Editorial: The Ashley Madison case, the dark web, the deep web and freedom of information

Christina M. Akrivopoulou

Greek Refugee Appeals Authority,
Kanellopoulou Avenue 2, PC 101 77, Athens, Greece
Email: akrivopoulouchristina@gmail.com

Biographical notes: Christina M. Akrivopoulou holds the post of Committee President in the Greek Refugee Appeals Authority. She has received her PhD in Constitutional Law and has been a Postdoctoral Researcher in the Greek Scholarship Foundation and the Aristotle University Research Committee. Her main research interests concern human and constitutional rights, the protection of the right to privacy, data protection, the private-public distinction, asylum and citizenship. She has lectured in the Faculty of Political Sciences of Democritus University of Thrace, in Hellenic Open University, in Aristotle University of Thessaloniki and in the EMA Unesco Chair inter-university master class. She also works as an Attorney-at-Law at the Thessaloniki Law Bar Association. She is collaborating with several Greek law reviews and she is an active member of many non-governmental human rights organisations in Greece and abroad.

The web, the internet, has many characteristics which make its use and function not only extremely interesting and useful but also risky and dangerous. The internet minimises all costs and time for communication and transportation of information. It enables the global flow of news, data and information, thus enhancing freedom of expression and speech, freedom of participation and also the right to knowledge since the web can be used for many as the most progressive, modern encyclopaedia. It enhances the right to financial freedom, since it is globally used as a very effective tool for financial engineering, for consuming, for online transactions, for marketing and for advertising. It is a means for public transparency, deliberation and democratic participation for the citizens, it enhances public dialogue and criticism and it augments a polity's perspective for accountability in public offices and open criticism to public policy making. The web has over the years advanced the society of knowledge and information as well as academic research and expression. Everyday, via the internet a vast amount of research data and academic information is exchanged, thus enabling the progress of science and knowledge in all fields. Of extreme importance is the ability of the web to assist the global transportation of news and broadcasting which proves to be of extreme significance in order to effectively respond to global catastrophes, in order to provide with global synergies, humanitarian aid or political arousement regarding abusing dictatorships and human rights violating regimes. Last but not least, the web is an extremely useful tool for social networking, therefore, enabling long distance human communication, friendship, companionship and relationships of all kind to be formed especially since the web can host the anonymous exchange of information.

Yet, the web is also a deep and unexplored sea, where individual autonomy reigns and it is unregulated by national laws, principles and rules. Even in cases where such

rules apply, they are becoming obsolete by the progressiveness of internet technology, or they are difficult to apply and even provide late responses to the vast speeds of internet information flows (as for example are court decisions that usually come long after a privacy or a human rights violation has taken place in the internet). The web is self-regulated by its user's ethics and by the *ad hoc* ethics preserved by the servers and the online data-bases. Nevertheless, the possible threats that the web entails for users and their human rights are many and important. Privacy and personal data protection can be easily threatened either by hacking, or by weak privacy security systems. The anonymity of users, which is so precious and important for the freedom of expression and the free flow of information, can in many cases be employed as a veil for malicious acts, including sex-trafficking, child abuse and exchange of children's pornographic material. Social networks can foster not only friendship and communication but also acts of bullying, of public humiliation, of spamming and of violation of personal information, in cases that false identities are used for acts of sexual harassment. Additionally, the free flow of information in social networks often jeopardises the truth and integrity of personal data in cases that personal photographs are altered, personal profiles are exploited or personal data information are jeopardised. In the field of financial freedom and commerce also the consumers' use of personal data can lead to acts of harassment via spam emails or telephone calls while the web posed serious threats to intellectual property by the widely spread, illegal downloading of music and movies. Moreover, the web can be used for human tracking, for hate speech actions or as a tool for terrorist and criminal groups.

The question which comes natural when someone enlists the advantages and risks of the web is whether the compelling goods deriving from its use should prevail or not against the risks and threats that the use of the web entails. Nevertheless, an answer to such a question cannot actually be provided *in abstracto*. The 'white' uses of internet definitely prevail over the 'dark' ones but nonetheless, in specific cases and in given circumstances, serious limits to free flow of information via the internet should be posed in order that other goods and rights can be protected as it is the case with privacy, data protection and confidentiality of information.

The Ashley Madison case illustrates in the most characteristic manner the conflict of interests between the need to protect the free flow of information fostered in the internet and the right to privacy. Ashley Madison Agency was founded in 2002 and functioned as an online dating service referring to people married or in committed relationships. The Ashley Madison offered discrete dating to people already in relationships who still wanted to date under the slogan 'life is short, have an affair'. On July 15, 2015, hackers stole all of the Ashley Madison Agency data including emails, names, home addresses and threatened to post it online if the agency did not close down. The hackers released on August 18, 2015 the first customers' data and more the following days. The case closed with the resignation of the agency's CEO. The total of the data stolen, approximately 20 GB has been archived in what is called, 'the deep web'. In the Ashley Madison case, the dark uses of internet, thus hacking, violated a series of rights, namely the right of privacy and personal data protection and the equally important freedom of enterprise.

The question is? What is the deep web? Also, what is the dark web? Are they categories of a part of the internet were malicious activities and actions are taking place? Can they mal uses be limited? The dark web is a term that refers to websites that are publicly visible but the IP addresses are hidden and thus the address of the servers that use them remains unknown. Thus, while it is very easy to visit such websites it is

extremely hard to figure out who 'owns' them. This effect is produced via the Freenet, I2P network or the Tor encryption tool which can be used in order to hide all identifying properties such as location or identity, with the same effect to websites. The Tor encryption tool is also referred as Onionland. One could say that the dark web would assist internet users living in totalitarian societies to communicate without consequences their thoughts and ideas. Nevertheless, from another point of view, users planning malicious acts could also be benefited by the dark web.

Another form of internet is the deep web, also called Deepnet, Invisible Web or Hidden Web. The deep web refers to all web pages that the search engines cannot find and it serves also as a confidentiality wall for payments. Thus, for example, the password protected bits of our online bank account are hidden in the deep web. In this framework, the deep web contains the dark web, pages behind paywalls that require specific registration and also the staging versions of many websites, as the preparation hall were information can be checked or reviewed before they are publicly broadcasted. Thus, the Deep Net is not a secret place but in general a storage internet area extremely large quantity of webpages and information.

Though the deep web seems a rather boring place were either the information flowing in internet is prepared or stored for safety reasons, the dark web can pose some serious dangers and risks. Thus, hate speech or terrorist incitement can take place via the encryption tools of the dark web. Pornography, internet fraud, sexual harassment, hacking or bullying can be covered under the dark web veil. The only tool in order to limit this secret world is technology itself, thus technology that can permit the identification of the perpetrators of malicious acts whenever it is needed. Nevertheless, even the mal uses of the dark web cannot annihilate the incredible contribution of the 'white web' as described above. The web during the past decades has been the symbolic place of an unprecedented free flow of information, the area of creative communication, research, exchange of ideas, the global public forum of world cultural exchange. Though the dangers are existent, the web is an invaluable tool for the fulfilment of autonomy and freedom in the modern globalised societies.