IBERIAN MUN GENERAL ASSEMBLY

Officer Report 2019

*The question of protecting individuals’ privacy from government surveillance programs*

As defined in the Human Right Council of 2013; privacy is the presumption that individuals should have an area of autonomous development, interaction and liberty, a “private sphere” with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used. Furthermore, the European Convention of Human Rights in Article 8 states that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Therefore, it is in no way illegal or against human rights for nations to collect information about their civilians as long as such data is collected outside of their personal life. However, such law may be exempted if an individual is seen as a national threat.

Within the past couple of years, there have been concerns about how governments and security agencies come to the conclusion that individuals are a national threat. States have changed their traditional legislature in order to facilitate the collection of their civilians’ private information. In certain nations, interception of communications can be authorized by a governmental minister or a committee while traditional communicational surveillance was authorized by the judiciary. Easier means of allowance for private surveillance of civilians has the potential of violating individuals’ privacy. There will be opposing viewpoints, some nations believing that it is up to their government to decide whom is a national threat and that if a civilian does feel violated he can submit a case to the European Court of Human Rights against the government while other nations may want to take further action in order to independently double check choices made by governments.

Another issue that has come to light in recent years are possible government access to communication data stored within internet companies and service providers. These companies have a legal access – agreed terms and conditions – to individual’s personal information and certain governments have compelled providers to build “lawful interception capabilities” into their technology to enable state authorities to have direct access to content stored by these providers, including e-mails, messages and voicemails. One of the most recent examples is with citizens being concerned about Huawei possibly sharing information with a certain government if they are to become a reputable and worldwide 5G provider in the future. Once more it is up to delegates to propose solutions in order to closely monitor this issue. The delegates are free to include similar issues or other topics as long as they take into consideration the previous definition of privacy.