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

Melanie Dulong de Rosnay

HAL Id: halshs-01103885

https://shs.hal.science/halshs-01103885

Submitted on 15 Jan 2015

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

Melanie Dulong de Rosnay

Abstract:

This article positions itself beyond the tension between copyright enforcement to preserve business models vs users' rights to access knowledge which are required to enjoy the opportunities provided by the disruptive technology. Instead of only applying law to peer-to-peer in order to control networks, and without implying that because a law is currently unenforceable, it should not exist, I propose to consider another angle of the relationship between law and technology, by applying peer-to-peer to the law, to introduce the argument of the distribution of 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 some of their technical features. This will lead to another kind of relationship between law and technology: after the control of technology by the law, which absorbs the new technology by expanding its scope of application, and in addition to the scholarship on regulation by code or of code (Lessig 2006; Brown & Marsden 2013) the law itself can try to integrate the technology. It might do so 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.

Keywords:

by Melanie Dulong de Rosnay, Permanent Researcher at the French National Centre for Scientific Research (CNRS) Institute for Communications Sciences & Visiting Fellow at the London School of Economics and Political Science Department of Media and Communications

Introduction

The relationship 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 this new type of activity. A polarised discourse leads copyright law to be extended to prevent file-sharing from disrupting existing business models based on the 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 users' rights. This relationship between law and technology assumes that the law must be adapted to take into account new forms of cultural practices – either to forbid them or to legalise them – and has been observed when there have been previous changes caused by peer reproduction to the distribution medium, what Walter Benjamin calls mechanical reproduction. Both ways to adapt the law to the technology entail that the law tries to control the technology, either negatively by outlawing certain behaviours, or positively by recognising them. Eventually, after a period of conflict between established rights-holders of the old technology disrupted by a new technology (mechanical piano, radio, VCR, etc), the law reconfigures itself by creating an exception to exclusive rights, to open up the system and accept the new reproduction technology. With peer-to-peer distribution, new forms of compensation can be considered. Propositions of creative contribution (Aigrain 2012) favour the concept of peers contributing to the creative process in a redistributed manner, instead of relying on the centralisation of a collecting 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 to access knowledge which are required to enjoy the opportunities provided by the disruptive technology. Instead of only applying law to peer-to-peer in order to control networks, and without implying that because a law is currently unenforceable, it should not exist, I propose to consider another angle of the relationship between law and technology, by applying peer-to-peer to the law, to introduce the argument of the distribution of 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 some of their technical features. This will lead to another kind of relationship between law and technology: after the control of technology by the law, which absorbs the new technology by expanding its scope of application, and in addition to the scholarship on regulation by code or of code (Lessig 2006; Brown & Marsden 2013) the law itself can try to integrate the technology. It might do so 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' rights and duties. The fictional notion of the individual person includes the citizen and the user, matching the notion of a real human being, 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. But this legal theoretical conception does not adequately take into account the concept of communities of peers, defined as non-stabilised, evolving, or non-formalised groups sharing a common interest or an *ad hoc* production purpose; from local communities (e.g. those using a commons-based governed fishery, compare Ostrom (1990) with Bessa (2013)) to online communities (e.g. the users of a platform) which do not have a legal status as an individually identifiable legal entity.

Law, as a technology of regulation, can be disrupted by peer-to-peer, not only in order to evolve to apply to new objects, but also in the sense that legal thinking can be influenced by its architectural design principles based on decentralisation. Peer-to-peer networks, sources of peer production of content or services, as disruptive online technologies, reconfigure the frontiers and assumptions of existing legal categories. Collective mechanisms of governance and ownership by peers are identified in the tradition of the natural commons (Ostrom 1990), of social movements and for the recognition of local communities' rights. They offer not only a political alternative, but also a theoretical break from envisaging the individual person as unique point of reference for the regulatory system composed of positive law and policies targeting individuals, and can bring this system towards the recognition of collectives as subjects, or holders,

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. The 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. I do not consider peer-to-peer as a way to fulfil individual needs. Here, I choose to focus on two specific instances of peer production to develop my argumentation: peer production of storage and peer production of connectivity.

