

Anonymous speech on the Internet

Preliminary remarks¹

The issue of anonymity on the Internet divides opinions. On the one side there are many who maintain that anonymity on the World Wide Web is an essential feature of its nature, and of its freedom.² On the opposite side are those who consider the Internet to be the same as any other public forum, where anonymity can only be the exception, not the rule.

This article aims to show that, from a legal point of view, the situation is extremely nuanced and it suggests a variety of answers which depend from many different, intrinsic and extrinsic, factors.³ One has to underline the legal approach in a field which is fraught with policy issues. Although the law is inevitably influenced by social, economic and political factors, a lawyer must take into account the general framework, suggest answers that are coherent with it and present them in a normative fashion.⁴ The starting point is that activity on the Internet can be, and widely is, anonymous.⁵

¹ Some of the views here expressed were presented first in a workshop at the European University Institute ('Policing the Internet: Policy, Politics and Consequences of Regulating Internet Content' December 2012) and subsequently in a conference at Milan University ('Anonimato, diritti della persona e responsabilità in rete' November 2013). I have profited greatly from the contributions of all those who intervened. Owing to time constraints, I have been unable to include in the article comments on the ECtHR decision *Delfi AS v Estonia* and the ECJ Grande Chambre decision *Costeja v Google Spain*.

² See M Manetti, 'Art. 21 della Costituzione e tutela degli scritti anonimi' (2014) *Il diritto dell'informazione e dell'informatica* 2, 139.

³ The most thorough examination of the various issues related to anonymity is contained in G Finocchiaro (ed), *Diritto all'anonimato. Anonimato, nome e identità personale* (Cedam 2008) where it is seen from the different perspectives of constitutional, private, criminal, and administrative law. More recently, see also RH Weber and UI Heinrich, *Anonymization* (Springer 2012).

⁴ One should note that the legal debate over anonymity is mostly American, with dozens of articles (generally monotonous). This does not mean that in Europe the problem has not been considered. For the most illustrious voice in favour of anonymity on the Internet, see, when he was already Italian Data Protection Commissioner (1997/2005) and in countless subsequent public occasions, S. Rodotà. The European Commission examined the various issues as early as 1997. See Recommendation 3/97 'Anonymity on the Internet' by the Working Party on the Protection of the Individual with regard to the Processing of Personal Data. The topic was recently discussed in the 2012 Deutscher Juristentag in the session devoted to 'Persönlichkeits- und Datenschutz im Internet: Anforderungen und Grenzen einer Regulierung'. See G Spindler's *Gutachten* (Beck 2012) 33. G Resta in 'Anonimato e identificazione: un approccio comparato', a paper presented at the conference 'Anonimato, diritti della persona e responsabilità in rete' ((2014) *Il diritto dell'informazione e dell'informatica* 2, 171), points out that the American view of anonymity is highly ideological and coherent with views widely shared in that country.

⁵ I shall analyse the 'common' Internet system, setting aside—for the sake of simplifying an already complex scenario—the so-called 'deep Internet' networks. See the Note, 'The TOR Network: A Global

Anonymity as a result of technology

This is due to technical and structural reasons: Whoever operates on the Internet does so through a machine which does not necessarily identify its user. The machine, which may range from a highly powered mainframe to a very small handset, may provide information as to its whereabouts, but excluding the not-so-common case of activities which can be performed only via biometric identification (fingerprints, iris), it is extremely difficult, from a practical point of view, to establish the author with any certainty. The structure of the Internet favours such situations, inasmuch as it is intrinsically cross-border and transnational and therefore defies typical systems of registration, identification and tracking. This feature has recently been enhanced by the growing phenomenon of cloud computing, which is characterized by the continuously changing location of computing facilities.

Anonymity as a social habit

This has generated a social habit of anonymous speech. While in the material world people tend to identify themselves when they enter into relations with other persons, on the Internet this is not widespread practice. As a matter of fact, one encounters the creation of multiple digital identities which parallel the 'official' and identifiable one.⁶ This tendency towards anonymity is not restricted to natural persons. Entities are created on the Internet that group common interests and use the immense potential of the Web to promote, reach, and bond. Business entities may also take advantage of the increased opacity granted by the Internet. Piercing the corporate veil on the Web may be extremely complex, especially when the only link to the outside world is a bank account, often opened in some tax haven.

