УДК 343.34:004(470+5:265)

DOI dx.doi.org/10.24866/1813-3274/2018-3/78-91

Я. О. Кучина¹

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: kuchina.yao@dvfu.ru

**ПРЕДМЕТ КИБЕРПРЕСТУПЛЕНИЙ И ЗАВИСИМОСТЬ
ЕГО ОПРЕДЕЛЕНИЯ ОТ ДИФФЕРЕНЦИАЦИИ
ПОНЯТИЙ «ИНФОРМАЦИЯ» И «ДАННЫЕ» :
СРАВНИТЕЛЬНО-ПРАВОВОЙ АСПЕКТ²**

Аннотация. Киберпреступность как проблема современного мира рассматривается огромным количеством учёных и практиков, в том числе и в Российской Федерации. Однако при более пристальном взгляде на отечественное уголовное законодательство становится очевидно, что избранный в главе 28 УК РФ объект преступлений, воспринимаемых как киберпреступления, выводит национальную уголовную практику за пределы трансграничной борьбы с киберпреступностью. По мнению автора статьи, причина этого – в выбранном законодателем термине «компьютерные преступления» и «компьютерная информация» и отказ от термина «цифровые данные».

Если рассмотреть компьютерную информацию и компьютерные данные с той же точки зрения, то очевидно, что основные различия будут лежать в поле неюридических свойств этих явлений. Автор полагает, что использовать термины «данные» и «информация» как синонимы в корне неверно, особенно когда речь идет о компьютерной или, правильнее, цифровой информации. В общем смысле данные представляют собой совокупность сведений, зафиксированных на определённом носителе в форме, пригодной для постоянного хранения, передачи и обработки. Информация, в свою очередь, представляет собой результат преобразования, обработки, анализа данных при решении конкретных задач. То есть, информация производна от данных, при этом, если вторые остаются неизменными в содержании и

¹ Ярослава Олеговна Кучина, кандидат юридических наук, LL.M., доцент, доцент кафедры уголовного права и криминологии Юридической школы Дальневосточного федерального университета, г. Владивосток, Россия.

Для цитирования: Кучина Я. О. Предмет киберпреступлений и зависимость его определения от дифференциации понятий «информация» и «данные»: сравнительно-правовой аспект // Азиатско-Тихоокеанский регион: экономика, политика и право. 2018. № 3. С. 78–91.

² Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16129.

смысле, вторая зависит от запроса и задачи, цели, для достижения которой данные анализируются.

Основываясь на проведённом исследовании и приводя в качестве аргументов судебную практику, нормы права и результаты сравнительно-правового анализа, автор предлагает отказаться от использования термина «компьютерная информация», которым описывается предмет преступлений в УК РФ. Это позволит модернизировать закон и привести его в соответствие с актуальным состоянием науки и техники.

Ключевые слова: киберпреступность, киберправо, искусственный интеллект, цифровые отношения, уголовный закон, компьютерная информация, киберпреступления, цифровые данные, персональные данные.

Yaroslava O. Kuchina¹

Far Eastern Federal University, Vladivostok, Russian Federation

E-mail: kuchina.yao@dvfu.ru

THE SUBJECT OF CYBERCRIME AND THE DEPENDENCE OF ITS DEFINITION ON DIFFERENTIATION OF THE CONCEPTS “INFORMATION” AND “DATA”: A COMPARATIVE LEGAL ASPECT²

Abstract. Cybercrime as a problem of the modern world is considered by a huge number of scientists and practitioners, including those in the Russian Federation. However, with a closer look at domestic criminal legislation, it becomes obvious that the object of crimes perceived as a cybercrime elected in Chapter 28 of the Criminal Code of the Russian Federation takes the national criminal practice beyond the borders of the trans-boundary fight against cybercrime. According to the author of the article, the reason for this lies in the term “computer crimes” and “computer information” chosen by the legislator, and the rejection of the term “digital data”. If we consider computer information and computer data from the same point of view, it becomes obvious that the main differences will lie in the field of non-legal properties of the phenomena. The author believes that the use of the terms “data” and “information” as synonyms is fundamentally wrong, especially when it comes to computer or, more correctly, digital information. In a general sense,

¹ Yaroslava O. Kuchina, Candidate of Law Sciences, Assistant Professor of the Department of Criminal law and Criminology, Law School, Far Eastern Federal University, Vladivostok, Russia.