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 question whether the law could integrate the architectural features of distribution from the inside of its categories in order to attempt to better regulate distributed technologies. Peer-to-peer ways of thinking about – and designing – the law are already being developed by the political movement of the commons and by network theorists. I consider in section 3 such attempts to design collective rights or collective legal persons beyond both a mere individualised law and individualised Information and Communication Technologies. A peer-to-peer law also relates to political theoretic questions of plural persons and the agency of collectives. Yet in order to truly challenge liberal legal design grounded in individualism, I conclude in section 4 with the need to develop metaphors and social imaginaries (Mansell 2012) to conceptualise empty spaces which are difficult to envision (Milun 2011), and contribute to the definition of distributed forms of ownership, responsibility or liability as examples of the integration of peer-to-peer as a principle for the design of law.

1. The Impact of Distributed Architectures on Legal Liability

The architectural design of peer-to-peer challenges conventional legal reasoning and the usual application of concepts such as property or the assignment of legal responsibility, because files and actions are fragmented, distributed between nodes hosted by peers, rather than directly attributable to individuals. Peer-to-peer networks rely 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 differs 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 constitute commons-based peer production (Benkler 2006).

Many technologies are designed according to distributed, decentralised principles. Distributed architectures are considered as social technologies, in the sense they allow peer production and achieve a common goal or satisfy individual needs through coordination of shared resources. The following presentation of distributed architectures draws from and builds upon the introduction of Musiani (2013). Instead of 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 does not exist; instead, applications rely 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).

For the sake of theoretical reasoning I will ignore these implementation considerations and focus instead on the distributed aspect of peer-to-peer architectures: how it may impact on the application of the law (section 1) and how it 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 the 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 others. 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 legal fictions of individualisable and individualised actions, objects and persons.

1.1 Distributed Storage

An example of peer-to-peer technology disrupting the law is Wuala, a case study analysed by Musiani (2013; 2014). Wuala, initially developed at the Swiss Federal Institute of Technology (ETH) in Zürich, is a distributed storage service, like Dropbox, except that the 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, it also features more traditional cloud data server modalities of hosting (Mowbray 2009). For the sake of argumentation, I will only consider the peer-to-peer portion of the service which could theoretically be used on a standalone basis without additional storage in the application's centralised cloud server. Even if it is not the best product from a marketing or usability point of view, the distributed part of the service is the relevant socio-technical arrangement and legal tendency for my observations.

When uploaded to 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 in its entirety, it is questionable whether contributory or induced liability would be triggered at all, if a file contains illegal content. Unlike BitTorent, peers do not know what they are hosting as the files, after being fragmented, are encrypted.

Besides, the service cannot technically monitor what is being uploaded because of the distribution of the process. There are similar instances of the technical impossibility for technology providers of revealing content – such as unlocking an encrypted iPhone – but the ability and legal responsibility to hand over data, for instance in case that a warrant is issued, still applies to Apple's centralised cloud architecture. External entities (such as major players in the entertainment industry and the police) are also not able to proceed to surveil the files. Indeed, at no time do the files exist in a reconstituted format – making them readable and perceptible to the senses – outside of the machine of the first peer, who uploads it bit by bit 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 even to detect guilt in the mere transient 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 contain holiday photos for back up purposes, copyrighted books, personal data, potential revenge porn or harmful content. And none of the nodes is essential since redundancy allows usage in other ways if one is missing or offline, diminishing responsibility even more.

A second version of Wuala added an aspect 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 being hosted, except if they manage to break the encryption – which is not currently possible, technically speaking. Therefore, no Digital Millennium Copyright Act notice-and-take-down procedure or Electronic Commerce Directive Internet Service Provider liability could apply, as the reconstituted content would never be visible nor made public: illegal content would remain unnoticed so there would be no means to notify of 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 process of justice as it would not reveal 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 would be intimidation (for instance, Lavabit, an encrypted email service provider, decided to close the service rather than giving over its encryption keys, but Wuala does not know the password of its users). Another more radical option is outlawing distributed services as a technology. This regulatory move would have a chilling effect and prevent legal activities, in the same way peer-to-peer filesharing protocols can be used both to download free software, public domain works or unauthorised content. But unlike Dropbox (which is hosting the files and does not permit the storage of certain files which might be copyrighted so that the service is not 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. Indeed, the encryption is performed locally on the user's machine before the fragments get duplicated and hosted on the hard drives of other peers.

