

Peer-to-peer as a design principle for law: distribute the law

Introduction

The relation between peer-to-peer and the law is often analysed from the angle of file-sharing regulation. Peer-to-peer is seen as a disruptive technology of distribution, requiring the law to adapt itself in order to control a new type of activity. A polarised discourse leads copyright law to be extended to prevent file-sharing to disrupt existing business models based on a strong enforcement of copyright; the alternative policy proposal to adapt copyright law to peer-to-peer file sharing technologies is to introduce limitations and exceptions to exclusive rights in order to preserve user's rights. This relation between law and technology assumes that the law has to be adapted to take into account new formats of cultural practices, either to forbid them or to legalise them, has been observed for previous changes of peer reproduction and distribution medium, what Walter Benjamin calls mechanical reproduction. Both ways to adapt the law to the technology mean that the law is trying to control the technology, either negatively by outlawing certain behaviors, or positively by recognising them. And eventually, after a period of conflict between established rightholders of the old technology disrupted by a new technology (mechanic piano, radio, VCR, etc), the law reconfigures itself by creating an exception to exclusive rights to open up the system and host the new reproduction technology. With peer-to-peer distribution, new forms of compensation can be considered. Propositions of creative contribution (Aigrain, 2012) favor the concept of peers contributing to the creative process in a redistributed manner, instead of relying on the centralisation of a collective society to collect and share remuneration based on usage.

This article positions itself beyond the tension between copyright enforcement to preserve business models *vs* users' rights required to enjoy the opportunities provided by the disruptive technology for access to knowledge. It proposes to consider another angle of the relation between law and technology and presents the argument of the distribution of the law itself. Peer-to-peer technologies disrupting established economic models and legal categories could also inspire an evolution of the law as a regulatory system in order to integrate their technical features. This will lead to another kind of relationship between law and technology: after the control of the technology by the law which absorbs the new technology by expansion, the law can try to integrate the technology by reconfiguring its internal operating system and shuffling the categories a bit more, instead of simply inflating them by adding an exception to the existing system.

My starting point is that the western conception of law is based on the legal category of the individual to which rights and duties are allocated in balance with others'. The notion of individual includes the citizen user, but also all individually identifiable actors which have been allocated a legal status as a single entity: corporations, non-profits, nation states, all kinds of organisations. This legal theoretical conception does not adequately take into account the concept of communities of peers, defined as non-stabilised, evolving, or non formalized groups sharing a common interest or an ad hoc production purpose, from local communities (e.g. those using a commons-based governed fishery) to online communities (e.g. the users of a platform) which do not have a legal statute as an individually identifiable entity.

Law, as a technology of regulation, can also be disrupted by peer-to-peer in the sense that legal thinking can be influenced by its architecture design principles based on decentralisation. Peer-to-

peer networks, source of peer production of content or services, as disruptive online technologies, reconfigure legal categories frontiers and assumptions. Collective mechanisms of governance and ownership by peers are identified both in the tradition of the natural commons (Ostrom, 1990) and for the recognition of local communities rights. They offer not only a political alternative, but also a theoretical break from envisioning the individual person as unique point of reference of the regulatory system composed by positive law and policies targeting individuals, towards the recognition of collectives as subjects of rights.

In this article, I consider law as a technology raising policy questions. I will first describe how the concept of distributed architectures, the technical underlying feature of peer-to-peer systems as opposed to centralised design of client-server communication, is disrupting the application of positive law. Legal disruption of copyright by peer-to-peer file-sharing services has been studied extensively, but other applications based on distributed technology also question liability, control, ownership and responsibility. Distributed storage and wireless mesh networks will be addressed in section 1. In section 2, I call for a transformation of legal thinking and logic. Instead of relying only on the concept of the individual, I am questioning whether the law could integrate the architectural features of distribution from the inside of its categories in order to try to better regulate distributed technologies. Peer-to-peer ways to think and design the law are already being developed by the political movement of the commons and by network theorists. I consider in section 3 such attempts of designing collective rights or collective persons beyond both a mere individualised law and Information and Communication Technologies. A peer-to-peer law also relates to political theory questions of plural persons and the agency of collectives. But in order to really challenge liberal legalism design grounded around individualism, I conclude in section 4 with the need to develop metaphors and social imaginaries (Mansell, 2012) to conceptualise empty spaces (Milun, 2011) and contribute to the definition of distributed forms of ownership or liability as examples of integration of peer-to-peer as a design principle for the law.

1. The Impact of Distributed Architectures on Legal Liability

The architectural design of peer-to-peer challenges legal reasoning and the usual application of concepts such as property, or the assignment of responsibility, because files and actions are fragmented and distributed between nodes hosted by peers, rather than directly attributable to individuals. Peer-to-peer networks are relying on decentralised architectures as opposed to direct relations between a server and clients (Dulong de Rosnay, 2013). Similarly, peer production is a system of production which differ from the centralised, liberal model of the firm in the sense it functions around collaborative dynamics with a non hierarchical, self-organising structure and if ownership is also distributed, it will be commons-based peer-production (Benkler, 2006).

