Международно-правовая защита персональных данных в сети Интернет: общие положения

Абрамова А. Г.
Аспирантка Российско-Армянского университета (Ереван, Армения)
anna.yakhshibekian@gmail.com

Ключевые слова: *персональные данные, интернет, сеть, Директива по защите данных, Европейская конвенция по правам человека, Европейский Союз, Совет Европы, автоматизированная обработка данных, анонимизация, биометрические данные, технология распознавания лиц, политика конфиденциальности*

Անձնական տվյալների միջազգային իրավական պաշտպանությունը ցանցում. Ընդհանուր դրույթներ

Աբրամովա Ա. Գ.
Հայ-Ռուսական համալսարանի ասպիրանտ (Երևան, Հայաստան)
anna.yakhshibekian@gmail.com

Ամփոփում: Սույն գիտական աշխատանքը նվիրված է համացանցում անձնական տվյաների միջազգային պաշտպանության հետ կապված առանձին խնդիրների ուսումնասիրությանը, ինչպես նաև անձին իդենտիֆիկացնելու և անձի բիոմետրիկ տվյալների հավաքագրման և պահպանման վերաբերյալ հարցերին:Մարդու իրավունքների եվրոպական դատարանը մի շարք որոշումներ է կայացրել կապված ֆիզիկական, ինչպես նաև իրավաբանական անձանց կողմից իրենց վերաբերող տվյալների պաշտպանության վերաբերյալ, որը թույլ է տալիս հետևողականորեն վերլուծել տվյալ ոլորտում առաջացող որոշ հարցեր:Հոդվածում հեղինակը ուսումնասիրել և վերլուծել է անձնական տվրյալների պաշտպանության վերաբերյալ մի շարք կարևոր նշանակություն ունեցող դատական գործեր: Հեղինակն հոդվածում նաև անդրադարձել է «Ֆեյսբուք» սոցիալական ցանցում գործող դեմքի ճանաչման տեխնոլոգիայի կիրառման օրինաչափությանը և փորձել է օբյեկտիվորեն և համակարգված գտնել տվյալ գործառույթից ծագող իրավական խնդիրները:Միաժամանակ, հեղինակն առաջարկոել է քննարկվող խնդիրների վերացմանն ուղղված գործնական, իրավական և, որոշ չափով, տեխնիկական լուծումներ:
Վճռորոշ բառեր՝ անձնական տվյալներ, ինտերնետ, համացանց, Անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգ, Մարդու իրավունքների եվրոպական կոնվենցիա, Եվրոպական Միություն, Եվրոպայի խորհուրդ, տվյալների ավտոմատացված մշակում, անանունացում, կենսաչափական տվյալներ, դեմքի ճանաչման տեխնոլոգիա, գաղտնիության քաղաքականություն

International legal protection of personal data on the Internet: general provisions

Abramova A. G.
PhD student in Russian-Armenian University (Yerevan, Armenia)
anna.yakhshibekian@gmail.com

Abstract: This scientific article is devoted to the study of certain issues related to the international protection of personal data on the Internet, as well as issues related to the identification of individuals, the collection and storage of biometric data. The European Court of Human Rights has ruled a number of cases regarding the protection of data concerning individuals / natural persons as well as legal entities, which allows for a consistent analysis of some issues arising in this area. In this article, the author studies and analyzes several of the most important lawsuits regarding the protection of personal data. In the present article author also referred to the regularity of the application of face recognition technology operation in the "Facebook" social network and tried to objectively and systematically find the legal issues arising from the given function. At the same time, the author proposed practical, legal and, to some extent, technical solutions to eliminate the issues under discussion.
Keywords: personal data, internet, network, General Data Protection Regulation, European Convention on Human Rights, European Union, Council of Europe, automated data processing, anonymization, biometric data, face recognition technology, privacy policy

В современных условиях нерегулируемого расширения информационного пространства, и господства, так называемой, «цифровой эры», право на защиту персональных данных должно

быть причислено к фундаментальным и основополагающим правам и свободам человека.

