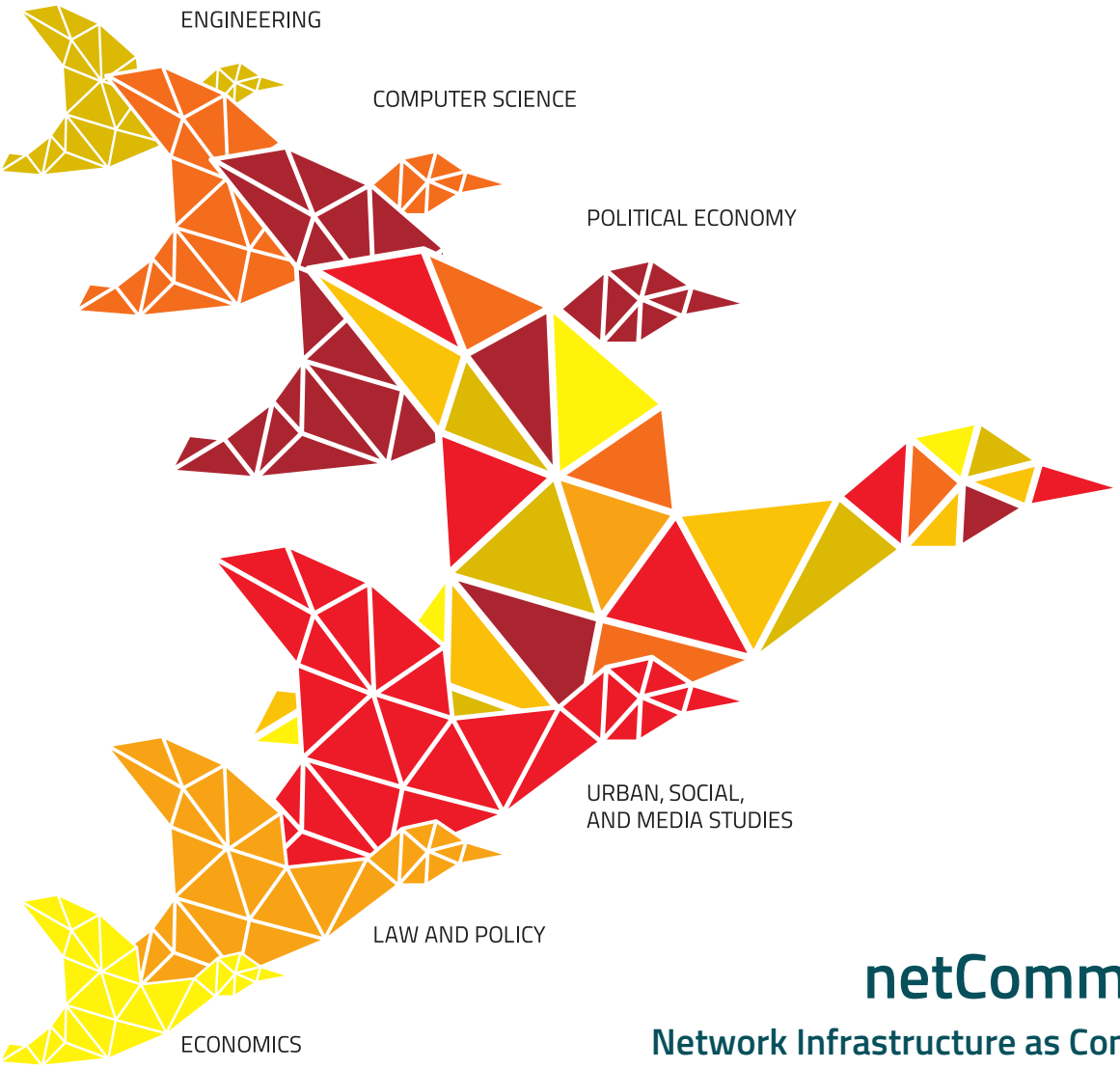


netCommons

Network Infrastructure as Commons

European Legal Framework for Community Networks (CNs) (v2)

Deliverable Number D4.2
Version 1.0
January 4, 2018

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

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:	Federica Giovanella, UniTN
Deliverable nature:	Report (R)
Dissemination level:	Internal
Contractual Delivery Date:	December 30, 2017
Date of Present Release	January 4, 2018
Number of pages:	94
Keywords:	Community Networks, Civil Liability, Privacy and Data Protection, Electronic Communications Code, Advocacy
Authors:	Federica Giovanella, UniTN Mélanie Dulong de Rosnay, CNRS Arthur Messaud, CNRS Félix Tréguer, CNRS
Peer review:	Renato Lo Cigno, UniTN Virginie Aubree, UniTN Roberto Caso, UniTN

History of Revisions

Rev.	Date	Author	Description
v0.1	19/06/2017	Federica Giovanella	First draft
v0.2	21/06/2017	Mélanie Dulong de Rosnay	Comments, suggestions
v0.5	29/06/2017	Federica Giovanella	Implemented suggestions and comments; added new appendixes
v0.51	30/07/2017	Renato Lo Cigno	Formal fixes and goal clarification; publication on the web site as interim report
v0.8	12/12/2017	Federica Giovanella	Update of v0.51. The part on advocacy activities has been removed as it will be part of D1.5; Interviews and their interpretation has been added; the update to 2017 novelties and the outcome of research in the second year has also been added
v0.9	23/12/2017	Federica Giovanella	Inclusion of the analysis of the survey
v1.0	30/12/2017	Renato Lo Cigno	Inclusion of the tables summarizing the survey, proofreading and analysis of impact and contribution

Executive summary

This deliverable, which draws on the findings of D4.1 [1], describes the research activities undertaken during M13-M24 for T4.1. It focuses on two main fields of activity:

1. the investigation of the actual application of EU law by Community Networks (CNs);
2. the description of the changes needed in EU law for electronic communications to encourage the development of CNs, based on this study and description we have fully developed proper Advocacy Guidelines in WP1, reported in D1.5 [2]).

As for the first field of activity, D4.1 described existing legislation and case law relevant to Community Networks and aimed at understanding whether the current law empowers or impairs the prosperity of exiting CNs and the birth of new ones. Conversely, **this Deliverable analyzes the actual application of law by and within CNs** (Chapter 2).

To allow a better understanding of the law and its application, we include a description of the novelties of 2017 in terms of legislation and case law with particular attention to personal data protection and data retention, which currently are among the most topical issues in EU law. More precisely, the main novelties that the ePrivacy Regulation will bring (Sec. 2.1.4.1) are highlighted and commented pinpointing the impact on CNs. The deliverable also goes into detail on the current status of data retention norms in Europe in light of the most important cases decided by the Court of Justice of the EU (Sec. 2.1.4.2 and Sec. 2.1.4.3) **highlighting how EU and National rules are often contradictory on this topic**.

After the introductory part regarding the current legal framework, the report thoroughly describes how CNs actually apply EU law. Two main sources of information have been used to obtain evidence on the actual application of law. First, face-to-face interviews with CNs' members were conducted by netCommons researchers (Sec. 2.2.1 and Sec. 2.2.2); second, based also on the responses obtained in the interviews, a survey was designed and run to collect further data from other CNs (Sec. 2.2.3, Annex 1). The results of the survey, which are analyzed and described in detail in this deliverable (Sec. 2.2.4 and Sec. 2.2.5), are the basis to draft some initial preliminary guidelines in Sec. 2.3, which will be fully developed in the "Best practices guide for CNs" (D4.5, due at M36).

The findings highlight that a possible solution to both liability and personal data protection issues would be the adoption of an agreement between each CN and its users. **A contract could distribute liability and at the same time be the right tool through which the CN can manage personal data protection duties as imposed by European law**.

With regard to the advocacy activities, this report illustrates what changes in European Union regulation for electronic communications are needed to shape upcoming laws also according to CNs' characteristics (Chapter 3). It mainly focuses on the adoption of the new European Electronic Communications Code, on its impact on CNs and on the amendments that would favour CNs' prosperity. This part of the deliverable is strictly linked to Task 1.3 on "Advocacy capacity-building" and to D1.5 that describes the advocacy activities carried out by the research group and includes guidelines for effective advocacy.

Contribution to netCommons Goals.

The specific objective this Deliverable tackles is **Objective 4: Best practices for CNs**. More precisely, it digs into the critical issue of whether CNs actually correctly understand and apply existing laws. Objective 4 is part of the domain of global action, but indeed this deliverable also contribute to the domain of local action, as it is clear that findings on CNs behaviors have also (and probably foremost) local consequences. In particular we can say that the findings in this Deliverable also contribute to **Objective 2: Sustainability**, as it is clear that a sound legal understanding and best practices are essential for the survival of CN.

The results of our analysis highlights a mixed and in general rather complex scenario. On the one hand, legislation and regulations are utterly unaware not only of CNs, but in general of the fundamental needs for the

correct development of digital communications for the benefit of citizens; in particular there is a complete lack of consideration and understanding of distributed (not decentralized, but truly distributed, without the presence of a central coordination, either legal or technical) communications infrastructures. On the other hand, CNs have in general a very vague understanding of the legislation and the requirements that are posed to anyone handling a communication infrastructure, and this clearly hampers the development and jeopardizes the sheer existence of many of them, which would probably not survive a "legal accident."

The content of this Deliverable informs netCommons and CNs as well on the situation, and it is the starting point for the development of recommendations and best practices.

Impact on Community Networks.

As this deliverable is mainly analytic and descriptive, its direct impact on CNs is still limited. Indeed, however, both running the interviews and collecting the survey answers, already had a measurable impact on CNs. First of all we found out that the apparent lack of attention of many CNs to legal details is not due to negligence, but the the utter difficulty in accessing legal advice and finding a way in the maze of rules and regulations. The interaction with netCommons had the immediate impact of helping them re-think their situation, and also have a legal advice (see the ninux Calabria case in Sec. 2.3). It is clear that all of this influences **Local Impact 1: Governance guidelines for CNs**, although we expect a greater impact from the formalized guidelines of D4.5.

Furthermore, this Deliverable gives preliminary guidelines on how to deal with civil liability and personal data protection issues under EU legal framework, which clearly has an impact on CNs life. We still don't know how many CNs are changing their bylaws or modifying some of their habits/internal rules, because decision processes in CNs obviously follow their own dynamics; however, many CNs are actually considering the question and we will monitor to see if they take also action.

Contents

List of Acronyms

Art. 29 WP	Art. 29 Working Party
CJEU	Court of Justice of the European Union
CN	Community Network
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECS	Electronic Communications Service
EDPS	European Data Protection Supervisor
EECC	European Electronic Communications Code
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
KPI	Key Performance Indicator
IAP	Internet Access Provider
IBAN	International Bank Account Number
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IRC	Internet Relay Chat
ISM	Industrial, Scientific, Medical
ISP	Internet Service Provider
LTE-U	Long Term Evolution–Unlicenced
MAC	Medium Access Control
NPO	Non-Profit Organization
NRA	National Registration Authority
OTT	Over-The-Top Providers
SLAAC	StateLess Address AutoConfiguration
ToS	Terms of Service
URL	Universal Resource Locator
VoIP	Voice over IP
VPN	Virtual Private Network
VPS	Virtual Private Server
XMPP	Extensible Messaging and Presence Protocol

1. Introduction

As already discussed in D4.1 [1], the first deliverable of Task 4.1, legislation and regulations play a major role in shaping CNs. After the intermediate version (v. 0.51) released June 2017 on netCommons web site, this final version of the deliverable illustrates the research activities on the Legal Framework CNs are bound to in Europe carried out during the second year of research (M13-M24).

The report is divided into two main parts. The first one describes the actual application of current laws by CNs. The second one illustrates what needs to be changeds in European Union regulation for electronic communications through upcoming laws in order to shape them also according to CNs' characteristics.

As for the first part, it briefly summarizes the findings of D4.1 describing existing legislation and case law relevant to CNs (from Sec. 2.1.1 to Sec. 2.1.3). The legal novelties occurred during the second year of research follow (Sec. 2.1.4).

D4.1 goal was to understand whether existing laws allow the prosperity of the current CNs and the deployment of new ones, or if they impair and jeopardize them, whereas this deliverable describes the actual application of laws by CNs as it emerges from the information retrieved through interviews and surveys carried out among CNs.

Between M15 and M17 netCommons researchers conducted some face-to-face interviews with CNs' members. The results of these interviews, which are described in detail in this report (see Sec. 2.2.1 and Sec. 2.2.2), served as a basis for designing a more general and detailed survey that was circulated among CNs' members (Sec. 2.2.3 - Annex 1), in order to collect as much information as possible about the way CNs deal with legal issues.

The results of the survey are summarized in Sec. 2.2.4 and then thoroughly analyzed in Sec. 2.2.5.

They show that CNs experience difficulties in properly applying some pieces of law as in some cases they do not have a correct understanding of the requirements and of the technicalities of the law. These results prove very useful, as they will serve as the starting point to draft some "Best practices guide for CNs" (T4.5-D4.5; due at M36). To this end, this report include some brief, preliminary guidelines in Sec. 2.3.

The second part of the report describes the ongoing changes in EU electronic communications law, focusing in particular on the draft for a new Electronic Communications Code as described in Chapter 3. It illustrates the weaknesses of the current draft and the amendments needed in order to address CNs needs and to foster their development (Sec. 3.1 and Sec. 3.2).

The last section draws some brief conclusions and explains what are the next steps to be taken in order to achieve the goals of T4.1 (Chapter 4).

2. European Legal Framework for Community Networks

2.1. First year findings

In order to allow a better comprehension of the research that has been carried out in the past few months, a brief summary of the findings of the first year of research is summarized hereinafter.

This summary partially complements D4.1 [1], which has been passed on to CNs as part of the interactive process to develop the legal analysis.

It is fundamental to stress that although D4.1 focussed on three main issues, namely: telecommunications policy, civil liability, and personal data protection, the current research focuses only on the latter two. The reason why we decided to narrow down the scope of our research is mainly related to the fact that the regulatory framework for telecommunication is undergoing significant changes at the European level. More precisely, as it will be described later in this report, the EU policy makers are in the process of adopting a European Electronic Communications Code (EECC). The proposal for a Directive establishing the EECC will merge four existing Directives on telecommunications: Framework Directive (Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services), Authorisation Directive (Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services), Access Directive (Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities) and Universal Service Directive (Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services).

Given the ongoing modifications, we decided not to focus on the application of these rules on CNs, but rather on the possibility to influence the making-process of the Directive through advocacy actions. This latter activity tackled by WP1 and is reported in D1.5 [2], so we refer the interested reader to this document for further reading and information.

2.1.1. Liability Issues

"**Civil liability**" can be defined as the **liability arising from private wrongs or breach of contractual duty** and that is **not criminal** liability; normally, civil liability implies a duty to compensate for damages.

Civil liability can for example arise when someone causes damages to someone as a consequence of a privacy breach or defamation, or in cases of intellectual property rights' damages. These are classical cases arising from the use of the Internet. The diffusion and use of CNs might entail similar cases.

An example will help to clarify how the current European and national rules apply.

Let us suppose that a user shares a movie within the CN without having the right to do so. This is a case of copyright infringement. Who could be held liable for such infringement?

Three hypotheses can be envisaged in CNs: **a) The final user; b) The gateway owner; c) The CN itself.** These three hypotheses are discussed in the following paragraphs.

2.1.1.1. Liability of the final user

The **first case** is the liability of the final user. It might however be difficult in the context of CNs to allocate liability to the final user, for two reasons:

- The **illicit action might be allocated to a high number of different users' machines** and it becomes impossible to understand who is the person that actually committed the action;
- Sometimes specific **software shields users' identity and allows anonymity**.

2.1.1.2. Liability of the gateway node's owner

If a video is **uploaded** by a user to the Internet **through a gateway node**, the person who runs the gateway node would be identifiable through his/her public Internet Protocol (IP) address. This person might be considered liable depending on national laws:

- **Some countries** (for instance, Germany with the Störerhaftung doctrine and France with HADOPI law) **hold someone liable for the mere fact of not securing his/her Wi-Fi network.** In such countries an individual can be ordered by a court to put a password on his/her Wi-Fi network and if s/he does not, s/he would be held liable in case of damages suffered by a third person. In the example, the action of sharing the video could cause a damage to the copyright holder of the video. The copyright holder may not be able to identify who uploaded it and could sue the owner of the gateway node (of course the prior step of identification of the gateway owner by the provider would be needed).

  Other countries do not have similar laws (Italy, for example).
- In addition, the owner of the gateway node normally signs a **binding contract with an Internet Access Provider (IAP)**, in which **often a clause expressly forbids the customer to share the connection**. Another frequent clause is the one that considers the **customer liable for the damages** suffered by the provider as a consequence of a conduct that is prohibited by the contract itself. Therefore, for the **mere fact that the customer shares his/her connection s/he will be liable for breaching the contract and** – in case of damages caused by a third party's wrongdoing – **s/he could also be asked to compensate the victim.**

2.1.1.3. Liability of the CN

Can the CN be held liable? This **depends** on two main issues:

- Is the CN organised as an association or a foundation? In other words, **has the CN a legal status?**
  - **If so, national rules applies.** Usually one or more individuals are in charge of the legal entity and these individuals are those who can be held liable for the wrongdoings occurring within the CN.
  - **If the CN does not have a legal status, it is not possible to hold it liable.**
- Is the CN also an **Internet Access Provider** under national law?
  - If so, European rules on Internet Providers' liability apply. In particular, access providers are those providers that transmit information provided by a recipient of the service or provide access to a communication network.
  - **Art 12, Dir. 2000/31**[1] – and its corresponding implementation in national law – states that a "provider is not liable for the information transmitted, on condition that the provider:

    (a) does not initiate the transmission;

    (b) does not select the receiver of the transmission; and

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

(c) does not select or modify the information contained in the transmission.