For example, The Pirate Bay has an index of links to available torrents, which can be legally problematic in some jurisdictions, and offers a means of technical control through a blocking order being sent to Internet Service Providers on the request of the government or major corporate rightsholders. The level of decentralisation matters: if only the delivery is distributed but the production remains centralised, the service will be vulnerable to this kind of legal action. But as there is no such centralised information on the torrents of the files for Wuala — acting as a distributed private storage cloud — there is no such option to remove or block a page with links to the content, or to ascertain which file fragment belongs to which user.

Musiani (2013) speaks about a 'shared techno-legal responsibility'. Crowd-sourced infringement management or distributed policing can work in the case of harmful content (e.g. child porn) disseminated on Facebook because a user can report the content in one click. Copyrighted images on Wikipedia can effectively be removed by patrols of editors who want to protect this commons-based peer production from legal liability. But private policing without accountability presents risks of discrimination and it seems unlikely that user self-regulation could 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 application's terms of service would probably not be helpful against a legal attack. Ethical considerations – such as community monitoring, or a commitment to host only lawful content – can be useful for auto-regulation to police a service and ensure its sustainability as a commons, as demonstrated by Ostrom Institutional Design Principles #4: 'Effective monitoring by monitors who are part of or accountable to the appropriators' and its complement'; and #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, then it seems very unlikely that a feeling of community responsibility could be developed.

Similarly, it is doubtful that liability could be assigned either to the service provider (except in the case that peer-to-peer technologies would be outlawed altogether), or to some nodes. Legal regulation has not yet reached that level of control, even if attempts have been made, such as the French Hadopi law which tried to hold users liable for not securing their internet connection and allowing other users to perform infringing activities using 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 an unknown nature. Judicial proceedings for negligence to secure wireless connections have occurred both in France with 'three strikes' 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 altered or spoofed, cannot be held to be an accurate identification of an individual.

1.2 Wireless Mesh Networks

Mesh wireless technology (Jun et al. 2003; Chen et al. 2006) makes it even more difficult to assign liability to an IP address, as an IP address 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 The Onion Router (Tor) distributed browser, ensuring the routing of communications through a network of nodes hosted by peers masking the IP address. The implication of such architecture is privacy by design (De Filippi et al. 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 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 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 may or may not be connected to the Internet, and communication can be organised either around a central server or in a decentralised way, as studied in this paper. One node will only transmit to the next node. In order to avoid secondary liability for the actions of other users of one's internet connection, in the jurisdictions where it exists, it is possible to use a VPN, and this is the case with the freifunk Freedom Fighter box for instance. There is community governance and self-regulation as many networks offering free transmit service commit to certain principles organising the relationship between nodes, such as the Pico Peering Agreement. Yet these agreements are intended to regulate the network's quality of service obligations among peers, and not the potentially infringing activities committed over the network. In applying the law concerning Internet Service Providers' liability, such as the E-Commerce Directive in the EU, to mesh node owners, nodes would not 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 which 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 a community mesh network having an association with a board and legal representatives, or if a node is held by an institution, that association or institution could be held liable for the traffic – but in the case of a distributed architecture without designated responsible persons or contractual relationships, it seems more difficult to enforce the law (De Filippi 2013; Giovanella 2014) – and all the more so when creating a node does not require registration and the overall number of nodes is unknown, in the case of an encrypted mesh network, forming a local darknet. As with distributed storage, allocating liability to individual nodes of the mesh is difficult because 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: 'Holding intermediaries liable for the content disseminated or created by their users 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, p. 12).

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 before the new technical environment manifested and, consequently, 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 also controlling legitimate activities which were previously unregulated. Legal doctrine has demonstrated the extension of the scope of copyright and the chilling effects 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, possibly, to better regulate it.

