Научные исследования в сфере нейробиологии, проводимые в мире в течение последнего десятилетия, убедительно показывают, что до определенного возраста несовершеннолетние лица не способны контролировать свое поведение в той мере, в какой этого необходимо социуму [3]. По мнению авторитетного нидерландского нейробиолога Д. Свааба, подростки в силу незрелости некоторых структур мозга (в частности, префронтальной коры головного мозга, отвечающей за способность к анализу, планированию и контролю) не могут в должной мере планировать и анализировать свое поведение [3, с. 136].

В своей известной книге «Мы – это наш мозг» Д. Свааб приводит результаты множества исследований, проведенных с участием несовершеннолетних. Для нас наибольшее значение имеет тот факт, что благодаря этим исследованиям было установлено: подростки не могут предвидеть последствия своих поступков [3, с. 136]. Следовательно, они и не задумываются об этих последствиях. Говоря юридическим языком, сознательно не допускают их наступление. Как отмечает Д. Свааб, у несовершеннолетних «из-за роста уровня половых гормонов во время полового созревания пробуждается … агрессивность и тяга к рискованному поведению. Повышается вероятность несдержанного, антисоциального, агрессивного и криминального поведения» [3, с. 136]. Благодаря исследованиям, проведенным по этой тематике в Нидерландах, удалось установить, что «среди подростков от 10 до 17 лет каждый третий совершал какое-нибудь правонарушение. Речь идет о воровстве, краже со взломом, применении насилия и вандализме. После достижения 17 лет число преступлений снижается. Очевидно, что снижение числа преступлений связано с параллельным развитием префронтальной коры головного мозга, ограничивающей импульсивное поведение и поощряющей моральные поступки» [3, с. 139].

Заключение. Таким образом, мы выяснили, что среди многочисленных факторов преступности несовершеннолетних есть, по крайней мере, один, на который очень сложно воздействовать до определенного момента. Возрастные особенности личности несовершеннолетних выступают в качестве объективного фактора, обусловливающего возможность их преступного поведения. Поскольку это так, правоохранительная система должна быть готова к тому, что преступность среди несовершеннолетних будет всегда, ведь «на место каждого повзрослевшегоподростка, обученного приличному поведению и выпущенного во взрослую жизнь, всегда придет свеженький паренек» [3, с. 139].

1. Сведения о видах преступлений, совершенных несовершеннолетними и при их соучастии в 2020 году [Электронный ресурс] // Официальный сайт Министерства внутренних дел Республики Беларусь. – Режим доступа: https://web.archive.org/web/20160731110204/http://mvd.gov.by/ru/main.aspx?guid=314773. – Дата доступа: 09.09.2021.

2. Ораметов, Э.Д., Стаценко В.Г. О создании профилактико-восстановительной модели предупреждения преступности несовершеннолетних в Республике Беларусь и Туркменистане / Д.Э. Ораметов, В.Г. Стаценко // Наука - образованию, производству, экономике : материалы XXII(69) Региональной науч.-практ. конференции преподавателей, научных сотрудников и аспирантов, Витебск, 9-10 февраля 2017 г. : в 2 т. - Витебск : ВГУ имени П. М. Машерова, 2017. - Т. 1 - С. 271-273 [Электронный ресурс] // Репозиторий Витебского государственного университета им. П.М. Машерова. – Режим доступа: https://rep.vsu.by/handle/123456789/10476. - Дата доступа: 10.09.2021.

3. Свааб, Д. Мы - это наш мозг : От матки до Альцгеймера / Пер. с нидерл. Д. В. Сильвестрова. - СПб. : Изд-во Ивана Лимбаха, 2014. – 544 с.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ СЕТИ ИНТЕРНЕТ В ЕВРОПЕЙСКОМ СОЮЗЕ

Мазурцова Д.О.,
студентка 4-го курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – ***Ивашкевич Е.В.,*** *канд. пед. наук, доцент*

Ключевые слова. Интернет-отношения, кибербезопасность, охрана персональных данных, кибер-рынок.