Согласно законодательству Европейского Союза, а также законодательству Совета Европы, «личные данные» определяются как информация, относящаяся к идентифицированному или идентифицируемому физическому лицу [**1**], то есть информация о человеке, чья личность либо явно ясна, либо может быть установлена с использованием этих данных путем получения дополнительной информации. Если данные о таком лице обрабатываются, то этот человек является «субъектом данных».

Право на защиту данных развивается из права на уважение частной жизни. Концепция частной жизни, как правило, относится к людям. Таким образом, физические лица являются основными бенефициарами защиты данных. Кроме того, согласно мнению Рабочей группы по статье 29 только живые существа могут быть под защитой евпропейского законодательства о защите данных [**2**].

Практика ЕСПЧ в отношении статьи 8 ЕКПЧ показывает, что полное отделение вопросов личной и профессиональной жизни практически довольно сложно [**3**]. Кроме того, если вопросы профессиональной жизни также могут быть предметом защиты данных, представляется сомнительным, что только физическим лицам должна быть предоставлена защита. Права в рамках ЕКПЧ гарантируются не только физическим лицам.

По этому поводу, существует практика ЕСПЧ, в которой рассматривались дела по заявлениям юридических лиц, утверждающих нарушение их права на защиту от использования их данных согласно статье 8 ЕКПЧ. Однако в подобных случаях Суд рассмотрел дело в соответствии с правом на неприкосновенность жилища и тайну корреспонденции, а не в рамках права на защиту личной жизни. Подобным примером может служить дело ‘Берн Ларсен Холдинг АС и другие против Норвегии’ [**4**]. Дело касалось жалобы трех норвежских компаний против решения налогового органа, в котором им было поручено предоставить налоговым аудиторам копию всех данных на компьютерном сервере, которые использовались совместно. ЕСПЧ установил, что такое обязательство для компаний-заявителей представляет собой вмешательство в их права на уважение «неприкосновенности жилища» и «тайну переписки» по смыслу статьи 8 ЕКПЧ. Однако Суд счел, что налоговые органы имеют эффективные и адекватные гарантии от злоупотреблений: компании-заявители были уведомлены заранее; присутствовали и могли делать заявления во время вмешательства на месте; и материал должен был быть уничтожен после завершения налогового обзора. В таких обстоятельствах справедливое равновесие было установлено между правом заявителей на уважение «неприкосновенности жилища» и «тайны переписки» и их заинтересованностью в защите конфиденциальности лиц, работающих на них, с одной стороны, и общественных интересов в обеспечении эффективного контроля для целей налогообложения, с другой. В результате, Суд постановил, что в этом случае не имело место нарушения Статьи 8 ЕКПЧ.

Согласно Конвенции 108 о защите физических лиц при автоматизированной обработке персональных данных (далее «Конвенция 108»), защита данных касается, прежде всего, защиты физических лиц, однако договаривающиеся стороны могут распространять защиту данных и на юридических лиц в своем внутреннем законодательстве. Так, например, законодательство о защите данных ЕС не охватывает защиту юридических лиц. Однако национальные регулирующие органы могут свободно регулировать этот вопрос [**5**].

К примеру, в деле Volker и Markus Schecke и Hartmut Eifert v. Land Hessen [**6**] Суд Евпропейского Союза, ссылаясь на публикацию персональных данных, касающихся бенефициаров сельскохозяйственной помощи, считает, что «юридические лица могут требовать защиту статей 7 и 8 Хартии Европейского Союза об основных правах от 2000 года, в связи с такой идентификацией только в том случае, если официальное название юридического лица идентифицирует одного или нескольких физических лиц. Право на уважение частной жизни в отношении обработки персональных данных, признанных в статьях 7 и 8 Устава, касается любой информации, относящейся к идентифицированному или идентифицируемому лицу» [**6**]. Таким образом, в данном деле Суд ЕС косвенно распространил действие соответствующих положений о защите персональных данных на юридических лиц, посредством указания факта наличия идентифицирующей информации о физическом лице в названии юридического лица.

