JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 4 Issue: 4 | Apr–2025 ISSN: 2720-6882

http://journals.academiczone.net/index.php/jiphr

Specific Aspects of Internet Regulation Legislation in the Usa

Ilkhombekov Jasurbek Ilkhombek ugli

Tashkent State University of Law Senior lecturer, Doctor of Philosophy in Law

E-mail: jafarbek22@mail.ru

Annotation: This scientific article analyzes in detail the regulatory legal documents of the United States, one of the developed countries of the West, regarding the regulation of the Internet. The article mainly focuses on the specific aspects of US Internet regulation. When comparing some aspects of the regulation and use of the Internet, there are aspects that have been analyzed in comparison with the legislation of European countries. Also, the importance of the Internet in the process of information exchange, its differences from other information resources, advantages and legal significance were scientifically analyzed.

Key words: Information, Internet, USA, GeoCities, HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, VPPA, FTC, law.

We will analyze the Internet world in the United States, one of the most democratic countries in the world and the birthplace of the Internet. In America, the Children's Online Privacy Protection Act (COPPA) [1] law came into force on April 21, 2000. The main purpose of this law is to prevent children under the age of 13 from accessing prohibited sites on the Internet. That is, when a child under the age of 13 tries to access this prohibited site, he is required to enter a lot of information. Many websites do not allow children under this age to use their sites. Also, another Internet law, the Children's Internet Protection Act (CIPA) [2], was passed in 2000. The main purpose of the law is to install an automated filtering system when accessing sites during Internet use in schools and libraries. That is, it provides for restrictions such as creating a system to prevent access to pornographic sites or to filter out prohibited images when using these computers, that is, the site will be automatically blocked if these prohibited actions are performed. In accordance with this law, many schools and libraries are obliged to block all other websites on the Internet, for example, pornographic, advertising, gaming, and any other sites that allow correspondence on social networks.

The average US household spends an average of $ 1,141 on cable and Internet bills every year. However, this figure has increased significantly during the COVID-19 pandemic due to the increase in the number of Americans working from home. During the pandemic, many Americans used the Internet to browse social networks, play games, conduct video conferences, and stream TV. According to the Wall Street Journal (WSJ) [3], this has significantly increased the speed of consumption and prompted Internet providers to impose restrictions on use. The average Internet speed for the US National Aeronautics and Space Administration (NASA) is 91 gigabytes per second. That’s 17,800 times faster than the average American consumer spends browsing. While the Internet was created to provide convenience to humanity, it has also led to an increase in cybercrime. For example, according to Small Business Trends (SBT) [4], at least 40 percent of cyberattacks are targeted at small businesses in the US and abroad. Cybercrime is currently the second most reported economic crime in the US. On average, cybercriminals launch attacks on about 4,000 ransomware programs every day, demanding at least $1,000 in ransom for each attack. A study conducted by the University of Maryland found that hackers attempt to attack computers and other digital devices connected to the Internet every 39 seconds. One in three Americans is a victim of a hacker attack [5].

Here, we will look at the uniqueness of the US government in regulating the Internet.

Volume: 4 Issue: 4 | Apr–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

If we look at Western countries in this regard, the US government stands out among them for its promotion of democratic principles: freedom of speech, freedom of information, etc. If we look at the US Constitution, the 1st Amendment states that Congress shall not pass a law restricting freedom of speech or the press. For example, many states have restrictions on telephone calls. If a US citizen swears or uses similar culturally inappropriate language while on the phone, the telephone company will automatically block that person's SIM card. Furthermore, the Bill of Rights [6] has been interpreted as "creating a right to privacy or some kind of constitutional guarantee of privacy" through a variety of rights.

"Most people believe that they are protected until they are not," says Ashkan Soltani, an independent researcher and former chief technologist of the Federal Trade Commission. Unfortunately, because this ecosystem is primarily hidden and opaque, consumers cannot see and understand the flow of information. Europe's comprehensive privacy law, the General Data Protection Regulation (GDPR) [6], requires companies to ask for certain permissions to share data and gives individuals the right to access, delete, or control the use of that data. In the United States, by contrast, there is no single law that covers privacy for all types of data. Instead, there is a patchwork of laws with acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA, which are intended to cover only certain types of data in specific (often outdated) circumstances.