Keywords. Internet relations, cybersecurity, personal data protection, cyber market.

В связи с тем, что интернет-технологии продолжают развиваться и неизменно влиять на многие аспекты человеческой жизни, все чаще встает вопрос о необходимости со-

здания всеобъемлющей, единой структуры правового регулирования онлайн-среды и обеспечения конфиденциальности персональных данных. Особенно актуально это является для Европейского союза, в рамках которого, несмотря на Шенгенское пространство и единство территории, остается обострившаяся в последнее время проблема соотношения европейского регионального и национального законодательства по некоторым аспектам. Деятельность бизнеса в рамках ЕС сопряжена с соблюдением требований законодательства государств-членов, которое иногда может значительно отличаться или противоречить друг другу, что вызывает сложности для нормального функционирования рынка. С целью избежать подобных ситуаций применительно к киберпространству, в последние несколько лет принимаются единые акты в области обеспечения кибербезопасности на уровне руководящих органов ЕС. Единое правовое регулирование онлайн-среды на наднациональном уровне призвано создать также единые исчерпывающие и четкие правила, охватывающие защиту всех видов личной информации и обеспечение максимально возможного уровня защиты. Цель данной статьи – охарактеризовать основные актуальные проблемы правового регулирования интернет-среды в странах Европейского союза на современном этапе.

Материал и методы. Основными материалами работы являются Общий регламент о защите данных ЕС и Закон ЕС о кибербезопасности. В ходе исследования были использованы формально-юридический метод и метод конкретного правового анализа.

Результаты и их обсуждение. В последнее время во многих европейских странах разразились скандалы вплоть до высшего государственного уровня, связанные с утечкой личных данных, прослушиванием коммуникативных каналов высших должностных лиц в связи с правовой пробельностью европейского законодательства и ненадлежащим контролем за соблюдением режима конфиденциальности со стороны IT-компаний. В связи с этим, в рамках общей внешней политики и политики безопасности на уровне ЕС был принят Общий регламент о защите данных 2018 г., который является наиболее полным, единым документом применимого кибернетического законодательства во всех государствах-членах ЕС. Регламент напрямую регулирует деятельность иностранных компаний, ведущих бизнес на европейской территории, а также распространяется на все организации, имеющие дело с персональными данными граждан ЕС независимо от того, где они находятся или зарегистрированы.

Общий регламент принят с целью гармонизации нормативно-правовой базы о защите данных и конфиденциальности в государствах-членах и позволяет странам ЕС вводить ограничения, преимущественно штрафы, в отношении организаций, которые не соблюдают общие установленные правила. Регламент направлен на защиту личных данных и конфиденциальности граждан ЕС и упрощает процесс регулирования для международных организаций. Документ требует от акторов неукоснительного следования определенным протоколам и принятия своевременных мер, гарантирующих, что данные не станут общедоступными без явного информированного согласия.

Общий регламент ЕС декларирует ряд прав физических лиц: право на получение информации, право доступа к собственной персональной информации, право на изменение информации о физических лицах, на удаление нежелательной для лиц информации, на ограничение обработки персональных данных, на переносимость данных с одного устройства на другое, на возражение, а также право на автоматизацию принятых решений и профилирование.

Среди основополагающих постулатов работы с персональными данными документ устанавливает 7 ключевых принципов: законность, справедливость и прозрачность; ограничение цели использования данных; минимизация данных; точность; ограничение по хранению данных; целостность и конфиденциальность (безопасность); подотчетность.

Общий регламент о защите данных ЕС является одним из самый жёстких и подробных НПА в области защиты персональных данных в мире, он расширяет возможности физических лиц получать доступ к собственной персональной информации и устанавливает ограничения для организаций по использованию личной информации граждан [1].