This social aspect—especially concerning individuals—cannot be ignored and without indulging in the libertarian rhetoric which will be examined further on, greatly influences the effectiveness of any legal intervention aimed at suppressing or curtailing anonymous speech. At the same time one must consider what are the aims of an intervention limiting anonymity on the Internet, what are the interests that require protection, where to strike the balance between competing values and what is the cost, financial and social, of enforcement.

Inquiry into the Legal Status of Anonymity Networks' (2012) 11 *Washington University Global Studies Law Review* 715.

⁶ See V Smith Ekstrand, 'The Many Masks of Anon: Anonymity as Cultural Practice and Reflections in Case Law' (2013) 18 *Journal of Technology Law & Policy* 1.

The ambiguous meaning of anonymity

A further preliminary remark is necessary. Anonymity is an extremely variable notion, which in some cases has a strong legal and normative background, but in other cases requires a more detailed definition.⁷ At any rate it appears obvious that there are significant differences between, say, the right of the mother who does not want to recognize her child to remain anonymous,⁸ the duty to safeguard the anonymity of a whistle-blower,⁹ or of a confidential source in a criminal investigation,¹⁰ or anonymous litigation.¹¹

The variety of cases in which the notion of anonymity arises (for all: the *société anonyme* in French company law) suggests the need for a careful examination of what exactly we mean when we are talking about ‘anonymous speech on the Internet’. This appears to be more a social and factual situation, and therefore it is necessary to better define its legal ambit, also to avoid terminological misunderstandings. As will be argued in more detail further on, careful distinction must be made between the various situations.

Right to anonymity *versus* duty of disclosure

Again, and from a more legal perspective, it is clear that there are significant differences between the right to remain anonymous and the absence of a duty to disclose one’s identity when communicating over the Internet. The former approach requires the establishment of procedures and remedies through which the right can be ensured and enforced. The latter is a much more factual approach, in which public and private authorities simply abstain from forms of normative and technological intervention that require the identification of who is operating on the Internet. To deepen this difference, on the one hand, the extent of a ‘right to anonymity’ must be established, and whether this right can be waived or superseded by over-riding interests. On the other hand, it must be established when it is both desirable and feasible to impose disclosure of a person’s identity.

Anonymity *versus* secrecy

The uncertainty is increased by the existence of legal notions which are in various ways related to that of anonymity. Most contemporary constitutions and international conventions

⁷ See E Pelino, ‘La nozione di anonimo’ in Finocchiaro (n 3) 31 ff.

⁸ See, for Italian law, A Avitabile, ‘Il diritto all’anonimato in ambito familiare’ in Finocchiaro (n 3) 143 ff.

⁹ See the EU Commission (internal) 2012 ‘Guidelines on Whistleblowing’ <<http://www.coe.int/t/dghl/standardsetting/cdcj/Whistleblowers/EU%20guidelines%20%20Whistleblowing.pdf>>. The issue of whistleblowing and of anonymity of sources is amply examined by M Cuniberti, ‘Democrazie, dissenso politico e tutela dell’anonimato’, (2014) *Il diritto dell’informazione e dell’informatica* 2, 111.

¹⁰ See, in an Italian context, D Tassinari, ‘Diritto all’anonimato e diritto penale’ in Finocchiaro (n 3) 173 ff.

¹¹ See in a comparative perspective G Resta, ‘Privacy e processo civile: il caso della litigation anonima’ *Diritto dell’informazione e dell’informatica* 681–725 (2005).

on human rights include the right to secrecy of correspondence. It is commonly believed that this right—pertaining to physical mail—is extended to digital correspondence, such as e-mails. However, on the Internet the notion of correspondence—meaning an interpersonal communication between two specified persons—is blurred, considering the possibility of sending the same message to a very high number of persons (eg a mailing list), and the possibility that receivers may, with the greatest of ease, forward such a message to third parties. But is secrecy the same as anonymity? Generally speaking the right to secrecy means that others (typically public authorities) may not apprehend the content of the communication, but it does not mean that they are prevented from knowing who is writing to (or telephoning) whom.