The acts of transmission and of provision of access referred to in the list above include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

– If a CN is an Internet Service Provider (ISP), it qualifies for the liability exemptions under Dir. 2000/31 and therefore it might be held liable only if it does not comply with art. 12 above quoted.

- In 2016 the Court of Justice of the European Union (CJEU) (*Tobias Mc Fadden v Sony Music Entertainment Germany GmBH*, September 15, 2016) decided that in order to discourage the illegal sharing of works protected by intellectual property rights a court can order a provider who runs a Wi-Fi network to password-protect the network. In case users want to access the network they must be identified, so that they cannot act anonymously. If a CN is qualified as an IAP this decision might be easily applied by national courts as well. This means that although the CN would be exempted from liability under art 12, Dir. 2000/31 (see above under IAP's liability), it could be the target of this kind of orders.

2.1.1.4. Open questions after the Mc Fadden case

Open questions remain after the CJEU's decision:

- What could **CNs modify in their feature**s in order to avoid the negative consequences of the Mc Fadden judgment? In other words, can the decision a**ffect the shaping and the sustainability** of ecology of CNs as alternative, peer-to-peer, commons-based solution to provide a service?
- Which dimensions would be likely to be affected?
- **Should CNs take pre-emptive measures** to avoid negative consequences, or would a modification of the design be so disruptive that it would signify the end of open CNs?

2.1.2. Data Protection and Privacy

2.1.2.1. General Obligations

CNs shall comply with the obligations imposed by the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)[2] when they **process** (collect, store, use or disclose) **personal data** (information relating to an individual and which may be directly or indirectly attributed to this individual), or may be fined up to 20,000,000 EUR. These obligations are imposed on all CNs, irrespective of their legal status.

1. Processing shall pursue and be limited to a lawful purpose, which is the case where:
   - users have freely given their explicit, informed and specific **consent**;
   - processing pursues a "**legitimate interest**" which is not overridden by users' own interests (CNs shall balance these interests);
   - processing is necessary for performing a **contract** with users; or
   - processing is necessary for complying with a **legal obligation**.
2. CNs shall implement security measures preventing accidental or unlawful processing and notify any security breach to authorities within 72 hours (and, in some cases, to individuals).
3. CNs shall provide users with complete information about each processing action (its purpose and duration, whether data are disclosed to third parties or transferred outside the EU).

[2] 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), OJ L 119, 4.5.2016, p. 1–88, so called "GDPR".

4. CNs shall allow users to freely exercise their rights (obtaining a copy of their data, asking for the rectification of inaccurate data or the erasure of unlawfully processed data) and comply with their requests within one month.
5. CNs shall maintain a record of its processing and, where a processing results in specific risks, carry out a prior impact assessment.
6. CNs shall only **transfer** data to a country **outside the EU** in three cases:
   - the European Commission has issued an "**adequacy decision**" about this country (Argentina, Canada, Switzerland, Israel, Uruguay, New-Zealand, ... or US companies which have submitted to the Privacy Shield);
   - data are transferred to a third party which has entered into a contract with the CN containing **standard contractual clauses or appropriate safeguards**;
   - users have **consented** to the transfer or the transfer is necessary for the performance of a **contract** with users.

CNs shall comply with these general obligations whenever the process personal data, but they can be subject to fewer or more obligations depending on their activities, as explained in the next section.

2.1.2.2. Specific Obligations

1. The main activity of CNs is to provide access to their network and to **transmit communications** over it: both the content and traffic data of such communications are personal data;
   - transmitting these data on behalf of users **always pursues a lawful purpose** (whether or not users have explicitly given their consent);
   - such transmission is regarded as an "**electronic communications service**" (Electronic Communications Service (ECS)).
2. Other activities of CNs (such as VoIP or email) imply processing personal data:
   - CNs shall pursue a lawful purpose (consent, "legitimate interest" or contract);
   - some of these services may be regarded as ECS (whose legal definition remains unclear).
3. Art. 6, Dir. 2002/58[3] provides that CNs may only **reuse the traffic data** processed for the provision of an **ECS**:
   - if the data have been fully anonymized; with user's consent;
   - in order to bill users or for interconnection payments;
   - or, in France and Germany, in order to ensure network security.

   ! CNs **may not reuse** such data for pursuing any "legitimate interest".
4. National laws provide that CNs have to **retain all traffic data** processed for the "transmission of communications" (IP addresses and date and time of call or log-in and log-off, International Mobile Subscriber Identity (IMSI), location data ...):
   - In **Germany**, for ten weeks or may be fined up to 500,000 EUR;
   - In **Spain**, for one year or may be fined up to 20,000,000 EUR;
   - In **Italy**, for one year for Internet access and two years for telephone service, or may be fined up to 50,000 EUR;
   - In **France**, for one year or may be fined up to 375,000 EUR; in addition French hosting providers shall retain during one year information about users.

[3] 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), OJ L 201, 31.7.2002, p. 37–47.

! The European Court of Justice found that such laws may be **violating the Charter of Fundamental Rights of the EU** (case *Tele2 v. Post-och telestyrelsen*, December 21, 2016)[4], but these laws have yet to be repealed.

2.1.3. Specific issues regarding decentralized networks

In practice, complying with these obligations may be **very burdensome** for distributed structures such as CNs. Thus, CNs may try to **adapt** these rules to their specific structure or to change them through **advocacy**. Otherwise, they should comply with the **strict framework** described below, as imposed by the GDPR.

1. Where decisions are made by a central legal entity and participants carry out processing on its behalf:
   - the central entity is liable for compliance with all CN's obligations;
   - participants shall implement security measures, keep records, retain traffic data;
   - participants shall enter into a **contract** with the central entity, providing for specific obligations.
2. Where decisions are **collectively** made by the participants:
   - participants shall enter into a **collective contract** determining their respective obligations (who shall obtain users' consent, provide them with required information or answer their requests, for instance);
   - each participant shall retain the traffic data he/she individually processes.

2.1.4. 2017 Novelties

2.1.4.1. Proposal for an ePrivacy Regulation

On January 10, 2017 the European Commission published a **proposal for an ePrivacy Regulation**[5]. 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[6] of the EU and it constitutes *lex 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, such as "electronic communications services" (art. 4(b) of the proposal)[7] and it will apply to Over-The-Top Providers (OTT) as well.

While the proposal recognizes the potential of metadata to reveal very sensitive information, **it does not include any provisions about data retention**. More precisely, it does not limit data retention or make it illicit; on the contrary, it confirms the exception introduced by art. 15, Dir. 2002/58 on the base of which Member States can keep or introduce national data retention laws. However, the proposal itself clarifies that in implementing such laws, Member States shall take into account the case law of the Court of Justice on the interpretation of

[4] Joined cases Tele2 Sverige AB v. Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15), December 21, 2016.

[5] Proposal for a Regulation of The European Parliament and of The Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10 January 2017.

[6] 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-releaseIP-17-16en.htm

[7] Art 29 Working Party expressed its concerns for these definitions that the WP calls "moving targets": Art. 29 Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)," Apr. 4 2017, p. 25; critiques have been presented also by the EDPS in its "Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)," Apr. 24 2017, p. 10-11.

existing directives and the Charter of Fundamental Rights. More precisely, the proposal explicitly refers to the cases *Digital Rights Ireland*[8] and *Tele2 Sverige*[9], later briefly described.

As regards to metadata, Art. 29 Working Party (Art. 29 WP) expressed its concern on the definition given in the proposal, which seems to be too narrowly worded to cover all the cases in which metadata is generated[10]. In addition, Art. 29 WP highlights that the proposal should be stricter on data retention. In spite of the declamatory wording recalling the CJEU's case law, in the Art. 29 WP's opinion the ePrivacy Regulation proposal broadens the possibility to retain data due to its loose wording[11].

The WP further states that national exceptions to EU law data processing protection are subject to the Charter of Fundamental Rights and therefore any national provision should only introduce necessary and proportionate measures[12].

The proposal of the Regulation states that it applies to "to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users" (art. 2). The material scope is therefore broader than that of Dir. 2002/58, which did not include terminal equipment.

The proposal also clarifies that **is applicable** to the provision of ECSs to end-users **regardless of whether users are required to pay for the service or not** (art. 3). It covers both content and associated metadata (Recital 14).

Very interestingly 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". Hence, 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[13].

The Regulation shall be **applicable starting by May 25, 2018** that means exactly on the same day when the GDPR will be applicable.

As highlighted by Art. 29 WP, among the processing of data that could be subject to users' consent there is **Wi-Fi tracking**. This actually depends on the circumstances and purposes of the data collection, but nonetheless the Art. 29 WP recommends anonymization[14].

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 European Data Protection Supervisor (EDPS) also suggest "**all public wireless internet hotspots should fall within the scope**": this might have an impact on CNs that offer Wi-Fi to the public at large[15].

It remains to be seen if the wording of the proposal will change and if the interpretation given by Art. 29 WP will be followed.

[8] CJEU, Digital Rights Ireland v Minister for Communications and others (C-293/12 and C-594/12) 8 April 2014.

[9] CJEU, Tele2 Sverige AB v. Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15), cit.

[10] Art. 29 Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)," Apr. 4 2017, p. 16.

[11] Art. 29 Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)," Apr. 4 2017, p. 23-24.

[12] Art. 29 Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)," Apr. 4 2017, p. 32.

[13] EDPS, "Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)," Apr. 24 2017, p. 7.

[14] Art. 29 Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)," Apr. 4 2017, p. 3.

[15] Art. 29 Working Party, "Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)," Apr. 4 2017, p. 27; EDPS, "Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)," Apr. 24 2017, p. 9.

2.1.4.2. Relevant CJEU case law on personal data protection

In the last months of 2016 the CJEU decided two cases on privacy matters that can have an impact on CNs as for the application of data protection law.

In the case ***Patrick Breyer v. Bundesrepublik Deutschland***[16] decided on October 19, 2016, Mr Breyer brought an action before the German courts to obtain an injunction to prevent some website run by a Federal German institution from collecting and storing his IP address. The institution registered IP addresses with the aim of preventing cyber-attacks and of making it possible to commence a criminal proceeding if needed.

The Bundesgerichtshof asked the CJEU for a preliminary reference to understand whether IP addresses, more precisely dynamic IP addresses could qualify as personal data in the specific case. In fact, only the ISP offering the connection to Mr. Breyer had the additional information needed to identify him, coupling his IP address with his identity.

The CJEU held that IP addresses registered by an online media service provider can be considered personal data under Dir. 95/46[17] when the operator has a legal means that enables him/her to identify the visitor with additions information detained by the ISP. This decision is in line with previous interpretation given by the Art. 29 WP[18] as well as with previous case law by the CJEU[19].

This judgment might affect CNs insofar as they collect and retain IP addresses, as below explained[20].

Another case related to personal data protection is ***Tele2 Sverige v. Post-och telestyrelsen*** (also referred to Tele2/Watson case)[21] decided on December 21, 2016. The judgment follows the seminal case Digital Rights Ireland of 2014 in which the CJEU declared Dir. 2006/24[22] invalid as it imposed a general obligation to retain traffic and location data in such a way that it violated the rights covered by arts. 7 and 8 of the Charter of Fundamental Rights, meaning the rights to respect for privacy and the protection of personal data.

Following this judgment, two references for preliminary ruling were made to the CJEU: in both cases the question related to the validity of a law imposing a general obligation on providers of ECSs to retain data. The request was made within a Swedish and a UK lawsuit and in both cases the law at stake was the result of the implementation of the later invalidated Dir. 2006/24.

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

In the UK case, three UK citizens brought an action challenging the UK norms on data retention. These norms asked public telecommunications operator to retain all the data relating to traffic for maximum 12 months. The request for preliminary ruling asked whether national laws imposing on provider a general obligation to retain data for purposes not restricted to the fight of serious crimes could be compatible with EU law. Furthermore, they asked whether access by competent authorities to the retained data without review by a court could be considered compatible with EU law. Concerning the access by competent authorities, national laws should define criteria and circumstances in which such access can be granted.

[16] CJEU, Patrick Breyer v. Bundesrepublik Deutschland (C-582-14) 19 October 2016.

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

[18] Art. 29 Working Party, "Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipment: the example of IPv6," May 30 2002, p. 3.

[19] Consider CJEU's decision in Scarlet Extended SA v. SABAM, (Case C-70/10) 24 November 2011, para 26.

[20] See Sec. 2.3 on Preliminary Guidelines.

[21] Joined cases Tele2 Sverige AB v. Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15) 21 December 2016.

[22] 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, OJ L 105, 13.4.2006, p. 54–63.

The most important part of the decision is the one in which the CJEU states that EU law does not allow national legislation that requires general and indiscriminate retention of data. This does not mean there cannot be derogation to personal data legislation, but these **derogations must apply only when strictly necessary**. For instance, derogations can be introduced if the objective is to fight serious crimes. When there is neither proportionally nor correlation between the retained data and the objectives for which that data is retained, the provision asking for retention is not compatible with EU law.

National legislation shall state clearly what data have to be retained and for what specific purposes. Whenever national laws do not comply with these requirements, they cannot be considered compatible with EU law. Hence, already existing legislations in the countries where CNs operate could be invalidated as incompatible with EU law.

The CJEU also highlighted that the Court specified that **providers of electronic communications services must put measures in place to ensure the security and integrity of the retained data**.

2.1.4.3. Data Retention after *Digital Rights Ireland* and *Tele2* cases

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[23].

In 2017 Eurojust conducted a survey to investigate current data retention regimes in EU[24]; 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 2017)[25];
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.

Many EU countries are in the process of adopting new laws or of amending existing ones[26]; amendments include for example the introduction of a distinction amongst different data or the broadening of the categories of providers that shall retain data [27]. This will be followed and updated if possible in D4.3.

Taking as examples the same countries analyzed in D4.1 [1], it is possible to state what follows:

- **France**: the laws existing before *Digital Rights Ireland* and *Tele2* cases are still in place. There is a pending challenge of décret n. 2011-219 and article R. 10-13 of *Code des postes et communications électroniques* before the French *Conseil d'Etat*. Apart from this pending lawsuit, there is currently no sign of legislative reform[28];

[23] 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, p. 12.

[24] Eurojust, "Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15," Nov. 6 2017

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

[26] Consider Eurojust, "Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15," Nov. 6 2017, p. 22.

[27] Eurojust, "Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15," Nov. 6 2017, p. 8-9. See the table in Privacy International, National Data Retention Laws Since the CJEU's Tele-2/Watson Judgment, cit., p. 15. For a synthetic account of the current state of data retention legislation throughout Europe consider also: European Union Agency for Fundamental Rights, "Data retention across the EU," 2017.

[28] Privacy International, "National Data Retention Laws Since the CJEU's Tele-2/Watson Judgment. A Concerning State of Play for

- **Germany**: while there are no ongoing changes, many constitutional challenges have been raised against existing law (Vorratsdatenspeicherung, adding §§ 113a – 113g to the Telekommunikationsgesetz) adopted in 2015. In a decision by the Higher Administrative Court of Nordrhein-Westfalen, the court found that the current German law does not meet the requirement stipulated by the CJEU in *Tele2* and therefore relieved the plaintiff ISP to retain traffic data. Consequently, Germany's Federal Networks Agency (*Bundesnetzagentur*) announced that it would desist from enforcing data retention law[29];
- **Italy**: data retention norms are included in art. 123 of the Privacy Code (legislative decree n. 196/2003); the retention period was extended through the Anti-Terrorism Decree (decree n. 7/2015, converted into L. 43/2015) that prescribed data retention until December 31, 2016 for some specific crimes. The decree was not renewed with the consequence that its provisions stopped to be applicable from July 1, 2017. However, on November 8, 2017 the Italian parliament passed a law implementing art. 20, Dir. 2017/541[30] that extended the retention period of traffic data, telephone data and unanswered calls to 6 years (art. 24, L. 167/2017). Although the Italian Privacy Authority harshly criticized this provision when was it was pending as a bill[31], the Parliament adopted it with large majority;
- **Spain**: no modifications intervened in the last year, after *Tele2* judgment. Hence, the obligation for Internet and telecommunications providers to retain general and indiscriminate traffic and location data from 6 months to 2 years is still in force[32].

2.2. Second Year of Research

D4.1 [1] and its update to new cases and changes analysed the European legal framework for CNs and focussed on three main area, namely: civil liability, personal data protection and telecommunications policy.

In the second year, the research on legal aspects concentrated only on two of these three areas, dropping telecommunications policy. The reason for this choice is the fact that telecommunications policy is undergoing deep changes at the EU level. In fact, the EU is about to adopt a new directive –the so called "European Electronic Communications Code" (EECC)– that will repeal and substitute a number of existing directives in the field of telecommunications law . The undergoing legislative process has been the focus of advocacy activities that are at the core of T1.5 (see D1.5 [2]). In fact, given that the EECC has not been adopted yet, netCommons priority for CNs legal sustainability has been to try to influence the EU legislator to amend the draft of the EECC to accommodate CNs' needs.

The research activities carried out on this second year are therefore linked to existing and applicable laws in the field of civil liability and personal data protection. More precisely, an in-field research was made in order to understand if and how CNs comply with the current legal framework as described in D4.1.

2.2.1. Information Collected through Interviews

The second year of research is aimed at understanding how CNs deal with legal obligations and duties imposed both by European and national legislation.

In order to collect this information, we have conducted a few face-to-face interviews with some CNs members. We mainly contacted people in charge of the community, or people dealing with legal issues (for example, the interviewed person could be a lawyer that is involved in a CN).

the Right to Privacy in Europe," 2017, p. 22-23.

[29] 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, p. 23-24. See also [10].

[30] Directive (EU) 2017/541 of The European Parliament and of The Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6-21.

