Truth, identification, responsibility, ownership, navigation, and regulation in the future of the Internet

Nuno Sousa e Silva

1. Truth

Humanity has always been relatively distrustful and for good reasons: we could not trust, nor verify, most of the stories and tales that reached us. Access to information was difficult and almost always mediated. Few had witnessed the facts reported, and its verification was not always possible.

The records and recordings, videos and photographs of increasing quality began to change our attitude and beliefs. There were certainly fakes, but there was a disproportion: the cost of producing a convincing fake picture or video was high when compared to the increasingly lower cost of photographing or recording. Thus, we began to take videos and photographs as "proof". The probability of a video or photograph being faked was generally considered very low.

On the other hand, the dissemination of information itself was restricted and controlled. The (now called "traditional") press had high production and distribution costs and a relatively limited reach. Moreover, it was a strictly regulated activity.

The impact of the Internet was, initially, to reduce to almost nothing the costs of information *distribution*. Whoever wanted, could publish whatever they desired, without needing authorization. And such a publication was potentially accessible everywhere, by all people, at all times.

The implementation of recommender systems, especially in social networks, allied to the increase in the supply of information, has contributed to the dilution of reality. Progressively, people began to see different things, refined and adapted to their convictions, desires, and preferences. Nowadays, research results in the same terms and in the same search engine vary according to the searcher. Teenagers no longer watch the same series or the same films. This affects the notion of culture and fragments reality. Depending on the habits, location, and preferences of each individual, their perception of the world is nowadays very different.

Now, with the tools of generative AI, there is simplified access to ways of creating deepfakes and generating complex and extensive texts. In other words, similar to what happened with the cost of distribution, the cost of *creating* information becomes minimal.

Thus, we are moving towards the dissolution of reality. This is not necessarily bad, but it requires us to be increasingly distrustful. With this, perhaps it is possible to avoid the thorny discussion about disinformation. After all, when reality is the subject of debate, and we are aware of this, there is no place for a single arbiter of truth that can tell what is false and what is factual.

2. Responsibility

In Portugal, the prohibition of smoking inside vehicles used for urban public transportation was established by the joint decree of the Ministers of Communications and Assistance No. 23440, of June 19, 1968. Until then, smoking took place inside buses and trains. Risk perceptions and social practices have changed a lot. We are witnessing an equivalent phenomenon regarding the rules of responsibility on the Internet.

The Internet is a means of communication, a network of computers using common protocols. Thus, those companies that limit themselves to providing the means of communication are, at the beginning, innocent intermediaries. In the same way that the post office will not be held responsible for insulting letters that I send to my friends and enemies, there was also no room for the responsibility of Internet service providers. This paradigm of exemption from liability was enshrined in the United States in Section 230 of the Communication Decency Act in 1996 and in the EU e-commerce directive in 2000.

However, a lack of responsibility (i.e. liability) does not mean an absence of duties. These intermediaries continue to have obligations to act to prevent access to and dissemination of certain content. And, in some cases, they can even be held liable if, having knowledge of the illicit content, they do nothing to neutralize it. This mechanism is called *notice and take down*.

With the evolution of these mechanisms, it quickly became clear that some of these services are not truly neutral and even have a substitutive effect. A significant chunk of the population does not watch television; it watches Netflix, Youtube and Tik Tok. It does not read newspapers or magazines; they read Facebook, Medium, Substack or excerpts and messages sent directly to them via Whatsapp or Telegram. And many of these services are not forthcoming about the content they promote or remove. In other words, they have an intimacy with the content that should not allow them to invoke a disclaimer of responsibility built on an idea of neutrality.

To ensure that they are taken seriously, the States have begun to take new approach like Twitter/X in Brazil and, in a different way, in France with Telegram's CEO. Going beyond a direct intervention in the blocking of certain services and content, the personal accountability of the officers of the companies that offer them has begun.

However, in my opinion, the current approach, especially for social networks, is insufficient. Some of these companies have developed truly toxic and addictive products, capable of negatively affecting the mental health of everyone, especially young female teenagers.[1] A little bit all over the world, proposals to limit the access of minors to social networks are increasing. As is already being done in relation to alcohol and tobacco. Such a law can and should exist to limit the damage that will inevitably result from this new reality.