This is because what is protected is the privacy—in the sense of seclusion—of the persons involved. Reflecting this approach are the provisions which require—even after the death of one of the parties of a correspondence—the consent of both to render public the content of the letters. On the Internet, instead, the situation is different: the content of the communication is public, and is meant to be so. Anonymity is used to hide not the content but its referability to a specified person. What is primarily protected is not privacy but discourse in the public arena, although what may also be relevant is the possibility of creating multiple, digital, identities.

The difference between the two notions—anonymity and secrecy—is made even clearer when one considers a vital institution of any democratic system, ie voting. Voting in elections is secret, in the sense that nobody may establish how one has cast the ballot. But surely voting is not anonymous. To the contrary, every precaution is taken in order to verify the identity of the voter and prevent attempts to vote in the place of someone else. As a matter of fact, the risk of fraudulent voting identities is one of the main obstacles to the introduction of electronic (ie digital, on-line) voting systems.

Anonymity and disguised identity

In fact one should consider that, commonly, anonymity is not meant—as it is in the material world—as an unsigned message (eg an anonymous letter), but instead is a message signed with a pseudonym (or nick-name).¹² This pseudonym (ie false name) may simply be the product of imagination, but often it can convey a deceitful impression, such as using someone else's identity or posing as a certain entity in order to attract disapproval (eg a right wing group which disseminates its views pretending it is a left wing group, or *vice versa*). Therefore, in a wider sense, anonymity does not only conceal one's identity; it may be used to disguise it with someone else's clothes.

¹² The right to use a pseudonym is enshrined in continental European copyright laws: see, for Italy, B Cunegatti, 'Anonimato e diritto d'autore' in Finocchiaro (n 3) 163 ff.

Is everything ‘speech’?

Furthermore, not only the notion of anonymity but also that of ‘speech’ may be ambiguous. One should note from the outset that the European approach does not share the all-comprising notion of ‘speech’ as derived from the interpretation of the First Amendment to the US Constitution which includes a great number of practical activities, from burning a flag to strip-tease. On the Internet any activity is digitally conformed and expressed through words or images but does that necessarily mean that we are witnessing a ‘speech’? For example, is selling memorabilia purportedly from Nazi concentration camps, giving instructions on the functioning of mechanical apparatus, or providing weather forecasts ‘speech’ in the sense we commonly apply to such a term from a legal point of view? As we shall see further on, qualifying activity over the Internet as ‘speech’ means that it is subject to the numerous limitations that generally apply to freedom of expression; first of all its definition and its boundaries.

The variables

Moving to a more detailed approach, this analysis will examine:

- who is communicating;
- with whom they are communicating;
- ‘where’ they are communicating;
- what is being communicated;
- what are the competing interests;
- gatekeepers and applicable law.

Who is communicating

Whether one frames anonymity as a right or disclosure as a duty, it is important to establish who is entitled to invoke anonymity and who is under an obligation to disclose their identity. One can easily detect a first logical difficulty: anonymity, *per se*, prevents us establishing who the speaker is, although the content of the communication may be useful to place them in a certain category. Here are some typical cases: an individual presents him/herself as a group or an entity; a business entity pretends to offer goods or services on an individual basis. It is therefore necessary to shift the analysis to what is being communicated (see below). At any rate one can, and should, distinguish between a) individuals, b) collective entities, and c) businesses.

a) Individuals, on a general basis, are entitled to the right to express their opinions freely; and at the same time they have a right to privacy. One could therefore posit that—provided they do not violate another person’s rights—they can keep their identity concealed. Therefore anonymous speech, *per se*, cannot be prohibited.

Only in the case in which there is a breach of a different norm, anonymity should not be used as a shield—it would, therefore, appear that anonymity is more a right than a concession. The problem, however, is establishing the extent of this right and when it can be forfeited. And this depends very much on the other elements that will be analysed further on.

b) If individuals are granted—subject to certain conditions—a right to anonymity (or are not obliged to disclose their identity), is the same right valid for entities that group individuals together? Is public discourse by political or social groups regulated in the same way as that of individuals—and should it be? The answers to these questions are heavily influenced by political options. It is necessary to state clearly—in order to avoid any misunderstandings—that we are talking about democratic regimes of the western world. What may be appropriate for these can be seen in a totally different light when analysing non-democratic and/or non-western political systems.