Many technologies are designed according to distributed, decentralized principles. Distributed architectures are considered as social technologies, in the sense they allow peer production and reach a common goal or individual needs through coordination of shared resources¹. Instead of a bidirectional client-server relations, all peers possess and demand the resource, and enter into a spontaneous collaboration without need of central coordination (Schollmeier, 2001), resulting in decentralised resources distributed among unpredictable IP addresses (Shirky 2000). Peer-to-peer designates “any networking technology where crucial responsibility lies at the end-points” (Oram 2004). From a strict technological point of view, it should be noted that purely decentralised peer-to-peer doesn't exist, applications are relying on hybrid models, with a small dose of centrality, as they are sometimes structured around supernodes which re-create a degree of centralisation. These implementation features are important to make the services more efficient and stable (Elkin-Koren, 2006). But I will ignore these implementation for the sake of theoretical reasoning and focus on the

¹ This presentation of distributed architectures draws from and builds upon the introduction of Musiani, 2013.

distributed aspects of peer-to-peer architecture, how they impact on the application of the law (section 1) and how they may influence the design of the law (section 2). Indeed, in order to improve quality of service, resource optimisation and resilience to network problems such as connectivity interruption, files are fragmented among peers. With Bittorent protocol for instance, only the final peer reconstructs the file (Cohen, 2003). This architectural configuration based on resource sharing has an impact on the localisation of data and exchange. Forces of decentralisation and autonomy characterise distributed services, as each node can be client and server and no node controls the other. Localisation and control are useful conceptual notions at the foundation of legal reasoning and therefore the allocation and attribution of rights such as responsibility or ownership. By looking more precisely at two distributed technologies, I intend to demonstrate how their design questions the application of traditional legal regulation which is based on *individualisable* and individualised actions.

1.1 Distributed Storage

An example of peer-to-peer technology disrupting the law is Wuala (a case study analysed by Musiani, 2013 and 2014). Wuala, initially developed at the Swiss Federal Institute of Technology (ETH) in Zürich, is a distributed storage service², like Dropbox, except that hosting of the files to be backed up is not centralised in the (single or multiple units of individually identifiable cloud) servers of the company, but rather distributed among the hard drives of users of the service which are linked in a distributed network architecture. In order to ensure a better quality of service, there is also hosting according to more traditional cloud data server modalities (Mowbray, 2009), but for the sake of the argumentation of the paper, I choose to consider only the peer-to-peer portion of the service which could theoretically be used on a standalone basis without additional storage in the application centralised cloud server. Even if it is not the best product from a marketing point of view, the distributed part of the service is the socio-technical arrangement and the legal tendency I want to observe.

With Wuala, data is fragmented, locally encrypted on the machine of the user and made redundant, in order to ensure availability for download even when not all the peers offering their internal disk for shared storage are online at the moment the user who uploaded the file wants to access it again (in the same way it is necessary to have at least one seeder to download a torrent). Therefore, if no file is stored entirely, it is questionable whether contributory liability would be triggered at all, if a file is illegal content. Unlike Bittorent, peers do not know what they are hosting as the files, after being fragmented, are encrypted. Besides, the service can't technically monitor what is being uploaded because of the distribution of the process, and external entities (majors, police) can't proceed to the surveillance of the files because at no time they are existing in a reconstituted format making them readable and perceptible to the senses outside of the machine of the first peer who upload it bits by bits and downloads it back fragment by fragment.

Therefore, it is legitimate to question, as Musiani does (2013, p. 221), whether users could be held liable for helping someone to reproduce and access an infringing file. It seems impossible to assign intention, awareness or guilt to the mere action of hosting fragments, as neither the peers nor the service developers have the technical means to know what they are hosting. Circulating in sealed envelopes fragmented among many hard drives, stored content can be holidays pictures for back up purposes, copyrighted books, personal data, revenge porn or harmful content. A second version of Wuala added a part of centralisation to improve the service, but it is likely that in a purely distributed configuration, neither the peers nor the service could know what is hosted, except if managing to break the encryption which is not possible in the current state of the art. Therefore, no

²<https://www.wuala.com/en/learn/technology>

procedure of notice-and-take down³ or liability of the Internet Service Provider could apply as the reconstituted content will never be visible nor made public, as illegal content would remain unnoticed so no-one could notify anyone or remove any content. If the data remains fragmented and private, even forcing the service to reveal the identity of the registered users would not help the justice as it would not inform of the lawful or unlawful nature of their activity. The only pressure public authorities could place on a service which may potentially host content infringing the law could be intimidation. Lavabit encrypted email service provider decided to close the service rather than giving its encryption keys⁴, but Wuala does not know the password of its users. The other option is outlawing all distributed services, which would have a chilling effect⁵ and prevent legal activities in the same way peer-to-peer filesharing protocols can be used both to download free software or unauthorised content. But unlike Dropbox which is hosting the files and does not allow to store certain files⁶ which might be copyrighted and the service incidentally used as a filesharing platform, a distributed Wuala would not be able to control what files or even file formats are being uploaded and fragmented as the encryption is performed locally on the user's machine before the fragments get duplicated and hosted on the hard drives of other peers. The PirateBay has an index of links to available torrents, which can be legally problematic in some jurisdictions, and offer a mean of technical control through an order of blocking to be sent to the Internet Service Provider on the request of the government or the major companies. But as there is no such centralised information on the torrents of the files for Wuala, which acts as a distributed private storage cloud, there is no such option to remove or block the page with links to the content, neither to know which fragment belongs to which user. The level of decentralisation matters and if only the distribution is distributed but the production remains centralised, the service will be vulnerable.

Musiani speaks about a shared techno-legal responsibility. I do not think self-regulation by the users is applicable to ensure the legality of the content hosted as only the uploader is aware of the content of the file. Also, the disclaimer of liability contained in the terms of service of the application would probably not be helpful against a legal attack. Ethical considerations such as community monitoring, or commitment to host only lawful content, can be useful for auto-regulation to police a service and ensure its sustainability as a commons: Ostrom Institutional Design Principle #4: "Effective monitoring by monitors who are part of or accountable to the appropriators" and its complement #5 "A scale of graduated sanctions for resource appropriators who violate community rules" (Ostrom, 1990). But more pragmatically in the case of a distributed service such as Wuala, if no infraction can be detected, it seems very unlikely that a feeling of community responsibility could be developed. Similarly, I doubt that liability could be assigned neither to the service provider (except in the case peer-to-peer technologies would be outlawed altogether), nor to some nodes (legal regulation did not reach that stage of control yet, even if Hadopi French law tried to hold users liable for not securing their internet connexion and allowing other users to perform infringing activities on their wifi). It seems difficult to allocate individual responsibility to individuals who share their computing resources with unknown peers to reproduce and communicate content of unknown nature. Judicial proceedings for negligence to secure wireless connexions have been practiced both in France with three strike law and in the US with police raids. However, the identification of the IP address of the device, which is dynamically changing over time and can be changed or spoofed, cannot be held as a proof identifying a person.