One way to think about the relationship between law and peer-to-peer technology is to question whether the law needs to be expanded to face a new regulatory challenge. People choose to use and 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)) that has been made to cyberlaw could be made to a law of distributed architecture, questioning its singularity and its *raison d'être*. Alternatively, if distributed architectures are unique, then we are facing the emergence of new legal categories that will produce new norms. But beyond the fact that these technologies may be used for both legitimate and illegal purposes and that the fragmented nature 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 (Fuster Morell 2012; Bailey & Mattei 2013). They all propose the peer production of a service as an alternative to the commercial centralised services exercising control over their users. Even if the increased technical effort required to set them up (as opposed to the ease of installation of their commercial counterparts) may prevent their mainstream takeoff, they form a contribution to user 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 rely on the contractual relationship between two individual entities (the corporation and the user), allowing the allocation of responsibility in cases of infringement. Instead, the latter services are not provided by an individual person; rather, they are offered by a mesh of nodes which ensure collectively that the service is possible, each providing a fragment of it, which is difficult or impossible to monitor technically and control legally. Distributed architectures fragment data and actions, thus challenging 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 technically insignificant fragments, while the law allocates rights and responsibilities to individual persons.

Individual legal entities are the basis of legal reasoning and the subjects of rights. Western legal systems tend to mostly recognise rights only of individuals, to protect their rights of private property, their commercial interests and personal freedoms. Law assigns rights to individuals (which can be states, corporations or non-profits) benefitting from autonomy and agency. Law arranges 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 among actors which are neither localised not stabilised, as the same peers are not necessarily present at all points in a given process of data communication.

I posit that this distribution of actors and actions requires a rethinking of legal categories, since the notions of the author of an action, action and content or object are no longer tangible units, but aggregated, open-ended 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. On this last question, my understanding is that fragmentation of actions between an unfixed network of peers at least blurs responsibilities and at most makes it an irrelevant concept.

Which method of ascertaining 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 in a future scenario. It might be the case that if no one entity is found liable, legal responsibility may lie with any identifiable entity related to the case. The reconfiguration through cooperation of the notion of individuals forming a collective triggers a deconstruction of legal categories in several domains: copyright, liability, cybercrime, processing of personal data, but also data security – in the case of service failures and data losses, it is not certain that a warranty disclaimer would be valid vis-à-vis consumer protection laws. No contractual relationship can be deduced: since users are unknown and unstable, the performance of the service depends on who is connected at what time, but none of the individual nodes is in itself essential. 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 data packet is circulating, and if the packet can take a different route 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 it. 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

Since 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 of common or shared property (Orsi 2013), which constitutes an alternative to exclusivity through individual private property and unregulated open access to *res nullius* thought negatively as inappropriable. Before the enclosure of the land, property was attached to utility, with different usage rights (De Moore 2009) and natural common-pool resources were 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 by the 19th century, the US doctrine of legal realism on fragmented property introduced doubt into pre-existing legal categories, describing property not as an absolute right but as a collection of social relations, rights, duties, obligations and responsibilities – see the [table](#) of eleven rights by John Commons (1893) in *The Distribution of Wealth*, reproduced by Johnson (2007), cited by Orsi (2013).

More recently, water in Italy has been the theatre of a movement of constitutionalisation of the commons to exclude both privatisation and nationalisation. Stefano Rodotà has called 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 common goods. A more profound legal epistemological turn transposed into distributed architectures studied in the previous section would depart from citizens as individual commoners, to start considering the actions of peers as operating in a collective of a different nature than the aggregation of individuals. With water as a commons, the epistemological transformation affects 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 over the collective object to individuals. An important step lies in not considering only property in terms of access or copyright, but also addressing 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 the case of failure or a security problem. Monitoring pollution and fixing mistakes as Wikipedia editors is the digital equivalent to the responsibility of caring. But if the production of Wikipedia 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 community mesh networks? Maybe the transformation into commons (instead of exclusive property or ownership) through copyleft licences applied to copyrightable intangible works and extended to open hardware (Söderberg 2013) could be used as a framework to extend this legal hack of copyright to other rights or legal concepts such as liability or legal person, and distribute them.

