Li Xiaoyu,
graduate student BSEU (Minsk, Belarus)
Scientific adviser – Candidate of Political Sciences Barakhvostov P.A.

ON THE GOVERNMENT'S OBLIGATION TO PROTECT CITIZENS' NETWORK INFORMATION SECURITY IN THE DIGITAL ERA

With the increasing degree of digitization and informatization, the Internet has greatly facilitated our lives, and the popularity of new lifestyles such as online stock speculation, online banking and online shopping has led to more and more people keeping their personal information on the Internet, and the security of Internet information has become a problem that cannot be ignored.

At the same time, the government should perform its functions to protect the security of citizens' online information. I believe that it should be mainly reflected in two aspects: firstly, it should take the initiative to protect citizens' online information from illegal collection, use and interference. Secondly, the government should fully respect citizens' online privacy and not arbitrarily disclose or make public citizens' online personal information that should be treated as privacy.

It is mainly targeted at internet service providers, enterprises and other organizations that collect personal online information driven by economic interests.

For example, Facebook and YouTube were fined US$5 billion and US$170 million by the Federal Trade Commission for violating the US Data Privacy Act and the Children's Online Privacy Protection Act respectively; Escort in Italy and the Netherlands was hacked for its forums and user data was sold publicly; a series of data breaches show that industries around the world are still suffering from data breaches The series of data breaches show that industries around the world are still suffering from data breaches, and the companies and users involved are suffering huge losses as a result.

As data breaches occur, governments are beginning to pass legislation to strengthen data protection.

In 2012, the EU introduced the EU General Data Protection Regulation (GDPR), setting the industry standard for global online data protection. in November 2018, the US Consumer Data Protection Act, the US Federal Trade Commission established minimum privacy and information security standards. In May 2019, China issued the Data Security Management Measures, which stipulate that online operators may only collect information if users are aware of the rules for collecting information and agree to it.

The attention of governments has helped to urge companies to raise awareness of the protection of customer data and provide legal safeguards for data privacy protection.

The government should fully respect citizens' online privacy and not arbitrarily disclose or make public citizens' online personal information that should be treated as private.

The government is the largest owner of information resources, as well as the largest collector, producer, manager, user and publisher of information, and its policies cannot be formulated, implemented and monitored without all kinds of information, including citizens' personal data. This gives it the power to obtain personal data through legal and proper procedures, but also reflects the seriousness and horror of the damage that could be done if the more detailed information it collects were to be leaked.

The Prism gate scandal of 2013, for example, illustrates the disgraceful role that the US government plays in violating citizens' privacy through online surveillance. Edward Snowden, a former employee of the CIA, revealed to The Guardian that Prism is a programme in which the NSA and the FBI, by default, take information about a person associated with a foreign government or engaged in terrorist activity when they intend to monitor that person. It is a program of surveillance of citizens' phones and the Internet that is measured by comparison with information about them.

While these government actions are more in the public interest, to protect national security and to combat cybercrime, they do not fully justify the government's control of individuals' online privacy, which in some ways creates a squeeze on the private sphere by public power. In addition, the size of the government itself is already a giant to the weak individual, and failure to restrict and limit its collection and use of citizens' online information is also detrimental to the government's own transformation and development and the protection of individual power.

Ловцов Е.В.,
студент, БрГУ им. А.С. Пушкина (Брест, Беларусь)
Научный руководитель к.полит.н. Северин Э.Н.

ПОЛИТИЧЕСКИЙ БУЛЛИНГ В ИНТЕРНЕТ ПРОСТРАНСТВЕ НА ПРИМЕРЕ ИЗБИРАТЕЛЬНОГО ПРОЦЕССА В США 2020–2021 гг.

Общество XXI века характеризуется постепенной заменой реального мира виртуальным, что в значительной степени ускорило обмен информацией и мнениями между людьми. Анонимность, которую дают интернет сети, пользователи используют по-разному, одни для поиска новых знакомств и друзей, а другие для высказывания своей политической позиции. Социальные сети, появившиеся в начале 2000-х годов, сейчас используются в качестве площадки для политических дебатов, более того они позволяют быстро мобилизовать сторонников на обсуждение и решение конкретной проблемной ситуации. Однако в новых реалиях политической борьбы привычными становятся такие явления как интернет травля и буллинг по политическим мотивам.

В современной психологии общепринятым является следующее определение: «Буллинг (травля) – это преднамеренное систематически повторяющееся агрессивное поведение, включающее неравенство власти или силы» [6, с. 14]. Кибербуллинг, электронная травля – это отдельное направление