1.2 Wireless Mesh Networks

³As requested by the Digital Millennium Copyright Act 1998 and the Electronic Commerce Directive 2000.

⁴<http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email>

⁵<https://www.chillingeffects.org/>

⁶<http://www.extremetech.com/computing/179495-how-dropbox-knows-youre-a-dirty-pirate-and-why-you-shouldnt-use-cloud-storage-to-share-copyrighted-files>

With the advent of mesh wireless technology (Jun et al, 2003, Chen et al, 2006) which is presented in this section, it becomes even more difficult to assign liability to an IP address, as IP can be shared among even more peers using the network than with conventional wifi. To increase security, these services can also be used in conjunction with applications for encryption and anonymisation, such as Tor, The Onion Router distributed browser ensuring the routing of communications through a network of nodes hosted by peers masking the IP. The implication of such architectures is privacy by design (De Filippi, Dulong de Rosnay, Bourcier, 2013). Both online privacy for activists in undemocratic countries or journalists who need to protect their sources and the dissimulation of illegal activities are target users of Tor. Anonymisation of the source should be well ensured if it is hard to find the source or the destination of the content (Li, 2007).

Wireless mesh networks, which can be used by wireless local communities (Antoniadis et al, 2008 and 2009), municipalities or hackers, apply the same principle of routing the communications between nodes (laptops, phones or other wireless devices). The network can be connected to the internet or not, and communication can be organised either around a central server or in a decentralised way, as I am interested to study in this paper. One node will only transmit to the next node. In order to avoid secondary liability for actions led by other users of one's internet connexion, in the jurisdictions where it exists, it is possible to use a VPN⁷. There is community governance and self-regulation as many networks offering free service of transit commit to certain principles organising the relation between nodes⁸. But these agreements intend to regulate tort regarding the quality of service, not the potential infringing activities committed on the network. Applying the law of Internet Service Providers⁹ to mesh node owners, nodes cannot be held liable for content infringement because “mesh nodes would be “common carriers” or “mere conduits”: simply relaying data, they benefit from a legal immunity (Hatcher, 2007). Law enforcement would be more difficult for distributed community-based networks formed by many individuals than for municipalities or universities who would demonstrate centralisation at the level of the ownership of the network, while peer-to-peer mesh network seem “copyright resistant” (von Lohmann, 2004). Depending on the legal status of the mesh network, the regime of ISP liability may or may not apply: in the case of an association with a board and legal representatives for the community mesh network, or if a node is held by an institution, it could be held liable for the traffic, but in the case of a distributed architecture without designated responsible persons or contractual relationship, it seems more difficult to enforce the law (De Filippi, 2013, Giovanella, 2014), all the more when creating a node does not require a registration and the number of nodes is unknown, and in the case of encrypted mesh network, forming a local darknet. Like for distributed storage, allocating liability to individual nodes of the mesh is difficult because the connectivity is made possible by a distributed network of devices. Peers hosting Tor relays or mesh network nodes should not be held liable as they are not the ones using the service to perform an illegal activity. Intermediaries in general should not be held liable “for the content disseminated or created by their users (as it) severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law.” (La Rue, 2011).

2. For a Transformation of Legal Thinking

Lobbying to prohibit peer-to-peer file sharing or peer-to-peer based technologies of anonymity, storage, browsing or access follows a traditional model of legal regulation, which aims at controlling the technology and maintaining the supremacy of legal rules which were developed

⁷<https://en.wikipedia.org/wiki/Freifunk>

⁸<http://www.picopeer.net/PPA-en.html>

⁹Directive 2000/31/EC of 8 June 2000 on Electronic Commerce, OJ 2000 L 178/1, Article 12; US copyright law 17 USC 512(a).

before the new technical environment and are trying to catch up. However, this position, instead of transposing legal values and general principles to the digital age, leads to constraining it beyond the initial regulatory objective of preventing infringement, by controlling also legitimate activities which were previously unregulated. Legal doctrine showed the extension of the scope of copyright and the chilling effect on users rights and socio-cultural practices of creation. The law has not been updated yet to scale to the technology. There has not been any change of legal paradigm to integrate transformations caused by digital technologies and peer production, with unidentifiable networks of peers instead of legally identifiable persons. Law can also interact with technology in a different way by trying to integrate some of its features in order to maybe better regulate it.

One way to think about the relationship between law and peer-to-peer technology is to wonder if the law needs to be expanded to face a new regulatory challenge. People choose to use and to contribute to services based on distributed architectures to preserve their privacy and escape censorship, but also legal control. The uniqueness of the distributed environment may fade away if the legislator catches up and blocks ports needed to deploy peer-to-peer architectures. The same attack of “law of the horse” (Easterbrook, 1996 and the answer by Lessig, 2001) which has been made to cyberlaw could be made to a law of distributed architecture, questioning its singularity and its *raison d'être*. Or, if distributed architectures are unique, we are facing the emergence of new legal categories which will produce new norms. But beyond the fact that these technologies may be used for both legitimate and illegal purposes and that the fragmentation of the services makes it difficult to assign liability, it should be noted that these peer-to-peer services are also part of the social movement of the commons. They all propose the peer-production of a service as an alternative to the commercial centralised services exercising control over their users. Even if technical efforts required to set them up as opposed to the ease of installation of their commercial counterpart may prevent their take-off, they participate to emancipation and autonomy through technology, and constitute a valid alternative to the commodification of free labour and the lack of security and privacy of the private commercial services.