For citing: Kuchina Y. O. The subject of cybercrime and the dependence of its definition on differentiation of the concepts “information” and “data”: a comparative legal aspect // Asia-Pacific RIM: Economic, Politics, Law. 2018. № 3. P. 78–91.

²The reported study was funded by RFBR within the research project № 18-29-16129.

data is a collection of information recorded on a particular medium in a form suitable for permanent storage, transmission and processing. Information, in turn, is the result of conversion, processing, data analysis in solving specific problems. That is, the information is derived from the data: while the latter remain unchanged in content and meaning, the former depends on the query and the goal for which the data is analyzed. Based on the research and judicial practice, legal norms and the results of a comparative legal analysis as arguments, the author suggests not using the term “computer information”, which describes the subject of crimes in the Criminal Code of the Russian Federation. This will allow modernizing the law and bringing it into line with the current state of science and technology.

Keywords: Cybercrime, cyber law, artificial intelligence, digital relations, criminal law, computer information, cybercrime, digital data, personal data.

Глава 28 УК РФ предусматривает уголовную ответственность за преступления в сфере компьютерной информации. Основополагающим в рамках этой главы УК РФ является Приложение 1 к ст. 272, в котором дано понятие предмета преступления. В нём компьютерная информация определена как *сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передач.*

До 7 марта 2011 г. под неправомерным доступом к компьютерной информации законодатель подразумевал доступ к информации *на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.*

Такая формулировка диспозиции ст. 272 УК РФ основывалась на ГОСТ 15971-90 и ГОСТ 27201-87 [1, 2]. Отступив в 2011 г. от терминологии ГОСТ и перейдя к использованию понятия «компьютерная информация», законодатель расширил возможность толкования содержания объекта и предмета преступления, исключив технические подробности и сосредоточившись на признаках защищаемого явления. Если выделять их непосредственно из примечания к ст. 272 УК РФ, то компьютерная информация должна представлять собой сведения, сообщения или данные, выраженные в определённой форме – в форме электрических сигналов.

При этом единообразного нормативно-правового разъяснения понятия «компьютерная информация» не существует. В научных работах часты ссылки [3] на «Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» Генеральной прокуратуры Российской Федерации (*далее – Рекомендации*).

Эти Рекомендации представляют собой позицию, в соответствии с которой органы прокуратуры РФ осуществляют надзор за исполнением законодательства при расследовании преступлений, предусмотренных гл. 28 УК РФ. Они же являются определяющими при поддержании государственного обвинения в совершении преступлений, запрещённых ст. 272 УК РФ.

Включённая в описательную часть ст. 272 УК РФ (равно как в иные статьи главы 28, а также в ст. 159.6 УК РФ), формулировка «охраняемая законом компьютерная информация» делает такой объект преступления бланкетным, так как, по сути, речь идёт об общественных отношениях, гарантирующих *правомерный* доступ, в том числе правомерные создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление её иными пользователями.

Разъясняя особенности квалификации ст. 272 УК РФ, Генеральная прокуратура РФ ссылается на ст. 2 Федерального закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в п. 1 которой информация определена как «сведения (сообщения, данные) независимо от формы их представления». Отсюда можно заключить, что у защищаемой законом информации должно быть, как минимум, три формы выражения – это сведения, сообщения и данные. Примечание 1 к ст. 272 УК РФ добавляет к этой форме ещё одну – форму электрических сигналов, тем самым отграничивая компьютерную информацию от иных видов информации. Способ отграничения – это, как совершенно верно отмечает В. Б. Вехов, способ внешнего оформления информации [4, с. 78], её объективизация, а не внутреннее содержание.

То есть, применяя положения главы 28, важно учитывать, что речь идёт не о компьютерной информации вообще, а о *компьютерной информации, охраняемой законом*. Применительно к информации в целом этот вопрос разрешён законодателем, т.к. виды охраняемой законом информации определены специальными нормативно-правовыми актами. В науке принято выделять понятие конфиденциальной информации, то есть информации, не подлежащей разглашению [5, с. 17]. В ч. 2 ст. 9 ФЗ от 27.07.2006 № 149-ФЗ этот термин используется при описании обязанности не разглашать информацию, доступ к которой ограничен, то есть обязанности соблюдать её конфиденциальность. В ч. 1 этой же статьи есть перечень информации, доступ к которой ограничен. Ограничение доступа к информации означает, что она подлежит охране. К охраняемой законом относятся такие виды информации, как сведения, составляющие коммерческую тайну, служебную тайну и иную тайну (ч. 4 ст. 9), информация о частной физической лица, в том числе информация, составляющая личную или семейную тайну (ч. 8 ст. 9), персональная информация (персональные данные).

