'interpréter comme un groupe n'étant pas susceptible d'évoluer constamment et librement. Ainsi, par exemple, nous considérons que ne serait **pas soumise à la neutralité du Net** une entreprise qui ne fournirait un accès qu'à ses salariés (et pas aux autres personnes), dès lors que le groupe des salariés ne peut être librement rejoint par toute personne.

À l'inverse, nous considérons, par exemple, que **doit respecter la neutralité du Net** une bibliothèque qui, bien que ne fournissant un accès qu'aux personnes inscrites ou disposant d'une carte, permettrait à toute personne de s'inscrire ou d'obtenir une telle carte. Dans ce dernier cas, le fait que la carte soit payante ou soumise à une condition d'âge ne nous semble pas constituer un critère suffisamment discriminant pour qu'on puisse parler d'un « groupe d'utilisateurs prédéfini » et échapper à la neutralité du Net.

Confidentialité des communications

Peu importe que la loi impose ou non aux organisations de respecter la neutralité du Net, celles-ci doivent systématiquement respecter la **confidentialité des communications** de leurs utilisateurs. La loi interdit toute mesure « d'interception ou de surveillance » des communications électroniques ainsi que des données de trafic nécessaires à la diffusion de ces communications[10]. Cette interdiction connaît les mêmes exceptions que la neutralité du Net (la sécurité ou l'obligation de la loi) ainsi qu'une troisième : le consentement des utilisatrices et utilisateurs (néanmoins, il est peu probable que les ceux-ci acceptent d'être surveillés, d'autant que l'accès à Internet ne peut leur être dénié s'ils s'y refusent[11]).

Nous considérons que le blocage de sites Internet implique certaines opérations (analyse et traitement de l'adresse des sites auxquels tentent d'accéder chaque personne) qui pourraient correspondre à des atteintes à la confidentialité des communications. À ce titre aussi, en dehors des exceptions prévues par la loi, nous conseillons à toute organisation de ne bloquer aucun site. Ne pas respecter la confidentialité des communications est passible d'une amende de **225 000 €** et d'un **an d'emprisonnement**[12].

---

[1] Le principe de la neutralité du Net est défini à l'article 3 du règlement 2015/2120 de l'Union européenne.

[2] Les atteintes à la neutralité du Net sont sanctionnées à l'article L. 36-11 du code des postes et des communications électroniques (CPCE).

[3] Le régime de responsabilisation prévue par la loi HADOPI est prévu à l'article L. 336-3 du code de propriété intellectuelle.

[4] L'absence d'obligation des fournisseurs d'accès à Internet de surveiller les contenus est garantie à l'article 6, I, point 7, de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[5] Le délit de mise à disposition de mineurs de certains contenus est défini à l'article l'article 227-24 du code pénal.

[6] Le régime de responsabilité limité des fournisseurs d'accès à Internet est prévu à l'article L. 32-3-3 du CPCE. Il prévoit qu'un fournisseur n'est responsable des contenus qu'il diffuse que si il est « à l'origine de la demande de transmission litigieuse », « sélectionne le destinataire de la transmission » ou « sélectionne ou modifie les contenus faisant l'objet de la transmission ».

[7] L'obligation de proposer des filtres aux utilisateurs est prévue à l'article 6, I, point 1, de la loi du 21 juin 2004

[8] En application de l'article L. 32 du code des postes et des communications électroniques, est opérateur « toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques ».

[9] La notion de groupe d'utilisateurs prédéfini est détaillée au points 10 à 12 des lignes directrices du BEREC quant à l'application de la neutralité du Net, traduites par l'ARCEP

[10] La confidentialité des communications électroniques est garantie à l'article 5 de la directive 2002/58 de l'Union européenne, en partie transposé aux articles L. 32-3 et L. 34-1 du CPCE.

[11] La CNIL considère que « le refus de consentir ne doit pas empêcher la personne d'accéder au service » .

[12] La peine sanctionnant les atteintes à la confidentialité des communications est prévue à l'article 226-15 du code pénal, devant être portée au quintuple s'agissant des personnes morales

B. Quelles informations peuvent être collectées ?

La collecte de **données personnelles**[13] La collecte de données personnelles[13] (telles que le nom ou l'adresse d'une personne) n'est autorisée qu'à cinq conditions[14] :

– avec le **consentement** de la personne (mais les personnes refusant de consentir ne doivent pas être empêchées d'accéder à Internet[11]) ;
– pour exécuter un éventuel **contrat** conclu avec la personne ;
– pour exécuter une **mission de service public** à laquelle participe l'organisation ;
– pour exécuter une **obligation légale** ;
– en raison d'un **« intérêt légitime »**.

Cet « intérêt légitime » n'autorise que les opérations qui sont effectivement utiles pour l'organisation ou pour des tiers, et dont l'utilité est plus importante que l'atteinte portée à la vie privée des personnes concernées. S'agissant de l'exécution d'une mission de service public ou d'un contrat, la collecte de données personnelles doit être indispendable à cette exécution.

Par exemple, recueillir l'identité d'une personne porte atteinte à sa vie privée mais n'est souvent d'aucune utilité pour les organisations qui fournissent un accès libre à Internet. En effet, **aucune loi n'impose aux fournisseurs d'accès à Internet de recueillir l'identité** des personnes utilisant leur service[15] et ne saurait donc justifier une telle collecte (ce n'est que dans des cas exceptionnels qu'un fournisseur d'accès à Internet peut être obligé de collecter l'identité des utilisateurs et utilisatrices, lorsqu'un juge le lui ordonne précisément[16]).