Важно отметить, что идентификация лица, согласно законодательству ЕС, а также по законодательству СЕ это информация содержит данные о человеке, если:

• индивид идентифицируется в этой информации; или

• если индивид, хотя и не идентифицирован, описывается в этой информации таким образом, который позволяет при дальнейшем исследовании узнать, кто является субъектом данных.

Касательно формы в которой используются личные данные, следует отметить, что персональные данные могут содержать как устные так и письменные сообщения или изображения [**7**], включая кадры или звуки [**8**]. Электронно записанная информация, а также информация на бумаге могут быть персональными данными и даже образцы клеток человеческой ткани могут быть персональными данными, поскольку они хранят в себе информацию касательно ДНК человека.

Что касается определения конфиденциальных данных, то как Конвенция 108 (статья 6), так и Директива по защите данных (статья 8) называют следующие категории:

- личные данные, раскрывающие расовое или этническое происхождение;
- личные данные, раскрывающие политические взгляды, религиозные или иные убеждения; а также
- личные данные, касающиеся здоровья или сексуальной жизни.

В Директиве по защите данных дополнительно указывается и «членство в профсоюзе» в качестве конфиденциальных данных, так как эта информация может быть сильным индикатором политических убеждений или принадлежности. В Конвенции 108 также учитываются личные данные, связанные с уголовными обвинительными приговорами.

В соответствии с принципом ограниченного хранения данных, содержащимся в Директиве по защите данных, а также в Конвенции 108, данные должны храниться «в форме, которая позволяет идентифицировать субъектов данных не более, чем это необходимо для целей,сбора или обработки этих данных» [**9**]. Следовательно, данные должны быть анонимизированы, если контроллер захочет хранить их после того, как они устарели и больше не служат их первоначальной цели.

Говоря об анонимизации, в первую очередь, следует указать что данные анонимны, если все идентифицирующие элементы были исключены из набора персональных данных. Ни один элемент не может быть оставлен в информации, которая могла бы, приложив разумные усилия, повторить идентификацию соответствующего лиц(а) [**10**]. Если данные были успешно анонимированы, они больше не являются персональными данными.

Следующей категорией являются псевдонимизированные данные. Личная информация содержит идентификаторы, такие как имя, дата рождения, пол и адрес. Когда персональная информация псевдонимизирована, идентификаторы заменяются одним псевдонимом. Псевдоомификация достигается, например, путем шифрования идентификаторов в личных данных. Псевдонимизированные данные прямо не упоминаются в юридических определениях Конвенции 108 или Директивы по защите данных. Однако в Пояснительном докладе к Конвенции 108 в своей статье 42 говорится о том, что «требование, предъявляемое в соответствии с временными ограничениями для хранения данных в их связанной с именем форме, не означает, что данные должны через какое-то время быть безоговорочно отделены от имени лица, к которому они относятся, но должно быть обеспечено только то, чтобы невозможно было легко связывать данные и идентификаторы» [**11**]. Ссылка на личность все еще существует в форме псевдонима плюс ключ дешифрования. Для всех, у кого нет ключа дешифрования, псевдонизированные данные вряд ли могут быть идентифицированы. Для тех, кто имеет право использовать повторную идентификацию ключа дешифрования, это легко.

В современном мире особо остро стоит защита персональных данных в сети интернет.

Во время «зеленой революции» в 2009 году иранские военные опубликовали фотографии с протестов на веб-сайте и пригласили граждан опознать двадцать отдельных лиц, которые были выделены на этих фотографиях [**12**]. Они утверждали, что арестовали по меньшей мере двух человек зафиксированных на фотографиях вскоре после протестов [**13**]. Согласно некоторым источникам, иранское правительство пыталось использовать технологию распознавания лиц для идентификации протестующих, хотя ее технология все еще находится на стадии разработки [**14**]. Представьте себе, если бы правительство просто могло сопоставить эти лица с сотнями миллиардов фотографий, доступных на Facebook. Сопоставления могли выявить не только имена протестующих [**15**], но и их местонахождение, их контакты, их онлайн-беседы с другими протестующими и, возможно, их планы на будущее. Из этого следует, в этом случае под угрозой будут находиться права индивида, которые закреплены в ст. 8 ЕКПЧ.