If one looks at European constitutional tradition, anonymous political activity in the form of political parties, movements and groups appears to be contrary to its basic principles, which have been established and have evolved over the last 60 years. The excruciating experiences which brought the downfall of liberal governments in the first decades of the twentieth century have demonstrated the venomous effects of hidden and disguised political action, and how it paved the way to dictatorships in most of Europe. As a result of this lesson the most important post-war constitutions have expressly barred secret associations.¹³ The reasons are self-evident. If one—quite rightly—requires that government be transparent, that same requirement applies to those who wish to influence or change government. An ‘open society’ cannot be limited to the upper spheres, but must involve all those who wish to play a role in it.¹⁴

¹³ See Article 21 of the German Constitution, and Article 22 of the Spanish Constitution on the publicity of political parties; and Article 18 of the Italian Constitution barring secret associations. This aspect is examined by GE Vigevani, in his paper ‘Diritto all’anonimato e trasparenza nell’ordinamento costituzionale italiano’, presented at the conference ‘Anonimato, diritti della persona e responsabilità in rete’. (2014) *Il diritto dell’informazione e dell’informatica* 2, 207.

¹⁴ The discussion on anonymous speech in the US generally takes as a starting point (quite correctly for that jurisdiction) the 1995 Supreme Court decision in *McIntyre v Ohio Elections Comm’n* striking an Ohio statute that made anonymous election leaflets illegal: ‘Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority’. The position taken in this paper is the one that goes back to Savigny’s timeless lesson in ‘Of the Vocation of our Age for Legislation and Jurisprudence’, ie that legal traditions may differ in the world and what is considered an ‘honorable tradition’ in the US, may not be so in Europe. One can only add that the notion of ‘tyranny of the majority’—deeply rooted in US political thought (John Adams)—appears to be, from a legal point of view, a purely rhetorical argument. In a democratic system, government is by definition majoritarian, with all the checks and balances that have been created in order to ensure that the majority will govern in accordance with the constitution and rule of law. If there is a ‘tyranny’ there is no democracy, but this assertion requires something more than simple *ex autoritate* quotes. Otherwise one could legitimately argue that it is only a catch-phrase that is used to allow a minority to violate the laws set, democratically, by the majority.

An essential element of this ‘open society’ is the right of citizens to know who is speaking in the public arena, in order to evaluate fairly and correctly their credibility. Knowing the identity of a speaker allows us to know about their past and their relations with others, and to have an idea about their motive and purpose. Furthermore, knowing the identity of the speaker in a public arena is necessary to establish their financial sources and whether their message is authentic or simply comes from a paid piper. This concern is behind the widespread legislation that requires political parties and movements to publish their balance sheets and the sources—above a certain (generally small) sum—of their income.¹⁵ If this is true of traditional political activity, it is even more so on the Internet, where the possibility of altering people’s perception of reality is extremely high: the number of contacts, the relevance of a piece of news, the creation of mirror effects. With the Internet becoming the most important arena for opinions to be discussed and formed and decisions taken, it would be paradoxical for it to be shrouded in the mist of anonymity.

c) Business activity cannot be anonymous. It is against the basic tenets of a modern economic system, which means entering into business relations with others, persons or entities, mostly through contracts; paying and being paid; being responsible for what one does. All these principles would be meaningless if whoever ran the business could be anonymous, as a swindler or a receiver of stolen goods. In addition, not only can there be no anonymity in business activity; there can be no ‘speech’ either. So-called ‘commercial speech’ is a contradiction in terms, first of all because freedom of speech is given to individuals and to the body politic to participate in social and political debate, and not to corporations. It is an individual right, not an economic freedom. In the second place, in business activity ‘speech’ is simply part of the production, distribution and marketing process and is subject to the same limitations as the rest. There is no ‘freedom of speech’ that can be applied to labels, packages or advertisements.¹⁶

All this is—or should be—quite obvious. The problem arises, however, when non-profit entities engage in economic transactions: when they ask for a membership fee, when they receive donations, when they sell advertising space on their website. Is anonymity of the entity only a ‘private’ issue that concerns those who expressly enter into relations with the entity, or should the public have a right to know who stands behind the name of the entity or its acronym? One returns therefore to the issues examined before under b).

¹⁵ One can measure the distance between the European and the US approach even from this perspective, see JM Shepard and G Belmas, ‘Anonymity, Disclosure and First Amendment Balancing in the Internet Era: Developments in Libel, Copyright, and Election Speech’ (2012) 15 *Yale Journal of Law and Technology* 92 (arguing that campaign-finance disclosure laws should also be submitted to ‘First Amendment scrutiny’).