De même, dans la mesure où les fournisseurs d'accès à Internet ne sont **pas responsables** des faits commis par les personnes utilisant l'accès[6], ils n'ont aucun intérêt personnel à pouvoir identifier les personnes qui commettent des actes illégaux via cet accès, ni donc aucun intérêt à collecter l'identité de tous les utilisateurs et utilisatrices pour y parvenir.

Au contraire, dans les cas où, pour une raison particulière, une organisation souhaiterait ne fournir l'accès qu'à un groupe limité de personnes (celles payant un prix, par exemple), et si cette limitation ne peut pas être réalisée autrement (en donnant le mot de passe unique qui permet d'accéder au réseau, par exemple), l'organisation pourrait avoir un intérêt à obtenir l'identité des personnes qui accèdent au service (mais elle devra alors se limiter à collecter les seules informations indispensables à cette fin).

Pour mettre en place une telle restriction, l'organisation doit toutefois pouvoir démontrer que l'objectif poursuivi (sécurité, facturation, etc.) ne peut pas être poursuivi au moyen d'une autre méthode n'impliquant pas de collecte d'identité.

Les organisations qui collectent ou traitent des données personnelles sans y être autorisées encourent une amende de **20 000 000 €** ou 4 % du chiffre d'affaire mondial[17].

Enfin, comme expliqué plus tôt, les communications et données de trafic ne peuvent être traitées que pour des raisons de sécurité, sur l'ordre de la loi ou avec l'autorisation de l'utilisateur ou utilisatrice.

[13] Une « donnée personnelle » est toute information qui porte sur un individu et qui peut être associée à cet individu, de façon directe ou indirecte.

[14] Les conditions de licéité d'un traitement de données personnelles sont listées à l'article 7 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[15] La CNIL a pu rappeler que « le cybercafé en question n'est pas obligé de relever et de conserver l'identité de ses clients pour fournir une connexion (ex : accès Wi-Fi ouvert) » (voir l'article « Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations ? » du 28 septembre 2010 sur cnil.fr).

[16] Par exemple, en application de l'article L. 336-2 du code de propriété intellectuelle, un juge peut ordonner à un fournisseur d'accès à Internet de faire cesser une infraction commise grâce à l'accès qu'il fournit. Le fournisseur peut alors choisir de mettre fin à cette atteinte en sécurisant, par exemple, son réseau à l'aide d'un mot de passe confié à certaines utilisatrices et utilisateurs, une telle mesure ayant été reconnue dans son principe comme conforme au droit européen par la Cour de justice de l'Union européenne (CJUE, McFadden, 15 septembre 2016, affaire C-484/14).

[17] À partir du 25 mai 2018, les traitements illicites pourront être sanctionnés par une amende maximale de 20 000 000 € ou 4% du chiffre d'affaire mondial, en application de l'article 83 du règlement général sur la protection des données.

C. Quelles informations doivent être conservées ?

Droit français

La loi française prévoit que toute organisation fournissant un accès à Internet doit conserver pendant un an[18] les informations suivantes :

– l'**identifiant du terminal** des personnes utilisant le service (telle que l'adresse MAC de son terminal, utilisée pour lui fournir l'accès) ;
– un **identifiant attribué** à chaque personne et à sa connexion (telle que l'adresse IP attribuée à chaque terminal) ;
– les **dates et heures** de début et de fin de l'accès à Internet fourni à chaque personne ;
– les **caractéristiques de la ligne** attribuée à chaque personne[19].

La loi française sanctionne le non-respect de ces obligations d'une peine d'un **an d'emprisonnement** et d'une amende de **375 000 €**[20].

Par ailleurs, les données conservées ne doivent en aucun cas concerner le **contenu** des informations reçues ou envoyées par les utilisateurs ou utilisatrices, et doivent se limiter au **strict minimum** de ce qui est requis[21], sans quoi il s'agirait d'une atteinte à la confidentialité des communications décrites ci-avant.

Enfin, dans les seuls cas où elle y est autorisée (dans les conditions exposées ci-avant), une organisation qui décide de recueillir de façon habituelle certaines informations doit conserver celles-ci pendant un an[22]:

– le nom et le pseudonyme de l'utilisateur ou utilisatrice;
– son adresse postale ou électronique;
– son numéro de téléphone ;
– le hash du mot de passe associé à la connexion;
– lorsque l'accès est payant, le type de paiement utilisé, la référence du paiement, le montant et la date et l'heure de transaction.

Cette obligation de conservation est soumise à la même peine que l'obligation générale.

Droit européen

La **Cour de justice** de l'Union européenne (UE) considère[23] que la Charte des droits fondamentaux de l'Union européenne **interdit aux États de l'UE** d'adopter une loi qui :

– impose « une **conservation généralisée** et indifférenciée de l'ensemble des données [...] de tous les abonnés et utilisateurs » ;
– « oblige les fournisseurs [...] à conserver ces données de manière **systématique et continue** » ;
– « s'applique donc même à des personnes pour lesquelles il n'existe **aucun indice** de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves » ;
– « ne requiert **aucune relation** entre les données dont la conservation est prévue et une menace pour la sécurité publique ».