Лица особенно полезны для целей идентификации, поскольку они являются отличительными и, в большинстве случаев, общедоступными. Другие персональные особенности, которые находятся на виду, такие как пальто или стрижка, могут быть легко заменены, но значительно изменить лицо, чтобы сделать его неузнаваемым, довольно сложно. И все же большинство людей могут оставаться анонимными, даже публично, потому что у них есть только ограничен-

ный круг знакомых, которые могут их распознать. Использование технологии распознавания лиц в социальных сетях сдвигает эту установку. Она может привязать анонимное лицо не только к имени, но также ко всей информации в профиле социальной сети. Учитывая риски технологии распознавания лиц в сочетании с огромным количеством персональной информации, объединенной в социальных сетях, в этой статье представлены две основные идеи.

- Во-первых, применяя теорию контекстуальной целостности профессора Хелен Ниссенбаум[1], можно утверждать, что технология распознавания лиц в социальных сетях нуждается в тщательном регулировании, поскольку она преобразует информацию, которую пользователи используют (например, она преобразует простую фотографию в биометрические данные, которые автоматически идентифицируют пользователей) и предоставляет эту персональную идентификационную информацию новым получателям, не учитывая волю пользователя.
- Во-вторых, есть большое количество недостатков в действующем законодательстве, и очевидно, что только закон не может решить эту проблему.

Полный запрет на автоматическое распознавание лиц в социальных сетях сдерживал бы развитие технологий, которые сами по себе являются полезными. В то же время традиционная система конфиденциальности уведомлений и согласия не может защитить пользователей, которые не понимают процесс автоматического распознавания лиц, и безрассудно продолжают делиться своей личной информацией из-за сильных сетевых эффектов. Вместо этого предлагаем многогранное решение, направленное на снижение затрат на переключение между социальными сетями и предоставление пользователям лучшей информации о том, как их данные используются.

Аргументация данного положения заключается в том, когда пользователи действительно могут свободно переключать между собой не связанные сети, они будут иметь возможность осуществлять свой выбор и требовать, чтобы социальные сети соблюдали и уважали их ожидания защиты их персональных данных.

Предлагаемое правовое решение направлено на то, чтобы реформировать действующие в настоящее время законы об уведомлениях и согласие требовать адекватного информативного уведомления и подлинного согласия. Этот предлагаемый закон должен предусматривать требование, чтобы социальная сеть предоставляла пользователям подробную, но понятную информацию о том, как она собирает, хранит, обрабатывает и совместно использует биометрические данные пользователя. Также будет предусмотрено получение согласия от пользователей, прежде чем собирать их данные или использовать их для новых целей.

Эти требования будут частью более широкого закона о защите данных, которое должно обеспечиваться инициативным агентством, которое имеет возможность исследовать сложные методы обработки данных в социальных сетях. В данном предложении признается, что даже улучшенная модель уведомления и согласия сама по себе не может решить эту проблему, если у пользователей нет реальной возможности выйти из сети без ущерба для их социальной жизни в Интернете [**16**].

С этой целью, структурные/архитектурные и рыночные решения данного предложения направлены на снижение вклада в переключения между социальными сетями, чтобы освободить пользователей от сетевого эффекта, который в настоящее время блокирует их в социальной сети.

Архитектурные решения позволят пользователям: (1) предотвратить централизованную социальную сеть от извлечения биометрических данных путем обмена фотографиями со своими друзьями через социальную сеть; (2) экспортировать свою личную информацию на платформу, которой они доверяют, по стандартам переносимости данных; (3) продолжать общаться с друзьями, которые остаются в централизованной социальной сети по стандартам совместимости; а также (4) защищать их конфиденциальность, когда они фотографируются в общественных местах или загружают фотографии в общедоступную сеть. Рыночные решения также позволят пользователям субсидировать использование своей социальной сети, чтобы избежать сбора особо чувствительной информации, такой как их биометрические данные, и обсуждать свои собственные условия использования данных при совместном использовании фотографий в социальных сетях.