[31] Garante per la Protezione dei Dati Personali, "Terrorismo: Soro, troppi 6 anni conservazione dati chiamate," Jul. 25 2017.

[32] 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, p. 37-38.

The interviews were conducted in the language spoken by the interviewed person and then transcribed and translated into English. The interviewee's name is not mentioned, in order to allow an appropriate level of anonymity. After transcription, the recorded interviews were deleted.

Based on the interviews conducted in the first months of 2017, we designed a questionnaire (Annex 1) that was circulated amongst CNs and their members. The questionnaire was created through "Limesurvey", an online tool that allows anonymization (for more details on ethical assessments, consider D8.1 Ethics Requirements [12], in particular Sec. 2.1.5).

As mentioned, the research on legal issues focuses only on two specific aspects, namely civil liability and personal data protection. As for telecommunications policy, the efforts of the research team have concentrated on the advocacy activities later described (Chapter 3).

This section will therefore **summarize the findings of the interviews** carried out with CNs' members. In an attempt to be clear, the information will be conveyed through a table; a detailed description of the responses will also be provided. The questions made in the face-to-face interviews were very close to those later included in the survey.

We grouped the information collected into five main areas: **organisation, services offered, relationship with users, processed data, data retention**.

Each subject area aims at clarifying the functioning of CNs and their way of dealing with specific obligations imposed by the law, especially from the point of view of personal data protection and data retention. At the same time, organizational and contractual aspects should help to clarify what would happen if a case of civil wrongdoing occurred.

2.2.1.1. Tables summarizing interviews findings

France 1	▷ Organized as an association ▷ General decisions are made by the members and/or board of CN ▷ Specific technical decisions are made by system administrators ▷ The CN is legally an IAP
France 2	▷ Organized as an association ▷ General decisions are made by the members and/or board of CN ▷ Specific technical decisions are made by system administrators ▷ The CN is legally an IAP
Italy 1	▷ Does not have any legal existence. ▷ Decisions are taken either through the mailing list or in personal meetings – the CN is a very small group of people (less than 10). ▷ With regard to the single nodes, each member does what s/he likes most. ▷ Some members do also manage other people's nodes (for instance because these people lack technical skills or because they are not interested in taking part to the CN, but allow to use their balcony/roofs and so on). ▷ There is an online board through which the CN manages projects (for instance: to create web applications)
Italy 2	▷ The CN was created in 2007 ▷ It became an association in 2011 ("associazione non riconosciuta" under the Italian legal system) ▷ In 2015 it applied to become an ISP but it has not had any answer yet. ▷ The services are managed by the representatives of the association. ▷ The representatives of the association also choose what services to provide and how. ▷ The general assembly was asked more than once to express their needs, but they never did.

Table 2.1: Organisation

France 1	▷ CN provides its subscribers with an access to the Internet through ADSL/VDSL.
	▷ They have access to the following services:
	  ▷ Mail
	  ▷ Domain name, hosting
	  ▷ Bittorent tracker
	  ▷ Virtual machine
	  ▷ VPN
	  ▷ Also, any user may use an ”open bar” VPN, which is not logging any information about users
	▷ Subscribers must pay around 30 euro per month.

France 2	▷ CN provides its subscribers with an access to the Internet through ADSL/VDSL.
	▷ They have access to the following services:
	  ▷ Mail
	  ▷ Domain name, hosting
	  ▷ Bittorent tracker
	  ▷ Virtual machine
	  ▷ VPN
	  ▷ Also, any user may use an ”open bar” VPN, which is not logging any information about users
	▷ Subscribers must pay around 30 euro per month.

Italy 1	▷ There is no payment ▷ The network is open; when someone connects to it, usually it introduces him/herself to the other community members. ▷ The CN is connected to the Internet because some users share their personal Internet connection. ▷ No services are offered against payment; any member can offer his/her own services: for instance some allow storing information of other users on their servers. There is a cloud server, but only for internal use.

Italy 2	▷ Access to the network is reserved only to those who are part of the association
	▷ Each associate gives an annual contribution (around 100 euros) to be part of the association.
	▷ To be part of the CN, a person has to be member of the association.
	▷ They offer internet connection, as they buy fiber; currently fiber to the cabinet – 160 mb (trying to have fiber to the home)
	▷ They offer some other services, including:
	  ▷ e-mail;
	  ▷ hosting;
	  ▷ cloud services;
	  ▷ game server;
	  ▷ some cameras that record the landscape and publicly displays the weather and the panorama in a website (publicly accessible).
	  ▷ an sms service for other associations (associations that are members of the CN): through this system, the representatives of the association has its own user profile and can send sms to any associate who subscribed to the service.

Table 2.2: Services offered

France 1	▷ Subscribers must become members of the CN association in order to access the services. This is done through a contract which describes that personal data are processed (but not really how or for what purpose)
France 2	▷ Subscribers must become members of the CN association in order to access the services. This is done through a contract which describes that personal data are processed (but not really how or for what purpose)
Italy 1	▷ There are no limitations on the admission of people ▷ Those who want to join must agree to the pico-peering agreement. ▷ There is no distinction between users and members. When someone connects to the network it agrees to have her data collected (see below).
Italy 2	▷ Those who enter the association have to sign a form with the Terms of Services (ToS). ▷ The ToS warn users that they are responsible for what happens using their login/password; that they bear the civil and criminal liability for wrongdoing committed by themselves or someone else using their login/password. ▷ Users also commit themselves not to use p2p software, in order not to impair shared resources (detected and stopped through a "next generation firewall" - NGF) ▷ The ToS also forbid some other possible uses of the network by its users.

Table 2.3: Relationship with users

France 1	▷ CN collects and stores users name, postal and email addresses, phone number, IBAN. Members may access these info and change them on a personal page of CN website ▷ These information are associated with the IP address allocated to the user. ▷ CN gives users' address and phone number to other operator for interconnection matters (ex: Orange needs to know which line CN will use in order to give it access). However, CN fails to specifically inform users about such transfer. ▷ CN monitors how some of their services are used: if some is downloading a lot of data for a long time through VPN, a system administrator will usually detect it and try to ask this users (through is email) to stop. ▷ Personal data are also used for billing and anonymized statistics. ▷ Only a limited part of CN board members may access users' personal data. Each individual access is not logged.
France 2	▷ CN collects and stores users name, postal and email addresses, phone number, IBAN. Users do not have the power to modify personally this data. ▷ These information are associated with the IP address allocated to the user. ▷ CN gives users' address and phone number to other operator for interconnection matters (ex: Orange needs to know which line CN will use in order to give it access). However, CN fails to specifically inform users about such transfer. ▷ CN monitors how some of their services are used: if some is downloading a lot of data for a long time through VPN, a system administrator will usually detect it and try to ask this users (through is email) to stop. ▷ The bandwidth consumption of each user is logged: how much was used during each hour of the last day; during each day of the last month; during each month of the last year. ▷ This information is displayed on users personal page and system administrators may access it for debugging and monitoring. ▷ Personal data are also used for billing and anonymized stats ▷ Only a limited part of CN board members may access users' personal data. Each individual access is not logged.
Italy 1	▷ There is no real collection of data; who connects is not given any specific information. They must register their IP, however, or the network does not work (they cannot connect to the CN). ▷ There is a map server, publicly available on the website of the CN. On the map server one can see the nodes and each node has information attached (for instance IP addresses). ▷ Information is not necessarily real, but at least a valid e-mail address must exist. ▷ IP are not public; the internal network has a double addressing. There is a Wki with the ipv4. When a node is on it is possible to build a list of active node. ▷ Given that private and public addressed must be unique, the CN registers them there. ▷ Internal IP are always the same. They can be found on the website of the CN. ▷ No logs are saved.
Italy 2	▷ The Tos includes an informed consent to be signed by each member. ▷ A database includes members' personal information: name, surname, date of birth, tax code, home address and a copy of their identification document. The information is given by each member at the time of entering the association. ▷ Information can be updated at least every year when the annual association quota is paid. ▷ They collect this information only for maintenance reasons. ▷ They do have a map of the nodes but it is not public, it is used only internally by the administrators/representatives of the association/CN. ▷ Users can modify their information; each year they are asked to check whether their information is correct or must be updated. ▷ The CN applies a technical monitoring: for instance to understand how much band is used. ▷ The CN uses a "next generation firewall" (NGF), to detect and to stop the use of p2p.

Table 2.4: Processed data

France 1	▷ For Internet access and VPN, for the duration of the contract : name, addresses, IP addresses, phone number + for 1 year time of start and end of the connection ▷ For email, for 1 year, information logged by default by the software used on the email server: ▷ users' login ▷ email addresses of sender and receiver ▷ message size ▷ IP and time from where the user's box was accessed ▷ IP and time from where the user send the message ▷ For web hosting, for 1 year, information logged by default by the server software (Apache): ▷ IP address of each person accessing a page + which page is accessed, when ▷ For bittorent tracker for 1 year: login of the user uploading a .torrent file
France 2	▷ For Internet access and VPN, for the duration of the contract : name, addresses, IP addresses, phone number + for 1 year time of start and end of the connection ▷ For email, for 1 year, information logged by default by the software used on the email server: ▷ users' login ▷ email addresses of sender and receiver ▷ message size ▷ IP and time from where the user's box was accessed ▷ IP and time from where the user send the message ▷ For web hosting, for 1 year, information logged by default by the server software (Apache): ▷ IP address of each person accessing a page + which page is accessed, when
Italy 1	▷ Technical information is kept for technical reasons (maintenance). ▷ Only IP are stored, together with what is it written in the website of the CN (including home addresses) ▷ Except for the table including IP addresses, no other information is collected. There is only information on the node, to which an e-mail address is linked. The map servers is managed by 2 or 3 people from the CN. ▷ Only those 2 or 3 people can access and modify data. ▷ Only if users give their data and consent to their publication, this data is public. ▷ There is a mailing list and e-mail are retained. ▷ E-mail addresses are stored, but personal information do not need to be added. ▷ Only the addresses of the nodes are kept, to build the map of the network. ▷ This data is saved on servers owned by some users of the CN.
Italy 2	▷ The CN stores the internal IP connections (some IP are static, some dynamic) towards the Internet: logs: door, protocol, date and time. ▷ Personal information and technical information are kept on two different servers. ▷ Users' personal data are on a server which is located within the premises of the association; the premises are locked with a key. These servers are not connected to the Internet. Any information is backed-up daily. ▷ Personal data are kept to know who is member of the association; log and other technical information are kept for security reasons. ▷ They record any access to a service, but not its length. ▷ They store IP addresses and logs because they believe there are data retention obligations (decreto Pisanu); for no more than 6 months in case the police came.

Table 2.5: Data retention

2.2.2. Analysis of the interviews

The answers summarized in the table allow drawing some preliminary conclusions, although limited from the point of view of geographical distribution.

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 "CN Italy 2", 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 and criminal 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.

CN Italy 2 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.

In the case of "CN Italy 1" 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.

As for **data protection**, "CN France 1", "CN France 2" and "CN Italy 2" 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 CN Italy 2, 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 cloud service.

The French CNs collect and **retain personal data** for billing purposes. In the case of "CN Italy 2" data is also retained as a database of the association. Users can modify their data: for instance in "CN Italy 2" 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, the French CNs as well as "CN Italy 2" 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 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.

2.2.3. Design and Running of the Survey

Based on the interviews conducted in the first months of 2017, an online questionnaire was designed (Annex 1) and created through "Limesurvey". The tool was chosen as it allows anonymization (for more details on ethical assessments, consider D8.1 Ethics Requirements, in particular Sec. 2.1.5).

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

The main sections concerned:

- *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;
- *organization 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 relays and in terms of relays 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 focussed 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;
- *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 the Court of Justice of the EU asked for[33].

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 will 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 has ever benefited from legal advice (either by a lawyer or a legal researcher) and if so, how often it has 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 was opened at the end of August and run until the mid of October. It was advertised via e-mail to all the known CNs in Europe. The responses obtained come from 5 countries; the interviews covered also another country, for a total of 6 different countries.

Each CN is assigned a pseudonym (France 3, Germany 1 and so on) in order to allow the analysis of the responses. Although a table summarizing the correspondence between "real names" and pseudonyms is kept by the researchers, it is not published here to avoid spreading information about CNs that might be sensitive.

2.2.4. Information Collected through the Survey

This paragraph **summarizes the responses obtained through the survey**. As already done with the face-to-face interviews, to improve readability the information collected is summarized in tables[34]; a detailed description of the responses follow. The specific questions made are reported in Appendix A. Tables in Sec. 2.2.4.1 are split in Part A (France 3, France 4, Germany 1, Germany 2, and Portugal 1) Part B (Slovenia 1, France 5, Germany 3, Germany 4, and Greece 1) for readability; in one case the split is in three parts.

[33] See above Sec. 2.1.4.

[34] The numbers used to create the pseudonyms for the CNs that responded to the survey are in progress with those used for the CNs that were interviewed face-to-face, as the survey was not submitted to those CNs whose members were already interviewed.

2.2.4.1. Tables summarizing the results of the survey

France 3	▷ organised as an association that acts as central entity through employees or members ▷ wireless relays are owned and managed by the association ▷ the CN has a form of insurance by an insurance company
France 4	▷ there is no central entity ▷ decisions are taken through a collective and horizontal process or independently by each participant ▷ the CN is also a non-profit ISP
Germany 1	▷ there is no legal nor central entity ▷ decisions are taken through a collective and two meetings per week; some decisions are made in IRC or on our mailing-list; important/bigger decisions require plenary sessions ▷ relays are usually owned by single individual; some relays where funded by the municipality or belong to a local association ▷ technically relays are managed by single participants ▷ users who provide services through the CN subscribe the pico-peering agreement; they can not advertise 'free WiFi' without mentioning the name of the CN; Commercial installations need plenary approval ▷ they have a few times benefited from the advice of a lawyer/researcher
Germany 2	▷ the CN is a registered association ▷ it provides a central infrastructure, but every user can extend the network on their own ▷ the central entity takes care of making services offered by users reachable ▷ decisions are taken by participants, through discussions at regular meetings but the central entity provides guidelines for compatibility reasons ▷ relays are owned by single participants but some are managed by the central entity
Portugal 1	▷ there is no legal entity, but there is a central entity ▷ the name of the CN is registered as a trademark but no association nor foundation exist ▷ services are provided by external participants, not acting on behalf of the central entity ▷ the CN manages and implements the network for the community as per participation agreement ▷ through a collective and horizontal process it was decided that decisions are taken by the central entity due to the lack of participation, decisions are made by the central entity based on user and participant feedback ▷ decisions are taken by amount of requests by the participants and or members, the need vs usage and the resources available and possibility of implementation. ▷ by default the central entity is open to implement new services if they meet the participation agreement requirements; participants are free to implement their services if no harm is caused to the network ▷ the central entity defines the technical implementation unless the individual participants have been delegated to take care of such tasks and have enough knowledge to carry on while still maintaining their participation within the user/participant agreement ▷ the participant 'level' determines higher weight in decision making by the central entity and usage privileges ▷ they have never benefited from the advice of a lawyer, but they have been looking for a pro-bono lawyers for the case it would be needed

Table 2.6: Organization of CNs – Part A

Slovenia 1	▷ no legal entity nor central entity ▷ decisions are taken based on discussions among participants ▷ relays are owned by each participant that technically manage the relays ▷ they have a few times benefitted from the advice of a lawyer/researcher
France 5	▷ the CN is a cooperative ▷ there is a central entity (the CN acts through the employees or members of this entity) ▷ users have to be members of the cooperative to access the services, except for the few free-access points ▷ the CN has a form of insurance by an insurance company for liability ▷ relays are usually provided by the CN
Germany 3	▷ the CN is a registered association ▷ the association is registered as ISP ▷ the central entity provides services to the users: all traffic between the community network and the internet is routed via servers provided by this entity ▷ relays are owned by users, but are technically managed by the central entity
Germany 4	▷ they are part of a larger project and run the autonomous system 6766 in its name, which they use for network traffic exiting towards the internet ▷ the services are provided by a central entity ▷ each participant owns and manages their own relays
Greece 1	▷ the CN has a legal entity that is responsible for policy drafting, administration of the network and orchestration of all activities of the community, while at the same time represents legally the community to 3rd parties. ▷ Decisions are made using a mixture of collective and individual processes. For example: decisions that relate to the expansion of the access network in a village can be taken in a local level, by local actors. In this case, the technical team of the CN acts as support. Decisions that relate to the overall operation / expansion of the backbone are taken by CN via participatory decision-making in assemblies. ▷ no individual participants provide services for the time being. The use of the network is open for everyone. ▷ they do benefit from legal advice as one member of the CN is a technology lawyer ▷ the CN owns and manages the relays

Table 2.7: Organization of CNs – Part B

France 3	▷ Internet access through WiFi to anyone ▷ no fees or other payments ▷ provides VPN, free of charge
France 4	▷ provides access through WiFi and cable ▷ offers VPN ▷ access to the network is provided against payment ▷ services are offered on a geographical base ▷ the CN also provides these local services: e-mail; chat; VoIP; VPN; DNS; Torrent tracker; mailing-list; tor node. These services are now provided free of charge but the CN plans to introduce fees
Germany 1	▷ provides access to the Internet through WiFi ▷ provides also the following services: email (for activists actively participating in the group); VPN; DNS; mailing-list; XMPP; cloud space (20 GB through Seafile)
Germany 2	▷ provides access to the Internet through WiFi ▷ provides also a mailing-list
Portugal 1	▷ provides access to the internet through WiFi ▷ provides also the following services free of charge: e-mail; chat; VoIP; VPN; DNS; mailing-list; Tor node; VPS–x86_64 machines & raspberry-pi

Table 2.8: Services offered by CNs – Part A

Slovenia 1	▷ provides access to the internet through Wi-Fi ▷ no other services are provided
France 5	▷ provides internet access both through cable and Wi-Fi ▷ usually services are offered against payment–some free Wi-Fi points exist in critical places ▷ no other services are offered
Germany 3	▷ provides access to the internet through Wi-Fi ▷ no other services are provided
Germany 4	▷ provides access to the internet through Wi-Fi and cable, via VPN ▷ also provides the following services: e-mail (for core members of the CN); VPN
Greece 1	▷ those who connect to the network can do it for free, but for sustainability reasons they require from the node owners (i.e., those who host active equipment in their premises) to contribute a specific yearly subscription as a donation to the NPO (currently 60 euros/yr) ▷ Wi-Fi access to the network is provided openly to everyone, and everyone can be, as node owner, part of the community, which as a whole shares resources and effort ▷ the CN is connected to the internet through a partnership with a local university, which wants to give back unused resources to local communities ▷ provides the following additional services: VoIP–Available to all: for receiving calls on a dedicated phone number it requires subscription to a 3rd party collaborating VoIP provider; VPN: available to a restricted group of network admins; considering the installation of webcams (modality and revenue model not yet clarified)

Table 2.9: Services offered by CNs – Part B

France 3	▷ no contract is signed or accepted by users ▷ no need to pay to be part of the CN ▷ they do not know whether users install anonymity software ▷ users are informed through the website of the CNs of the nature and purpose of data they collect. They are informed of their rights with regard to personal data protection laws in the country where the CN operates
France 4	▷ no contract is signed or accepted by users ▷ users use Tor & encryption; the CN does not log its services ▷ it has occurred that foreign police asked the CN to cooperate and give the IP addresses of some users (for copyright infringement) but the CN does not cooperate with non-French juridical process ▷ they have an agreement with users; the agreement includes the following rules: fair use of the resources not to compromise the network; do not circulate illegal content
Germany 1	▷ no contract is signed or accepted by users ▷ they do not know whether users use anonymity software, as users are connected to the internet through gateways and not directly
Germany 2	▷ no contract is signed or accepted by users ▷ users apply VPNs ▷ there was one case of copyright infringement
Portugal 1	▷ users have to sign the project user/participant agreement, based on pico-peering ▷ 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 degree of participant level also determines higher weight in decision making by the central entity and usage privileges; for example, a participant who donates an internet gateway or contributes with donations has more privileges, voice and assurance of service than regular user in case resources run out for everyone else or the network is too loaded ▷ a small percentage of users uses cryptography although the central entity encourages users and participants to be anonymous and use end to end cryptography at all times.