Nous considérons donc que l'obligation de conservation imposée aux fournisseurs d'accès à Internet français est contraire à la Charte de l'UE. Cette Charte étant **hiérarchiquement supérieure** aux lois françaises, les hébergeurs français ne devraient être obligés de conserver aucune donnée : or, conserver des données personnelles sans justification est puni en droit européen d'une amende de **20 000 000 €** ou 4% du chiffre d'affaire mondial[17].

En conséquence, tant pour respecter le droit que les personnes qui utilisent leurs services, **nous recommandons aux organisations d'appliquer le droit européen**.

Cependant, une organisation peut avoir un besoin légitime de conserver certaines données pour des raisons techniques et de sécurité. Ainsi, pour la durée strictement nécessaire, elle peut conserver les données techniques (adresses MAC et IP, dates et heures de connexion) impérativement nécessaires pour des raisons techniques et de sécurité.

---

[18] L'obligation imposée aux fournisseurs d'accès à Internet de conserver des données est prévue par l'article L. 34-1 du CPCE (détaillé par le décret n° 2011-219 du 25 février 2011). Ces deux textes ont des conséquences très proches pour les organisations visées par le présent guide, et sont donc ici présentées conjointement. Le premier de ces deux textes concerne tout type de communications électroniques, et non le seul accès à Internet : il vise ainsi des données qui concernent d'autres types de communications (des communications téléphoniques), notamment des données liées à des « services complémentaires » et à des « destinataires » qui ne concerne pas l'accès à Internet et ne doivent pas à être prises en compte par les organisations visées par ce guide.

[19] Dans le cadre du présent guide, l'obligation de conserver « les caractéristiques de la ligne attribuée à l'utilisateur » ne devrait concerner que les organisations qui fournissent un accès à Internet par cable et qui ont attribué un identifiant unique à chacune des prises qu'elles mettent à disposition du public, ce qui n'est généralement fait que pour répondre à des impératifs de sécurité particuliers.

[20] L'article L39-3 du CPCE et l'article 131-38 du code pénal fixent la sanction attachée à la conservation des données, qui doit être portée au quintuple s'agissant des personnes morales.

[21] La CNIL rappelle l'obligation de ne conserver que les données strictement requises, regrettant que de nombreuses personnes en conservent plus que nécessaire (voir l'article « Internet et wi-fi en libre accès : bilan des contrôles de la CNIL » du 22 décembre 2014 sur cnil.fr).

[22] L'obligation de conserver les données spontanément collectées est prévue à l'article 6, paragraphes II et VI, de la loi du 21 juin 2004

[23] Arrêt Tele2 Sverige (C-203/15) de la Cour de justice de l'Union européenne du 21 décembre 2016, dont sont ici cités les paragraphes 97, 105, 106 et 108.

C. Annex 3

This annex reports the entire e-mail exchange, already documented in D4.2, of the consultancy Federica Giovanella gave to the ninux Calabria community. It is in Italian, given the context and the fact that it regards specifically Italian law.

Grazie mille dell'opportunità da parte della community calabra

Nota: artXcYZ = articolo X, comma Y, lettera Z

== I VINCOLI IN CAPO AI DETENTORI DI AUTORIZZAZIONE GENERALE AD USO PRIVATO DECADONO PER CHI RIENTRA NELLE FATTISPECIE DI "LIBERO USO"? ==

L'art105c1 stabilisce che le attività che elencherà in seguito sono "di libero uso". L'art99c5 ha inoltre stabilito che queste attività sono "in ogni caso libere".

Mentre è chiaro cosa significhi "libero uso", ovvero (da definizione art1c1p) che non necessitano di autorizzazione generale, la locuzione "in ogni caso libere" non trova una definizione formale nel codice e sembra lasciare il lettore alla loro definizione intuitiva che ha per forza di cose una portata molto ampia. È possibile definire meglio "in ogni caso libere"?

La problematica del dominio troppo ampio di "in ogni caso libere" può essere confinata a due elementi determinanti e pertanto prioritari:

* Nel Titolo III art99c5 vengono delineate come "in ogni caso libere" le attività art105c1, mentre invece ad altre fattispecie di attività elencate in seguito nello stesso comma viene applicata una qualificazione "nonché [...] per proprio uso esclusivo"
* Nel Titolo III art101c1 il requisito della "pertinenza propria", "divieto traffico conto terzi" viene posto in carico esplicitamente ai "titolari di autorizzazione generale ad uso privato".

La domanda è: questo linguaggio è sufficiente ad escludere che i requisiti/vincoli di A) "proprio uso esclusivo", B) "pertinenza propria" e C) "divieto traffico conto terzi" si applichino alle attività "in ogni caso libere" del art105c2?
In altri termini, ribaltati: se si svolgono attività di comunicazione elettronica "non per proprio uso esclusivo", con traffico "anche di pertinenza non propria" e pertanto "anche per conto terzi", si rientra comunque nella fattispecie di "libero uso" per attività art105c1?