Несмотря на то, что предложение предназначено для всех современных и будущих технологий распознавания лиц в социальных сетях, примеры будут приведены из самой популярной социальной сети- Facebook [**17**]. Отметим, что Facebook имеет важную социальную функцию. Действительно, недавно Совет Европы провозгласил, что «социальные сети служат защитой прав человека и катализаторами демократии» [**18**]. Они особенно важны для молодежи, которая полагается на социальные сети для «разви-

[1] профессор информатики в Cornell Tech .

тия своих личностей и как часть их участия в дискуссиях и социальной деятельности» [**18**].

Таким образом, Facebook способствует социальному взаимодействию и политическому дискурсу, которые считаются для нашего общества очень ценными функциями, если не существенными [**19**]. Именно благодаря своей важной роли Facebook должен соблюдать конфиденциальность своих пользователей. Он должен уделять особое внимание тому, как он использует фотографии и биометрические данные, потому что нет ничего восприимчивого к идентификации, чем лицо человека.

Технология распознавания лиц стремится объединить превосходные навыки восприятия людей с огромной вычислительной мощностью и емкостью памяти компьютеров. Люди узнают друг друга на основе их внешности, сосредоточив свое внимание на чертах лица, а также используя другие органы чувств, такие как обоняние, осязание, слух и так далее [**20**]. Хотя узнавание/опознание является естественным человеческим умением, человеческий мозг может запомнить только ограниченное количество лиц. С другой стороны, компьютеры могут обрабатывать и запоминать огромное количество черт лица, чтобы распознавать еще большее количество людей. Но следует учитывать, что человеческий мозг выполняет более полную работу по распознаванию лиц, чем компьютеры, потому что он способен сочетать визуальное распознавание с другими человеческими органам чувств. Компьютеры не имеют контекстуального знания о том, какую одежду человек намеревается носить или в чьей компании лицо может быть найдена. Тем не менее, компьютерное зрение заимствует методы человеческого восприятия. Эти методы идентифицируются посредством психологических исследований того, на какие черты лица люди обращают больше внимания, когда они узнают других.

Точность распознавания зависит от таких факторов, как применяемая точная методология, количество доступных исследуемых изображений, качество фотографий и видимость личности на этих фотографиях [**21**]. Процесс распознавания лиц постепенно улучшается, тогда как технологии раннего распознавания лиц едва ли могли распознать одно лицо с фронтального ракурса, в настоящее время разработаны технологии, которые могут идентифицировать людей с разных ракурсов и отличать лица от загроможденного фона. Как показывают исследования, проведенные исследователями из Университета Карнеги-Меллона, фотографии, доступные на Facebook без входа в систему, достаточны для того, чтобы идентифицировать студентов в кампусе с показателем успеха в 31,18% при использовании технологии распознавания лиц, которая была общедоступной до ее недавнего приобретения компанией Google [**22**].

В декабре 2010 года Facebook представила новую функцию - «Рекомендация фото тегов» - которая использует ранее отмеченные фотографии и технологию распознавания лиц, чтобы идентифицировать людей на новых фотографиях, на которых пользователей могут затем отметить. Facebook собирает и сохраняет большое количество информацию о своих пользователях. Эта информация включает фотографии, в том числе, автоматически помеченные, из которых извлекаются биометрические данные. Она также включает всю информацию, отображаемую в профиле Facebook, поскольку, путем «отметки» фотографии, эта функция создает гиперссылку на профиль пользователя. Несмотря на то, что Facebook собирает и хранит огромный объем данных, ниже будут рассмотрены биометрические данные, необходимые для распознавания лиц.

Пользователь предоставляет большую часть информации в профиле Facebook. В первую очередь, Facebook требует, чтобы новый пользователь предоставил «имя, адрес электронной почты, день рождения и пол». По желанию пользователю также предлагается предоставить свои религиозные убеждения, политические взгляды и сексуальную ориентацию. Далее пользователь проходит процесс «добавления в друзья» с другими пользователями, которые, в свою очередь, в реальной жизни могут быть друзьями, одноклассниками, родственниками или коллегами в автономном режиме, Facebook также сохраняет список этих «друзей». Более того, совсем недавно Facebook начал просить пользователей описать их отношения со своими друзьями.