Table 2.10: Relationship of the CNs with users – Part A

Slovenia 1	▷ no contract is signed or accepted by users ▷ they do not provide any information to users, they can just connect and use the network
France 5	▷ users have to be members of the cooperative to access the services, except for the few free-access points ▷ they do not know whether users apply anonymity software as they do not monitor users. Every (paying) users is a member, has vote right, and may act on the network to keep it running (less than 10% of them do)
Germany 3	▷ no contract is signed or accepted by users ▷ users do not use anonymity software
Germany 4	▷ no contract is signed or accepted by users ▷ users do not use anonymity software
Greece 1	▷ no contract is signed or accepted by users ▷ as far as they know, users do not use anonymity software

Table 2.11: Relationship of the CNs with users – Part B

France 3	▷ no personal data is collected from users ▷ keep a log of assigned IP addresses for VPN but not for WiFi ▷ to comply with law enforcement requests the CN collects MAC addresses (WiFi) and source IP addresses (VPN), Wi-Fi and VPN start time and duration; logs are associated with the location (WiFi) of the access point through which the service was accessed (postal address) or with the gateway (VPN) through which the session was set up ▷ WiFi sessions information (MAC address, date and duration, identity of access point) are associated ▷ VPN session information (Source IP address, date and duration, assigned IP addresses, identity of the gateway) are associated ▷ do not log any information related to recipients, content or service accessed ▷ users are informed through the website of the CN of the nature and purpose of data they collect. They are informed of their rights with regard to personal data protection laws in the country where the CN operates ▷ users can access their personal data and ask for erasure/update via postal mail
France 4	▷ process name, postal and email addresses as well as IP address, user/password to services ▷ for some users IBAN (bank account information) is collected ▷ IP addresses are associated with user account in configuration file ADSL user/pass is associated to user name ▷ users can ask for modification or deletion of their personal data via e-mail, post, or phone
Germany 1	▷ email addresses and nicknames of WiFi relay owners are collected in order to contact them in case of important updates ▷ MAC addresses of WiFi relays are collected in order to provide and maintain access to the gateways ▷ MAC addresses of users are collected temporary in order to provide IP addresses ▷ IP addresses ▷ email, in case they want one ▷ xmpp handle, in case they registered for the service ▷ MAC address of Wi-Fi relays, permanent ▷ MAC address of users, temporary ▷ DHCP Operations ▷ relay ID as long as the user is online, otherwise routing becomes hard. there is no onion routing in our mesh network ▷ the CN monitors number of users per WiFi relay and bandwidth per WiFi relay; statistics are accessible through the CN website
Germany 2	▷ e-mail addresses are stored if user register for the mailing-list ▷ for operating a relay, the location of the relay and mail address of the operator are optional, each relay holds MAC addresses to provide access to the network ▷ for statistical reasons some data is collected centrally if the relay operator wishes to, these are: number of users per relay, used traffic per relay, system load, number of network connections; data that have been assigned by the CN to users (Examples: IP address, phone number, user ID) ▷ static IP addresses for relays are managed via a public wiki ▷ dynamic IP addresses and mac addresses are used by the relays while users are connected ▷ locations of relays are public ▷ what data is collected and which is not is documented in a public wiki ▷ users can ask for the erasure, access or modification of their data via e-mail; personal data in the public wiki can be edited by the user himself ▷ no data is collected from users; data from relay operators can be given optionally

Table 2.12: Data Processed by CNs – Part A

Portugal 1	▷ only name and email or telephone are required (to be provided) or any other method of functional contact for node owner, hardware owners and resource providers due to technical administration reasons ▷ no personal information is collected from the users, it has never been and there are no plans to change ▷ routers send daily logs (if any) about their functioning which may include MAC addresses; all this information is used for statistics, troubleshooting, software development, region survey and access management depending on the case and or situation; this does not include access logs about the users online activity; no user activity logs are collected ▷ IP address may be assigned to specific users and hardware for the following reasons and typically upon user request: to establish manual network routing paths and gateway exit nodes; network servers; IP cameras; hardware that needs a fixed address in order to be found; troubleshooting ▷ as for user ID, the closest that is done, is that upon voluntary user forum registration, if known, the user account is inserted into the user's matching usage group or region in order to facilitate contact and news update to that same group and or region ▷ by default, DHCP operations are reset every time the nodes reboot; routers may send logs daily if they were used and those logs may contain DHCP operations for the time period before the next reboot; reboots are at least 1 time a day; leases are for 24h hours; logs are sent before the reboot and may contain DHCP information; these default settings may be changed by the local mesh administrator and be done as per local need and purpose ▷ a map is created and updated if the participants contact the central entity and let the central entity know the location of the nodes; this is optional and the nodes firmware do not do it automatically; the central entity has no way to know about the location of all the nodes ▷ no email address and phone number of recipients; URLs of accessed websites are collected or are able to be collected ▷ no banking information is required; services like Paypal are preferred and participants are free to choose how they prefer to deal with financial transactions if there is the need ▷ users are informed that nothing is disclosed to third party operators; this information is provided by Wiki documentation and the agreement/usage policy, and distributed in person, through the forum mailing list, chat rooms and social media channels created for such tasks ▷ to access their personal data and ask for modification, the CN website provides direct contact with central entity and local mesh administrators and additionally, the forum, chat rooms and official social media channels; there is also a direct phone number available to the main administration for node owners to send text ▷ personal data such as email and name or phone number is only made available to local mesh administrators and central entity; DHCP operations and MAC address that may be collected by node logs are firmware default settings which upon being activated, sent to the firmware developer only; local mesh administrator can decide where those logs are sent for its own local mesh and if shared which central entity firmware development; each local mesh administrator is voluntary responsible for the management of the local mesh
Slovenia 1	▷ store hashed MAC addresses to compute statistics of use through time ▷ store only that somebody got a DHCP lease and how long the lease was in effect ▷ store that somebody used each relay, for statistics and to monitor the network ▷ collect data such as contact information, location and technical characteristics of users' relay in the centralized database, to help coordinate the network, but it is not required for an individual to participate in the network, they can have a relay even if they do not register information about their relay in the database ▷ they do not collect anything they think is personal data about users, and in case they collect data they not know which data they collected is by which user

Table 2.13: Data Processed by CNs – Part B

France 5	▷ for members with access, they collect name, address, phone number, email and bank account number; they associate name with delivered IP addresses; for free WiFi users, they collect MAC address and timestamp of connection ▷ a user id and one or more IP ▷ they know relating to the characteristics of the device as they provide the devices; for free WiFi users collect the MAC address ▷ IBAN for members only ▷ don't disclose any data to a third party except a summarized information (global and city by city counters of members, device up & down, . . .) ▷ monitor bandwidth on every link (wired and wireless) and up & down devices of the whole network ▷ about what data is collected, the CN has a transparent policy published on our wiki, on the website ▷ users have a full access (read & write) on their data (personal account on a website)
Germany 3	▷ do not collect any user data ▷ name & postal address for people who buy a device from the CN ▷ MAC address, IP address, in order to technically run the IP network ▷ they operate a central DHCP server with logging disabled ▷ as for the location of the relays the network has two segments; while a device is online it is possible to see in which segment it is ▷ the network does not encrypt anything. Everything is transferred as clear text; it is the users responsibility to use encrypted connections ▷ they know which node has which hardware ▷ they use VPN gateways to access geo-blocked content
Germany 4	▷ end users: temporarily MAC address to assign DHCP lease ▷ node operators: router primary MAC address, sometimes email, when participants send in VPN public keys ▷ IPv4 address via DHCP; IPv6 address via SLAAC ▷ geodata set in access points and mesh routing information for each client can be correlated during usage ▷ contact information configured by participant in his/her router; location configured by participant in his/her router (routers advertise their technical characteristics throughout the mesh when asked)
Greece 1	▷ do not collect personal data ▷ node owners' data is stored in the controller data base (no 'regular users' data is collected) ▷ IP address, user ID and subnet sets for node owners, for the needs of network maintenance and usage analysis ▷ MAC address for the needs of network maintenance and usage analysis ▷ access network controller logs the users' access to the CN ▷ MAC addresses are logged in the access network controller level ▷ MAC addresses are associated with IP addresses in a central database; user ID is kept in separate database ▷ do not transfer data outside EU; they used to use unifi cloud controller but not anymore; now use local hosted unifi controller, although for the old openmesh devices the cloudtrax controller is hosted in openmesh cloud service ▷ CN is monitoring only users' usage of the network statistics for all offered services, in order to perform impact measurement and to update the CN social business plan's KPIs ▷ users are informed about the data that is collected and the use of this data; this information is given through the splash page of the network ▷ data are only accessible by network administrators who access them though ssh and https only

Table 2.14: Data Processed by CNs – Part C

France 3	▷ information related to WiFi and VPN sessions are never disclosed to third parties unless lawfully requested by law enforcement ▷ no information related to recipients, content or service accessed is kept ▷ data are retained and used only to fulfil legal obligations ▷ data are stored on servers located in CN premises ▷ only the legal representative of the association/CN has access to the data and the access is tracked through standard operating system logs
France 4	▷ IP addresses are associated with user account in configuration file ADSL user/pass is associated to user name ▷ data are processed through Dolibarr[35] ▷ data can be accessed only by a limited number of individuals and each access is logged ▷ infrastructure is kept up-to-date in terms of security ▷ data are kept to fulfil legal obligations (national laws on users' connection) ▷ the CN does not transfer data outside EU in principle, but users are free to use their VPN where they want, hence data might be transferred outside EU
Germany 1	▷ nickname, email and WiFi relay position are in one database. ▷ in some specific cases, data are transferred overseas ▷ the CN does not retain data to comply with the law
Germany 2	▷ data of relay operators is not anonymised if provided ▷ data of users is not collected ▷ personal data are kept on Server operated by the CN in the country where it operates ▷ data that is not public can only be accessed by a limited number of individuals ▷ the CN does not retain data to comply with the law
Portugal 1	▷ nodes that are gateways are associated with DHCP operations and MAC addresses given the fact they they take care of the routing and are exit nodes to the Internet; there is no way to know who owns which MAC address and/or IP unless the user of such MAC or IP requests specific setup or is given a specific route and gateway due to technical reasons ▷ no data is disclosed to third party operators for interconnection matters ▷ node functioning logs are only accessed by the central entity if troubleshooting needs arise; aside from possible MAC addresses and DHCP operations logs, no personal data is stored ▷ the CN does not retain data to comply with the law

Table 2.15: Data Retention Policy of CNs – Part A

Slovenia 1	▷ information about relays and who is managing them is kept together, then for each relay there is information about its use, which is kept together in the same database about relays ▷ they provide all data collected publicly ▷ data is kept on one server, in a PostgreSQL[36] database ▷ the CN does not retain data to comply with the law
France 5	▷ they store data to comply with national law: association between names & IP addresses for one year ▷ data is stored on two servers accessible only by elected board directors ▷ they said they may disclose information upon legal request, but they did not have to, so far
Germany 3	▷ they do not collect data, hence they do not retain data
Germany 4	▷ no information of the one collected is kept ▷ the CN does not retain data to comply with the law
Greece 1	▷ they retain data in order to comply with the law: through the controller they gather some data like MAC addresses that are accessing the network, but they don't authenticate each user who uses our network nor do they identify mac addresses to users ▷ the CN is retaining MAC addresses of devices used to access the network, for 2 years maximum. ▷ data is automatically stored in the database of the network monitoring tools, on an hourly basis

Table 2.16: Data Retention Policy of CNs – Part B

2.2.5. Analysis of the survey results

The analysis of the responses aims at understanding how CNs actually deal with laws on civil liability and on personal data protection. Following the structure of the survey, the present analysis first investigates civil liability and later personal data protection.

2.2.5.1. Organization

From the point of view of **organization**, the slight majority of the respondents CNs do not have a legal status. Although in many cases decisions are nonetheless taken at a central level, implying a sort of central organization, there is no formal entity nor any legal status. 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".

As for the other CNs, which instead are legal entities, they usually are associations, as only one of the respondents is organized as a cooperative.

The formal organization of a CN also dictates what rules should apply in case of a civil wrongdoing. In fact, as it has been explained above, **civil liability is governed by national laws**.

At the same time, **some respondents qualified themselves as ISP or IAP**. These CNs (CN France 4 and CN Germany 3) probably asked and obtained an authorization by their National Registration Agency. This implies that the above summarized rules on providers' liability are to be taken into account for these CNs.

Two of the respondents have declared that their CN is **insured by an insurance company for the case of liability**. Both CNs are French. This choice might be the outcome of the liability rules existing in France. As seen, the regime introduced by HADOPI law is quite restrictive and imposes a third-party liability for the case someone else infringes copyright through a non-secured (i.e., non-password-protected) network. This is probably one of the reasons that led these two CNs to the decision of insure themselves.

CNs were also asked if and to what extent their network is **decentralized**; the questions inquired the ownership and the management of the relays as well as about the process of decision-making. As for the property, there is no general trend. Relays can be owned and managed by the CN or by the users; in some cases the CN owns all the relays but lets users manage them, in other cases the opposite is true. It is interesting to notice that whenever the CN manages the relays (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.

Irrespective of the ownership of the relays, it is fascinating 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 members' participation in the CN life and are an **indicator of distribution of power and commons-based governance**.

2.2.5.2. Services Offered

All of the surveyed CNs offer Internet **Wi-Fi connectivity**; some of them do also offer **cable connectivity** in addition to the wireless. What is interesting to note is that **only very few CNs ask their members to pay a fee**: CN France 4 and CN France 5.

In one instance (CN France 4) this goes hand in hand with the qualification of the CN as an ISP, more precisely a non-profit ISP. The CN also offers a number of other services (for instance: e-mails, chat, VoIP, Tor nodes);

currently it offers these services for free but it declared that they plan to introduce fees.

On the contrary, CN France 5 did not qualify itself as an ISP or an IAP; however, it is a cooperative. These characteristics are probably linked to one another.

CN France 5, CN Germany 3 and CN Slovenia 1 are the only respondents that offer only Internet connectivity. The other surveyed CNs offer at least another service (for instance CN France 3 offers VPN; CN Germany 2 offers a mailing list) with CN France 4 and CN Portugal 1 being those offering the highest number of services. Regardless of the number of services provided, it is important to consider what services CNs actually offer.

In particular, two services are of special interest in understanding the applicability of the current laws: **Tor and cloud**. **Tor**[37] nodes shield users' identity and constitute a way for them to avoid liability. Indeed, as explained in the footnote, it is completely impossible to understand who is behind the node who committed the wrongdoing.

As for **cloud** services they might create difficulties as for the applicability of data protection laws as cloud implies the storage of information that very often qualifies as personal according to the definitions given by Dir. 95/46/CE and Reg. 679/2016 (GDPR). This issue will be later analysed when dealing with personal data processing and retention.

A final remark shall be made with regard to the method of offering Internet connectivity adopted by CN Greece 1. 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 that once again highlights the remarkable role that CNs can have in enhancing the development of a region or of a country. In addition, it represents a stimulating model that could be replicated elsewhere in the same country or in other European countries.

2.2.5.3. Relationship with Users

Only two out of ten respondents have answered positively to the question "Does your CN enter into a contract or any kind of agreement with each of its users?".