L'art. 99 co. 5 prevede che "sono in ogni caso libere le attività di cui all'articolo 105". Ciò che segue- cioè la parte della norma che segue la virgola dopo "articolo 105" è altra cosa.
Significa che ai sensi dell'art. 99 co 5 sono libere sia le attività di cui all'art. 105, sia "la installazione, per proprio uso esclusivo, di reti di comunicazione elettronica per collegamenti nel proprio fondo o in più fondi dello stesso proprietario, possessore o detentore purché contigui, ovvero… (etc etc)".
Le caratteristiche richieste a queste altre attività secondo la mia interpretazione non si applicano a quelle di cui all'art. 105, che sono ***in ogni caso libere****.*
Sulla eventuale differenza fra "in ogni caso libere" e "di libero uso" non so rispondere. Potrebbe trattarsi di un problema
Io direi che le due locuzioni sono intercambiabili. Sarebbe forse utile leggersi un commentario al Codice delle Comunicazioni Elettroniche, ma se non ho dato risposta/indicazioni quando ho scritto nel 2015, probabilmente io stessa non ne ho trovate (a me pare non si possa dare altra interpretazione: il co. 5 dell'art. 99 e il co. 2 dell'art. 105 si richiamano l'un l'altro).

La necessità di questo approfondimento viene dal fatto che a pagina 112-114 di "Reti di Libertà" (IL DIRITTO CIVILE A CONFRONTO CON LE NUOVE TECNOLOGIE: WIRELESS COMMUNITY NETWORKS E RESPONSABILITÀ EXTRACONTRATTUALE*) l'esposizione si concentra sul dedurre l'assenza di necessità dell'autorizzazione generale (ovvero il rientro nel "libero

uso"), ma si perde di vista cosa succede ai requisiti di "pertinenza propria", "proprio uso esclusivo" e "divieto traffico conto terzi" ora che si rientra nel caso di libero uso (a meno che non se ne deduca la non applicabilità dall'espressione "in ogni caso libere". È così?).

L'art. 99 ci dice che le attività di cui all'art. 105 sono in ogni caso libere. Non necessitano di nessuna autorizzazione (come ci dice l'art. 99 co. 3; non necessitano infatti nemmeno quella di cui all'art. 99 co 4). Conseguentemente i requisiti che sono elencati secondo me non si applicano alle attività di cui all'art. 105, perché tali requisiti concernono soltanto attività che richiedono l'autorizzazione generale – sebbene solo quella per 'uso privato'.

== QUALE DIFFERENZA CONCRETA C'È TRA RETE PUBBLICA DI COMUNICAZIONI E SERVIZI DI COMUNICAZIONE ELETTRONICA AD USO PRIVATO CHE RIENTRANO NELLA FATTISPECIE DI "LIBERO USO"? ==

N.B. Questa intera sezione presuppone che la risposta alle domande della sezione precedente sia "si".

Il Codice all'art1c1ff nella definizione di servizi di comunicazione elettronica ad uso privato riporta "svolti esclusivamente nell'interesse proprio dal titolare della relativa autorizzazione generale". Dal punto di vista letterale è impossibile rientrare in questa definizione nel caso del "libero uso", proprio perché manca la necessità di autorizzazione generale.
Il che lascerebbe, sempre dal punto di vista letterale, un vuoto nel concetto di "rete di comunicazione ad uso privato".

Una cosa è una "rete di comunicazione ad uso privato", altra cosa è il "libero uso". Le reti di cui all'art. 1, co. 1 lett. ff) sono reti che hanno una autorizzazione (cf. art. 99). Mentre il libero uso esula totalmente da autorizzazioni di qualunque genere.

Cosa rimane nel linguaggio usato nel codice e dal punto di vista concreto a distinguere una rete di comunicazioni ad uso pubblico (ad esempio secondo la definizione art1aa) da una ad uso privato quando si rientra nella fattispecie di "libero uso"?
Ad esempio, concretamente che differenza ci sarebbe tra "servizi di comunicazione elettronica accessibili al pubblico" e la possibilità di effettuare traffico di non esclusiva propria pertinenza, anche per conto terzi?
In altri termini, ribaltati: se si svolgono attività di comunicazione elettronica "non per proprio uso esclusivo", con traffico "anche di pertinenza non propria" e pertanto "anche per conto terzi", quale sono le distinzioni utili a classificarla, dal punto di vista del codice, ancora come "ad uso privato"?

*La definizione di cui all'art. 1, co. 1, lett. aa) parla di una rete utilizzata "**interamente o prevalentemente** per fornire servizi di comunicazione elettronica **accessibili al pubblico**". Di conseguenza io credo che la 'frequenza' con cui queste reti sono utilizzate per dare accesso al pubblico sia rilevante: se prevalentemente/interamente, allora non è sicuramente ad uso privato (il che si riverbera sul tipo di autorizzazione necessaria).*
Inoltre una rete ad uso pubblico necessita di una autorizzazione generale diversa da quella ad uso privato (cf. art. 99).
Altra cosa però è il libero uso.

L'interpretazione più lineare sarebbe che, sebbene le attività che rientrano nella fattispecie di "libero uso" vengano introdotte solo nel titolo del Codice relativo all'uso privato, per esse decada la necessità di qualsiasi tipo di autorizzazione, sia ad uso privato che ad uso pubblico (un'idea supportata dall'assenza di specificazioni nella definizione art1c1p, che parla solo di "autorizzazione generale"); e che, di conseguenza, perda di senso il classificare le attività di cui art105c1 come "ad uso pubblico" o "ad uso privato". Una simile interpretazione concilierebbe in un solo colpo le criticità della "lettera del Codice" sopra esposte e concretizzerebbe la locuzione "in ogni caso libere" associata alle attività di cui art105c1.

È supportabile questa interpretazione?