Из политики использования данных Facebook, видно, что Facebook использует все помеченные фотографии человека в качестве базы данных изображений, не выделяя фотографии, которые пользователь предоставляет только некоторым друзьям через свои настройки конфиденциальности. Это означает, что если пользователь ограничивает доступ к фотографии, чтобы она была видна только для ее семьи (например), Facebook может, тем не менее, извлечь из нее биометрические данные и использовать ее с помощью Photo Tag Suggest, чтобы позволить другим друзьям из Facebook определить ее/его на новых фотографиях.

Из-за различного восприятия защиты данных в разных странах возникает большое количество

нарушений основополагающих прав человека, таких как право на защиту личных данных и т.д..

На наш взгляд, использование биометрических данных, без предварительного четкого уведомления и получения разрешения является строгим нарушением правил ЕС в сфере защиты данных. В частности, наблюдатели по защите данных Ирландии подняли ряд вопросов, связанных с Фейсбук и его реинтродукции технологий распознавания лиц в Европе. Раннее, в 2012 году социальная сеть была вынуждена закрыть данную функцию распознавания лиц.

Таким образом, несмотря на то, что Facebook американская компания, и в целом, пытается соотвтетствовать нормам защиты данных США, тем не менее, данная социальная сеть пользуется популярностью во всем мире. Данный факт должен обязать Фейсбук установить более эффективную защиту персональных данных и при этом обеспечить соблюдение основополагающих прав человека.

18 апреля 2018 года Facebook объявил о ряде мер, которые, по его словам, помогут соблюдению строгих новых законов о данных в Европейском союзе- GDPR, которое вступит в силу 25 мая настоящего года. Среди данных мер, предположительно ожидается:

- Разрешение пользователей на то, чтобы Facebook использовал данные от партнеров, (например, других веб-сайтов), чтобы показывать им рекламу.
- Разрешение пользователей на открытость информации о политических и религиозных взглядах.
- Разрешение пользователей на технологию распознавания лиц.
- Согласие людей на обновление политики конфиденциальности и условий обслуживания Facebook.

В рамках анонса представитель Facebook указал, что он вернет технологию распознавания лиц на платформу. Как уже было отмечено, Facebook прекратил эту функцию в Европе в 2012 году после беспокойства со стороны регулирующих органов и сторонников защиты частной жизни.

В рамках данной статьи также Рассмотрим дело K.U. v. Finland [**23**], которое затрагивает вопрос о конфиденциальности и цифровых правах, который был решен Европейским судом по правам человека (ЕСПЧ) второго декабря 2008 года.

В целом, дело касается 12-летнего мальчика, который был объектом рекламы сексуального характера на сайте знакомств в Интернете. Реклама была опубликована без его ведома и включала его имя, год рождения, подробное описание его физических характеристик, фотографию его и его номер телефона, который был правильным, за исключением одной цифры. В рекламе утверждалось, что он ищет интимные отношения с человеком его возраста и старше. Жертва узнала о существовании рекламы, когда пожилой мужчина связался с ним по электронной почте, чтобы встретиться с ним, и «затем, чтобы увидеть, что он хочет» [**23**]. Основной проблемой этого дела был отказ поставщика услуг раскрыть личность автора с объяснением того, что он связан конфиденциальностью телекоммуникаций. Законодательство, действующее в то время, запрещало поставщикам интернет-услуг раскрывать идентификацию пользователя. Цель законодательства заключалась в защите свободы выражения мнений и праве на анонимное выражение. Национальные суды Финляндии подтвердили, что поставщик услуг не должен был предоставлять какую-либо информацию из-за своей обязанности поддерживать конфиденциальность. После решения национального суда ребенок пожаловался в Европейский суд по правам человека на то, что его право на уважение его личной жизни было нарушено (статья 8 Европейской конвенции о правах человека) и что Финляндская Республика не смогла предоставить ему эффективное средство правовой защиты, как того требует статья 13 ЕКПЧ.