Creative Commons licences 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 licences, a non-commercial verbatim sharing grant, can be interpreted 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.

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 would not be produced or nurtured – and available – in the first place. Therefore, it is necessary to reason in a systemic way and also to consider how other rights and duties might be assigned to collectives. Network science provides examples of distributed responsibility or allocation of responsibility to entities other than individuals.

Literature in law and artificial intelligence has considered the rights of non-human 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 organisation, 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).

However, 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 networks 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 – be it 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 wireless mesh networks for infringement by fragmenting liability among identifiable nodes requires trust within a community. An *in solidum* obligation would require liability to be spread among different members of the network instead of having a single person (the owner or the coordinator) held responsible for the entire network. However, I have already explained that holding nodes accountable for the traffic of a wireless network is an arbitrary decision and not sustainable (another more simple option would be the absence of regulation and policing 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 logic which seeks responsible individuals? Or should the system be rethought entirely if the traditional notion of liability is not sustainable, and another model be developed to organise risk and distribute liability? Networks have been envisioned as connected contracts 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 insurance, voluntarily paid by the members of a community to cover the possible risk of legal proceedings and losses and fines by users, but this 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 platform according to commons-based governance mechanism. This 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 non profit organisation Musique Libre

(dogmazic.net): they 'only distribute labels releasing works under open licenses (Creative Commons, Copyleft); albums are available for download in CD quality with no DRM, some are also available in CD format; 65% of retail price (excluding tax) goes to beneficiaries; 17.5% goes to a free music support fund; 17.5% goes to the platform'. This seems to be 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 which future project should be financed with the money collected from these 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 that 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 connection.

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 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 culpable 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 formation (see Section 14 of the US Uniform Electronic Transactions Act (Solum 1992)), but in contract law, 'agents are supposed to dispose of a certain decisional autonomy' (Teubner 2007), which is not the case for participation in a distributed project where peers do not review what they circulate through their participation. The answer may be further searched for 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 do not 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 to bird watching or making music when describing the latter. 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 '[o]ne 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 peer production on distributed platforms could be considered as that kind of action. But if there seems 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):

[d]oes 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.

Nations and corporations, the first group to which collective intention and responsibility can be recognised according to Smiley (2011), have a single representative legal person, thus a centralised decision-making body. This does not apply to distributed storage and community mesh networks to the extent that 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 recognise slavery as 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 individualist conception which lies deep inside the legal paradigm prevent the conceptualisation of collective responsibility?

The second group with collective intention and responsibility in Smiley's analysis are social movements (Bailey & Mattei 2013) 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 those who get caught.

When joining a distributed project like Wuala or hosting a Tor node to facilitate anonymous connection, 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 for 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), the law needs to develop metaphors (Larsson 2013) and narratives to be able to conceptualise what may be unthinkable. The recognition and protection of the commons is difficult because they are empty spaces lacking 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 polyamorous relationship of three persons as close as possible to marriage). However, it is still difficult to apply the concept of collective directly into law. It is not surprising that the commons are invisible spaces about 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 no one rather than *res communes* which belong to everyone (Milum 2011). 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, regarding the reform of 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. […] 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 (Mattei 2013, p. 23).

Conclusion

The Western legal system is grounded on the individual (private or public) person, while there is a need for cultural change away from the neoliberal paradigm (Teubner & Negri 2011) to recognise community rights and duties and collective persons as opposed to individual persons. Indeed, I demonstrated in this article that applicable law and legal theories are not capable in addressing commons-based distributed collective endeavours where actions, data and persons are fragmented. The fall of the individual, or of the individualisable person as the 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 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 level (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 borrow Wielsch: 'Don't occupy the system, occupy the law!' (Steinbeis 2012).