È una possibile interpretazione. Essendo 'in ogni caso libere' potrebbero esserlo sia se utilizzate ad uso privato, sia ad uso pubblico.

== MEMORIA SUL "LIBERO USO E AUTORIZZAZIONI NELLE ATTIVITÀ PRIVATE DI COMUNICAZIONE ELETTRONICA" DELL'ISPETTORATO TERRITORIALE EMILIA-ROMAGNA DEL MISE ==

LINK:
http://www.sviluppoeconomico.gov.it/images/stories/documenti/Libero_uso_ed_autorizzazioni_nelle_comunicazioni.pdf

Considerata l'assenza di casi di giurisprudenza relativa a casi assimilabili a quello delle WCN che si menziona più volte in Reti di Libertà, la cosa più simile che abbiamo trovato ad un "parere" o "circolare" di una delle autorità a cui il Codice conferisce poteri di controllo e autorizzazione è la memoria (aggiornata due volte da quando il Codice è in vigore) dell'Ispettorato Territoriale dell'Emilia-Romagna, scritta dall'Ing. Marco Cevenini che ne è (stato?) il Direttore. È incerto quanto possa essere considerata autoritativa l'interpretazione del Codice offerta dalla memoria, però è sicuramente di interesse perché l'ambito in cui si concentra la memoria è proprio quello più strettamente applicabile alle WCN.

La memoria offre un'interpretazione del codice che associa la necessità o meno di autorizzazione generale alla valutazione contestuale di tre elementi di una comunicazione elettronica: "natura, luogo e mezzo trasmissivo" (pag 13). Mentre "luogo" e "mezzo trasmissivo" ricalcano le conclusioni di "Reti di Libertà", sulla "natura della comunicazione" l'interpretazione offerta contrasta nettamente e arriva a conclusioni finali diametralmente opposte.

La memoria definisce le "attività di comunicazione ad uso privato" come quelle che avvengono tra "entità riferibili [in quanto ad essa associate da un rapporto di dipendenza/collaborazione/convenzione/associazione/compartecipazione di fini] alla stessa realtà organizzativa (o ragione sociale) che possiede la rete di comunicazione [o detiene in ragione di proprietà, locazione, comodato d'uso, leasing, ecc]". Ribaltando la prospettiva, asserisce che "non sono legittimate in ambito privato le comunicazioni non riferibili ad una ragione sociale mediante una rete riferibile alla ragione sociale medesima". A pagina 1 alla definizione di "pertinenza propria" si specificava che esse sono "comunicazioni che avvengono a supporto della propria attività lavorativa o scopi istituzionali dell'ente o comunque a propri fini, non avendo esse il significato di core business del soggetto che ne ha la titolarità". A pagina 21 si sostiene più esplicitamente che "quando la comunicazione avviene fra entità qualsiasi, è necessario un intermediario autorizzato al fornitura di un servizio pubblico in concorrenza, secondo le regole stabilite dall'AGCOM." La memoria sostiene anche che la ratio di ciò è la possibilità di concorrenza sleale verso gli operatori che detengono autorizzazione generale per reti di comunicazione ad uso pubblico.

Non si può riscontrare nel Codice un tale livello di dettaglio nella definizione di "pertinenza propria" o persino menzioni esplicite di "ragione sociale" o termini equivalenti, e nemmeno dei concetti di "prevalenza delle comunicazioni nelle attività di business dell'entità" o di vincoli così specifici nella proprietà della rete.
In seguito (pag. 16) l'autore ammette che questi concetti sono funzionali ad una classificazione susseguente che non è presente nel Codice, ed è lecito supporre che ciò costituisca un'ammissione che anche i 3 elementi di cui sopra siano una tassonomia che non discende dal Codice senza una forte dose d'interpretazione:

"""
Dalla combinazione di questi tre elementi (la natura dell'attività, il luogo e il mezzo) derivano le diverse ipotesi autorizzative illustrate

nel seguito. secondo una declaratoria per categorie che è stata qui introdotta nella speranza di facilitare la comprensione della materia, ma che non è presente nel Codice. E' un tentativo di classificare una materia articolata e distribuita in varie parti del Codice.
"""

Nella classificazione delle attività di comunicazione elettroniche che immediatamente in seguito la memoria propone, l'interpretazione segue quella proposta in "Reti di Libertà" ma diverge sull'applicabilità dei vincoli di "pertinenza propria", "uso esclusivo", "divieto conto terzi" discussi in precedenza anche nel caso di "libero uso". In sostanza l'autore risponde "No" alle domande che abbiamo posto alla fine della prima sezione e pertanto non colloca le WCN tra le reti che sono qualificabili come "ad uso privato", e nemmeno di "libero uso" e pertanto tra quelle che necessitano di autorizzazione generale.

Cosa pensa di questa interpretazione offerta? Qual'è la forza autoritativa di un documento così come formulato in virtù della sua provenienza?

Essendo un documento del Ministero (anche se di un ispettorato) un giudice vi darebbe molto peso; le Pubbliche Amministrazioni sono vincolate, perché si tratta di una circolare interpretativa.

== CI SONO STATE SENTENZE RILEVANTI NEGLI ANNI 2015-2017? ==

"Reti di Libertà" risale a Gennaio 2015, e riporta chiaramente che mancano casi di giurisprudenza che direttamente o indirettamente possano chiarire il framework normativo delle WCN. Ci sono stati casi degni di nota a partire da allora?