- ✓ The Health Insurance Portability and Accountability Act (HIPAA) has little to do with privacy, and only covers communications between "covered entities," which include doctors, hospitals, pharmacies, insurers, and other similar businesses. People often think that HIPAA covers all health information. But that's not true. For example, some of your medical information is not protected, and the law doesn't limit who can or cannot ask about your COVID-19 status.
- ✓ The Fair Credit Reporting Act (FCRA) covers information on your credit report. It limits who can see your credit report, what credit bureaus can collect, and how the information is obtained.
- ✓ The Family Educational Rights and Privacy Act (FERPA) provides detailed information about who can request student education records. This includes giving parents, eligible students, and other schools the right to inspect educational records maintained by the school.
- ✓ The Gramm-Leach-Bliley Act (GLBA) requires consumer financial products, such as credit services or investment advisory services, to explain how they share information, as well as the customer's right to opt out. The law does not limit how companies can use the information they collect, as long as they disclose it in advance. The law does, however, provide some protections for personal information.
- ✓ The Electronic Communications Privacy Act (ECPA) limits government wiretapping of telephone calls and other electronic signals (although the USA Patriot Act has largely rewritten this). It also sets out broad rules about how employers can monitor employee communications. Critics often argue that the ECPA, which was enacted in 1986, is outdated. Because ECPA was written long before the modern Internet, it does not protect against modern surveillance tactics, such as law enforcement access to old data stored on servers, in cloud storage, and in search queries.
- ➢ The Children's Online Privacy Protection Act (COPPA) places certain restrictions on companies' collection of data from children under 13.

At least four states, Massachusetts, New York, North Carolina, and Pennsylvania, have serious, comprehensive consumer privacy proposals in their legislative committees. Other states have various laws in the early stages. It can be difficult to keep track of all of these proposals, but the International Association of Privacy Professionals maintains a tracker that shows which states are developing privacy legislation and where those bills are being implemented. According to research by The Markup, at least 14 proposals would push Virginia to overhaul its largely unenforceable laws. As with

Volume: 4 Issue: 4 | Apr–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

national laws, there are also state-level laws that cover specific aspects of data privacy. Missouri has e-book privacy rules. Illinois' Biometric Information Privacy Act (BIPA) gives people privacy rights to their biometric data, such as fingerprints or facial scans. When it comes to data breach notifications, it can be especially difficult to know your rights with at least 54 laws that vary by region. Amie Stepanovich of the Silicon Flatirons Center argues that while such state laws can be confusing, they are still useful. "You can think of them as a high water mark," she says, and that when legal standards are raised, companies often choose to "apply a stronger, more protective standard for everyone." Furthermore, too many state laws risk creating confusion for both companies and, in practice, consumers.

The Federal Trade Commission Act (FTC Act) gives the FTC the power to take action against an app or website that violates its privacy policy. The FTC can also investigate privacy-related marketing language, as in the case of Zoom, which misled users into believing that its video chats were end-to-end encrypted. Some groups have also recently called on the FTC to extend this power to data privacy practices. Title 5 of the FTC Act specifically requires companies to protect consumers' information privacy when they wrongfully or fraudulently collect or share personal information. For example, in August 1998, the Commission brought its first online privacy case against GeoCities. In that case, the Commission alleged that GeoCities, one of the most visited websites on the Internet, collected personally identifiable information from its members, both adults and children, and abused the trust that individuals had in its use of that information. When visitors sign up, they must complete an online application that requires them to disclose certain personally identifiable information and asks for voluntary information about their education level, income, marital status, occupation, and interests. Through the registration process, GeoCities created a rich database of target markets for advertisers. In its complaint, the Commission alleged that GeoCities falsely stated that the mandatory information provided by members would not be shared with third parties without their consent. In addition, GeoCities collected personally identifiable information from children, promoted the GeoKidz club for them, and conducted events, contests, and games. The FTC accused GeoCities of misrepresenting that it was the sole owner of this personally identifiable information collected from children, when in fact a third party had collected and stored it. Ultimately, GeoCities settled the case by agreeing to disclose what information it collects on its website, for what purpose, to whom it is disclosed, and how consumers can review their personal information and, if they wish, have it removed from its databases. The consent order also prohibits GeoCities from misrepresenting who sponsors the various events offered on its website and who actually collects and stores personal information. Finally, to protect children, the order requires GeoCities to obtain parental consent before collecting information from children 12 and younger and to delete information that has already been collected if GeoCities does not obtain affirmative parental consent to retain it. GeoCities has grossly violated consumers' privacy and has been punished for it.