¹⁶ I have tried to present this argument more extensively in *Freedom of Expression. A Critical and Comparative Analysis* (Routledge-Cavendish 2008) 58 ff.

With whom they are communicating

Before the digital age the distinction between correspondence and public communication was quite clear. The former was covered by the fundamental right of secrecy, which could be set aside only in cases established by the law and in some countries only by a court order. The latter, however, was subject to strict disclosure and liability rules—the name of the printer had to be indicated on every piece of printed matter; newspapers and periodicals were required to indicate a person responsible for their content; criminal and civil legislation was enacted to punish clandestine press and content that violated public interests and private rights. This legislation was extended to radio and television, first of all keeping these new media under a very strict State monopoly, and subsequently allowing only a limited amount of enterprises to enter the market. At any rate—even in present times—television content is extremely restricted and broadcasters are under a special obligation towards the public.

The Internet has subverted these rules, making it clear how restricted public discourse has been since the rise of full democratic systems. Not only can practically anybody communicate with the rest of the world at hardly any expense, but there are no restrictions on how much can be communicated. The new ways of communication via the Internet defy the traditional distinctions: it is up to the speaker to decide whether he wishes to restrict his speech to a single person or a wider audience, which again he has the ability to limit or to widen. What are the boundaries of correspondence on the Internet? Within them the issue of anonymity is irrelevant, because the speaker does not wish to render the content of his communication public. To establish if boundaries have been overstepped it is necessary to consider two elements, subjective and objective. First of all, the intent of the speaker, which is made clear not only by the external form of the communication but also by its content, typically if it is of a personal and confidential nature. In the second place the number of addressees of the message is relevant (eg a mailing list) and the way they are selected. If they are selected by the speaker on an individual basis one might consider the communication as a sort of expanded correspondence. But if selection is on a very perfunctory basis (eg simple registration with no other requirement or control) it can reasonably be seen as a public discourse, to which all the relevant guarantees and limitations apply.

‘Where’ they are communicating

If one applies the principle that individuals have a right to communicate, publicly, in an anonymous way, however that does not mean that the forum where they are communicating is irrelevant. In some cases there appears to be a legitimate expectation of anonymity—one just has to think of the many websites where people meet for sentimental or sexual reasons and can do so only if they are guaranteed anonymity. However, one should consider that the anonymity of the speaker does not imply that the

forum should also be anonymous.¹⁷ As will be seen further on, this double shield is inconsistent with the basic rules of modern legal systems. But it also appears to be difficult to justify from a logical point of view. If what is being protected is the individual's freedom of expression, the forum, quite clearly, is not an 'individual', and is not entitled to, or does not exert, fundamental rights for the simple reason that the opinions expressed belong to someone else. And one should further consider that there is a difference between an occasional expression of anonymous views, and a systematic and professional hosting of other people's views. Clearly this fosters public debate, but one should consider whether it is significantly different from a radio station which allows listeners to phone and express, live, their views, or a television programme to which the audience may send texts that are broadcast at the bottom of the screen. Is the technology so different as to justify an entirely diverse legal regime? As will be seen further on, the fact that one chooses someone else's medium to express anonymously one's views may entail responsibilities for those who carry them.

What is being communicated

Contrary to common belief, regulation of public speech is not 'content neutral'—obscenity, hate speech, instigation to commit crimes, advertisements, financial information, emergency warnings are some of the many cases in which specific regulations are implemented in all democratic systems, even in those that are considered the most open, such as the US. Again a careful exercise of distinguishing is required. In all the cases listed above what are being protected through a restriction of speech are paramount public interests. Those interests would be (or risk being) severely imperilled if one could hide beneath the cloak of anonymity. But if one recognizes that there are wide areas of speech that do not warrant anonymity, one should ask oneself if this is also the case when private interests are jeopardized, typically personality rights such as reputation or privacy.

Again it should be stressed that not all cases should find the same solution; however what is important is that certain forms of speech require that the speaker be clearly identified. The problem is that, generally speaking, in the case of speech violating public interest, one can decide beforehand whether anonymity should be allowed, while if private interests are at stake, knowing who the speaker is becomes extremely relevant for establishing whether this is legitimate or not. Is it sufficient to claim that one has been damaged to obtain disclosure? Or is something more required, and who should decide?