Nessuna novità.
Il solo caso che potrebbe avere un'influenza sulle CNs è il caso McFadden della Corte di Giustizia Europea. Su di esso vi invito a leggere il D4.2 a par. 3.2 (alcune parti riguardano altri Paesi, ma ci sono riferimenti anche all'Italia).

== ESISTE LA POSSIBILITÀ DI AVERE UN PARERE UFFICIALE DA PARTE DELLE AUTORITÀ COINVOLTE? ==

In passato membri della community Ninux hanno contattato uffici del MISE interrogando alcuni funzionari a proposito della situazione legale di uno scenario WCN, ottenendo risposte contradditorie o parziali. Si registra inoltre l'assenza quasi totale di "circolari", "direttive" o documenti simili che aggiungano ulteriori dettagli utili ai lavori interpretativi della normativa, oltre alla già citata assenza di casi di giurisprudenza rilevante.

Esiste la possibilità di intraprende una procedura, attivabile da parte del cittadino, che possa portare ad ottenere un qualche livello di risposta formale da parte delle autorità competenti sulle problematiche interpretative della norma, in assenza di giurisprudenza rilevante? Se sì, quale sarebbe tale procedimento?

Ci sono delle possibilità (su cui occorre documentarsi).
La questione è che ovviamente richiedere ed ottenere un parere di questo tipo può essere problematico sotto due profili:
   a. *Se l'interpretazione fornita va nel senso opposto a quanto sperato a quel punto vi si è comunque vincolati*
   b. *Un simile parere vincola tutte le CN italiane e situazioni assimilabili*

Sarebbe necessario capire se siano maggiori i benefici o gli effetti negativi.

== SITUAZIONE NORMATIVA DI TECNOLOGIE ALTERNATIVE PER WCN ==

Già in "Reti di Libertà" si conclude che "fintanto che la tecnologia alla base di tali reti [wcn] non muterà, essere rientreranno nelle libere utilizzazioni, senza necessità di ottenere autorizzazioni o

licenze.". Finora un cambio tecnologico è rimasto più o meno sempre una possibilità teorica. Ultimamente sta suscitando interesse Koruza (http://www.koruza.net), un sistema ottico in spazio libero (FSO), open source e open hardware, pensato per connettività senza interferenze a banda ultralarga per l'ultimo miglio.

È corretto sostenere che tale sistema in Italia comporterebbe la necessità di richiedere autorizzazione generale per uso privato, ai sensi dell'art104c1b, ovvero che i "sistemi ottici" menzionati dall'articolo in questione includerebbero il sistema sopra menzionato?

È inoltre giusto considerare che per tale sistema vige la situazione che era in essere per le radio hiperlan prima del 2012, ovvero la limitazione dell'utilizzo su proprio fondo per poter rientrare sotto il profilo del "libero uso", ai sensi dell'art105c2a?

A questo fatico a rispondere; diciamo che la risposta dipende dai tecnicismi della tecnologia utilizzata. Se essa non rientra nelle attività elencate dall'art. 105, allora occorre una autorizzazione generale (per uso privato).

== IPOTETICO: PROVIDER PARTECIPANTE ALL'INFRASTRUTTURA NINUX ==

Sebbene non esista un caso pratico, in Ninux non è esclusa per principio la partecipazione alla rete di soggetti come ISP o più in generale aziende che possano offrire i propri servizi a pagamento agli utenti Ninux.

Dal punto di vista normativo, come sarebbe interpretabile la situazione dove un ISP partecipa all'infrastruttura della WCN con propri nodo/i e fornisce servizi a pagamento ad altri partecipanti alla rete?

Si fanno 3 precisazioni sullo scenario ipotetico su cui verte la domanda:

* L'ISP è dotato di una sua infrastruttura e di una autorizzazione generale ad uso privato. La partecipazione alla WCN sarebbe un "supplemento" alla gestione della propria infrastruttura, non un'alternativa.
* Si fa l'esempio preciso dell'ISP nella convinzione che la risposta non sarebbe fondamentalmente diversa da una generica azienda che partecipi alla rete per offrire i propri servizi commerciali, anche diversi dalla fornitura di connettività alla rete Internet, è che, anzi, sia quello dell'ISP che partecipa alla WCN per offrire i propri servizi lo stress-case più duro per il framework normativo. Si riconosce che assunto potrebbe facilmente essere errato.
* L'ISP o azienda sono in questo scenario "un membro ninux come un altro". Ovvero: l'aderenza al picopeering, alle "regole non scritte", e la partecipazione attiva alla governance della community vengono date per scontate.

L'ISP sarebbe sottoposto alle proprie regole (in termini di autorizzazioni, responsabilità, gestione dei dati personali, etc).
La cosa più semplice in assoluto sarebbe avere un contratto fra l'ISP e Ninux (anche se presumo non esista un ente giuridico che rappresenta Ninux; tuttavia si può sempre pensarlo come un'associazione non riconosciuta) dove si dettagliano per bene diritti e doveri delle parti. In questo modo si potrebbe regolare qualunque questione relativa – ad esempio – alla responsabilità o al pagamento/utilizzo dei servizi etc.

D. Annex 4

The final annex of this deliverable reports the text of the advocacy letter netCommons researchers participated in extending and distributing to help foster coordinated and distributed advocacy for the application of the Sverige/Tele2 jurisrudence.