In particular, CN France 5's 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 processing as well as a right to act on the network to keep it up and running (although only a small number of members do).

A different approach is the one of CN Portugal 1: this CN requires users to sign the **"project user/participant agreement" that is based on the pico-peering agreement**. 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[38].

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

[37] Tor, is a strong anonymization P2P network based on *onion routing* and nested cryptographic tunnels that ensure that the origin of the communication cannot be identified even by an "omniscent" attacker, i.e., an attacker who can observe all the traffic in and out of every tor node. See https://www.torproject.org/ for further details.

[38] See D4.1 [1] Sec. 3.1.

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 the CN's website, this might not be enough for an informed consent as required by Dir. 95/46 and especially by Reg. 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.

2.2.5.4. Processed data

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 most lack knowledge of the legal framework and of the corresponding obligations pursuant to European and national laws.

As for processed data, many of the respondents firmly asserted that they **do not collect personal data**; this is the case of CN France 1, CN Portugal 1, CN Germany 3 and CN Greece 1. However, reading the responses they gave to specific questions, almost all of the respondents actually collect and process personal data (some of them also retain data, as described below).

In fact, according to European law personal data is "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 online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Art. 4(1), Reg. 679/2016)[39].

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 be qualified as such according to the case law of the CJEU.

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 gain this qualification because of the processing it undergoes.

As above summarized, in the case *Patrick Breyer v. Bundesrepublik Deutschland*[40] the Court of Justice of the EU clearly stated that IP addresses can be personal data. This statement is not new as previous decision by the same CJEU already clarified this issue. The difference is that this time IP addresses are qualified as personal data as they are linked to an *identifiable* person. 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. Indeed, nine out of ten declared that they collect IP addresses; in two cases (CN France 4 and 5) 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 addresses, WiFi logs, URLs of accessed websites, and so on.

The only CN that seem to handle data in a way that could not be linked to the real identity of uses is CN Slovenia 1. 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". The list of data they collect and store does not include either personal information (name, surname, ...) or IP addresses. The way CN Slovenia 1 describes how it

[39] The definition is close to, but more detailed than, the one given by Dir. 95/46/CE, art. 2, lett. a).
[40] Patrick Breyer v. Bundesrepublik Deutschland (C-582-14) 19 October 2016, cit.

handles data recalls **anonymous data** that is not subject to either Dir. 95/46/CE[41] or Reg. 679/2016[42].

On the contrary, **pseudonymized information** that was not mentioned in Dir. 95/46/CE, is subject to Reg. 679/2016. Art. 4(5) states: "'pseudonymization' means the processing of personal data in such a manner that the personal data 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". This idea is very close to the interpretation given by the CJEU in the case of Patrick Breyer[43] and could be applied to a variety of situations in which CNs **believe** they are not handling personal data or are handing it as pseudonymized data, while this is not the case.

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

As CNs determine the means and purposed of the processing of users' data, they qualify as data controller under art. 4(7) of the GDPR. When the CN is organized as association or cooperative, there is a legal entity and therefore there are no issues 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.

Data controller is a key concept of both the Directive of 1995 and of the GDPR. The GDPR introduces a number of duties for CNs that can be qualified as data controller (art. 4(7), art. 24), the first of which is the **duty to inform data subjects** (in this case, CN's members/users) about their rights as granted by current national laws implementing Dir. 95/46 and by soon-applicable Reg. 679/2016[44].

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 webpage 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 (CN Portugal 1) the CN informs its users through the contract by which users join the network.

The information provided through the webpage 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**, unless the data collected are truly anonymous. Since truly anonymous data are rare, any CN should provide its users/members with information about their rights with regard to their personal data processing.

Art. 13, Reg. 679/2016 list the information that must be provided, among which:

- the identity and the contact details of the controller,
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,
- where applicable, the fact that the controller intends to transfer personal data to a third country or inter-

[41] See Recital n. 26: "[...] whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable".

[42] See Recital n. 26: "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person [...]".

[43] R. Hu, S. Stalla-Bourdillon, M. Yang, V. Schiavo, and V. Sassone, "Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR," in Data Protection and Privacy: The Age of Intelligent Machines, R. Leenes, R. van Brakel, S. Gutwirth, and P. De Hert, Eds. Hart Publishing, 2017.

[44] For a deeper understanding of the duties imposed by GDPR on controllers, see D4.1 [1], Sec. 4.2–4.6

national organization,

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,
- the right to lodge a complaint with a supervisory authority.

While CNs could easily supply users with clear and complete information through their websites/wiki, a more troublesome issue is the one of **data subject's consent**.

Art. 4(11), Reg. 679/2016 describes consent as "any **freely given, specific, informed and unambiguous indication** of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action, signifies agreement** to the processing of personal data relating to him or her". In addition, according to art. 7 "the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data".

This does not mean consent has to be written "on a paper". Recital n. 32 specifies that it can also be given by "ticking a box" in an Internet website. What really matters is that *a)* there is a clear indication of data subject's acceptance of the proposed processing (that is included in the information given to the subject), and *b)* that the data controller –the CN– is able to demonstrate that there was such a consent.

Consent makes the vast majority or processing activities lawful. For instance, a problematic case might be the one of CN Germany 1 that explicitly answered that sometimes **it transfers data overseas**. There are a number of mechanisms that govern the so called "trans-boarder data flow", but the presence of 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 a 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 subject's **informed consent** is the first step to have a legal processing of personal data.

In addition, some CNs' activities could be qualified as ECS and therefore be subject to Dir. 2002/58/CE (soon to be repealed by a new regulation mentioned above, so called ePrivacy Regulation)[45]. Despite the fact that the qualification of CNs' services as ECS is questioned[46], 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.

2.2.5.5. Data retention

The answers given by CNs as for data retention provide a very interesting framework. Except for a CN that stated that as they do not collect personal data, they do not retain personal data (CN Germany 3), the other respondents can be divided into two groups: those who retain data to comply with national law and those who do not.

Interestingly, all French CNs, the Portuguese and the Greece CNs fall into the first category, while all the German CNs and the Slovenian one fall into the second.

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**[47]. Member States introduced these provisions

[45] Proposal for A Regulation of the European Parliament And Of The Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.1.2017, cit.

[46] See what already reported in D4.1 [1], Sec. 2.1.2–2.1.3 and Sec. 4.5.1–4.5.4.

[47] See D4.1 [1], Sec. 4.5.5-4.5.11.

mainly as an implementation of Dir. 2006/24/EC[48]. However, in 2014 the CJEU declared this Directive was invalid as it violated arts. 7 and 8 of the Charter of Fundamental Rights of The European Union granting "Respect for private and family life" and "Protection of personal data"[49].

More recently, in the Tele2 Sverige case (see above Sec. 2.1.4.3) the CJEU decided on the compatibility of national laws requiring data retention on the base of an exception introduced by art. 15 of Dir. 2002/58. The Court once again held that laws asking for a general and indiscriminate retention of traffic data and location data are not compatible with EU law[50].

Besides the fact that these statutes could be declared invalid under EU law, for what our survey is concerned, France requires providers to retain data for one year and providers that do not fulfill these obligations can be fined up to 375,000 €.

On the contrary, Germany does not have a law on data retention (Sec. 2.1.4.3). More precisely, even though such a law exists, it is currently not applied as German courts have declared its invalidity. 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 do not retain all the data requested by the law. For instance, CN France 3 does not retain data related to recipients as French law instead asks[51].

As above illustrated, the issue of data retention is a very thorny one. According to the CJEU's decisions, national laws that do not comply with the requirement dictated by the Court itself could be considered invalid as conflicting with EU law and the Charter of Fundamental Rights. Therefore, where a country has such national statutes (for instance: France) CNs could theoretically be free not to comply with the law. At the same time, given the ambiguity of the situation generated by the decisions of the Court of Justice, it must be stressed that not complying with national law might imply legal risks for CNs.

2.2.5.6. Legal advice

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.

These answers denote the need for CN to have clear guidance in the field of law: as seen and demonstrated in D4.1 [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. For this reason, the guidelines that will follow this deliverable and are due at M30 will be a valuable tool to have an impact on CNs lives.

2.3. Preliminary Guidelines

Starting from the analysis of the answers, some preliminary advice can be given. This can be considered as a first step towards the legal recommendations of the "Best practices guide for CNs" (D4.5 due at M36).

As for the **organization of the community**, a good way to deal with both the issues linked to civil liability and to personal data protection would be to formalize the CN, meaning shaping the CN's organization under a legal

[48] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, cit

[49] CJEU, 8 April 2014, Digital Rights Ireland v. Minister for Communications and others, cit.

[50] CJEU, 21 December 2016, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Cases C-203/15 and C-698/15, cit.

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

form. What form should be adopted (association, foundation, cooperative) largely depends on national law and its requirements, as all options could allow the governance model of choice.

For those CNs that already are formalized, the **adoption of an insurance** seems to be a good compromise. On the one hand, it protects the CN (and/or its possible legal representative if incorporated into an entity) from damages caused to users and to third parties (for instance also linked to personal data protection violations); on the other hand, it prevents the need for the CN to transpose liability onto its members by means of a contract. The fact that two French CNs already have an insurance indicates that insurance companies may have an interest in developing such contracts and a confirmation that such contracts are in fact possible.

As for the services offered, **Tor nodes and cloud services** present the highest risks. Running Tor nodes might implicate that users could never be identifiable also in case of wrongdoing. More in particular, two different interpretations are possible:

- According to a first interpretation, the CN would bear all the costs and damages of a possible action against anonymous users. Buying an insurance could perhaps help also with regard to this issue (depending on the terms of each contract).
- According to a second interpretation, running a Tor relay could be considered as a "mere conduit" activity and therefore shield the CN from liability in light of Dir. 2000/31, art. 12.

It must be hereby noted that tor is a global network, so that even if members of the CN run one or more tor nodes, it is never possible to know where the traffic was generated, so that the liability cause may involve multiple countries, that are however impossible to identify. Liability due to running tor goes way beyond the scope of this Deliverable, and only marginally involve CNs, as anyone can run a tor node on his PC. Only exit point of tor can be back-tracked, as normal relay nodes traffic is completely hidden in the nested onion tunnels.

Running a **cloud service** could imply more responsibility in terms of personal data processing. This is particularly true if data is transferred outside the European Union territory. However, if CNs obtained consent from their users/members almost any issue related to personal data protection could be overcome.

In fact, as above reported, the vast majority of information collected and then stored by CNs is personal data and therefore subject to the GDPR[52]. Hence, CNs have **two main possibilities**:

1. proceed with the anonymization of data[53];
2. collect users' informed consent.

Collecting users' informed consent might not be always easy, especially for the CNs that do not have any formal agreement with their users. However, a simple "registration page" where the contract is displayed and information on data protection is provided could be enough according to Reg. 679/2016[54].

If this was the choice, the provision of art. 7(2), GDPR would be applicable, as it states that "If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding".

Having a "freely given, specific, informed and unambiguous indication" of consent as asked by GDPR would overcome any issue related to data processing, both within EU and outside EU. Moreover, as above explained, given that the definition of and conditions for consent in the upcoming ePrivacy Regulation are the same of those contained in the GDPR, complying with the requirements of the latter would automatically imply complying with the former.

In addition, having a simple contract could help CNs also from the point of view of liability: they could clearly state that some specific behaviors are forbidden and that each users assumes her own responsibilities in case of violation of law – and hence of the contract.

[52] See also [4] p. 27 stating that "Communications data generally are personal data".
[53] On anonymization techniques consider: [14].
[54] Information given shall contain what listed by art. 13, GDPR.

A final remark is needed as for data retention: assuming that CNs qualify as providers of ECSs, they should be more careful in what data they retain and how. There is a legal obligation to retain specific data for a given period and its violation may result in high fines.

Very high fines were also introduced by the GDPR that punishes the violation of some specific obligations with fines up to millions of Euros. Among the provisions generating such high fines there are those related to the conditions of consent.

What just explained lead us to suggest that **an agreement could solve some problems both in terms of distribution of liability and of lawfulness of personal data processing**. An insurance would then further help as for the first of these issues.

2.4. 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, are included in Annex 7.

2.5. Next Steps

The next and final year of research about the European legal framework for CNs will result in two more deliverables: the first one will be an update of D4.1 and D4.2, while the second one will describe legal and other "Best Practices Guide for CNs".

D4.3 will describe the European legal framework at M30: it will constitute an update of the previous deliverable and will include human readable guidelines and codes of conduct.

The three deliverable will be the base on which the legal part of the "Best Practices Guide" will be built. The method to produce this guide will be a Booksprint. A book sprint is a method of creating a book through collaboration where specific techniques endure that a group of experts guided by a facilitator can create a book in a short period of time.

The "Best Practices Guide" aims at drafting guidelines to allow the prosperity and diffusion of CNs; the guidelines, which will include also policy, socio-economic and technical recommendations, are meant as a way to strengthen existing CNs, to support them as sustainable commons, and to encourage the creation of new ones.

3. Upcoming Legislation in the Telecom Sector

As previously explained, the second year of research moved its focus on telecommunications policy from legal analysis to policy and advocacy work. The main reason of this choice was linked to the upcoming reform in this field at the European Union level and its potential crucial effect on the legal sustainability of CNs.

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

The text of the proposal raises many issues concerning CNs and it has therefore been quite harshly criticized.

netCommons has been working at the advocacy level to raise awareness of the difficulties in which CNs would incur if the current text of the proposal was adopted. Advocacy activities with regards to this so-called telecom-package, are reported in D1.5 [2].

The last part of this report focuses instead on the troublesome provisions currently included in the text of the proposal for an EECC and in other EU upcoming directives that might impair CNs development.

3.1. What EU lawmakers could do to foster CNs' development

On September 14, 2016, the European Commission adopted set of initiatives and legislative proposals that will change the regulatory framework for electronic communications in the next few years. As above explained, the proposal for a Directive establishing the "**European Electronic Communications Code**" will **merge four existing Directives on telecommunications**: Framework Directive (2002/21/EC); Authorisation Directive (2002/20/EC): Access Directive (2002/19/EC) and Universal Service Directive (2002/22/EC)[1].

In addition, the EECC will affect **Spectrum Regulation**[2] and could affect **end-to-end encryption** for interpersonal communication, with a clear impact on privacy and personal data protection.

After discussion with European CNs, netCommons decided to initiate the drafting an open letter to EU policy-makers, pushing forward previously drafted "Policy recommendations for sustaining community networks" (see the related blog post - Annex 4)[3].

The letter was drafted in collaboration with several European CNs and advocacy groups and it was intended to offer a collective voice to this growing movement.

The content of the letter covered many important issues highlighting the downsides of the upcoming legislation (Annex 2)[4].

[1] The text of the proposal can be found at https://ec.europa.eu/digital-single-market/en/news/proposed-directive-establishing-european-electronic-communications-code.

[2] Cf. D4.1 [1] Sec. 2.6.4.

[3] http://netcommons.eu/?q=content/letter-eu-policy-makers-making-regulation-work-community-networks

[4] The letter was open for signatures both of CNs and of other supporting organizations during February and March 2017. More than 30

The first issue concerned the introduction or preservation of **unnecessary regulatory and financial burdens**. Existing legislation includes unnecessary regulatory burdens, such as fees or red-tape that are unnecessary or illegitimate when imposed on small non-profit entities. The best solution would be that the EECC harmonized the procedures for declaration fees (first registration) as well as administrative charges (annual fees). With particular attention to non-profit ISPs and small (or micro) businesses the upcoming laws should impose that National Registration Authority (NRA) do not apply any (or only minor) fees or charges.

A second issue linked to the overhaul of telecommunications legislation is **third-party liability when sharing Internet access**[5]. As briefly summarized above, some EU countries' regulation prevent the sharing of Internet connections amongst several users by making people responsible (and potentially liable) for all communication made through their Wi-Fi connection. This is the case for instance of Germany and France. A major successful change could be not only to abolish third-party liability but also to prohibit contractual clauses usually introduced by ISPs that forbid subscribers to share their connection.

In order to give better answers to the need of CNs an important change could be made with regard to **spectrum regulation** and, more precisely, **spectrum commons**[6]. In the current situation WiFi frequency bands are very limited. This implies that they are subject to congestion in densely populated areas. In addition, they are also exposed to new technical standards that use the so-called Industrial, Scientific, Medical (ISM) frequency band (like Long Term Evolution–Unlicenced (LTE-U)) that hamper the reliability of WiFi communications. In addition, existing frequency bands for Wi-Fi (5.6 Ghz and 2.4,Ghz) have physical constraints that prevent them for being used for longer radio links.

The EU lawmaker could intervene to ameliorate this situation with a variety of different actions, among which:

- expand unlicensed Wi-Fi bands;
- make other types of frequencies available on unlicensed schemes (or at least with affordable and flexible authorization schemes);
- include "white spaces" in lower frequencies (which allow for cheap and resilient long-distance links), as well as the 12 Ghz and the 60 Ghz bands (for which radio equipment is affordable and which can help us build high-bandwidth point-to-point radio links).

A further possible intervention that would improve the current state of regulation for CNs is to adopt **open-access rules in telecom infrastructures**. While telecommunications networks were and are built with taxpayers' money, they are treated as something private. Indeed, public authorities often delegates to corporate network operators the management and exploitation of these networks. In addition, network operators often apply aggressive pricing schemes that make it extremely costly for small access providers to interconnect with these networks.

Access to these publicly funded networks should instead be guaranteed at a reasonable and proportionate cost. Such an approach is of utmost importance nowadays as the deployment of optical fibre networks is (re)creating monopolistic conditions on local loops through pricing schemes that preclude small actors from accessing these private networks.