From a legal perspective, the main difference I want to observe between commercial and peer-to-peer services is that the former services rely on the contractual relation between two individual entities (the corporation and the user), allowing to allocate responsibility in case of infringement, while the latter services are not provided by an individual person. They are offered by a mesh of nodes which ensure collectively that the service is possible, each ensuring a fragment of it, which is difficult or impossible to monitor technically and control legally. Distributed architectures are fragmenting data and actions, thus exploding the localised rights model where each object or right can be assigned to one actor. The problem comes from the fact that peer-to-peer architectures aggregate and distribute technical insignificant fragments, while the law allocates rights to individual persons in a bijective relation. Individual legal entities are the basis of legal reasoning and the subjects of rights. Western legal systems tend to mostly recognise rights only to individuals, to protect their rights of private property, their commercial interests and personal freedoms. Roman law assign rights to individuals (which can be states, corporations or non-profit) benefitting from a autonomy and agency. Law is arranging responsibilities, rights, duties, obligations and conditions between moral or physical persons in localised determined jurisdictions, while distributed architectures operate with fragmented data and share the process between actors which are neither localised not stabilised, as they are not necessarily the same peers present all along a given process of data communication. I claim that the distribution of the actors and the actions requires to rethink legal categories as notions of author of an action, action and content are not tangible units any longer, but aggregating and evolving fragments. Legal reasoning will question whether distributed services are really of a different nature, if localisation really matters, if the association of encryption and fragmentation ensures anonymity or untraceability, how to distinguish or link the request of an action from the implementation or performance of the action. From the last question, my understanding is that fragmentation of actions between an unfixed network of peers at least blurs

responsibilities and at most makes it irrelevant. Which method of research of the responsible person can be applied if there is no identifiable owner or service provider? *In solidum* responsibility and the joint liability of all identifiable nodes has not been applied but the absence of case law does not mean this could not happen. It might be the case that if no entity is found liable, any identifiable entity related to the case would be sentenced. The reconfiguration through cooperation of the notion of individuals forming a collective triggers a deconstruction of legal categories in several domains, copyright, liability, cybercriminality, processing of personal data, but also data security: in case of service failures and data loss, it is not certain that warranties disclaimer would be valid facing consumer legislations. No contractual relationship can be deduced since as users are unknown and unstable, the performance of the service being dependent on who is connected when. In the absence of contract and user identification, it is difficult to assign responsibility in the traditional way. A complex network of users and contractual relationships could be inferred from who is online when, but if peers do not know what package is circulating, and if the package may take a different road when they are not online, all peers could just be irresponsible nodes among others, unaware of the content of the traffic they are collectively facilitating, but neither individually allowing or blocking. The presence or the absence of one peer in the network is irrelevant to the performance of the service, diminishing claims for collective responsibility.

3. Precedents, Legal Hacks and Analogies

The law reasons by analogy, it is therefore useful to examine the state of law in similar or comparable areas. Precedents and contributions to a movement of peer-to-peer law can be found in two areas: the commons and network science.

3.1 Fragmented Property Rights Over Physical and Digital Commons

The legal framework for ownership and copyright has been able to address peer production with specific governance arrangements for both physical and digital commons.

Elinor Ostrom's bundle of rights opened a new positive space to think common or shared property (Orsi, 2013), which constitute an alternative to exclusivity through individual private property and unregulated open access to *res nullius* thought negatively as inappropriable. Before enclosure of the lands, property was attached to utility, with different usage rights (De Moore 2009) and natural common-pool resources are considered common property with a distributed bundle of rights (access and withdrawal operational rights, management and governance, exclusion, alienation as collective choice rights). This conception is clearly a conceptualisation of fragmented property among different types of users. Orsi also recalls that already in the XIXth century, the US doctrine of legal realism on fragmented property introduced doubt on the preexisting legal categories, describing property not as an absolute right but as a collection of social relations, rights, duties, obligations and responsibilities¹⁰.

More recently, Italian water has been the theater of a movement of constitutionalisation of the commons to exclude both privatisation and nationalisation. Stefano Rodotà is calling for “a new definition of “citizen”, one that goes beyond “a set of rights and duties allocated in a statist perspective” (Rodotà, 2013). Defining political participation mechanisms still refers to the citizen as an individual in reference to the right to access to the common goods. A more profound legal epistemological turn transposed to distributed architectures studied in the previous section would depart from citizens as individual commoners, to start considering the actions operated by peers as operated by a collective of a different nature than the aggregation of individuals. With water as a

¹⁰See the table of eleven rights by John Commons (1893) in *The distribution of Wealth*, reproduced by Johnson (2007) cited by Orsi (2013): <http://regulation.revues.org/docannexe/image/10471/img-1.png>

commons, the epistemological transformation is affecting the nature of the object of rights, the commons, but not the nature of the subject of rights who remains an individual citizen even if she is granted access to rights to a commons which belongs to everyone.

What is required is to surpass that and define rights and duties directly for collectives, instead of granting rights on the collective object to individuals. It really matters to not consider only property in terms of access or copyright, but also to address the question of the responsibilities of the collective of commoners to take care, contribute and repair the infrastructure of the common-pool resource to be maintained in case of failure or security problem. Monitoring the pollution and fixing mistakes as Wikipedia editors translate well as equivalent to the responsibility of caring in the digital area. But if Wikipedia production is distributed, its technical infrastructure is centralised. Is there an equivalent treatment for an infringement somewhere in the nodes of the collective for distributed service such as Wuala or informal communities mesh networks? Maybe the transformation into commons (instead of exclusive property or ownership) through copyleft licenses applied to copyrightable intangible works and extended to open hardware (Söderberg, 2013) could be used as a framework to extend the legal hack which has been operated to copyright to other rights or legal concepts such as liability or legal person, and distribute them.