Still, there are other examples of collective thinking in the law. The movement of Buen Vivir (Gudynas 2011) constitutes an alternative paradigm to capitalism's individual rights of ownership, with the collective rights of nature, culture and communities (in the case of Pachamama, the Bolivian government has recognised rights to Mother Earth – *la 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 generations of human rights, however they are, in the end, not assigned to collectives but to individuals as part of groups: the right to culture, right to housing, right of collective action for an organisation which is another individual entity representing a collection of individual persons. It will be useful to consider in further research how non-Western legal orders consider the concept of collective vs individual. Concepts needed to distribute the law may be available among the following experiences: *res communis* spaces of the planet (Milun 2011) and the UNESCO World Heritage Convention; mechanisms of traditional knowledge and folklore (Chen 2011); social centre 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 places (contained in the former section 6 of the UK Criminal Law Act 1977) rather than through ownership (Finchett-Maddock 2011).

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 the self-management of cooperatives, or social centres, or of the commons as a self-governance method for deliberation and decision-making (and the communal management of resources, being commons-based peer production, the CBPP of Benkler, or of common-pool resources, the CPR of Ostrom). Nevertheless, they can be useful sources of inspiration and provide metaphors to conceptualise collective persons, rights and duties.

Acknowledgements

References

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

Antoniadis, P, Le Grand, B, Satsiou, A, Tassiulas, L, Aguiar, R, Barraca, J P and Sargento, S 2008. 'Community building over Neighborhood Wireless Mesh Networks', *IEEE Technology and Society Magazine*, vol. 27(1), pp. 48-56.

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*, vol. 5(2), pp. 179-194.

Barlow, J P 1996. 'A Declaration of the Independence of Cyberspace', available from: https://projects.eff.org/~barlow/Declaration-Final.html [Accessed: 10 December 2014]

Barron, A. 2014. 'Intellectual Property and the 'Open' (Information) Society', in David, M and Halbert, D (eds), The SAGE Handbook of Intellectual Property, London: Sage, [forthcoming].

Bailey, S & Mattei, U 2013. 'Social Movements as Constituent Power: The Italian Struggle for the Commons', *Indiana Journal of Global Legal Studies*, Vol. 20(2)

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

Bessa, A 2013. 'Traditional local communities in international law', unpublished EUI PhD thesis, Florence.

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

Brown, I & Marsden, C 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age*, MIT Press: Cambridge

Chen, S L 2011. 'Collaborative Authorship: From Folklore to the Wikiborg', *University of Illinois Journal of Law, Technology and Policy*, Vol. 1, pp. 131-167.

Chen, S M Lin, P Huang, D W Yang, S R 2006. 'A study on distributed/centralized scheduling for wireless mesh network', proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, ACM: New York, pp. 599 – 604

De Filippi, P 2013. 'Flawed cloud architectures and the rise of decentralised alternatives', *Internet Policy Review*, Vol. 2(4), available from http://policyreview.info/articles/analysis/flawed-cloud-architectures-and-rise-decentral-alternatives [Accessed: 6 December 2014]

——, Dulong de Rosnay M, Bourcier D 2013. 'Democracy-by-design:

Distributed architectures as a tool for distributed democracy', paper presented at the Conference Democracy and Technology: 'Europe in Tension', 19-21 September, Sorbonne University Paris IV: Paris

Dulong de Rosnay, M 2013. 'Peer-production online communities infrastructures', Proceedings of the First Conference on Internet Science, Brussels: ACM, 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, U Chi Legal F 207.

Elkin-Koren, N 2005. 'What Contracts Can't Do: The Limits of Private Ordering in Facilitating a Creative Commons', *Fordham Law Review*, Vol. 74(2), pp. 375–422.

—— 2006. 'Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic', *New York University Journal of Legislation & Public Policy*, Vol. 9(15), pp. 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. School of Law, Birkbeck College.

Fuster Morell, M 2012. The Free Culture and 15M Movements in Spain. Composition, Social Networks and Synergies. Social Movement Studies, *Journal of Social, Cultural and Political Protest*, pp. 1–7.

Gilbert, M 2006. *A theory of political obligation*, Oxford University Press: Oxford

——, 1992 (2nd Edition). *On social facts*, Routledge: London, New York

Giovanella, F 2014. 'Liability issues in Wireless Community Networks', paper presented at the Final Symposium of the ADAM project, MINES ParisTech: Paris

Gudynas, E 2011. 'Buen Vivir: Today's tomorrow', *Development*, Vol. 54(4), pp. 441–447.