¹⁷ This should be the sense of several provisions (mostly German) which establish that use and payment of Internet services should be made, inasmuch as is possible, anonymous (for a detailed indication see Resta (n 4) para 2).

The competing interests

These last remarks bring us to the core of every legal question: the balancing of the competing interests in an effort to ensure what is considered the heart of the law, justice, avoiding the paradox well phrased by the Latin maxim *summum ius, summa iniuria*. From this standpoint the approach which favours, always and on any occasion, the right to anonymity appears to be absolutist, inasmuch as it disregards the need to protect equally valuable interests. Therefore, on one plate of the scales one has to put two concurring interests, one public, and the other private.

The Internet has opened up an unprecedented age of freedom of information and of expression. Never before have human beings been able to communicate, create, exchange, disseminate, and access thoughts, opinions and facts with such ease. This promotes some of the basic values of every democratic system, starting from knowledge and moving towards an open participation in the political, social, religious, philosophical and cultural life of the community. Clearly one cannot imagine returning to the past. Anonymity is one of the features that have allowed the system to develop, and therefore it should be kept in utmost consideration from a policy perspective.

On the same plate one should place the individual's right to privacy, or, to frame it in a continental European approach, the right to self-determine one's identity. In an age of increasing private profiling of everybody's habits and thoughts, and of public surveillance of millions of citizens¹⁸ anonymity is one of the techniques that can help preserve a small area of imperscrutability.¹⁹ Here again one can note a significant difference between the US and European approaches. While the former—in this as in many other fields—generally bestows the (*ex post*) protection of individual rights on the courts, the latter has an (*ex ante*) regulatory approach well expressed by the lengthy EU Directives on data protection and, if passed, by the even bulkier General Data Protection Regulation.

On the other plate we have, again, public and private interests. First of all, that of the prevention and repression of crimes. If it is impossible or extremely difficult to identify the authors, this means that the Internet is actually a lawless environment.²⁰ What is a crime—even a hideous crime—in the material world becomes without sanction if committed on the Internet. All contemporary societies are based on a balance between individual freedom and social protection which is ensured by the law. The contract between citizens and institutions has as an implied term that certain interests will be

¹⁸ S Niger, 'Sorveglianza e nuovi diritti di libertà' in Finocchiaro (n 3) 3 ff.

¹⁹ This is the argument behind the Note, 'Anonymity on the Internet: How does it Work, Who Needs it, and What are its Policy Implications?' (2006) 24 *Cardozo Arts & Entertainment Law Journal* 1395.

²⁰ An obvious remark is that a robber generally wears a mask in order not to be identified. The numerous US anti-mask laws are examined (critically) by M Kaminsky, 'Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech' (2013) 23 *Fordham Intellectual Property, Media & Entertainment Law Journal* 815.

protected and that the law will be enforced by the public authorities. The answer is clearly a question of degrees, and it is quite easy to list the areas in which everybody, in a civilized community, agrees that offences should not go unpunished. Generally speaking, therefore, there cannot be a right to anonymity when it comes to prosecuting and punishing crimes. There clearly is a grey zone which is open to debate, but this is not about anonymity, but rather whether certain behaviours should, or should not, be considered a criminal offence.

There are also important private interests which deserve protection—both patrimonial and non-patrimonial—and that are defenceless if whoever is considered responsible can hide behind anonymity. If one thinks of it, anonymity as a shield from private action is against the basic rules of natural law, which impose a duty not to harm others (*neminem laedere*) and to make good those who have been damaged by one's illicit behaviour. Again the debate is generally placed on the wrong perspective, which is not a case of being in favour of, or against, anonymity but of whether certain interests deserve protection, wherever and however they are violated. Insisting on a right to anonymity is simply an indirect way of asserting that those interests are legally worthless or that, on the Internet, they can receive only very limited and exceptional protection. Obviously this can be a matter open to debate, but one has to clarify the policy reasons behind a dual legal system based on the distinction between material activity and digital activity.²¹