Creative Commons licenses organise a private ordering of a bundle of rights in copyright (Elkin-Koren, 2005), segmenting the right of access (equivalent to Roman category of *usus*), reproduction, derivation, commercial exploitation (or *fructus*) and exclusion (or *abusus*), the latter being neutralised by the Share Alike clause. Distributed property, with the legal hack of the copyleft clause, started from the need to maintain distributed production in the commons in order to avoid exclusion and private enclosure (as defined by Boyle, 2003). But the organisation of shared property relies on the decision of the licensor, an individual person with exclusive control, comforting “an author-centric individualism” and an “implicit adoption of liberal legalism: a perspective on the social world that privileges the rights of individuals over the claims of any social group” (Barron, 2014). The smallest denominator across the various licenses, a non-commercial verbatim sharing grant, can be interpreted it as a concession of rights by the licensor. Exceptions to exclusive rights, fair use or fair dealing secure better collective rights in the sense they are taken out of the bundle of rights available to the original author. Copyleft licenses can also be seen as “societal constitutionalism” as defined by Teubner, and as “an example for civil society appropriating a legal regime in order to protect the conditions of its own autonomy” according to Wielsch (both cited in a conference report by Steinbeis, 2013).

3.2 Network Science and the Agency of Collectives

Distributed ownership can be arranged by copyleft private ordering, guaranteeing rights to the collective. But the governance of the usage, even if all aspects of the bundle of rights are well considered, does not solve the question of the provision and the maintenance of the resource, otherwise it will not be produced or nurtured and available in the first place. Therefore, it is necessary to reason in a systemic way and also consider how other rights and duties may be assigned to collectives. Network science provides examples of distributed responsibility or allocation of responsibility to other entities than individuals.

Literature in law and artificial intelligence has been considering rights of non-humans electronic agents (Teubner, 2006) and the intentionality of software agents (Sartor, 2009). For electronic contracting, a solution to avoid a vacuum in contract law is “to combine the quasi-actions of the non-human contract partner with the actions of an individual person or an organization, usually the owner of the non-human, and to attribute contractual acts – meeting of minds, breach of contract, performance – to this socio-technical ensemble, safely hidden behind the screen of the well-acquainted juridical person” (Teubner, 2006, p. 506). But the reasoning is still based on the

singularity of one juridical person. If a non-human cannot be held liable, the manufacturer or the owner could be, which does not translate well for distributed storage or mesh network if the activity of hosting or providing the access is fragmented and in the absence of centralised ownership or governance of the service by a company or a non-profit or a municipality with a representative having a singular legal personality. And for manufacturing, these technologies can be easily replicated and re-developed by others, or mirrored and hosted elsewhere, all the more if they are free or open source software.

Current legal rules applicable to distributed platforms and networks, being privacy, tort or ownership, have been developed for firms and individuals rather than for distributed communities and fragmented data. There is no legal theoretical framework to take into account hybrid and evolving networked communities. Regulating mesh wireless network for infringement by fragmenting the liability among identifiable nodes requires trust within a community. *In solidum* obligation would require to spread the liability among different members of the network instead of having a single person (the owner or the coordinator) to be held responsible for the entire network. But I already explained that holding nodes accountable for the traffic of a wireless network is an arbitrary decision which is not sustainable (another more simple option would be the absence of regulation and police with the collective tolerance or acceptance of infringements). So, if the traditional approach to allocate responsibilities cannot be applied, should we look for an alternative system to the tort logic which is looking for responsible individuals? Or should the system be rethought entirely if the traditional notion of liability is not sustainable and another model developed to organize risk and distribute liability? Networks have been envisioned as connected contracts¹¹ rather than legal categories (Teubner, 2011), raising the question of where to transfer the risk in this form of cooperation and complex relations. An approach could be the development of collective insurances, voluntarily paid by the members of a community to cover the possible risk of trial and losses by users, but it is just a coping mechanism reproducing the logic of a single individual or a group of single individuals jointly found liable. Mechanisms of commons-based mutualisation have been developed to redistribute monetary gains of the sale of a music platform¹² according to commons-based governance mechanism. I interpret it as an adaptation of the collective management observed for commercial music and organised by civil societies often with a public monopoly, where part of the sums collected for private copying in some countries are dedicated to creation funds managed by collecting societies. Instead, the remunerations collected from commercial use are to be redistributed according to a collective decision on to which future project to finance with this money collected from past projects. This collective fund could serve to pay for fines and be a sort of commons-based insurance funded by an entry fee to join the platforms which would not be free but reserved to members. But this modality does not take into account the evolving, anarchic nature of the moment when nodes are and are not sharing their connexion.

If the malicious intentionality of the collective can be hard to demonstrate for the distributed platforms besides the peer-production of a performant and autonomous service, is the definition of plural persons less problematic? Collective actors and collective conscience have been the subject of many studies. A state will become a collective actor because of its capacity for action, rights and

¹¹German Civil Code Bürgerliches Gesetzbuch (BGB) §358 organises connected contracts in consumer law, with good faith in contract. http://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p1260

¹²Such a commons-based mutualisation model has been implemented in 2007 to share the revenues of the sale of music on the platform Pragmazic, a project of the Musique Libre non profit organisation (dogmazic.net)

- ¹²“we only distribute labels releasing works under open licenses (Creative Commons, Copyleft) ;
- ¹²albums are available for download in CD quality with no DRM, some are also available in CD format ;
- ¹²65% of retail price (excluding tax) goes to beneficiaries ;
- ¹²17,5% goes to a free music support fund ;
- ¹²17,5% goes to the platform”

