Legal Aspects of Cyber Security - Essay

1 Introduction

Jean-Jacques Rousseau, famous writer from Geneva, said, "To renounce one's freedom is to renounce one's quality of man, the rights of humanity, even one's duties."[1].
No one is legitimate enough to decide how cyberspace should be used. No one is legitimate enough to impose a control to reduce the freedoms of their fellow human beings. The best regulator is not a group established by elites, by governments. The best regulator that can be, is decentralized, built by the collective intelligence of humans.

2 Liberation, the essence of cyberspace

The cyberspace we know today has its roots in 1969, when the Arpanet[2] network exchanged its first messages. Originally, a network allowing to link university research centers and military installations. This innovative network allowed to connect different research centers, in order to share knowledge to promote scientific advances and encourage evolution. Nearly 50 years later, Arpanet has been widely democratized, its name has changed to the Internet, but its function has remained the same: sharing information.
Cyberspace is getting bigger every day, each user contributes to its development, which makes it by definition a decentralized space. As such, wanting to control it is unnatural.
Indeed, the liberalism in place allows the sharing of knowledge, and encourages innovation. It is true that some uses are malicious, and that a lot of criminals use cyberspace. Nevertheless, imposing control for this reason would be to punish the majority of users, perfectly innocent in their uses, in order to try to limit the scope of action of criminals. We can make the analogy, a knife is mainly used for its primary function: cutting food, and even if it can be used for bad purposes, this does not legitimize the fact of consigning it to all.
Finally, imposing a general control in the hope of preventing malicious actions is illusory. Cybercriminals will always find a way around the limitations to conduct their activities. We can mention Telegram[3] or The Tor Project[4], two solutions for online anonymity, allowing to easily bypass censorship or other limits. The average user will then be the only victim of the consequences of a control in place.

3 Attempts to control cyberspace

We can ask ourselves how to limit, control, or restrict cyberspace. The writing of Deibert and Rohozinski[5] describe several approaches, which are involved at different technical levels of the network and thus of cyberspace.

The first approach is the most classical one coming from governments, it consists in creating legal frameworks and laws in order to define the rights and duties within cyberspace. This allows some states to censor access to certain online resources under the pretext that it exceeds the regulations.[6] Of course, this censorship is only applicable across a given

geographical dimension.
Justifying these limitations by a need for national security, wouldn't these decisions finally be a brake on the freedom of expression? From a purely conceptual point of view, cyberspace knows neither limits nor borders. We have already mentioned its principle of decentralization, which is the very basis of its initial functioning: each person is, at his or her own level, a node of the web, with information to read or share. This concept goes beyond the principle of geography that we know, no matter the origin of the user, he is part of cyberspace as well as the others.
Nevertheless, it is possible to make a connection between the nodes that make up cyberspace (users, servers, etc.) with the location of the connection. A trend is then clear, giants of the cyberspace are drawn as being almost inescapable boulevards at the time of our use, the GAFAM (Google - Apple - Facebook - Amazon - Microsoft)[7]. Should we then be wary of these giants, which by their size have the ability to control, or at least limit, the uses of other users of cyberspace? To a certain extent, we can qualify these giants as the most likely to become control actors. It becomes essential to protect ourselves from their influence, and not to participate in their growth. To do this, making data privacy[8] sacred by using only transparent solutions on the subject can be a key.

To continue, Deibert and Rohozinski mention what seems to be the most effective measure for restricting cyberspace, the filtering of requests at the level of Internet Service Providers (ISP). This measure is certainly the most effective, and for proof it is widely exploited by China in order to control the use of the Internet. Indeed, how to make sure that the maximum time allowed for a shower is respected only by managing the water supply? The Great Firewall (GFW)[9] is the Chinese solution allowing the government to block access to certain Internet services by positioning itself as an intermediary between the Chinese network and the rest of cyberspace. The censorship acts at a level that is essential for the proper functioning of cyberspace: DNS resolution. By positioning itself at the level of the access provider, the GFW solution intercepts DNS requests in order to answer and lie about those that are forbidden. Therefore, a cyberspace user based in China, who asks the name resolvers what is the IP address of the domain name facebook.com, will receive a wrong IP address, preventing him from accessing the social network. This powerful mechanism helps control the overall use of Chinese, following rules set by the government. However, even this particularly powerful solution remains flawed, the use of Tor Browser allowing to escape the limitations thanks to the anonymizing network proposed by the Tor Project (a certain knowledge is nevertheless necessary to succeed in exploiting the tool correctly to bypass the Great Firewall).