Некоторые авторы полагают данный перечень исчерпывающим, считая процитированный закон от 27.07.2006 № 149-ФЗ основным актом, регулирующим охрану

информации [3, с. 43–44], а установление критериев конфиденциальности – единственным признаком [6, с. 179–182]. Это мнение более чем спорно, поскольку отграничение видов охраняемой информации от неохраняемой определяется специальными нормативно-правовыми актами¹, Гражданским и Семейным кодексами Российской Федерации и, в некоторых случаях, правоприменителем – например, при объявлении закрытого судебного заседания по просьбе одного из участников процесса для обеспечения сохранности информации².

То есть, под информацией, охраняемой законом, надо понимать не только информацию, которую законодатель целенаправленно наделил признаками конфиденциальности и в отношении которой установил режим охраны. Охраняемая законом информация – это *любая информация, признаваемая законом, определённая законом, если в её отношении установлен любой правовой режим, то есть если она признана объектом правоотношения*. Наличие такого признания, исходя из положений действующего на территории РФ законодательства, позволяет прибегнуть к общим и специальным средствам защиты объекта правоотношения, например, согласно ст. 17 и ст. 23 Конституции РФ, ст. 1, ст. 11, ст. 150 и ст. 152.2 ГК РФ и пр. Следовательно, охраняемая законом компьютерная информация – это вся подобная информация, если она имеет форму электрических сигналов; и именно эта информация, по смыслу ст. 272 УК РФ, и должна составлять предмет преступления. Сужение предмета преступления, на наш взгляд, влечёт существенное снижение качества государственной защиты этой категории правоотношений от преступных посягательств.

Отсюда следует вывод, что существующее в практике толкование понятия компьютерной информации игнорирует бланкетный характер ст. 272 УК РФ и является исключительно толкованием примечания к ней. Кроме того, довольно часто правоприменитель не учитывает мнение, содержащееся в Постановлении Конституционного Суда РФ от 26.10.2017 N 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова», которым п. 5 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» признан не противоречащим Конституции РФ.

¹ К примеру, ст. 13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» устанавливает, что сведения о факте обращения гражданина за медицинской помощью, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну, разглашение которой в какой-либо форме не допускается.

² Так, согласно постановлению Пленума Верховного суда РФ от 13.12.2012 № 34 «Об открытости и гласности судопроизводства и о доступе к информации о деятельности судов», вопросы частной жизни лиц, не являющихся участниками дела, не могут подлежать оглашению среди неопределенного круга лиц, а вопросы, затрагивающие права и законные интересы несовершеннолетних, рассматриваются в открытом судебном заседании только при наличии согласия их законных представителей.

В нём, во-первых, Конституционный Суд признал лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам, не противоречащим Конституции РФ, *обладателем информации*. Во-вторых, постановил, что передача подобной информации (а, следовательно, и иные действия с ней) вопреки запрету, установленному *правовыми, в том числе локальными, актами или договором*, представляет собой нарушение прав и законных интересов обладателя информации. Это мнение полностью подтверждает сделанный нами вывод о бланкетном характере ст. 272 УК РФ.

Исходя из процитированного постановления Конституционного Суда РФ, а также анализа норм Конституции РФ и иных норм права Российской Федерации, мы можем определить критерий отделения неправомерных действий с компьютерной информацией от правомерных. В качестве него выступает нарушение запрета на получение доступа к компьютерной информации. Запрет может быть установлен законом, иным актом, в том числе локальным или правоприменительным, или договором. Последняя формулировка влечёт за собой очень важное правовое последствие, которое становится очевидным только при рассмотрении его вкупе с понятием «компьютерная информация». Для этого нам вновь необходимо вернуться к содержанию этого термина.