Продолжая работу над созданием эффективного единообразного правового регулирования онлайн-пространства, в 2019 г. Европарламент ЕС принял Регламент № 881,

известный как Закон ЕС о кибербезопасности. Данный документ является первым сводом правил, касающихся сертификации кибербезопасности для всех стран ЕС, и преследует две цели:

1. создание Агентства по кибербезопасности ЕС (ENISA) как структуры, постоянно регулирующей онлайн-пространство на уровне ЕС;

2. создание единой системы сертификации кибербезопасности для разъяснения установленных стандартов соответствия для организаций, работающих в странах ЕС.

Закон ЕС о кибербезопасности не только усиливает полномочия ENISA, но и позволяет компаниям, ведущим бизнес в государствах-членах, сертифицировать продукты информационно-коммуникационных технологий (ИКТ) по всему Союзу. Европейская система сертификации кибербезопасности фактически заменяет собой все национальные системы, что обеспечит применение единообразного подхода при проверке соответствия заявленных товаров и услуг ИКТ единому списку общих стандартов сертификации. В рамках данной системы существует 3 уровня гарантии для этих товаров: базовый; средний; высокий.

В перспективе ENISA планирует принять несколько нормативных приложений для каждого уровня сертификации кибербезопасности, которые будут разработаны с указанием типа охватываемых товаров ИКТ, цели их применения, требуемых стандартов безопасности, методов оценки и срока действия выданных сертификатов. Данные положения о сертификации должны будут в дальнейшем применяться в каждом государстве-члене ЕС, в свою очередь агентство ENISA будет отвечать за регулярный обзор принятых нормативных стандартов о сертификации каждые 5 лет с целью проверки их на соответствие критериям, установленным Законом ЕС о кибербезопасности.

Закон ЕС о кибербезопасности предоставляет компаниям, работающим в ЕС, возможность подтвердить, что их товары или услуги соответствуют стандартам кибербезопасности ЕС. На данный момент сертификация не является обязательной, решение об участии принимает сама организация. Основное преимущество участия в сертификации– гарантия того, что соответствие товаров и услуг общим стандартам ЕС в области кибербезопасности будет признано всеми странами Союза. Фактически, структура направлена на установление единого стандарта для сертификации кибербезопасности и недопущение разрозненного подхода, при котором наблюдалось введение государствами-членами ЕС разных стандартов при определении соответствия товаров и услуг организации политике кибербезопасности [2].

Заключение. Таким образом, ЕС начал активную работу в области правового регулирования онлайн-среды и создания общей системы кибербезопасности на наднациональном уровне доя всех государств-членов, что призвано решить возникшие коллизии разных государственных систем, связанные с отличающимся требованиями к бизнес-участникам среды интернет, а также создать эффективный механизм взаимодействия государств как единый скоординированный ответ на возникающие кибер-угрозы.

1.The General Data Protection Regulation[Electronic resource]. – Mode of access:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725&qid=1631032339989. – Date of access: 05.09.2021.

2. EU Cybersecurity Act (Regulation (EU) 2019/881) [Electronic resource]. – Mode of access: https://eur-lex.europa.eu/eli/reg/2019/881/oj. – Date of access: 06.09.2021.

3. Мазурцова, Д. О. Правовое регулирование кибер-рынка в странах Северной Европы / Д. О. Мазурцова // XIVМашеровские чтения: материалы международной научно-практической конференции студентов, аспирантов и молодых ученых, Витебск, 21 октября 2020 г. / Витеб. Гос. ун-т; редкол.: Е. Я. Аршанский (гл. ред.) [и др.]. – Витебск: ВГУ имени П. М. Машерова, 2020. – С. 473-475. – Режим доступа: https://lib.vsu.by/jspui/bitstream/123456789/25851/1/%d0%9c%d0%b0%d1%88%d0%b5%d1%80%d0%be%d0%b2%d1%81%d0%ba%d0%b8%d0%b5%20%d1%87%d1%82%d0%b5%d0%bd%d0%b8%d1%8f%202020.pdf. – Дата доступа: 07.09.2021.