Gatekeepers and applicable law

The highly complex and variable scenario that has been presented in these pages does not allow straightforward solutions. One can only try to resort to classical principles of the law, distinguishing between areas of non-liability, areas of personal liability, and areas of vicarious liability. In the first there is a right to anonymity (or no duty to disclose one's identity). In the second, instead, identification is a requisite of speech. In the last case a third party becomes liable for anonymous speech in the light of its role in disseminating content which is considered illegal (whether from a penal law or from a private law perspective). In some instances this liability would be automatic, typically when whoever hosts anonymous speech that violates public duties or private rights endorses the content. When, instead, there is no direct relationship between whoever hosts the digital space and the anonymous material which the latter contains, one could adapt the principles stated by the EU e-commerce directive: no liability if—duly warned—the host removes the illegal anonymous content and/or renders identifiable

²¹ I am not considering other harmful social uses of anonymity as instruments for intimidation, bullying, discrimination (see V Smith Ekstrand, 'The Many Masks of Anon: Anonymity as Cultural Practice and Reflections in Case Law' (2013) 18 *Journal of Technology Law & Policy* 23).

the author.²² Following this line one could imagine establishing *bona fide* proxies which allow identification in justifiable and predetermined cases.²³

A similar pattern of solutions meets, however, a severe practical obstacle related to the applicable law. Most of the companies which host (websites that contain) anonymous speech are US-based and generally specify that when it comes to disclosure and liability they will apply US law.²⁴ And even if this were not stated, the possibility of obtaining compliance to EU court orders and administrative decisions in the US is highly problematic and objectively incompatible with Internet time, which is measured in seconds and minutes.²⁵ It is paradoxical that information on the Internet is generally retrievable at any moment and with no expense and effort, but if one attempts to discover who is operating on the Internet this becomes an impossible task.

Surely, the solution that has been adopted in many US states—disclosure of the identity of the speaker can be granted only after a lengthy judicial procedure²⁶—is totally

²² The notion of ‘best risk-avoider’ is used by G Finocchiaro, ‘La responsabilità civile di terzi per gli scritti anonimi in rete’, paper presented at the conference ‘Anonimato, diritti della persona e responsabilità in rete’ (Milan University, November 2013).

²³ A similar solution is suggested by TZ Zarsky, ‘Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society’ (2003) 58 *University of Miami Law Review* 991, 1041.

²⁴ See eg the terms of service of Blogspot Google: ‘We do not remove allegedly defamatory content from www.google.com or any other Google US dot com domains.’ ‘US domain sites such as Google.com, Blogger, Google Sites, etc are run in compliance with US law. Given this fact, and pursuant to Section 230(c) of the Communications Decency Act, we do not remove allegedly defamatory material from US domains. We will remove material if the material has been found to be defamatory by a court, as evidenced by a court order.’ ‘The language of Section 230(c) of the Communications Decency Act fundamentally states that Internet services like Google.com, Blogger and many of Google’s other services are republishers and not the publisher of that content. Therefore, these sites are not held liable for any allegedly defamatory, offensive or harassing content published on the site.’ ‘Please note that a copy of each legal notice we receive may be sent to the Chilling Effects project (<http://www.chillingeffects.org>) for publication and annotation. *Chilling Effects will redact the submitter’s personal contact information (i.e. phone number, e-mail and address).*’ ‘We may also send the original notice to the alleged infringer or, if we have reason to suspect the validity of your complaint, to the rights holder.’ (Italics added.)

²⁵ See CT Kotuby, ‘International Anonymity: The Hague Conventions on Service and Evidence and Their Applicability to Internet-Related Litigation’ (2003) 20 *Journal of Law & Commerce* 103.

²⁶ This appears to be one of the main topics of discussion in the US: see K. Ringland, ‘Internet User Anonymity, First Amendment Protections and Mobilisa: Changing the *Cahill* Test’ (2008) 5 *Shidler Journal of Law, Commerce & Technology* 16 (discussing Arizona case-law); Note, ‘Protecting Copyright at the Expense of Internet Anonymity: The Constitutionality of Forced Identity Disclosure Under §512(h) of the Digital Millennium Copyright Act’ (2004) 23 *Temple Journal of Science, Technology & Environmental Law* 243 (arguing in favour of the unconstitutionality); Comment, ‘A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover an Internet User’s Identity’ (2010) 40 *Seton Hall Law Review* 1257 (arguing that the Fourth Amendment on unreasonable searches and seizures should be extended when trying to identify an anonymous speaker); Note, ‘*Dendrite v. Doe*: A New Standard for Protecting Anonymity on Internet Message Boards’ (2001) 42 *Jurimetrics* 465 (discussing a New Jersey case); Note, ‘Anonymity in Cyberspace: Judicial and Legislative Regulations’ (2012) 81 *Fordham Law Review* 3651; Note, ‘And the I(SP)s Have It ... But How Does One Get It? Examining the Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation’ (2002) 81 *North Carolina Law Review* 1218 (suggesting to extend to ISPs the privilege journalists have