The US approach to protecting consumer privacy online - which relies on industry self-regulation with minimal legislation and administrative powers - differs from that of the European Union, which relies more on legislative protection. In particular, the European Union adopted a Directive in 1995 that broadly regulates the buying and selling of personal data. This Directive, which entered into force on October 25, 1998, sets out general rules that companies must follow when collecting, storing or transferring personal data in the course of their business or administrative activities. The most important for companies is the obligation to collect data only for specified, legitimate purposes and to keep it only relevant, accurate and up-to-date. In turn, European citizens are guaranteed a number of rights - the right to access their personal data, the right to rectify any inaccurate data, the right to object to the use of their data for activities such as direct marketing, and the right to recourse if processing is unlawful. Importantly for the US, the Directive prohibits the transfer of personal data to any country that does not provide "adequate" (meaning "comparable") protection. Each EU member state will

Volume: 4 Issue: 4 | Apr–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

develop its own laws to implement the Directive. However, the Directive may impose significant restrictions on US subsidiaries that buy and sell personal data in the EU or on companies that receive and transfer personal data to the United States.

We have already analyzed the views of the constitutional legal system in the United States on the regulation of the Internet, personal privacy and freedom of speech. However, in the United States, in addition to constitutional law, laws have been developed that regulate other areas related to the Internet. In early 1996, Barlow, the founder of the Electronic Frontier Foundation, declared that the Internet is independent of national governments. For many years, this antiquated thinking served as the guiding philosophy of the Internet Valley, as technology companies rejected attempts to regulate them or monitor online behavior. The lack of regulation of the Internet has allowed them to build large monopolies and make huge profits. Today, the Internet Valley is facing its own obstacles and problems. Against the backdrop of widespread concerns about fake news, influence campaigns, cybersecurity and the exchange of violent and extremist content, an increasing number of countries are seeking to regulate high-tech.

In short, US law is unique. However, it is impossible to develop a comprehensive law for regulating the Internet. However, it is advisable to regulate some basic actions when using the Internet. Firstly, there are technical possibilities to bypass any obstacle (VPN, proxy servers), and everyone can use them. Secondly, restricting the means through which illegal information is disseminated, whether it is social networks or the media, is not the solution. In this regard, we should all understand that the freedom to search, receive and distribute information, including via the Internet, imposes special obligations and responsibilities on them, and certain restrictions may be imposed on them in accordance with the law. Only if we all understand our responsibility in this matter and are able to distinguish black from white, truth from fake, and evidence from provocation, will we find a systemic solution to the problem.

This development of civilization, the high level of informatization and computerization of social relations proves that the Internet has penetrated all spheres of human activity today.

In conclusion, it can be said that the Internet space we have analyzed is currently the hegemonic Internet in terms of satisfying the need for information, its fast, organic and unlimited delivery. After all, it would not be wrong to say that the Internet is today the global information space and the author of the globalization process. We have analyzed its unlimited possibilities above using the example of the developed country of the USA.

References:

1. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312
2. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act
3. https://www.wsj.com/
4. https://maff.io/media/sbt_sloulbound_tokens/
5. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds
6. https://gdpr-info.eu/
7. Jasurbek, I. L. H. O. M. B. E. K. O. V. (2022). DEVELOPMENT TENDENCIES OF THE RIGHT TO RECEIVE INFORMATION IN THE VIRTUAL SPACE. INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLINARY RESEARCH ISSN: 2277-3630 Impact factor: 7.429, 11(11), 17-22.
8. Ilkhombekov, J. (2022). THE ROLE AND ROLE OF THE MEDIA IN THE INFORMATION DISTRIBUTION PROCESS. Академические исследования в современной науке, 1(17), 80-84.

Volume: 4 Issue: 4 | Apr–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

9. Илхомбеков, Ж. И. Ў. (2022). Ўзбекистон Республикаси қонунларида оммавий ахборот воситалари эркинлигини таъминлашнинг ўзига хос хусусиятлари. Scientific progress, 3(4), 1068-1074.
10. ИЛХОМБЕКОВ, Ж. (2022). АХБОРОТ ТУШУНЧАСИ, МОҲИЯТИ, ҲУҚУҚИЙ ЖИҲАТИ ВА КАФОЛАТЛАРИ. ЮРИСТ АХБОРОТНОМАСИ, 2(6), 49-53.
11. Jasurbek, I. (2024). Comparative Legal Analysis of Reforms Conducted for the Development of the Information Sector in the New Uzbekistan. American Journal of Public Diplomacy and International Studies (2993-2157), 2(1), 72-81.
12. Jasurbek, I. (2024, February). Internet activity coordination organizations. In E Conference World (No. 4, pp. 158-166).