Анализируя Рекомендации Генеральной Прокуратуры РФ, судебную практику и позиции учёных [5, с. 20], мы должны отметить сформировавшееся устойчивое мнение о том, что охраняемая законом компьютерная информация – это та же информация (сведения, сообщения, данные), что охраняется законом в иных формах (визуальной, вербальной, письменной и пр.). Например, это информация, содержащая государственную тайну, только размещённая в компьютере или в ином равнозначном устройстве, в сети Интернет или т.д., которую законодатель назвал информацией в форме электрических сигналов, а современные источники чаще называют цифровой, компьютерной и пр.

Такое толкование приводит к мнению, что существует неохраняемая и охраняемая законом компьютерная информация, поскольку вступает в действие аналогия правоприменения, к примеру, положений об охраняемой законом тайне телефонных переговоров от незаконного вторжения. В этом случае незаконным будет считаться доступ к самим переговорам посредством технического или иного вторжения в телефонную сеть без наличия на то предусмотренных правовых и процессуальных оснований¹.

¹ Это и другие последствия незаконного сбора информации о частной жизни лица были разъяснены в определении Конституционного Суда РФ от 28.06.2012 № 1253-О «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьёй 137 Уголовного кодекса Российской Федерации».

В случае с компьютерной информацией обобщенной судебной практики, как ни странно, не возникло. Законодатель, а вслед за ним и правоприменитель, проводят аналогии с другими видами информации и не задаются вопросом, насколько это оправданно. Однако от других видов информации компьютерная отличается несколькими существенными признаками, основным из которых (особенно для УК РФ) является *осознанный* характер её размещения. Информация становится компьютерной в силу совершения ряда технических действий, то есть она не может приобрести «форму электрических сигналов» самостоятельно или в результате бессознательной деятельности человека. Законодатель внёс в статью признак независимости компьютерной информации от средств её хранения, обработки и передачи, однако не учёл, что современные правоотношения в сфере информационных технологий подразумевают практически полную правовую определённость, установленную законом или договором.

Отсюда мы видим, что дефиниция, которая должна была исключить чрезмерную описательность из диспозиции статьи, наоборот, привела к её аморфности и казуальности. Более того, использование термина «компьютерная информация» в качестве определяющего в перечне деяний, которые представляют собой отечественную трактовку киберпреступлений, повлекло за собой непонимание ещё на международном, сравнительном уровне. Учитывая, что большинство современных киберпреступлений носят транснациональный характер, этот аспект также нельзя обойти вниманием.

Для этого вновь вернёмся к Приложению У к ст. 272 УК РФ, в котором законодатель объясняет компьютерную информацию через термины *сведения (сообщения, данные)*. Термин «данные» в сочетании с термином «компьютерная информация» стали основой для наиболее, на наш взгляд, важной научно-практической дискуссии в сфере отечественного киберправа. Термин «данные» автоматически отсылает нас к другому нормативно-правовому акту действующим в РФ: Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (Далее – ФЗ № 152).

Согласно п. 1 ст. 3 этого закона, персональные данные – это *любая информация, относящаяся к прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных)*. Сравнивая п. 1 ст. 2 ФЗ № 149 с аналогичным пунктом ст. 3 данного закона, мы видим, что оба термина «информация» и «данные» определены друг через друга, и только общий смысл и толкование всего ФЗ № 152 позволяет понять, что персональные данные, по мнению законодателя, являются частным случаем охраняемой законом информации.

Это вносит существенное непонимание в международную практику киберправа. Выше мы уже кратко разъяснили взаимозависимость технологических (неюридических) и юридических свойств при правоприменении. По сути, с аналогичными проблемами правоприменитель сталкивается и при квалификации деяний иного

характера, где объект и предмет преступления, определённые ранее, столкнулись с более сложными в концептуальном смысле явлениями и, как следствие, показали несовершенство выбранных критериев. Например, «дизайнерские наркотики» и беспилотные воздушные системы (дроны) вызвали подобный эффект при применении статей из глав 25 и 27 УК РФ.