Проблема, стоящая перед Судом, заключалась в том, должно ли государство требовать от интернет-провайдеров раскрывать личность частного пользователя, разместившего информацию о ребенке без их согласия на веб-сайте, который сделал его целью для педофилов. Суд постановил, что имело место нарушение конфиденциальности заявителя в нарушение статьи 8. Судебная практика заявила, что «как общественный интерес, так и защита интересов жертв преступлений, совершенных в отношении их физического или психологического благополучия, требуют наличия средства правовой защиты, позволяющего выявлять и предавать суду фактического правонарушителя». Суд указал, что отсутствие уголовной санкции, которая может быть применена к текущему делу, является серьезным вопросом, поскольку акт был преступным, привлек несовершеннолетнего и сделал его объектом для педофилов. Статья 8 Конвенции не только защищает от вмешательства правительства, но также налагает позитивные обязательства по обеспечению уважения частной жизни граждан. Суд подчеркнул, что дети и другие уязвимые лица заслуживают большей государственной защиты в форме эффективного сдерживания от таких серьезных вмешательств в основные

аспекты их личной жизни. Суд отклонил аргумент правительства о том, что достаточная защита неприкосновенности частной жизни обеспечивается наличием уголовного преступления клеветы, поскольку «наличие преступления имеет ограниченные сдерживающие последствия, если нет средств для идентификации фактического правонарушителя и привлечения его к ответственности» [**23**]. Он также отклонил аргумент правительства о том, что заявитель имел средство правовой защиты, поскольку он мог получить возмещение от поставщика услуг, заявив, что оно «недостаточно в обстоятельствах этого дела». Наконец, Суд заявил, что, хотя свобода выражения мнений и конфиденциальность сообщений являются важными соображениями, и пользователи этой технологии должны иметь гарантию уважения их личной неприкосновенности и свободы выражения, такая «гарантия не может быть абсолютной и должна уступать предотвращению беспорядков или преступлений или защите права и свободы других». Учитывая, что нарушение статьи 8 уже было установлено, Суд не рассматривал предполагаемое нарушение Статьи 13.

Учитывая растущую зависимость общества от сетевых систем ясно, что преступления против персональных данных представляют собой серьезную угрозу нашему будущему благосостоянию. Кибербезопасность и защита данных создает много проблем для законодательной власти. С одной стороны появляются случаи, которые не охватываются традиционными условиями уголовных преступлений в нашей законной правовой системе, поскольку данные не являются физическим объектом и не могут быть классифицированы классически. С другой стороны, законодательный орган находится в постоянной конкуренции с хакерами и уголовными преступниками, поскольку новые способы правонарушения могут регулироваться только после их возникновения в определенной последовательности и появлением последствий. Новые технологии, более быстрая сетевая связь и Интернет являются необходимостью для современного общества и его надлежащего функционирования, благополучия и прогресса. Таким образом, благодаря этой сверхзависимости, которая сложилась между сетями и людьми, защита данных приобретают все большее значение. Правительство все в большей и большей степени несет ответственность за криминализацию и регулирование законодательных правонарушений, но также сохраняя соразмерность праву на свободу выражения. В рамках этой оценки ценностей законодательный орган должен иметь ввиду столкновение различных законных интересов и оправдывать любые посягательства, которые могут возникнуть.

В работе мы проанализировали следующие основные идеи:

- применяя теорию контекстной целостности, можно утверждать, что технология распознавания лиц в социальных сетях должна регулироваться, поскольку она связывает анонимное лицо с другим личным информационным ресурсом в Интернете.
- усовершенствование нынешней модели конфиденциальности и защиты персональных данных в законодательстве ЕС, которая требует более информативного уведомления пользователей и получение конкретного согласия, прежде чем собирать и использовать личную информацию, которая находится под защитой ряда международных соглашений.
- установление более строгих правил для отправления уведомлений и получения согласия, на данном этапе не решат проблему незаконного сбора и обработки персональной информации, пока сетевой эффект блокирует пользователей в одной общей социальной сети.