[1] This is not be understood as sexist. That's what the data has shown so far: https://hsph.harvard.edu/news/exploring-the-effect-of-social-media-on-teen-girls-mental-health/

3. Navigation

The Internet is a network of computers using a common communications protocol, the TCP/IP protocol. Just as each of us has a telephone number, a unique identifier for communication, each device on the Internet has an IP address. The sites are hosted on servers, computers, with their unique "home".

For this reason, in the first phase, navigation was done by IP address (and this is still how some sites of the so-called *dark web* are accessed). In 1983 a more convenient system emerged. Each IP address (number) corresponded to a domain name. Thus, "www.ucp.pt" corresponds to " 158.162.0.3". This system of correspondence between addresses and names was created and is administered by a private entity based in Los Angeles, ICANN (Internet Corporation for Assigned Names and Numbers) and, by delegation, by national entities, which manage the domain names of each country, such as ".pt" in Portugal.

To help Internet users access information, directories (the equivalent of telephone lists, but with more organization) began to appear, such as Yahoo, which organized and categorized *sites*. From this indexing emerged the first search engines, which quickly became the dominant way of browsing. From this date on, most people started to search for information in search engines, with Google quickly assuming the dominant role.

In addition to this more active way of researching content, in 2005 the first *feeds* emerged, forms of information subscription, such as newsletters and blogs. These *feeds* quickly evolved to the provision of information initiated by the digital service provider. Thus, since 2006, Facebook has been continuously providing updates, advertising, and content adapted to each user. (Google search results also change according to user).

Since then, the experience of an Internet user involves not only the search for information, but also the reception of "unsolicited" information. The consumption of content is no longer necessarily initiated by the user. As is evident, this state of affairs gives rise to a greater risk of manipulation and abuse. For this reason, there have also been initiatives to regulate the role of some intermediaries, such as search engines and large platforms, with special emphasis on the European Regulations No. 2022/2065 (concerning digital services) and No. 2022/1925 (concerning digital markets).

In this phase of technological evolution, it is foreseeable that, within a few years, we will have artificial intelligence agents that will navigate the Internet for us or with us. These software agents will be able to read both layers of the Internet (visible, designed for humans, and invisible, such as metadata, machine-legible) and thus adapt the information to our preferences, capabilities and needs. It remains to be seen whether these "digital butlers", if they exist, will be better or better for the evolution of society.

4. Identity

One of the first "memes" (before the concept was used to describe a cultural artifact, such as an idea, set of images or behaviors, which is disseminated through the Internet) originated in a cartoon by Peter Steiner published in the *New Yorker* magazine in 1993. In this cartoon, two dogs talk and one of them, in front of the computer, explains to the other: "On the Internet no one knows that you are a dog".

In fact, in the early days of the Internet, there were no proper means of identifying Internet users or verifying their identity, so anonymity was more or less guaranteed.

However, with the development of commercial and advertising applications, the identification of Internet users has become common. Most people navigate in a *browser* that knows their personal account (typically associated to an email account). In addition, a large number of websites use *cookies*, small text files that are stored on the user's computer and can be read by any other website, thus allowing the reconstituation of the navigation path and pattern. From these elements, namely an email address, the site from which they navigate, the IP address and other details, it is often possible to find a name and reconstitute a profile. Most people, unless they take special precautions, surf in a "public" way and have a digital footprint. It is relatively trivial to know who they are and what their habits and preferences are.

The European legislator has tried to reverse this state of affairs. In the European Union, privacy and data protection are especially valued, seeking to guarantee citizens a right of informational self-determination. However, most citizens are not willing to give up the convenience and gratuity of many of the services offered, apparently free of charge, in exchange for their privacy.

It does not have to be this way. Between anonymity and total identification, there is a third way: the so-called pseudonymization. As proposed by Balaji Srinivasan, a system that admits the selective and partial management of several identities (grouped by pseudonyms) it is perfectly conceivable.[2] This allows a single person to manage his or

[2] https://www.youtube.com/watch?v=urtXRg9Nl3k&ab_channel=CoinCenter

her reputation, positioning and communication in a compartmentalized way, limiting certain risks, particularly that of cultural cancellation.

