UDC 342

IMPLEMENTATION OF HUMAN RIGHTS ON THE INTERNET

IHAR KUDZELIA, ANDREI VALIAUKA
Polotsk State University, Belarus

Because of rapid development of information technology and in particular cryptocurrency the issues of anonymity, free expression and security on the internet have become increasingly common. Further, in this scientific work some of them will be considered, and possible solutions are proposed.

There is a so-called "clear net" this is what we use every day or what we can see on the Internet search. Clear net takes only 4 percent of the information throughout the Internet. There is also a "Deep Web" which takes 96 percent of the information not indexed by Internet search. These are archives, databases and the stuff like that. And just in the deep web's lies the dark net, access to which is opened through special browsers that encrypt the ip address with vpn technology, i.e., they constantly change your Internet address, which allows you to remain anonymous. The popularisation of cryptocurrency is not accidental, as it implies decentralisation, reliability, security, and, above all, anonymity. This is the main currency used in the darknet. The darknet, although it has its advantages, also contains a huge number of hidden sites where illegal services are provided. Entire stores of stolen credit cards, with large amount of money. Sale of passports of any country, both fake and original. I.e, representatives of the authorities by themselves, commit corruption crimes, selling or passports, as mentioned earlier, or, for example, goods confiscated at customs.

Even after the small part that was listed, it is clear that through the use of the darknet, many offenses and crimes are committed, so it makes sense to consider a couple of examples of how states are fighting them. The fight against drug trafficking on the Internet includes receiving and checking information about network resources which offer to purchase drugs, including those made known by the appeals of citizens. In 2015, the Department of the Federal Drug Control Service of the Russian Federation (Federal Drug Control Service of Russia) in Moscow checked about two hundred network addresses presumably involved in drug trafficking. Information on some sites sent to Roskomnadzor (rkn) to block access. Operational-search activities are being conducted to identify and suppress the activities of the organizers of the online drug business. Fighting against financial fraudsters is lead by banking servers. As soon as a suspect enters a stolen account or e-wallet, outgoing traffic begins to slow down on the server. Despite the secure connection used by the criminal, the same delays will appear in his encrypted traffic - this is how it can be proved that he committed the crime. [1]

In the UK, special services were created to fight against pedophilia in darknet. This project involves the Government Communications Headquarter and the National Crime Agency. The goal is to "destroy the secret digital shelters of pedophiles," according to GCHQ head Robert Hannigan. What is already happening: the year is not over yet, but there were already a thousand British criminals in the prisons, five times more than they managed to catch last year.

Very popular social network Vkontakte is also the subject of crimes, as hackers sell their services in darknet, and, in fact, often hack profile pages to steal correspondence and personal data. Also there are sold training certificates and high-quality fake currency. In addition to all this, the darknet has a huge number of various kinds of secret state archives, court registers and much more. According to Articles 25 and 28 of the Constitution of the Republic of Belarus, the State provides the freedom, integrity and personal dignity, and everyone has the right to have protection from unlawful interference with his / her privacy, including from encroaching on the secrecy of his correspondence, telephone and other communications, his honor and dignity [2]. If we talk about the stock exchanges of information, then we can give a recent example of Novaposhta (the most popular postal service in Ukraine). Information archives were hacked, and then were placed on the open spaces of the darknet. Passport details, names, phone addresses. All this could be obtained for a few hundred dollars. Although Novaposhta refutes all this data and tries to refer to the fact that it could be data of any other mail, however in these files there is a direct confirmation of the opposite. In our country, in the Republic of Belarus, the actions of the Novaposhta would be considered by the article 28 of the law on Information, Informatisation and Information Protection [3]. Since they were obliged, to provide reliable protection of the information of their users and prevent this offense. There are also information exchanges with personal

correspondence and documents of public servants and important or media personalities. A recent example is bought on a darknet, and then published for all people personal information of Dmitry Kiselyov. From this information it is clear that his speeches are written to him by a scientist Fedotova, and not for free, but for salary. Also from his correspondence it is clear that TV channels release pro-gang information. There are letters from the Minister of Culture of the Russian Federation (Vladimir Medinsky), who asks to employ his friend in the Russia. Today news agency headed by Kiselyov. You can also contemplate how his wife buys a thesis. And of course this is not all that we can talk about.