Another key sector in which the EU legislator recently intervened is the one of "**radio equipment**". In 2014, the European Union adopted **Directive 2014/53** on radio equipment[7]. The goals pursued by the Directive are sound policy goals, but at the same time, the Directive can nevertheless impair the development of CNs.

CNs and more than 40 organizations – including for instance EDRi, EFF, Free Software Foundation Europe – supported the letter. On March 16, 2017 the letter was sent to EU institutions, in particular to members of the EU Parliament, national delegations at the Council of EU and to key officials from the EU Commission. To allow a better understanding and a wider diffusion of the letter, it was translated into many European languages. On the same day the letter was sent, there was also a joint press release to give to make the letter spreading widely.

[5] Cf. D4.1 [1] Sec. 3.2.1.

[6] Cf. D4.1 [1] Sec. 2.2.

[7] 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.

Indeed, article 3.3(i) of the said Directive creates legal pressure for manufacturers of radio devices to ensure the compliance of the software loaded on these devices with the European regulatory framework. However, CNs usually need to replace the software included by the manufacturer in radio hardware with free and open source software especially designed to suit their needs. The incentive for manufacturers to lock down their devices and prevent third-party modifications of the hardware is an obstacle for CNs that would instead greatly benefit from a general exception for all free software installed on radio devices by end-users and operators.

As above explained (Sec. 2.1.4), a thorny issue of the EU personal data protection legislation is that of data retention. As the EU lawmaker is about to adopt a **regulation for electronic communications (ePrivacy Regulation)** soon, such text should include clear norms on data retention, following the CJEU's case law. Targeted and limited data retention could help in protecting privacy and confidentiality of communications, two topics that CNs value the most.

Another essential step would be to bring **direct and targeted public support**. Small grants or subsidies could be used by CNs to buy equipment needed to develop new software or to extend their networks so to cover larger territories. CNs have often demonstrated to be capable of reaching the same policy-goals of mainstream operators but at a much smaller cost.

More in general, **EU lawmakers should open the policy debate to CNs** to avoid regulatory capture by big telecom operators. They should be more and better represented in the policy-making process for those subject matters that could affect CNs development.

3.2. The upcoming European Electronic Communications Code

As mentioned before, the EU is going to adopt an Electronic Communications Code very soon.

While a harmonization and an update of the current policy seem more than appropriate, the upcoming Code could greatly hamper CNs development. After sending the letter to the EU policy-makers, netCommons worked more closely on the amendments of the EECC, which were the most crucial for CNs. It published a few notes and voting recommendations for MEPs concerning **five key issues** upon which the EECC touches (Annex 3 - see also the related blog post in Annex 6).

1. **Enhancing data protection**: amongst of the core values of CNs is the protection of privacy and of electronic communications. A way to foster this protection would be to make end-to-end encryption mandatory for interpersonal communication service providers (such as mail and chat). In addition, forcing Member States to adapt to the CJEU's case law on data retention would be another step forward;
2. **Fostering the development of wireless community networks**: as previously mentioned, some EU member states impose liability on operators and on natural person that do not secure their Wi-Fi connection so enabling third-parties to infringe the law (for instance, violating copyright). This liability is a threat to the development of CNs, especially because it creates a distortion in competition. In fact, this regime is not applicable to commercial ISPs that cannot be liable for infringement committed by their users (due to the applicability of Dir. 2000/31/EC on electronic commerce). At the same time, CNs might be subject to the same strict obligations[8]. Some of these obligations are clearly unjustified and disproportionate where imposed on individuals. In addition, commercial ISPs normally include a liability limitation clause in the contract for Internet supply and forbid individuals to share their connection. Therefore, possible measures could include:
    - extend the protective liability regime of Internet access providers to individuals sharing their WiFi connection;
    - prohibit ISPs from charging users in case they want to share their WiFi connection;
    - exclude individuals sharing their WiFi connection from the scope of obligations imposed on professional providers;

[8] On this issue consider the so called "McFadden case": D4.1 [1], Sec. 3.2. See also [15].

3. **Promoting a shared and unlicensed spectrum**: as already mentioned the lack of shared (through flexible authorization schemes) and unlicensed spectrum is an obstacle for deploying community networks. In addition, the duration of rights to use radio spectrum shall be limited and subject to regular review in order to assess the efficiency of the use of spectrum in light of technological and market evolution, and ensure that spectrum policy continues to serve the public interest. Possible intervention could introduce regular reviews of the authorizations granted by NRAs to use radio spectrum;
4. **Creating the appropriate conditions for small Internet access providers**: small providers, such as some CNs, have not enough funding to deploy their own cables. This means that they have to rent access from wired network of big operators in order to provide users with its enhanced services. A small provider may rent two kinds of access: passive and active. Through passive access a provider actually rents physical cables, installs its own equipment on the network and manages every technical aspect of the access provided to users. This process is usually expensive since ISPs have to rent space in each local infrastructure (thousands of euros per month for each) in order to install their equipment. Active means to simply use part of a network already managed by another operator. It does not require to install equipment nor to rent space. It is cheaper and adapted for providing Internet access to fewer users in each location. An important action that could be taken would be to oblige ISPs to grant passive and active access to their networks, both in terms of ADSL and of optical fiber. Such an approach would multiple the possibility for small providers to develop their activities;
5. **Enhancing competition and addressing oligopolistic situations**: in some countries (such as France) only very few operators are deploying optical fibre. Often operators act as monopolists in some specific areas to the detriment of end-users. This is one of the consequences of what above just explained (sub n. 4). Such monopolistic situations and those where "significant market power" exists should be patrolled and regulated in order to enhance competition.

In order to amplify the impact of the letter and, more in general, of the effort made by netCommons to obtain better conditions for CNs, a **workshop at the European Parliament premises was organized**[9]. The workshop, which held October 17, 2017, aimed at:

- contributing to the discussion on the Telecom Package,
- conveying stakes for CNs in less technical terms,
- supporting sustainable commons in telecom infrastructures.

The workshop, that is described in detail in D1.5 [2], involved researchers, Members of the EU parliament, activists, and members of CNs.

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

4. Overall Conclusions

The second year of research demonstrates once again that the European legal framework for CNs is far from being easily understandable by CNs themselves, let alone being easily applicable and appropriate.

The novelties introduced in 2017 as for data protection do not seem to alleviate CNs' obligations. On the contrary, the burdens that the **upcoming ePrivacy Regulation** would introduce are higher of the existing ones. However, the protection of personal data and confidentiality of information is of utmost importance and shall be encouraged. Therefore, CNs should take the appropriate steps to ensure compliance with the upcoming law.

As for **data retention**, the CJUE's case law has deeply affected existing legislation: first, in the Digital Rights Management case the Data Retention Directive 2006/24 was declared invalid; second, in the Tele2 case the CJEU stated what criteria Member States should follow in case they want to implement or keep data retention legislation. As seen, except for Germany, Member States have not complied with the requirement of CJEU's case law yet. This creates confusion and increases difficulties for CNs in applying the law.

The **results of the interviews and of the survey** also indicate the CNs are facing problems in correctly applying the law. In some cases, especially with regard to data protection law, CNs do not have a clear understanding of some of the key concepts of the law. This inevitably leads to wrong application or violation of existing laws.

A possible way to deal with both civil liability and data protection laws is to **enter into contract with the users**. An agreement could distribute liability and could be the basis through which obtain the consent required by EU laws on data protection for users' data processing.

In addition, as for liability, another efficient tool would be to buy an **insurance**, as some French CNs already do, or to pool a commons-based insurance mechanism if no private solution is available. This would shield CNs at least from some cases of liability. For what personal data is concerned, **anonymization** could be of help in respecting the law.

These findings can serve as a starting point for the "Best practises guide for CNs" that will be the outcome of year third and the continuing interactions with the CNs.

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

[3] 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

[4] 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/document.cfm?docid=44103

[5] 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/17-04-24eprivacyen.pdf

[6] Art. 29 Working Party, "Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipment: the example of IPv6," May 30 2002. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp58_en.pdf

[7] 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://www.privacyinternational.org/node/735

[8] Eurojust, "Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15," Nov. 6 2017. http://www.statewatch.org/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf

[9] European Union Agency for Fundamental Rights, "Data retention across the EU," 2017. http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[10] S. Assion, S.-E. Heun, and V. Jenny, "German Traffic Data Retention Law considered invalid by Higher Administrative Court of North Rhine-Westphalia," Jun. 26 2017. https://www.twobirds.com/en/news/articles/2017/germany/german-traffic-data-retention-law-considered-invalid

[11] Garante per la Protezione dei Dati Personali, "Terrorismo: Soro, troppi 6 anni conservazione dati chiamate," Jul. 25 2017. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/6651715

[12] R. Lo Cigno, R. Guidolin, R. Caso, and M. Dulong de Rosnay, "Ethics Requirements," netCommons Deliverable D8.1 (Confidential, Delivered to the EC), May 2017.

[13] R. Hu, S. Stalla-Bourdillon, M. Yang, V. Schiavo, and V. Sassone, "Bridging Policy, Regulation, and Practice? A Techno-Legal Analysis of Three Types of Data in the GDPR," in *Data Protection and Privacy: The Age of Intelligent Machines*, R. Leenes, R. van Brakel, S. Gutwirth, and P. De Hert, Eds. Hart Publishing, 2017. https://ssrn.com/abstract=3034261

[14] Art. 29 Working Party, "Opinion 05/2014 on Anonymisation Techniques," Apr. 10 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216en.pdf

[15] F. Giovanella and M. Dulong de Rosnay, "Community wireless networks, intermediary liability and the

McFadden CJEU case," *Communications Law. Journal of Computer, Media, and Telecommunications law*, vol. 22, no. 1, pp. 11–20, 2017. https://halshs.archives-ouvertes.fr/halshs-01478116

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 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

POLICY RECOMMENDATIONS FOR SUSTAINING COMMUNITY NETWORKS

OPEN LETTER TO EU POLICY-MAKERS
POLICY RECOMMENDATIONS FOR SUSTAINING COMMUNITY NETWORKS

PREAMBLE

We represent European Community Networks, a growing movement of organizations that operate local communication infrastructures, sometimes federated at the regional or national levels. These networks, most of which also provide access to the global Internet, are operated as a commons. That is, rather than being driven by for-profit motives, our key focus is on providing connectivity while striving for democratic governance, social inclusion, education, and human rights with respect to communication technologies.

Our organizations vary considerably in terms of sizes, types of network infrastructures and political cultures. Yet, despite this diversity, we are united by the common objective to build networks that meet the communication needs of humans (rather than those of objects and machines), through networks that are built and run by our communities, for our communities, focused on local empowerment, affordability and resiliency.

Today, we collectively provide broadband connectivity not only to tens of thousands of individual European citizens and residents in rural or urban settings, but also to organizations including small and medium sized companies, schools, healthcare centers, social projects and many more. In many cases, we have out-competed mainstream operators, by providing cheaper and faster Internet connectivity than incumbent players. Thanks to our infrastructures and through our various activities, we foster scientific and engineering experiments, we help local hosting and service providers come together to mutualise investments and share costs, we support digital literacy and data sovereignty through workshops and other educational activities.

Yet, despite our achievements, policy-makers at the national and European levels have so far mostly neglected our existence and specific regulatory needs. Worse, regulation is often hampering our initiatives, making the work of our participants and volunteers harder than it should be. This is why, as you start working on a European code of electronic communications, we decided to contact you and voice our ideas and recommendations regarding the future of the legal and policy framework regulating our activities.

1. Lifting unnecessary regulatory and financial burdens

We first ask you to review the regulatory framework and get rid of unnecessary regulatory burdens, such as fees or red-tape that are unnecessary or illegitimate when imposed on small non-profit entities. 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 1M€, 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. In France, Spain and Germany, it is free, which might explain why the community networkmovement is much more dynamic in these countries. The proposed code for electronic communications aims to harmonize procedures for declaration fees (first registration) as well as administrative charges (annual fees). EU lawmakers must ensure that the fees and charges imposed by national NRAs are null or negligible for non-profit ISPs and reasonable and proportionate for micro and small businesses. Likewise, taxes designed for large corporate firms in the telecom sectors should not apply to smaller, non-profit operators.

2. Getting rid of third-party liability when sharing Internet access
Several laws seek to prevent the sharing of Internet connections amongst several users by making people responsible (and potentially liable) for all communication made through their Wi-Fi connection, and create legal risks for people sharing their connection. In Germany, rights-holders have used a "secondary liability" doctrine to chill the growth of the community networks movement. In France too, copyright law imposes a secondary liability regime that creates significant legal uncertainty for people sharing their network connections with other users. The so-called "mere conduit", inscribed in EU law since 2000 in the directive on information society services, needs to be guaranteed and expanded to small-area wireless access points. In the same spirit, contract clauses that forbid subscribers to share their connections with others should be prohibited. Promoting a right to share Internet connections is all the more vital considering the economic and ecological crises, as well as the rapid increase of populations that cannot afford access to the Internet. In this context, connection sharing can play a critical role in fostering a more equitable and sustainable use of telecommunications infrastructure.

3. Expanding the spectrum commons
It is not just Internet wireless access points that can be shared, but also the intangible infrastructure on which radio signals travel. Wi-Fi, as an unlicensed portion of the spectrum and therefore a commons, is a key asset for community networks willing to set up affordable and flexible last-mile infrastructure. However, these Wi-Fi frequency bands are currently very limited. Not only are they getting increasingly subject to congestion in densely populated areas, they are also exposed to new technical standards that use the so-called ISM frequency band (like LTE-U) that hamper the reliability of Wi-Fi communications. Last but not least, existing frequency bands for Wi-Fi (5,6 Ghz and 2,4 Ghz) have physical constraints that prevent them for being used for longer radio links. In the face of such challenges, a new approach to spectrum policy is needed. Policy-makers should expand unlicensed Wi-Fi bands. Other types of frequencies should also be made available either on an unlicensed (preferred scenario) or, if not possible, based on affordable and flexible authorization schemes. Such frequency bands for instance include so-called white spaces in lower frequencies (which allow for cheap and resilient long-distance links), as well as the 12Ghz and the 60Ghz bands (for which radio equipment is affordable and which can help us build high-bandwidth point-to-point radio links). Once made accessible to community networks, they can help roll-out and expand cheap and resilient wireless infrastructures.

4. Updating open-access rules in telecom infrastructures
Networks built with taxpayers money should also be treated as a commons and, as such, remain free from corporate capture. Today, their management and exploitation is often delegated by public authorities to corporate network operators. These entities usually adopt aggressive pricing schemes designed for incumbent players that make it extremely costly for small access providers to interconnect with these networks. Access to these publicly-funded networks for non-profit entities like community networks as well as small businesses should be guaranteed, at a reasonable and proportionate cost. Similarly,

community networks often cannot have access to the private local infrastructures of incumbent players, despite the fact that these are the only way to connect willing subscribers. Indeed, in many European markets, the deployment of optical fiber networks is (re)creating monopolistic conditions on local loops through pricing schemes which preclude small actors from accessing these private networks. Policy-makers and regulators should ensure that every area is covered by at least one telecom operator with a so-called "bitstream" offer affordable for smaller players.

5. Protecting free software and user freedom in radio equipment
In 2014, the European Union adopted Directive 2014/53 on radio equipment. Although the Directive pursues sound policy goals, it might actually impair the development of community networks. Indeed, community networks usually need to replace the software included by the manufacturer in radio hardware with free and open source software especially designed to suit their needs, a collective process that improves security and encourages the recycling of hardware, among other benefits. Article 3.3(i) of the said Directive creates legal pressure for manufacturers of radio devices to ensure the compliance of the software loaded on these devices with the European regulatory framework. As a result, there is a strong incentive for manufacturers to lock down their devices and prevent third-party modifications of the hardware. We therefore ask policy-makers to provide a general exception for all free software installed on radio devices by end-users and operators (the latter being liable if their software lead to violations of the regulatory framework), so that users' rights are safeguarded.

6. Abrogating blanket data retention obligations
Community networks strive to safeguard human rights in communication networks, and in particular the right to privacy and the confidentiality of communication. While we welcome recent rulings by the Court of Justice of the European Union holding that indiscriminate retention of metadata violates the Charter of Fundamental Rights, we are concerned about several member states' willingness to circumvent these rulings to protect capabilities for indiscriminate surveillance. As EU lawmakers start discussing the overhaul of the ePrivacy Directive, we call on them to oppose any blanket data retention obligations and close existing loopholes in EU law to ensure that only targeted and limited retention obligations can be imposed on hosting and access providers.

7. Bringing direct and targeted public support
Countless other policy initiatives can help support community networks and the significant associated benefits they bring. Such policies include small grants, crowd-funding and subsidies to help our groups buy servers and radio equipment, communicate around their initiative, giving them access to public infrastructures (for instance, the roof of a public building to install an antenna), but also to support their research on radio transmission, routing methods, software or encryption. As many local authorities have found, supporting community networks is a sound policy option. As EU lawmakers move forward on the WiFi4EU initiative, we would like to remind you that we have pioneered various models for the provision of free public access points. We believe that public money invested in this initiative should primarily go to groups pursuing a bottom-up logic, seeding local groups that can foster the empowerment and cohesion of local communities, nurture competition, and meet the same policy-objectives at a fraction of the cost that would be charged by mainstream telecom operators.

8. Opening the policy-making process to Community Networks

Although we have often partnered with municipalities and local public authorities, we ask that national and European regulators pay more attention to our activities when drafting regulation. Community networks have both the expertise and legitimacy to take an integral part in technical and legal debates over broadband policy in which traditional, commercial ISPs are over-represented. Community networks can bring an informed view to these debates, allowing for a policy-making process more attuned to the public interest.