In the end for the question of control, it is obvious that large private companies (GAFAM in particular) are in an ideal position to operate in cyberspace, and in a much more important way than any government. This situation is certainly the most harmful for the users of cyberspace, since they and their data become sales products between the big companies[10]. This data is recorded, processed and exploited, allowing the giants of cyberspace to act according to their will or that of the governments that mandate them to limit certain actions of users. This control is at the same time one of the easiest to circumvent, but also the one that will require the most time. Indeed, in order to get rid of it, we have to review the habits we have acquired, and replace little by little each tool proposed by these companies by open-source and data compliant tools. For example, drop Facebook Messenger and WhatsApp and replace them with Signal[11].

4 How to make AI an ally for the many

Artificial intelligence is spreading rapidly in our daily lives. For the moment, its role is limited to relatively basic tasks, but with the advances of research in this field, AI should sky rocket in the coming years. From the popular point of view, AI is misunderstood, a subject of expertise and therefore too complex for the majority of users. The ignorant, untrained in technology, fear these developments, feel threatened, and hope for control to protect themselves indicates Yuval Noah Harari[12]. Making sure that AI does not become the enemy of man is irrational. Luc Julia, co-designer of the personal assistant Siri, and recognized as one of the greatest engineers specialized in Artificial Intelligence today: "So-called intelligent machines are only tools that we control, that work thanks to rules that we write."[13].
However, it is necessary to gain the trust of the largest number of people in order to hope to make AI a solid ally for the future of innovation. To do this, promoting open-source software is the most logical thing to do. Indeed, by making public the AI models, the experts present in cyberspace will be able to validate them or not. This will influence the community's confidence in the product, the service or even the target technology. This operation, called peer validation[14], has already proved its worth, and ensures decentralized control on many subjects. Such as Estonia, which has created a free-to-use source code repository for its AI-based solutions[15].
Decentralization being the real strength of cyberspace, we can evoke the cryptocurrencies[16], allowing to answer the needs of the users in any circumstances. Indeed, by the design of the decentralized model, even if a node collapses, it does not have any consequence on the other nodes or on the service provided. To take the counter example of the Facebook, Messenger, WhatsApp and Instagram services, centralized in the Meta company and which were unavailable for several hours, in October 2021[17]. A problem to which a decentralized service, such as Bitcoin[18], will never be exposed.

5 Conclusion

In conclude, Jean-Jacques Rousseau said "I prefer freedom with danger than peace with slavery". And so it is essential to understand that a perfect cyberspace without cybercriminals does not exist, given the many possible ways to bypass the control. And for this reason it is better to live with a liberation cyberspace, including all its benefits, than with a futile control that will only penalize classic users.

6 Sources

1. *Jean-Jacques Rousseau*
2. *Arpanet, the Internet origins*
3. *Telegram, end-to-end encrypted chats and videos solution*
4. *Tor Project, nonprofit organization responsible for maintaining software for the Tor anonymity network*

5. *Liberation vs. Control in Cyberspace - Ronald Deibert & Rafal Rohozinski*
6. *Internet censorship in Iran*
7. *GAFAM Explained*
8. *What is Data Privacy*
9. *Measuring the effectiveness of the Chinese Great Firewall*
10. *The GAFAM user data use*
11. *Signal, the nonprofit foundation for encrypted instant messaging*
12. *Technology Tyranny - Yuval Noah Harari*
13. *There is no such thing as Artificial Intelligence - Luc Julia*
14. *The Validation of Peer review principles*
15. *Estonia is creating a source code repository for its AI-based solutions*
16. *Cryptocurrency Explained*
17. *Gone in Minutes, Out for Hours: Outage Shakes Facebook*
18. *Bitcoin, an innovative payment network and a new kind of money*