European Commission
Secretary-General
B-1049 Brussels
BELGIUM

June 25, 2018

SUBJECT: APPLICATION OF THE TELE2 SVERIGE/WATSON JURISPRUDENCE THROUGHOUT EUROPE

Dear Sir or Madam,

We are organisations that, in different ways, defend digital rights.

We are **NGOs and litigation groups** upholding the rights to privacy, data protection and freedom of expression through advocacy, workshops and other educational activities.
We are **community networks**, organisations that operate on local communication infrastructures managed as commons good, for the people and by the people.
We are **academics**, analysing and teaching law in compliance with democratic values and the hierarchy of norms without which there is no rule of law.
We are **activists**, voicing a common concern for the preservation of rights and freedoms, including privacy and personal data protection.

On several occasions in the past, we have already pointed out existing hurdles in our legal framework for the protection of our rights to privacy and data protection.[1]

Together, we would like to address to the European Commission our concerns about the respect for CJEU case law on data retention by various Member States.

Directive 2006/24, which required the collection and retention of personal data significantly infringed privacy and data protection of people. Although it expressly excluded the content of telephonic or electronic communications and the communicated informations from it scope, it obliged Member States to ensure the conservation of personally identifiable data and allowed investigatory authorities to trace back a person's communication patterns and online activities.

Four years ago, the CJEU judged that Directive 2006/24/EC was invalid (CJEU April, 8th 2014, Digital Rights Irland) and, more than a year ago, the Court reiterated the same points, clearly and without ambiguity, in a preliminary ruling requested by courts in Sweden and in the United Kingdom (CJEU, December 21st 2016, Tele2 Sverige/Watson).

[1] Open letter to European Commissioner for Home Affairs Cecilia Malmström
Global civil society groups call for suspension of the EU-US Privacy Shield
Open letter to EU policy makers on community networks

In this judgement, the Court stated that:

"Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (…). National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society."

European law prevails over national laws. Therefore, the Court's aforementioned judgements must apply to all similar legislations across the European Union. Yet, we have found that at least **17 EU Member States**[2] still implement national measures mandating general and non-targeted bulk data retention, thus directly infringing the CJEU's interpretation of data retention law and interfering indiscriminately in each individual's rights to the respect for private and family life, the protection of personal data, and freedom of expression. These countries are: Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, France, Germany, Hungary, Ireland, Italy, Luxembourg, Poland, Portugal, Slovenia, Spain, Sweden, and the United Kingdom. On the issue of data retention, these countries' legal framework do not comply with the case law of the Court of Justice.

Today, 62 organisations, community networks and academics, in 19 member States share the concern expressed in this letter.
At the same time and as a consequence, in 11 Member States – Belgium, Czech Republic, France, Germany, Ireland, Italy, Poland, Portugal, Spain, Sweden and United Kingdom – we are filing complaints to the European Commission, to demand action, and to stand for the protection of fundamental rights enshrined in Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union, as interpreted by the Grand Chamber of the European Court of Justice.
We call for the application of sanctions for non-compliant Member States by referring to the Court of Justice, which should logically strike down all current data retention national frameworks.

Thank you in advance for acting and upholding the rights of EU citizens and residents.