Для достижения этого:

- должны быть приняты базовые правила защиты персональных данных основанные на ст. 8 Европейской Конвенции по правам человека а также Будапештской конвенции от 2001 года, которые включат в себя более конкретные требования к уведомлению и соглашению, либо добавление этого положения в GDPR.
- в предлагаемых правилах должен быть включен пункт, согласно которому, государствам-участникам необходимо будет внедрить в свои государственные образовательные программы для информирования детей и взрослых о защите данных в Интернете,
- техническая реализация уведомления и согласия, а также стандартов переносимости и совместимости данных будет предоставлена компаниям. В таких социальных сетях как Фейсбук, например, личная информация должна быть максимально защищена. То есть, все настройки «по умолчанию» будут в интересах пользователей, что может способствовать уменьшению риска несанкционированного доступа к данным.

Таки образом, обобщая, можно отметить, что сновной вклад этого исследования заключается в предложении снижения сетевого эффекта в централизованных социальных сетях, дополняя требования юридического уведомления и согласия на сбор, хранение и обработку персональных данных.

Список использованных источников

1. Data Protection Directive 1995, Art. 2 (a); Конвенция 108 1981, Ст. 2 (a).
2. Article 29 Working Party (2007), Opinion 4/2007 on the concept of personal data, WP 136, 20 June 2007, p. 22.
3. *Rotaru v. Romania* [GC] No. 28341/95 (ECtHR, 4 May 2000), para. 43
4. *Bernh Larsen Holding AS and Others v. Norway* No. 24117/08 (14 March 2013)
5. Data Protection Directive 1995, Recital 24.25
6. *Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen* Joined cases C-92/09 and C-93/09, (CJEU, 9 November 2010)
7. *Von Hannover v. Germany* No. 59320/00 (ECtHR, 24 June 2004)
8. Data Protection Directive 1995, Recitals 16 and 17; *P.G. and J.H. v. the United Kingdom* No. 44787/98 (ECtHR, 25 September 2001), paras. 59 and 60
9. Data Protection Directive 1995, Art. 6 (1) (e); and Convention 108 1981, Art. 5 (e).
10. Convention 108 1981, Art. 42
11. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434
12. *Iranian Officials 'Crowd-Source' Protester Identities*, GLOBAL VOICES (June 27, 2009, 5:28 PM), http://globalvoicesonline.org/2009/06/27/iranian-officials-crowd-source-protester-identities-online/ (фотографии выложенные: http://www.gerdab.ir/fa/pages/?cid=407).
13. Colin J. Bennett, Convergence Revisited: Toward a Global Policy for the **Protection** of Personal **Data**?, **in** Technology and Privacy: The New Landscape 99-103 (Philip E. Agre & Marc Rotenberg eds., 1997) (noting that the development of global networks has exacerbated privacy concerns)
14. Frederick Schauer, **Internet** Privacy and the Public-Private Distinction, 38 Jurimetrics J. 555, 557-61 (1998).
15. Alexander Dix, The German Railway Card: A Model Contractual Solution of the "Adequate Level of **Protection**" Issue?, Proc. XVIII Int'l Conf. **Data** Prot. Comm'rs (1996) .
16. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS, no. 4, 2011, at 32, 35 (2011)
17. Justin Mitchell, "*Making Photo Tagging Easier"*, THE FACEBOOK BLOG (Dec. 15, 2010), https://www.facebook.com/blog.php?post=467145887130.
18. *Recommendation CM/Rec (2012) 4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services*, COUNCIL OF EUR. (Apr. 4, 2012).
19. Recommendation, COUNCIL OF EUR., supra note 10.
20. FACE PROCESSING: ADVANCED MODELING AND METHODS 8-9 (Wenyi Zhao & Rama Chellappa eds., 2006).
21. FACE PROCESSING, *supra* note 15, at 10-11.
22. Alessandro Acquisti, Associate Professor of Information Technology and Public Policy, Heinz College at Carnegie Mellon University, BlackHat Webcast: Faces of **Facebook**: **Privacy** in the Age of Augmented Reality (Jan. 9, 2012)
23. *K.U. v Finland* App no 2872/02 (ECtHR, 2 December 2008)

Сдана/Հանձնվել է՝ 21.08.2020
Рецензирована/Գրախոսվել է՝ 24.08.2020
Принята/Ընդունվել է՝ 25.08.2020