¹²From <https://web.archive.org/web/20070521101640/http://www.pragmazic.net/bin/accueil.php>

responsibilities (Luhmann as recalled in Teubner, 2007), but can this self-referring definition be applied to distributed architectures if no node is indispensable to perform an action which cannot be identified or attributed to the guilty person requesting it because of the fragmentation of the data among peers cooperating blindly? The lack of intentionality of computers is not a barrier to contract formation¹³ (Solum, 1992), but in contract law, “agents are supposed to dispose of a certain decisional autonomy” (Teubner, 2007), which is not the case for the participation to a distributed project where the peers do not review what they participate to help circulating. The answer may be further searched in the concepts of actants and hybrids (Latour, 2004): “In hybrids, the participating individual or collective actors are not acting for themselves but are acting for the hybrid as an emerging unit, the association between human and non-humans”. So are Wuala and mesh networks hybrids? If they don't know what they are carrying, there is no a common will or common action, so they do not form an association.

Lindahl (2013) has been looking for “a theory of law in the first-person plural”: the definition of the “we” of a cyber-community can be found in the Declaration of Independence of the Cyberspace (Barlow, 1996), which is “potentially everyone; not, however, as an aggregation of individuals but rather as a whole, as a collective that acts jointly”. This relies on the distinction operated by Margaret Gilbert between “we, each” and “we, together”, with opposed functions as “aggregative” vs “integrative” in a joint collective action. She refers with the latter to bird watching or making music. Can the joint provision and usage of distributed storage or connectivity be found under the same banner? According to her, this plural subject can be found when “One is willing to be the member of a plural subject if one is willing, at least in relation to certain conditions, to put one's own will into a 'pool of wills' dedicated, as one, to a single goal (or whatever it is that the pool is dedicated to)” (Gilbert, 1996) and group intention can be found when several persons are “jointly committed to intending as a body to do A” (Gilbert, 2000, p. 22), therefore the peer-production on distributed platforms could be considered as that action. But if there seem to be a plural subject, a joint collective action and group intention, does it automatically lead to collective and distributed responsibility?

The concept of collective responsibility has been discussed in relations to horrors committed during wars (Smiley, 2011): “Does it makes sense to distribute collective responsibility in general? Is it appropriate to hold individual group members morally responsible for harm that other group members caused? that the group itself caused? that the group as a whole failed to prevent? (...) Only particular kinds of groups are capable of acting and intending collectively and (...) are capable of being collectively responsible for harm”, which means, to have agency:

1. Nations and corporations which have a single representative legal person, thus a centralised decision-making body. This doesn't apply to distributed storage and community mesh networks to the extend their governance is also distributed and not top-down structured around a legal person (which will be the case for mesh network provided by a municipality).

Smiley continues with the question of collective responsibility for past generations with an interesting hypothesis: the US does not recognize slavery as a genocide and does not pay any reparations as a liberal individualistic society, while Germany has been paying reparations as a State to other States for WWI and to Jewish people for WWII. Thus, could the liberal individualism conception which lays deep inside of legal paradigm prevent the conceptualisation of collective responsibility?

2. The second group with collective intention and responsibility are social movements where members have a collective interest. Collective intentionality can be found in such subjects lacking of legal personality: social movements share a political agenda, but they lack of rights or duties. Therefore, individual members will be prosecuted by the state in order to try to stop the movement, with all the unfairness which may derive from that for the ones who will get caught.

¹³Section 14 of the US Uniform Electronic Transactions Act

When joining a distributed project like Wuala or hosting a Tor node to facilitate anonymous connexion, contributing people have no way of knowing whether their fragmented contribution to the network will help a political dissident, a cybercriminal, a privacy-concerned individual or someone downloading music. Therefore, it is questionable whether joint commitment or responsibility or contract may be applicable and helpful notions in the quest of distributed legal persons, rights or duties.

4. Looking for Metaphors for a Distributed Law

In the same way the information society is grounded in social imaginaries (Mansell, 2012), law needs to develop metaphors and narratives to be able to conceptualise what may be unthinkable. The recognition and the protection of the commons is difficult because they are empty spaces lacking of a definition (Milun, 2011). The collective is conceptualised in other disciplines, where complexity has been applied: the multitude of Deleuze and Guattari, the collective intelligence of Pierre Levy). It is possible to hack the law to make existing categories fit a new purpose, for example copyleft against enclosure, or *throuple* in the US, one marriage and an additional contract to bind the couple with the third person and give a legal protective status to a polyamory relation of three persons as close as possible to marriage. But is still difficult to apply the concept of collective directly into law. It is not surprising that the commons are invisible spaces which western law has a hard time thinking. The material foundations of legal norms, such as the concepts of territory and exclusive property, are being challenged by the global commons, which international law is failing to protect against enclosure (Milun, 2011); beyond peer-to-peer filesharing, international law is failing to protect global commons which are being invaded by technological innovations: the sea is depleted by industrial fisheries, space is polluted by satellite garbage, genetic material and biodiversity are privatised by patenting. These commons are treated as *res nullius* that belong to noone rather than *res communes* which belongs to everyone (Milun). In the realm of copyright, the notion of public domain is hard to conceptualise as a positive space with rights and only Chile has a definition of the public domain in positive law (Dusollier, 2011). According to Mattei about the reform on the governance of water in Italy, transforming a private good into a common good is impossible because the neoliberal order is supported by the legal system:

“The basic problem is that the neoliberal political order – and particularly the system of law – favors private property rights and the corporate sector. “No matter whether you are a revolutionary or reformist, the neoliberal order is biased toward the private. The law makes it extremely easy to privatize resources. If you are a municipality and want to sell your water company, you will find it very easy from a legal point of view. But there are no laws in the Italian legal order that shows you how to go the other way around. (...) It took us a year and half of hard work and research to reinterpret the Italian legal code in such-and-such a way that we could make a legal argument for the transformation of a private resource to public control. You need a good argument to get around the logic of neoliberal law and make the case that it is not serving the collective good.” Mattei said that his challenge was, “Can you convince a judge that your interpretation is a good one, especially when it is clearly outside of the law? Let’s face it. The transformation of the Naples [water management] corporation into a public entity was, technically speaking, illegal. It depended on a very expansive interpretation of the law.” That was possible only because the court was willing to regard the referendum results as compelling evidence of the public will, and thus to approve the re-publicization of the Naples water system. For a corporation, the market is theoretically the agency of control. Once you get to a commons, there is no formal agency of control – so you need to create one. This is where we are now.” (Mattei, 2013)

Still, there are other examples of collective thinking in the law. The movement of *Buen Vivir* constitutes an alternative paradigm to capitalism individual rights to own, collective rights of nature, culture and communities. With the *Pachamama*, the Bolivian government has also been recognising rights to Mother Earth (*Ley de Derechos de la Madre Tierra*), conceptualised as a person, but representing the interests of the collective. There are also some collective rights enacted in the second and third generation of human rights, but they are more difficult to conceptualize than individual human rights and they are at the end assigned to individuals as part of groups: right to culture, right to housing, right of collective action to an organisation which as another individual entity representing a collection of individuals. It will be useful to consider in further research to grasp concepts needed to distribute the law around the following experiences: cooperatives in Argentina; *res communis* spaces of the planet and UNESCO World Heritage Convention; mechanisms of traditional knowledge and folklore (Chen, 2011), anarcho-communism and the control of resources and production means by local communities; experiences of *autogestion* in Zapatism, in Barcelona; social center law as a collective law through re-occupation and re-enactment, the right of residence for squatters as a collective through occupation of vacant, abandoned rather than through ownership¹⁴ (Finchett-Maddock). It is likely that a distributed law based on common ownership (not on collective ownership by a corporation or a cooperative representing a sum of individuals) will be different from self-management of cooperatives, or social centers, or of the commons as self-governance method for deliberation and decision-making (and the communal management of resources, being commons-based peer-production, the CBPP Benkler or of common-pool resources, the CPR of Ostrom). Nevertheless, they can be useful sources of inspiration and provide metaphores to conceptualise collective persons, rights and duties.

Conclusion

The legal western system is grounded on the individual (private or public) person, while there is a need for cultural change from neoliberal paradigm to recognise community rights and duties and collective persons as opposed as individual persons. Indeed, I demonstrated in this article that applicable law and legal theories are not capable to address commons-based distributed collective endeavours where actions, data and persons are fragmented. The fall of the individual, or of the individualisable person as unique, centralised point of reference, seem to be the only solution to organise the rise of the assignment of legal personhood, and therefore rights and duties, to such communities. To accommodate this evolution of the legal regulation and address socially valuable forms of distributed peer-production, transformation is needed at the level of the state and its positive law, not only at the community- (the movement of the commons and its self-governance rules) and market-level (crowdsourcing and the insufficient self-regulation of services like Über or Airbnb). To conclude and borrow Wielsch, “Don’t occupy the system, occupy the law!” (Steinbeis, 2012).

References

Aigrain, P. (2012). *Sharing: Culture and the Economy in the Internet Age*, Amsterdam University Press.

Antoniadis, P., Le Grand, B., Satsiou, A., L. Tassioulas, R. Aguiar, J.P. Barraca, and S. Sargento, (2008). *Community building over Neighborhood Wireless Mesh Networks*, IEEE Technology and Society.

¹⁴ Former section 6 of the UK Criminal Law Act 1977.

Antoniadis, A. and Le Grand, B. (2009). Self-organized virtual communities: Bridging the gap between web-based communities and p2p systems, *International Journal of Web-based Communities (IJWBC)* 5(2).

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*.

Barron, A. (2014), *Intellectual Property and the 'Open' (Information) Society*, in David, M. and Halbert, D. (ed.), *The SAGE Handbook of Intellectual Property*, Sage.

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale University Press.

Boyle, J. (2003). *The Second Enclosure Movement and the Construction of the Public Domain*. *Law and Contemporary Problems*, Vol. 66, pp. 33-74, Winter-Spring 2003.

S.M. Chen, P, Lin, D-W Huang, S-R Yang, (2006), *A study on distributed/centralized scheduling for wireless mesh network*, *Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing*, pp 599 - 604. Vancouver, British Columbia, Canada.

Chen, Shun-Ling, *Collaborative Authorship: From Folklore to the Wikiborg* (Apr 29, 2011). *Journal of Law, Technology and Policy*, Vol. 2011, No. 1, 2011.

De Filippi, P., Dulong de Rosnay M., Bourcier D. (2013). *Democracy-by-design: Distributed architectures as a tool for distributed democracy*, *Conference Democracy and Technology. Europe in Tension*. Sorbonne University Paris IV, 20-9-2013.

De Filippi, P. (2013). *Flawed cloud architectures and the rise of decentralised alternatives*. *Internet Policy Review*, 2(4).

Dulong de Rosnay, M. (2013). *Peer-production online communities infrastructures*, *ACM Proceedings of the First Conference on Internet Science*, Brussels, Belgium, 10-11 April 2013, pp. 65-68.

Dusollier, S. (2011). *Scoping Study on Copyright and Related Rights and the Public Domain*, CDIP/7/INF/2), *Committee on Development and Intellectual Property of the World Intellectual Property Organisation*

Easterbrook, Frank H. (1996). *Cyberspace and the Law of the Horse*, *University of Chicago Legal Forum*.

Elkin-Koren, N. (2005). *What Contracts Can't Do: The Limits of Private Ordering in Facilitating a Creative Commons*. *Fordham Law Review*, Vol. 74.