Similarly, it is also possible only to grant access to certain aspects of the identity. For example, a website can have access to a government management digital identity (the digital citizen card) only to establish that a given person is over the age of 18, for example to access pornographic content, buy alcohol or tobacco without knowing whether that person is 85, 58 or 19 years old. This last system is the one that the European Union sought to institute with Regulation (EU) 2024/1183 (known as eIDAS2), which, among other things, provides for the creation of a digital identity card. This mechanism will come into force in 2026 and is expected to contribute to a better Internet.

5. Ownership

The younger generations no longer have a collection of discs, cassettes or DVDs. The digitization has brought great ease to the consumption of content. In exchange for a monthly subscription, we have access to a vast collection of films and series, a very extensive music repertoire, or even a wide collection of video games.

This situation has some consequences.

First, there is the role that platforms such as Spotify or Netflix have on consumer preferences. Recommendation systems are not neutral and run the risk of homogenizing cultural production, which, in order to be featured as a suggestion or highlight, has to exhibit certain characteristics determined by a set of algorithms that it neither knows nor controls.

On the other hand, the content that does not consist of the platforms runs an increased risk of being condemned to total obscurity. Even if someone is particularly interested in a given film or disc, (s)he runs the risk of not being able to find it. This perpetuates the power imbalance between these platforms and the content producers, which, to that extent, is not very different from what already happened in the relationships between musicians and producers.

Second, this movement of transformation of goods into services through digitalization constitutes, in a certain sense, a phenomenon of consumer impoverishment.

It is true that, in the case of these platforms, consumers paid an entry "ticket", an (almost) unlimited access in terms of choice (the “buffet” of culture), but of limited duration. More surprising is that even those digital goods that consumers apparently "bought", such as files with musical, audiovisual or literary content (*e-books*), are not really theirs.

The legal rules applicable to books on paper or vinyl records are markedly different from those governing books or albums in digital format. If anyone can sell, without great restrictions, used books on paper, that person can no longer do the same to the copy of the e-book that has been acquired. This means that, without a legislative intervention,

my children will not be able to inherit my digital library. These restrictions are simultaneously legal, essentially based on copyright, and of a technical nature, based on technical protection mechanisms that prevent copying or other unauthorized use. The issue of digital inheritance is beginning to be discussed all over the world. It is necessary to adapt the rules if we still want to become the owners of something in the digital realm.

6. Regulation

After having looked at the issues of truth, identity, responsibility, ownership, and navigation in the future of the Internet, it is worth asking: what should be regulated and how?

The first thing to point out is that, in the digital world, the main threat to the rights of citizens and companies comes from private entities and not from the State.

On the Internet, the structure of economic and social relations ceased to be bilateral (e.g. between consumer and professional) and became triangular, including an intermediary, typically a platform, which mediates the relationship between service providers and service users. This intermediary benefits from network economies (the more participants it has, the greater its attractive power) and economies of scale (allowing cost reduction), which generate a monopolistic tendency and lead to a concentration of power.

Thus, the role of the State should essentially be to protect citizens through regulation of the Internet, especially the regulation of platforms. Therefore, the resulting risk is the so-called "invisible handshake" or regulatory capture; that is, the development of a regulatory framework so demanding and heavy that it favors the incumbents, who have more resources and can hire more lawyers and manage *compliance* departments.

We can think of regulation as having an impact on procedures, on content, and on practices.

Currently, the Digital Services Act, the current European regulation, tackles procedures in detail. Citizens can challenge the actions of intermediaries, especially large platforms, which cannot do what they want. Although they are private companies, their essential role in guaranteeing citizens' rights, especially freedom of expression, is recognized.

There is a great debate as to the type of content to be regulated. While it is true that there are consensual minimums (child pornography and videos with beheadings should not be acceptable), it is no less true that concepts such as "hate speech" or "*fake news*" are vague and nebulous and their control risks limiting individual liberties in an undue manner, impoverishing public debate. In this regard, I am a supporter of freedom as a prevailing value, i.e., I believe that the regulation of content should be minimalist.

However, freedom presupposes the possibility of choice, absence of manipulation, and a correct perception of the options presented. Thus, manipulative and misleading practices cannot be admitted, such as the so-called *dark patterns*, ways of

presenting information to users that promote an action or choice that they probably would not make.

For this reason, Member States and the European Union must guarantee the technical and legal means for the Law to be enforced. Robust and active supervision is an essential condition to ensure the safety and security of cyberspace. After all, it is a "place" where we spend a large part of our time.