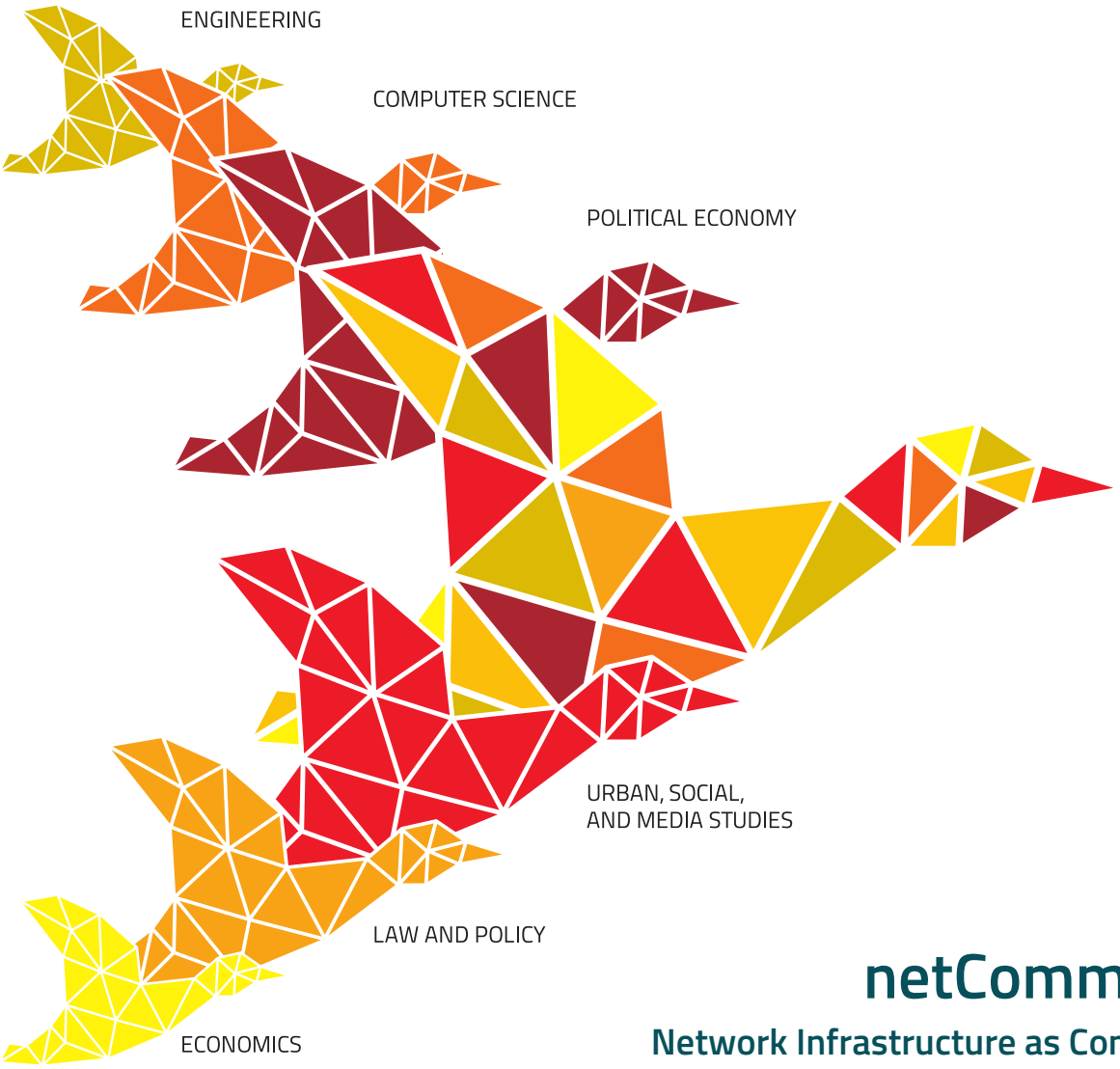
Sincerely,

[2] A Concerning State of Play for the Right to Privacy in EuropeNational Data Retention Laws since the CJEU's Tele-2/Watson Judgment

Signatories :

Les Exégètes Amateurs
La Quadrature du Net
netCommons
Privacy International
Pangea.org
Renewable Freedom Foundation
Aktion Freiheit statt Angst e.V.
Open Technologies Alliance - GFOSS
Digitalcourage e.V.
BlueLink.net
Frënn vun der Ënn
Asociatia pentru Tehnologie si Internet
Freifunk.net
Arbeitskreis Vorratsdatenspeicherung (Working Group on Data Retention)
Datenschutzraum e.V.
Franciliens.net
Aquilenet
ILOTH
FAImaison
NetHood.org
Tetaneutral
Digital Rights Ireland
Xnet
Hermes Center for Transparency and Digital Human Rights
epicenter.works – for digital rights
Bits of Freedom
Associação D3 - Defesa dos Direitos Digitais
Rézine
NURPA (Net Users' Rights Protection Association)
Access Now
Iuridicum Remedium
Panoptykon
DFRI - Föreningen för digitala fri- och rättigheter
Commons Network
Digitale Gesellschaft
Otvorena mreža
MeshPoint
Statewatch
Coalizione Italiana per le Libertà e i Diritti civili (CILD)
igwan.net
Network Bogotá
WirelessPT.net
Chaos Computer Club Lëtzebuerg
Initiative für Netzfreiheit
FDN
SCANI
Illyse
FFDN
Neutrinet
Open Rights Group
ALDIL
Liberty
APS Progetto Wireco Ciminna
Internet Society France
Touraine Data Network
Article 19
Mycelium
EDRi
IT-Political Association of Denmark
Sarantaporo.gr
Association for Progressive Communications (APC)
Electronic Frontier Norway (EFN)


Exégètes Amateurs
exegetes.eu.org
LA QUADRATURE DU NET
PANGEA
Internet ètic i solidari
BlueLink
freifunk.net
Renewable Freedom Foundation
netCommons
AK VORRAT
AKTION FREIHEIT STATT ANGST
GFOSS
Open Technologies Alliance
// datenschutzraum
Faimaison
{{ Franciliens.net }}
Fournisseur Associatif d'Internet
Aquilenet
digitalcourage
Digital Rights Ireland
ApTI
PRIVACY INTERNATIONAL
HERMES
NetHood
EPICENTER .WORKS
Xnet
BITS OF FREEDOM
DEFESA DOS DIREITOS DIGITAIS
Rézine
accessnow
nurpa
DIGITALE GESELLSCHAFT
iure
...není nám to jedno
FUNDACJA PANOPTYKON
Connect many. Anywhere.
MeshPoint
:DFRI
Föreningen för digitala fri- och rättigheter
Otvorena mreža
igwan.net
Commons Network
tetaneutral.net
WIRELESSPT
Network Bogotá
CILD
Italian Coalition for Civil Liberties and Rights
statewatch
SCANI
Internet autrement
OPEN RIGHTS GROUP
illyse
Internet Libre
C3L
CHAOS COMPUTER CLUB
LETZEBUERG
FDN
Wireco
LIBERTY
PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS
FFDN
EFN
Association Lyonnaise pour le Développement de l'Informatique Libre
Internet Society
France Chapter
IT-Political Association of Denmark
ARTICLE 19
TDN
EDRi
APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS
Sarantaporo.gr



netCommons

Network Infrastructure as Commons

European legal framework for CNs (v3)

Deliverable Number D4.3
Version 1.2
August 23, 2018

netCommons.eu