Elkin-Koren, N. (2006). "Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic." *New York University Journal of Legislation & Public Policy*, 9 (15), 15-76.

Finchett-Maddock, L. (2011). *Observations of the Social Centre Scene: How a Law is Performed through Archiving the Memory of the Commons*. PhD Thesis.

Gilbert, M. (2nd ed. 1992), *On social facts*. London, New York: Routledge, (1989, reprinted 1992).

Gilbert, M. (2006). *A theory of political obligation*

Giovanella, F. (2014). Tort Liability, Uncertainty and New Technologies: The Case of Wireless Community Networks, Second Biennial Meeting of the International Research Network on Technological Innovations, Uncertainty and the Law of Civil Liability.

Hatcher, J. (2007). Mesh Networking: A look at the legal future. 11:5 Journal of Internet Law 1. Preprint available at SSRN: <http://ssrn.com/abstract=814984>

J. Jun, M.L. Sichitiu (2003). The nominal capacity of wireless mesh networks, IEEE Wireless Communications, vol 10, 5 pp 8-14. October 2003.

Latour, B. (2004). Politics of Nature: How to Bring the Sciences into Democracy, Harvard University Press.

La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Office of the United Nations High commissioner for Human Rights, 22 p. <http://www.article19.org/data/files/pdfs/reports/report-of-the-special-rapporteur-on-the-promotion-and-protection-of-the-right.pdf>

Lessig, Lawrence (2001). "The Law of the Horse: What Cyberlaw Might Teach". Communications Law and Policy: Cases and Materials, by Jerry Kang (New York: Aspen Law and Business)

Lindahl, H.K. (2013). We and cyberlaw: The spatial unity of constitutional orders. Indiana Journal of Global Legal Studies, 20, 697-730.

Mansell, R. (2012). Imagining the Internet: Communication, Innovation, and Governance, Oxford University Press.

Mattei, U. (2013). Economics, Nature and the Commons. A report on an international conference on the future of the commons. Organized by the Heinrich Böll Foundation, Commons Strategies Group, Charles Léopold Mayer Foundation and Remix the Commons, Berlin, Germany, May 22-24, 2013. http://www.boell.de/sites/default/files/ecc_report_final.pdf

Milun, K. (2011). The Political Uncommons. The Cross-Cultural Logic of the Global Commons, Ashgate.

Mowbray, M. (2009). The Fog over the Grimpen Mire: Cloud Computing and the Law. SCRIPTed Journal of Law, Technology and Society vol 6 issue 1, pp.132-146.

Musiani, F. (2013). Nains sans géants. Architecture décentralisée et services Internet, Dwarfs without giants. Decentralized architectures and Internet-based services. Paris, Presses des Mines.

Musiani, F. (2014). Decentralised internet governance: the case of a 'peer-to-peer cloud'. Internet Policy Review, 3(1).

Rodotà, S. (2013). Constituting the Commons in the Context of State, Law and Politics, Economics and the Common(s): From Seed Form to Core Paradigm. A report on an international conference on the future of the commons. Organized by the Heinrich Böll Foundation, Commons Strategies Group, Charles Léopold Mayer Foundation and Remix the Commons, Berlin, Germany, May 22-24, 2013. http://www.boell.de/sites/default/files/ecc_report_final.pdf

Sartor, Giovanni (2009). Cognitive automata and the law: electronic contracting and the intentionality of software agents, *Artificial intelligence and law* (0924-8463), 17 (4), p. 253.

Orsi, F. (2013). Elinor Ostrom et les faisceaux de droits : l'ouverture d'un nouvel espace pour penser la propriété commune, *Revue de la régulation*, 14(2).

Ostrom, E. (1990). *Governing the Commons. The Evolution of Institutions for Collective Action*, Cambridge University Press.

Schollmeier, R. (2001). "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications." *Proceedings of the First International Conference on Peer-to-Peer Computing*, 27–29.

Söderberg, J. (2013). How open hardware drives digital fabrication tools such as the 3D printer. *Internet Policy Review*, 2(2).

Smiley, M. (2011). Collective Responsibility", *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (ed.).

Solum, L.B. (1992). Legal Personhood for Artificial Intelligences, *70 North Carolina Law Review* 1231-83, 1267.

Steinbeis, M. (2012) *Occupy the Law!*, Report of the Conference on Transnational Societal Constitutionalism, *Frankfurter Allgemeine Zeitung* and *VerfBlog*.
<http://ww.verfassungsblog.de/occupy-law>

Teubner, G. (2006), *Rights of Non-Humans? Electronic Agents and Animals as New Actors in Politics and Law*. *Journal of Law and Society*, Vol. 33, pp. 497-521.

Teubner, G. (2007), *In the Blind Spot: The Hybridization of Contracting*. *Theoretical inquiries in law* (1565-1509), 8 (1), p. 5.

Teubner, G. (2011), *Networks as Connected Contracts*, Hart Publishing.

von Lohmann, F. (2004). Symposium *Tracking Pirate in Cyberspace*, 24 *Loyola of Los Angeles Entertainment Law Review* 73, 98.

Acknowledgments

This work is partially supported by the French ANR (Agency for National Research) through the participation to the ADAM interdisciplinary project on Distributed Architectures and Multiple Multimedia Applications (<http://adam.hypotheses.org/>) and the Framework programme FP7-ICT-2013-10 of the European Commission through the project P2Pvalue (grant no.: 610961).

I first presented on the impact of distributed technologies on the law during ADAM internal seminars and I am grateful for discussions with partners of these projects, especially Danièle Bourcier who introduced me to the various relations between law and technology, Francesca Musiani who introduced me to distributed architectures and Primavera De Filippi with whom I am also working on both projects. My first presentation on a distributed law was at an internal seminar at LSE and I am grateful to the colleagues of the law and media departments for their comments.