Which conclusions can be drawn after this? With the development of cryptocurrency, Internet users have the opportunity to make purchases anonymously, which gave rise and impetus to such system as a darknet. A lot of people are fighting for their independence on the Internet, not understanding what consequences this can lead to. Human Rights Council of the United Nations held a meeting according to which anonymous use of the Internet, encryption of personal data and communication media are an inalienable human right. Members of the Council concluded that anonymity on the Internet is an important tool for free expression in the digital age [4].

A Council of Europe and European Court have developed a certain legal position about the right to anonymity. For example, the Committee of Ministers of the Council of Europe adopted declaration on freedom of communication on the Internet. Principle 7 of the document provides that:

"In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member States should respect the will of users of the Internet not to disclose their identity. This does not prevent member States from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police"[5].

This is one of the main advantages of the darknet, as some states simply do not allow people to speak on the Internet under the threat of sanctions. But on such a plus, there are a huge number of disadvantages that were listed earlier. By using the survey data of Centre for International Governance Innovation, we can see that the 70% of respondents approve the closure of the darknet [6]. But taking into account the problems that some countries have to block access to one site, it can be concluded that closing more than 7,000 hidden entry points to the darknet will be simply impossible. A way out of this situation may be Internet access via identity confirmation. That is, when registering with the provider and at the website of any social network, passport data will be required. In our vision of this situation, this will happen like this:

a citizen who wants to get an Internet connection will give his/her passport data to the provider, in addition to connecting to any network, even for example wi-fi in a cafe, will also be required to enter passport information. In the future, this will allow law enforcement agencies to more quickly carry out both verification and capture of offenders and criminals, as providers, by police request, will give the data from previous Internet sessions of the suspects. This will not be in conflict with the law, as article 23 of the Constitution of the Republic of Belarus says:

Restriction of personal rights and freedoms shall be permitted only in the instances specified by law, in the interests of national security, public order, protection of the morals and health of the population as well as rights and freedoms of other people. This will not affect the use of the Internet by the law-abiding population, as the anonymity of the Internet will be saved (as entered passport data will only be entered into the provider database), and law enforcement will be able to stop more crimes.

REFERENCES

1. Новостное интернет-издание [Электронный ресурс]. – Режим доступа: https://lenta.ru. – Дата доступа: 10.02.2019.
2. Конституция Республики Беларусь [Электронный ресурс] : с изм. и доп., принятыми на респ. Референдумах 24 нояб. 1996 г. и 17 окт. 2004 г. – Режим доступа: http://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/konstitutsiya-respubliki-belarus/. – Дата доступа: 13.02.2019.
3. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З : с изм. и доп. от 11 мая 2016 г. № 362-З : с изм. и доп. от 18 мая 2016 г. № 362-З. – Режим доступа: http://pravo.by/document/?guid=3871&p0=h10800455. – Дата доступа: 15.02.2019.

4. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression [Electronic resource] : version of 22th may 2015 // Human Rights Council Twenty-ninth session Agenda item 3 Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. – Mode of access: https://ru.scribd.com/doc/266938105/A-HRC-29-32-AEV. – Date of access: 18.02.2019.
5. Декларация о свободе общения (коммуникаций) в Интернете [Электронный ресурс] : (заключена в г. Страсбурге 28.05.2003 г.). – Режим доступа: https://www.osce.org/fom/31507?download=true. – Дата доступа: 20.02.2019.
6. Новостное интернет-издание [Электронный ресурс]. – Режим доступа https://www.cigionline.org. – Дата доступа: 21.02.2019.