We thank you for your attention and very much look forward to engaging with you on these important issues,

First signatories (EU-based community networks)
020wireless (Netherlands)
AIL-Network (France)
Alsace Réseau Neutre (France)
Aquilenet (France)
Association Ribaguifi - Eresué 2.0 (Spain)
Asoc. SevillaGuifi (Spain)
Common Net (Italy)
FAImaison (France)
FDN (France)
FFDN (France)
Franciliens.net (France)
Freifunk.net (Germany)
Fundació guifi.net (Spain)
Funkfeuer (Austria)
Grenode (France)
Grifon (France)
Ilico (France)
Illyse (France)
Iloth (France)
Neutrinet (Belgium)
Ninux.org (Italy)
Open Network in Croatia (Croatia)
Progetto Neco (Italy)
Progetto Wireco Ciminna (Italy)
Rézine (France)
Sarantaporo.gr NPO (Greece)
SCANI (France)
Tetaneutral.net (France)
Tourraine Data Network (France)
Wireless België (Belgium)
Wireless Leiden (Netherlands)
WirelessPT.net (Portugal)
Wlan slovenija (Slovenia)

Supporting organizations (signing in support of the general approach and/or specific proposals put forward in the letter)
ApTI (Romania)
ARTICLE 19 (UK)
Bits of Freedom (Netherlands)
BlueLink.net - Civic Action Network (Bulgaria)
Brazilian Association of Digital Radio (Brazil)
Chaos Computer Club (Germany)
Chaos Computer Club Lëtzebuerg (Luxemburg)

Colnodo (Colombia)
Common Ground (Germany)
Commons Network (EU)
Dugnadsnett (Norway)
EDRi (EU)
EFF (US)
Electronic Frontier Norway (Norway)
epicenter.works (Austria)
Free Knowledge Institute (Netherlands)
Free Software Foundation Europe (EU)
Frënn vun der Ënn (Luxemburg)
GreenNet (UK)
hackAIR (EU)
Initiative für Netzfreiheit (Austria)
Instituto Bem Estar Brasi (Brazil)
Instituto Nupef (Brazil)
La Quadrature du Net (France)
MAZI (EU)
netCommons (EU)
netHood (Switzerland)
Network Bogotá (Colombia)
NEXTLEAP (EU)
NURPA (Belgium)
Nuvem (Brazil)
One World Platform (Bosnia Herzegovina)
Open Rights Group (UK)
Open Technologies Alliance- GFOSS (Greece)
P2P Foundation (Netherlands)
P2P Lab (Greece)
PIE News Project (EU)
Project Arig (Israel)
Rhizomatica (Mexico)
Renewable Freedom Foundation (Germany)
VECAM (France)
Xnet (Spain)
Zenzeleni Networks (South Africa)

C. Annex 3

Notes on the European Electronic Communications Code

1. Enhancing data protection

Articles 40, 93

Data protection, a core value of Community Networks (CNs)

In Europe, Community Networks (CNs) are a growing movement of organizations that operate local communication infrastructures, sometimes federated at the regional or national levels. These networks, most of which also provide access to the global Internet, are operated as a commons. That is, rather than being driven by for-profit motives, their key focus is on providing connectivity while striving for democratic governance, social inclusion, education, and human rights with respect to communication technologies.

As such, one of their core values is to protect the privacy of their users and not to process their personal data for business purpose or any other purpose not necessary for the provision of their services.

Obstacles faced by community networks

Governments of numerous Member States intend to abolish users' freedom to encrypt their communications. Furthermore, they have lately adopted several laws strengthening the powers of intelligence services to intercept communications and to monitor networks for purposes such as protecting national economical health or the detection of minor crimes or simple misconducts.

In the same spirit, and in breach of the Charter of Fundamental Rights (as clearly interpreted last winter by the Court of Justice of the European Union in its Tele2 case), many Member States are refusing to revoke or review their national laws which require telecommunication operators to retain traffic data of all their subscribers.

All of these issues directly and drastically impact CNs' activities, by preventing them from implementing policies that fulfill one of their core social values.

Amendments

IMCO

Amendments **377 and 378 should be adopted** as they would make end-to-end encryption mandatory for interpersonal communication service providers (such as mail and chat).

Amendment **530 should be adopted** as it would explicitly force Member States to comply with the Tele2 case of the European Court of Justice.

ITRE

Amendments **565, 566, 567 and 568 should be adopted** as they would make end-to-end encryption mandatory for providers of interpersonal communication services.

Amendment **1099 should be adopted** as it would provide a framework anchored in fundamental rights for the interception of communications by competent national authorities.

2. Fostering the development of wireless community networks

Articles 2, 55, 95

Freifunk, a wireless community network

Freifunk is a German community network whose members are single-handedly installing and maintaining free networks, using their own Freifunk firmware on off-the-shelf wireless (WiFi) devices and routers. Every member of the network configures his or her router to relay the traffic of other participants to the Freifunk network. In return, he or she can also transmit data, such as text, music and movies through the network or use services setup by participants. Many members also share their Internet access and allow others to use it to access the World Wide Web and other internet services.

In 2013, there were 40.000 Freifunk relays all over Germany and neighbouring countries and, given the coverage achieved in Berlin, more than 350,000 people can have access to the network. Since the provision of free Internet for all is part of Freifunk core identity, its network is essential for many communities, such as underprivileged individuals.

Finally, based on user-driven networks, services and usages, Freifunk depends on perpetual innovation through, for instance, the development of new communication protocols that any other operators or companies may freely used to provide innovative services all over the EU.

Obstacles faced by Freifunk

Several national laws seek to prevent the sharing of Internet connections amongst several users by making people liable for all the communications made through their Wi-Fi connection. In 2017, two German courts have found individuals sharing their Wi-Fi connection liable for copyright infringements committed by other users. They were found liable because, despite having been warned by rights-holders about such infringements, they did not take measures to stop those infringements and to prevent new ones.

Such liability is a major threat for Freifunk members and a clear distortion of competition since 'traditional' Internet access providers cannot be liable for infringements committed by their users, even if they are aware of them, as provided by article 12 of Directive 2000/31/EC ('Directive on electronic commerce').

Furthermore, while they do not benefit from the same liability regime as professional providers, CNs are subject to the same strict obligations. Some of these obligations are clearly unjustified and disproportionate where imposed on individuals.

Finally, two practical obstacles may prevent individuals from sharing their Internet connection. Firstly, router manufacturers may prevent users from loading into their devices customized software necessary for maintaining free and open wireless networks (such as those developed by Freifunk). Users' ability to use Free Software in order to regain control over their devices is also threatened by ambiguous language in the Directive 2014/53 on radio equipment. Secondly, Internet access contracts may directly forbid subscribers to share their connections with others, or charge them for doing so.

Amendments

Article 55 of the proposed Code intends to foster the development of wireless community networks but fails to address the obstacles underlined above.

IMCO

Amendment **68 should be rejected** as it would hinder the development of community networks by making the community liable for the actions carried-out by end-users.

Amendments **408 and 409 should be adopted** as they would explicitly extend the protective liability regime of Internet access providers to individuals sharing their Wi-Fi connection.

Amendment **411 should be adopted** as it would allow members of Community Networks to install Free Software (software that can be freely used, studied, modified and shared as such) onto their wireless devices, which is a prerequisite and standard practice in wireless networks.

Amendment **566 should be rejected** as it would have the opposite effect.

ITRE

Amendments **298**, **316 and 333 should be adopted** as they would exclude individuals sharing their Wi-Fi connection from the scope of obligations imposed on professional providers, thereby fostering the development of wireless community networks.

Amendments **702**, **703 and 706 should be adopted** as they would explicitly extend the protective liability regime of Internet access providers to individuals sharing their Wi-Fi connection.

Amendments **708 and 710 should be rejected** as they would remove the provisions giving end-users the rights to access wireless networks of their choice and to share their own access with other uses.

Amendments **712 and 713 should be adopted** as they would not allow Internet access provider to charge users in case they want to share their Wi-Fi connection.

3. Promoting a shared and unlicenced spectrum

Articles 4, 18, 45, 46, 49

Tetaneutral, a not-for-profit Internet service provider

Tetaneutral is a not-for-profit French Internet service provider that provides connectivity for everyone, including digital exclusion areas. While fibre optic networks are costly, wireless networks are a flexible and affordable way to provide broadband wireless network to all citizens.

Through WiFi unlicensed spectrum, Tetaneutral is able to deliver symmetrical very high capacity network (up to 30 megabytes) in all areas, including where fiber is not deployed. It is a key enabler that supports the digital uptake in rural areas and spreads digital literacy. It involves users in the deployment of the network and thus empowers citizens in both urban and rural zones. To that extent, bringing connectivity to everyone crucially depends on wireless unlicenced spectrum.

Obstacles faced by Tetaneutral

The lack of shared (through flexible authorisation schemes) and unlicenced spectrum is an obstacle for deploying community networks. Deployment of 4G and 5G should not be an excuse to reduce or even slow the release of shared and unlicenced spectrum (supported by the European Commission), which embodies the core principle of general authorisation mechanism enshrined since 2002 in the current telecoms package. To prevent the often exagerrated risk of congestion, technical harmonisation within the EU should ensure the coexistence of both spectrum licensed through individual rights and of free spectrum.

Besides, the duration of rights to use radio spectrum shall be limited and subject to regular review in order to assess the efficiency of the use of spectrum in light of technological and market evolution, and ensure that spectrum policy continues to serve the public interest. Authorisations should be withdrawn if necessary and National Regulatory Authorities (NRAs) have appropriate powers to carry out such assessments.

Amendments

ITRE

Amendment **393 should be rejected** as it aims at reducing the obligations of the Member States to develop the shared and unlicenced spectrum.

Amendment **420 should be rejected** as it aims at limiting the possibilities for Member States to add amendments to spectrum usage plan.

Amendment **603 should be adopted** as a solution for increasing the access to shared and unlicenced spectrum.

Amendments **636 and 645 should be rejected** as they would increase the number of cases where authorisations to use radio spectrum are needed, which is not an efficient way to foster innovation but would on the contrary add constraints.

Amendments **670 and 674 should be adopted** as they would enable regular reviews of the authorisations to use radio spectrum.

4. Creating the appropriate conditions for small Internet service providers

Articles 59, 70, 71, 72

French Data Network, a not-for-profit Internet service provider

French Data Network (FDN) is the oldest French Internet service provider (ISP) still operatingI It exists since 1992.

FDN provides hundreds of subscribers with services that major French ISPs do not offer: it systematically provides static IP addresses (a critical condition for self-hosting), refrains from monitoring the behaviour of its users for any commercial purpose and guarantees the neutrality of its network far beyond what is imposed by the Open Internet Regulation.
FDN is a non-profit entity: it provides access to the Internet against payment, but its revenues are entirely dedicated to the development of its network and services. Its governance is open to anyone.

Obstacles faced by FDN

As most landine ISPs, FDN has not enough funding to deploy its own cables. It has to rent access to the wired network of big operators in order to provide users with its enhanced services. It may rent two kinds of access: passive and active.

Passive access means that a provider actually rents physical cables, installs its own equipment on the network and manages every technical aspect of the access provided to users. It is usually expensive since ISPs have to rent space in each local infrastructure (thousands of euros per month for each) in order to install their equipment. Thus, passive access is more suited for providing Internet access to many users in the same area or to companies with very specific needs.

Active (also called “bitstream”) access means to simply use part of a network already managed by another operator. It does not require to install equipment nor to rent space. It is much cheaper and adapted for providing Internet access to fewer users in each location. It does not give as much control as passive access but still allows ISPs such as FDN to provide the services their members and subscribers are looking for.

Regarding ADSL lines, operators are obliged to grant passive and active access to ISPs requesting so. Therefore, there are now thousands of ISPs in France that provide customized and enhanced services to individuals or SMEs through the ADSL infrastructure of a few big operators.

However, this situation is limited to ADSL: operators are free not to grant access to their fibre-optic lines at all. Since FDN and most ISPs are not in a position to deploy their own lines (nor participate in the deployment of fibre lines), they simply cannot and do not offer any fibre access to end-users.

This impedes competition drastically, limits the diversity and the quality of services provided to SMEs and individuals and is destroying the pre-existent economic fabric of small ISPs used to work with companies. Now, these companies may only rely on the four big French ISPs which are unable to provide them with services specifically fitting their needs.

Amendments

Article **59** (symmetric regulation), **70** (access to civil engineering), **71** (general access including active) of the proposed Code intend to create obligations to grant access (active and passive) at relevant cost (article **72**) but fails to address efficiently the obstacles underlined above.

ITRE

The following amendments **should be adopted** as they would strengthen operators' obligations to grant access and NRAs' power to order them to do so: **737, 738, 743, 745, 748-752, 757, 905, 907, 908, 909, 912, 939, 940, 948, 953, 954, 959, 965-970, 974, 976, 977, 979, 980**.

The following amendments **should be rejected** as they would have the opposite effect: **735, 746, 747, 889, 893, 894-900, 906, 913, 918, 924-926, 932-937, 943, 971, 984**.

Amendments **917 and 923 should be adopted** as they would specifically ensure that active access is not relegated to a minor role compared to passive access.

The following amendments **should be rejected** as they would have the opposite effects: **739, 740, 741, 742, 880, 930, 931**.

5. Enhancing competition and addressing oligopolistic situations

Articles 61, 65, 71, 72, 74, 77

Federation FDN, a federation of not-for-profit ISPs

The Federation FDN gathers 26 not-for-profit Internet service providers in France and Belgium. Some rely on bitstream access provided by incumbent players. Others create their own fiber-optic or wireless networks in both urban and rural settings, in many cases bringing connectibity to "white zones".

Obstacles faced by Federation FDN

In France, more than 1000 operators are on the ADSL market, offering connection to both individuals or companies. To some extent, this allows competition between a variety of actors, and can ensure the possibility for users to choose between several offers. While ensuring competition at a retail level, such providers also stimulate competition on wholesale markets.

But the situation on the fiber-optic local loop is very worrying: only four operators are developing this kind of infrastructures in France, which cannot be considered as the same competition conditions as for the ADSL market. Furthermore, operators are often alone in a specific area, which leads to a monopolistic situation from the end-users point of view, as they cannot choose between several operators. The root cause is that there is currently no bitstream offers allowing smaller operators or Community Networks (CNs) to use the infrastructure of the dominant players to provide their services to end-users. This situation brings national markets back to the early days of European regulation where single dominance is the rule but with several players theoretically active. Deprived of the proper regulatory incentive to remedy this situation, NRAs are not taking the necessary steps to ensure competition.

To solve these issues, the definition of "significant market power" (SMP) should be broadened, so as to include all operators having a position equivalent to dominance, including through a commercial or co-investment agreement, and be subject to an asymmetric regulation. This would ensure competition in the face of oligopolistic situations.

Also, smaller operators or Community Networks need more flexibility and less administrative burden, such as analysed by the Federation FDN within its answer to the French consultation on the land-line market (www.ffdn.org/en/node/129). Community networks (CN) can be a solution for non competitive markets in bringing connectivity over the territory, such as observed in the scandinavian countries (https://openmedia.org/en/access-success-nordic-countries-0).

Regulatory holidays (art 74-77), limitations to symmetrical regulation (art 59.2) and amendments going further in this direction will inevitably lead to duopolistic and non-competitive situations Thanks to access regulation, this is precisley what we have so far avoided in Europe. As the political economy of networks further concentrates, if CN are not supported (notably through bitstream access) we will step back from this situation.

Amendments

IMCO

Amendment **436 should be adopted** as it deletes the provision on article 72 that would reduce the NRA regulation powers depending on the investments. The role of NRAs is not only to secure the investments of operators but to ensure a harmonious development of faster and affordable networks across territories.

Amendment **440 should be rejected** as it aims to put the burden of proof on NRAs when they aim at regulating costs and tariffs. Due to classical asymmetry of information issues, NRAs cannot face such a burden and would deprive them of the capacity to regulate tariffs even when reasonable and not cost oriented.

Amendment **441 should be rejected** as it aims to remove any transparency related to cost accounting system. Again, transparency is crucial when related to cost-regulation. Cross susbidies issues could not be properly addressed under such circumstances.

Amendment **442 should be adopted** as it gives back to NRAs the capacity to appreciate how much New Network Elements shall be subject to regulation. On the contrary, automatic and potentially temporary deregulation would greatly disturb the market and impede competition.

Amendment **444 should be rejected** as it worsens the European Commission's proposals by letting monopolistic players unregulated.

Amendment **448 should be rejected** as it aims to put at the same regulatory level any kind of agreements among market players, and would lead without any control mechanism to raise barriers to market entry for any operators that are not part of such agreements.

Amendment **449 should be adopted** as it clarifies that co-investment agreement must have been concluded in order to be taken into account by NRAs. Assessing a mere co-investment offer is not enough to allow NRA to play its role and ensure a proper competitive dynamic.

ITRE

Amendments **793, 794, 800 and 818 should be adopted** as they would also enhance the definition of SMP and remove provisions that weaken the SMP regime.

Amendment **971 should be rejected** as it aims at securing the network investments by operators whereas the role of NRAs is to ensure a harmonious development in the territories and give to all equal access to the market and services.

Amendment **973 should be rejected** as it would worsen the oligopolisation of fiber-optic networks and thus worsen the distortion of competition. This amendment gives operators more possibilities to exclude competitors either by increasing prices or discriminating the undertakings.

Amendment **1045 should be adopted** as it removes article 77 that imposes less obligations to vertically separate undertakings. As it stands, this article would leave monopolistic players unregulated.

Amendment **1130 should be adopted** as it would enable local ISPs to participate in the investments and thus enhance connectivity and competition at the local level.