Hatcher, J 2007. 'Mesh Networking: A look at the legal future', *Journal of Internet Law*, Vol. 11(1), pp. 1-16. Preprint available at SSRN: http://ssrn.com/abstract=814984

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

Larsson, S. 2013. 'Metaphors, law and digital phenomena: the Swedish pirate bay case', *International Journal of Law and Information Technology*, Vol. 21(4), pp. 354–379.

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, available from: http://www.article19.org/data/files/pdfs/reports/report-of-the-special-rapporteur-on-the-promotion-and-protection-of-the-righ.pdf

Latour, B 2004. *Politics of Nature: How to Bring the Sciences into Democracy, Cambridge*, Harvard University Press: MA

Lessig, L 1999. 'The Law of the Horse: What Cyberlaw Might Teach', *Harvard Law Review*, no. 113, pp. 501-546.

—— 2006. *Code and Other Laws of Cyberspace*, Basic Books: New York

Lindahl, H K 2013. 'We and cyberlaw: The spatial unity of constitutional orders', *Indiana Journal of Global Legal Studies* Vol. 20(2), pp. 697-730.

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

Mattei, U 2013. 'Economics, Nature and the Commons', a report on an international conference on the future of the commons, organised by Heinrich Böll Foundation, Commons Strategies Group, Charles Léopold Mayer Foundation and Remix the Commons, 22-24 May, Berlin, available from: 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: Farnham

Mowbray, M 2009. 'The Fog over the Grimpen Mire: Cloud Computing and the Law,' *SCRIPTed Journal of Law, Technology and Society*, Vol. 6(1), pp. 132-46.

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

—— 2014. 'Decentralised internet governance: the case of a 'peer-to-peer cloud'', *Internet Policy Review*, Vol. 3(1). Online: DOI: 10.14763/2014.1.234.

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*, Vol. 14(2). Online: http://regulation.revues.org/10471

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

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. Organised by the Heinrich Böll Foundation, Commons Strategies Group, Charles Léopold Mayer Foundation and Remix the Commons, 22-24 May: Berlin, available from: http://www.boell.de/sites/default/files/ecc_report_final.pdf

Sartor, G 2009. Cognitive automata and the law: electronic contracting and the intentionality of software agents, Artificial intelligence and law 17 (4), pp. 253-290.

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, IEEE, pp. 27–29.

Smiley, M 2011. 'Collective Responsibility', in Edward N. Zalta (ed) *The Stanford Encyclopedia of Philosophy*, available from: http://plato.stanford.edu/archives/fall2011/entries/collective-responsibility/ [Accessed: 6 December 2014]

Söderberg, J. 2013. 'How open hardware drives digital fabrication tools such as the 3D printer', *Internet Policy Review*, Vol. 2(2). DOI: 10.14763/2013.2.138

Solum, L B 1992. 'Legal Personhood for Artificial Intelligences', *North Carolina Law Review*, Vol. 70, pp. 1231-1287.

Steinbeis, M 2012. 'Occupy the Law!', report of the Conference on Transnational Societal Constitutionalism, Frankfurter Allgemeine Zeitung and VerfBlog, available from: http://ww.verfassungsblog.de/occupy-law [Accessed: 6 December 2014]

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(4), pp. 497-521.

——, 2007. 'In the Blind Spot: The Hybridization of Contracting', *Theoretical Inquiries in Law*, Vol. 8(1), pp. 51-71.

——, & Collins, H 2011. *Networks as Connected Contracts*, Hart Publishing: Oxford

——, & Negri, A 2010. 'The Law of the Common: Globalization, property and new horizons of liberation', in J Klabbers, (ed) *Finnish Yearbook of International Law*, Vol. 21, pp. 1-25

von Lohmann, F 2004. 'Tracking Pirate in Cyberspace', Symposia—2003 Stanford Law & Technology Association Conference: Ideas without Boundaries: Creating and Protecting Intellectual Property in the International Arena, *Loyola of Los Angeles Entertainment Law Review*, Vol. 24(1), pp. 73-98.