inconsistent with basic European constitutional principles, for which access to judicial remedies is a fundamental right that cannot be prevented or rendered too cumbersome.²⁷ A system such as that adopted in the US would introduce a generalized form of *certiorari* which is known only in exceptional cases (eg action against Heads of State and Members of Parliament; actions to establish or deny paternity). Here, instead, for the mere fact that an action has been committed on the Internet a special procedural regime would apply, that in most cases—considering also the costs of access to justice—would be tantamount to granting *de facto* immunity.

We come here to one of the most debated issues in contemporary international law and international relations, that of so-called digital sovereignty: to what extent should the law—and the law enforcement agencies and the judicial institutions—of one country be able to govern the actions that occur in a different country, or prevent them from being governed? And how can one avoid conflicts between States and jurisdictions? The matter is beyond the scope of this paper. Suffice it to note that if one does not agree with the libertarian view that the Internet is a zone without external regulation based only on technical rules and self-regulation, any solution must be widely shared in the international community, as already happens in many other areas of the law.²⁸

Some conclusions

The discussion on the legal aspects of anonymous speech on the Internet is not the ultimate issue in this field. It is only one of the many problems that such a revolutionary invention brings to civilized communities.²⁹ Together with a bundle of blessings there

regarding their confidential sources: a similar argument is presented by M Manetti (n 2); Note, 'Unmasking 'Anon12345': Applying an Appropriate Standard When Private Citizens Seek the Identity of Anonymous Internet Defamation Defendants' (2009) *University of Illinois Law Review* 947 (suggesting a lighter, but always judicial, burden for private figures claims'). J McNealy, 'A Textual Analysis of the Influence of *McIntyre v. Ohio Elections Commission* in Cases Involving Anonymous Online Commenters' (2012) 11 *First Amendment Law Review* 149 suggests that the Supreme Court decision in favour of anonymous speech has not been so important. However the fact remains that in order to know the name of whoever one wants to bring to court a preliminary judicial procedure is required. A similar distinguishing interpretation of *McIntyre* is presented in the Note, 'Applying *McIntyre v Ohio Elections Commission* to Anonymous Speech on the Internet and the Discovery of John Doe's Identity' (2001) 58 *Washington and Lee Law Review* 1537. The only US article openly against mainstream positions I have found is by GR Lucas, 'Privacy, Anonymity, and Cyber Security' (2013) 5 *Amsterdam Law Forum* 107 (the author teaches at the US Naval Academy)

²⁷ This is the reason of the criticism of two—often quoted—recent German decisions (Landgericht München 3.7.2013 and OLG Hamm 3.8.2011) analyzed by Resta (n 4) para. 4.2. Some US commentators come to similar conclusions: see JB Eisenberg and JB Rosen, 'Unmasking "crack_smoking_jesus": Do Internet Service Providers Have a Tarasoff Duty to Divulge the Identity of a Subscriber Who is Making Death Threats?' (2002) 25 *Hastings Communications & Entertainment Law Journal* 683.

²⁸ See Weber and Heinrich (n 3) 23 ff.

²⁹ Appropriately BH Choi, 'The Anonymous Internet' (2013) 72 *Maryland Law Review* 501 points out that what deserves most protection on the Internet is its 'generativity' (stimulus to creativity and knowledge), rather than anonymity.

are—as in any step in the evolution of mankind—dangers and concerns that need to be examined and discussed. Once again what is required is a holistic approach which takes into account the complexity of modern societies and the not always converging instances for individual freedom and for social safety. One cannot expect that the balance that one may strike today will last forever, and one must imagine adaptable solutions that require a great deal of distinguishing, contrary to the quest for uniformity and the dislike for casuistry. This requires an open-minded (which is the contrary of one-sided) debate which can slowly, through a trial-and-error procedure, move us towards the most acceptable order.