About netCommons

netCommons is a Horizon2020 research project supported by the European Commission (2016-2018), which proposes a trans-disciplinary methodology to study and support the development of local network internet infrastructures as commons, for resiliency, sustainability, democracy, privacy, self-determination, and social integration.

netCommons is participated by 4 universities, one research center and one ONG (UniTn, UPC, AUEB-RC, UOW, CNRS and Nethood, respectively from Italy, Spain, Greece, UK, France and Switzerland). The consortium brings together research groups and institutions in the area of “networks” and collaborative platforms with expertise in engineering, computer science, economics, law, political science, interdisciplinary research.

netCommons aims to help existing community networks like guifi.net and ninux.net, to grow and replicate in more European cities and rural areas. To become more extrovert, more inclusive, and better understood by the wider population. To empower them to form both a means for equitable and affordable access to the Internet and community-owned infrastructures for the provision of local services.

D. Annex 4

Letter to EU Policy-Makers: Making Regulation Work for Community Networks

SUBMITTED BY MELANIE ON FEBRUARY 21, 2017 - 1:48PM

UPDATE: *The consultation is now closed and a joint press release is published on March 16th, 2017. Help us to spread the word!*

After many discussions with many European Community Networks (CNs), researchers from netCommons are happy to present a draft open letter on "policy recommendations for sustaining Community Networks".

The letter is targeted at European policy-makers, who recently started working on an overhaul of the telecom regulatory framework. It is drafted in collaboration with several European CNs and advocacy groups and is meant to offer a collective voice to this growing movement.

Until March 15th, we would like to collect signatures from as many European CNs as possible, as well as other supporting organizations (be they advocacy groups, research projects, non-profits, SMEs, local authorities, etc.).

After this consultation period and the collection of signatures, we would like to send the letter to members of EU Parliament, national delegations at the Council of the EU, as well as to key officials from the EU Commission.

Several outcomes can be expected, including:

- The publication of a joint press release by all signatories to disseminate the open letter as widely as possible (by the end of March).
- Proposals for amendments reflecting the recommendations of this open letter, to be sent to key members of the EU Parliament before the first crucial vote on the Telecoms Package in late April.
- A policy workshop to be organized later this year in Brussels.

Of course, all of these potential outcomes will depend upon the involvement of signatory organizations, and in particular of the willingness of CNs to work together.

But first, we are sharing the draft to a wider circle of CNs and other people interested in their activities for consultation and potential amendments to the text. Until March 8th, many people read and commented on the draft letter, offered corrections and suggested changes or additions by using co-ment, an online tool for collaborative writing, in the iframe below or directly on the dedicated co-ment page.

If and when you agree to sign the letter, please send the name of your organization, the country where it is based and its high-resolution logo before **March 15th** to: advocacy@netcommons.eu

(note that if your signature is dependent on the response brought to a specific comment you have made, please be sure to tag comment as "blocking").

https://lqdn.co-ment.com/text/RI42W44XAc6/view/

-/ **1** discussione (filtro: 1/1 commento 2/3 repliche), naviga per: posizione

commento

OPEN LETTER TO EU POLICY-MAKERS

POLICY RECOMMENDATIONS FOR SUSTAINING COMMUNITY NETWORKS

The letter has been sent to EU institutions on March 16th, 2017.

For background, see: http://netcommons.eu/?q=content/letter-eu-policy-makers-making-regulation-work-community-networks).

Translations in various European languages are available at this page: https://wiki.laquadrature.net/Paquet_Telecom_2017/lettre_NetCommons

If your organization want to **sign the letter, please send the name of your organization at: advocacy@netcommons.eu**

PREAMBLE

We represent European Community Networks, a growing movement of organizations that operate local communication infrastructures, sometimes federated at the regional or national levels. These networks, most of which also provide access to the global Internet, are operated as a commons. That is, rather than being driven by for-profit motives, our key focus is on providing connectivity while striving for democratic governance, social inclusion, education, and human rights with respect to communication technologies.

Source URL: https://lqdn.co-ment.com/text/Rl42W44XAc6/view/

Image:

melanie's blog

Recent blog posts

Notes on European Electronic Communications Code before decisive votes in European Parliament

Stockholm Internet Forum

Draft report on "Electronic Telecommunications Code" calls for immediate action

E. Annex 5

Draft report on "Electronic Telecommunications Code" calls for immediate action

SUBMITTED BY FEDERICA ON MARCH 22, 2017 - 7:40PM

On March 16th, more than 30 European Community Networks, joined by over 35 supporting organizations from around the world, sent an open letter to EU policy-makers. The letter, which was translated in many European languages, aims at including CNs' needs in the upcoming reform of the telecommunications policy of the European Union through an "Electronic Communications Code", which is currently discussed in the European Parliament.

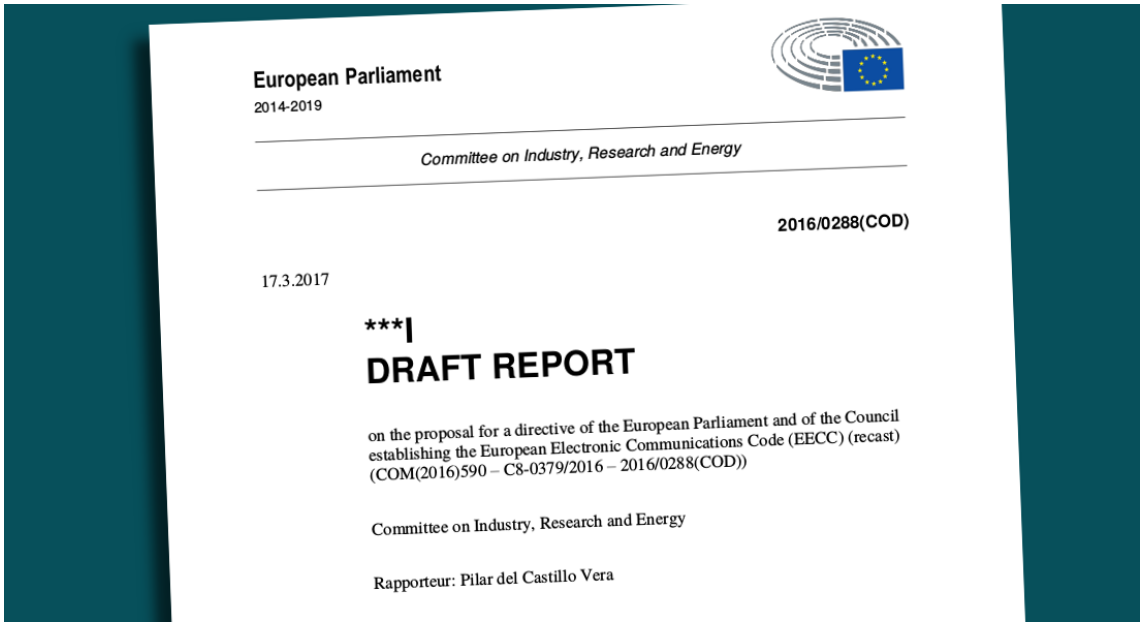
The Code will repeal the existing directives on telecommunications and mainly aims at increasing connectivity in the EU territory. While an harmonization and an update of the current policy seem more than appropriate, the upcoming Code could greatly hamper CNs development. Among other issues, the Code initially proposed by the European Commission would prevent small actors to participate in the investment of the network infrastructure, would extend to a minimum of 25 years the duration of the rights to use radio spectrum and would provide for unbalanced Universal Service obligations, making persons geographically isolated or in difficult situations into second-class citizens.

On March 17th, the Industry committee of the European Parliament (ITRE) – responsible for assessing the proposed Code – has issued its draft report, which will contain the main amendments that will be discussed by the whole Parliament in few months. Until April 4th, members of the ITRE committee may propose further amendments to this report (La Quadrature du Net works hard to provide them with positive amendments).

Such additional amendments will be necessary given that, in its current state, the draft report is even worse than the initial proposal, aggravating the gap between small operators and incumbents, extending to 30 years the duration of radio spectrum rights and removing the initial provisions in favor of the open spectrum. Its sole merit is to remove the administrative fees for small operators.

The report and its amendments will be voted on 11th July. Until then, members of the ITRE committee should be encouraged to defend the amendments under preparation in favor of CNs. Once adopted by ITRE, the report will go before the whole European Parliament: then, all MEPs will have another opportunity to table positive amendments before the Code being ultimately voted, possibly before the end of the year.

Image:


European Parliament
2014-2019

Committee on Industry, Research and Energy

2016/0288(COD)

17.3.2017

***I

DRAFT REPORT

on the proposal for a directive of the European Parliament and of the Council establishing the European Electronic Communications Code (EECC) (recast)
(COM(2016)590 – C8-0379/2016 – 2016/0288(COD))

Committee on Industry, Research and Energy

Rapporteur: Pilar del Castillo Vera

federica's blog

Recent blog posts

Notes on European Electronic Communications Code before decisive votes in European Parliament

Stockholm Internet Forum

Draft report on "Electronic Telecommunications Code" calls for immediate action

Letter to EU Policy-Makers: Making Regulation Work for Community Networks

CNs promoted as 'the other' way to connectivity at IGF2016

netCommons at the NinuxDay, the meeting of the ninux Community Network

Sarantaporo.gr Non Profit Organization is awarded financial and consulting support by the Ashoka Impact Project

DIY networking: the path to a more democratic internet

Finding "commons ground" with Sarantaporo.gr

Workshop on the History and Theory of Alternative Media

More

Log in

Credits

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

F. Annex 6

Notes on European Electronic Communications Code before decisive votes in European Parliament

SUBMITTED BY ARTHUR ON JUNE 7, 2017 - 1:11PM

In February, European Community Networks (CNs) and supporting organisations have expressed their concerns about the upcoming "European Electronic Communications Code" in an open letter sent to EU policy-makers.

The European Parliament will soon have two major opportunities to address these concerns.

First, on **June 22th**, the Consumer Protection committee of the European Parliament (IMCO) – one of the two associated committees responsible for the draft Code – will adopt its report.

Second, on **July 11th**, the Industry Committee of the European Parliament (ITRE) – the other and responsible associated committee – will adopt its own report (based on the alarming draft report it issued on March 17th, and on the IMCO report).

The ITRE report will be adopted in plenary session and thus be the basis for the negotiations between the rapporteur Pilar del Castillo and the Council of the European Union. The coming votes are therefore key for the next steps.

In order to assist Members of the European Parliament to adopt a text that take into account the rights of CNs and users, as well as to help Europeans to understand how the European Electronic Communications Code may impact them, netCommons is publishing five notes on the following subjects:

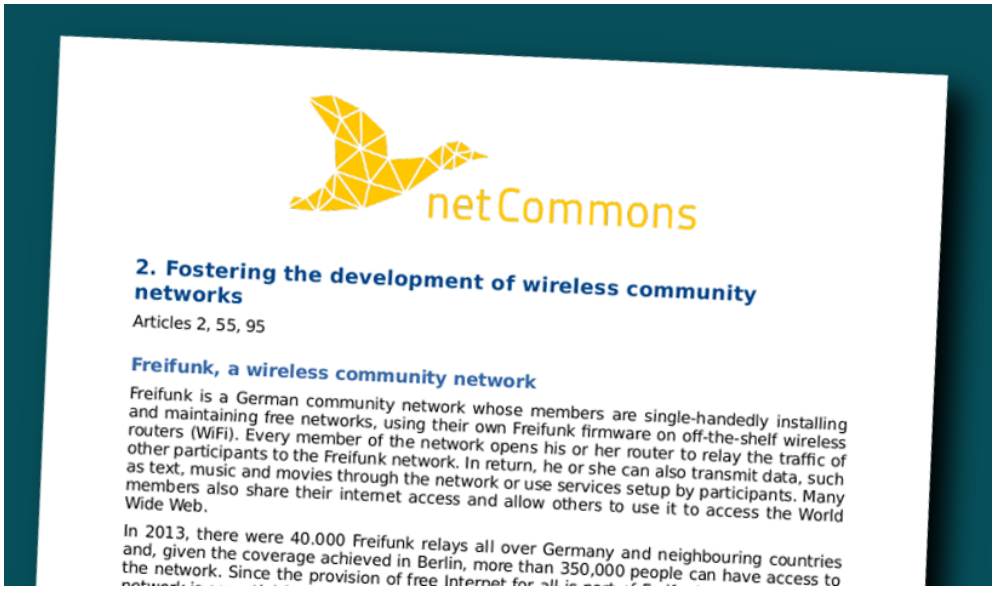
1. Enhancing data protection
2. Fostering the development of wireless community networks
3. Promoting a shared and unlicenced spectrum
4. Creating the appropriate conditions for small Internet access providers
5. Enhancing competition and addressing oligopolistic situations

These notes also intend to list which of the specific amendments tabled in IMCO and ITRE would be in favor or against Eureopeans' interest, as identified in the open letter and the netCommons work.

Download the detailed notes

Call an MEP

Image:



attachment:

netcommons_eecc_notes_imco_itre.pdf

Arthur's blog

Recent blog posts

Notes on European Electronic Communications Code before decisive votes in European Parliament

Stockholm Internet Forum

Draft report on "Electronic Telecommunications Code" calls for immediate action

Letter to EU Policy-Makers: Making Regulation Work for Community Networks

CNs promoted as 'the other' way to connectivity at IGF2016

netCommons at the NinuxDay, the meeting of the ninux Community Network

Sarantaporo.gr Non Profit Organization is awarded financial and consulting support by the Ashoka Impact Project

DIY networking: the path to a more democratic internet

Finding "commons ground" with Sarantaporo.gr

Workshop on the History and Theory of Alternative Media

More

Log in

Credits

G. Annex 7

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 ==

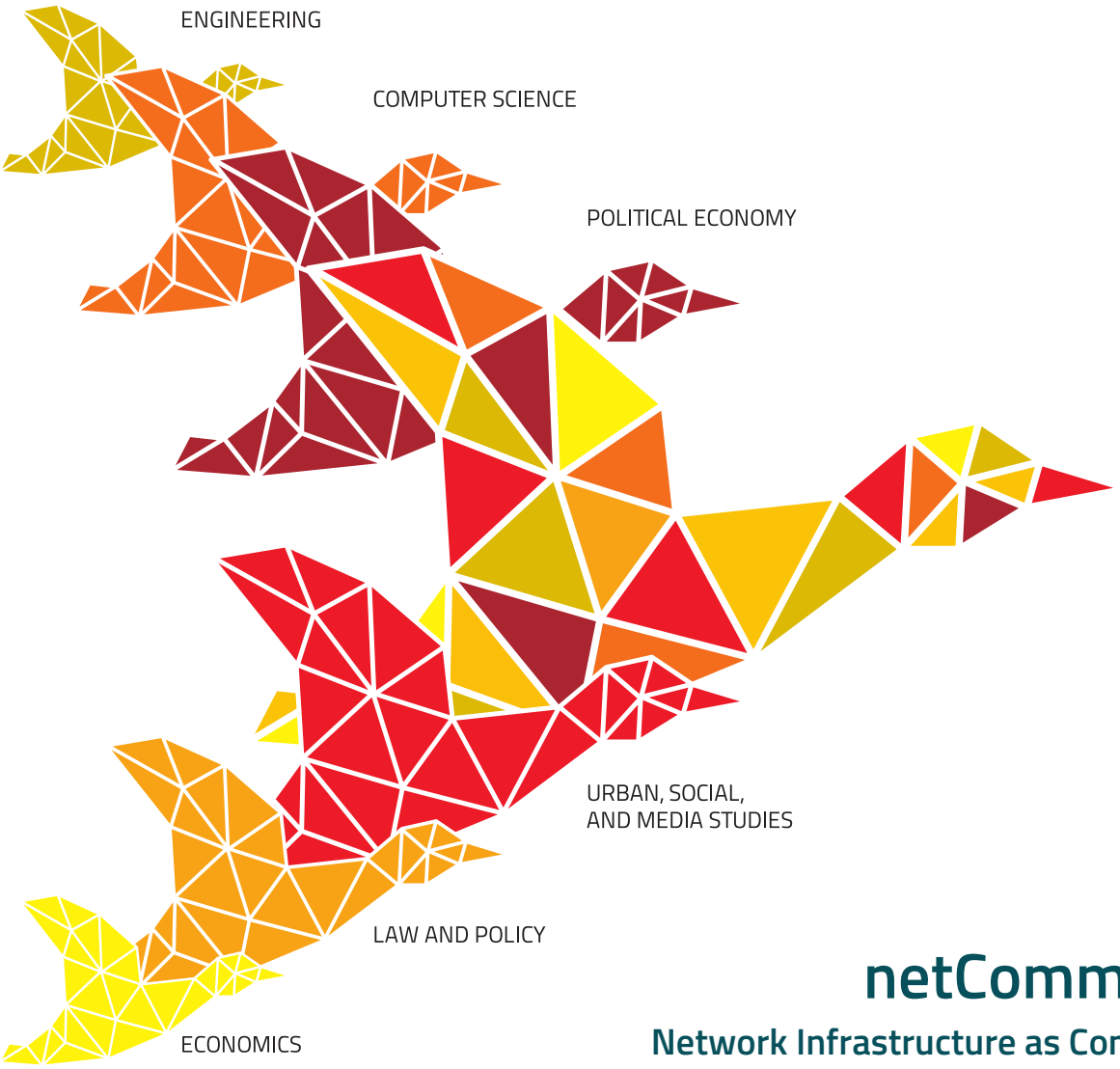
Sebbene non esista un caso pratico, in Ninux non è esclusa per principio la partecipazione alla rete di soggetti come ISP o più in generale aziende che possano offrire i propri servizi a pagamento agli utenti Ninux.

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.



netCommons

Network Infrastructure as Commons

European Legal Framework for CNs (v2)

Deliverable Number D4.2
Version 1.0
January 4, 2018

netCommons.eu