Если рассмотреть компьютерную информацию и компьютерные данные с той же точки зрения, то очевидно, что основные различия будут лежать в поле неюридических свойств этих явлений. Обращаясь за разъяснением к специальной литературе, мы можем заключить, что использовать термины «данные» и «информация» как синонимы в корне неверно, особенно когда речь идет о компьютерной или, правильнее, цифровой информации. В общем смысле данные представляют собой совокупность сведений, зафиксированных на определённом носителе в форме, пригодной для постоянного хранения, передачи и обработки. Информация, в свою очередь, представляет собой результат преобразования, обработки, анализа данных при решении конкретных задач. То есть информация производна от данных, при этом, если вторые остаются неизменными в содержании и смысле, вторая зависит от запроса и задачи, цели, для достижения которой данные анализируются.

В пределах киберотношений соблюдение этого терминологического различия крайне важно именно в силу производности юридического свойства от неюридического. Но самое главное заключается в том, что мы не можем вводить уголовную ответственность за изменение информации, поскольку информация меняется в зависимости от конкретного запроса конкретного субъекта (группы субъектов), а данные имеют постоянные фиксированные признаки, позволяющие определить степень вмешательства и причинённого вреда. Информация такой возможности не даёт. Более того, учитывая взаимопроизводность данных и информации, их тесную связь, признание в качестве определяющей именно информации приводит к тому, что под защиту попадает бесчисленное множество нефиксированных явлений, момент существования части которых невозможно реально установить. Всё это противоречит учению об объекте и предмете преступления, поскольку норма становится, как мы уже сказали, казуальной. Казуальность нормы уже приводит к проблемам квалификации составов преступлений, вызывая конкуренцию норм там, где их быть не должно [6].

Ещё одним существенным отличием информации от данных является их объективизация, тогда как информация может и не иметь материального выражения. Особенно ярко это различие проявляется в компьютерной, цифровой сфере, в том числе позволяя установить факт совершения преступления посредством выявления следов его совершения. Данные – это совокупности знаков. Хранимые данные представляют собой совокупности символов, а передаваемые данные – совокупности сигналов. Это и есть та причина, по которой в Примечании 1 к ст. 272 УК РФ

законодатель говорит о «форме электронных сигналов», тем самым позволяя нам заключить, что, фактически, под компьютерной информацией необходимо понимать именно цифровые данные.

Подтверждение этому нашему выводу мы находим и в международной, а также зарубежной практике применения законодательства. При этом сразу стоит отметить, что ряд нормативно-правовых актов, имеющих экстрагосударственный характер действия, вынуждены соблюдать и субъекты, относящиеся к Российской Федерации. К примеру, таким актом является Общий регламент по защите данных, более известный как General Data Protection Regulation (GDPR)¹. Это постановление Европейского Союза, с помощью которого Европейский парламент, Совет Европейского Союза и Европейская комиссия усиливают и унифицируют защиту персональных данных всех лиц в Европейском Союзе. Его исполнение обязательно для всех лиц, вовлечённых в оборот персональных данных граждан ЕС, направленно или косвенно. Учитывая последнее требование – то вообще всех лиц, если они прямо не ограничивают возможность граждан ЕС разместить свои персональные данные в систему их оборота.

Аналогичные требования мы можем обнаружить и в других законодательных актах. Все нормативно-правовые акты, касающиеся цифровых и киберотношений как непосредственно, так и регулирующие их опосредованно², базируются на определении личных (персональных) данных и их отделении от иных категорий данных, поскольку только так данные вообще могут быть защищены законом. Использование термина «конфиденциальная информация» или «компьютерная информация, защищаемая законом» нам не встретилось³, даже при наличии термина «информация» в законодательстве этих государств [8]. При этом в перечень данных могут включаться, помимо персональных, государственная тайна, профессиональная и коммерческая тайна [9].

К этому заключению также позволяет прийти анализ Сборника законов о конфиденциальности данных от 2015 г. [10], Справочника о законодательстве о защите данных в мире [11]. Аналогичный вывод можно сделать после анализа практики многолетнего применения первого по-настоящему международного акта, регулировавшего оборот персональных данных в ЕС до принятия Общего регламента – Директивы Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, вступившей в силу для регулирования оборо-

¹ Полное наименование акта Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

² Когда законодатель предпочитает широкое регулирование, а не специализированное.

³ Нами было исследовано 36 стран в целом: ведущие страны АТР и Евросоюз.

та и защиты информации в пределах Евросоюза, принятой в 1995 г. для обеспечения безопасности персонализированных данных на территории Евросоюза [12].

Также хотелось бы отметить, что использование термина «данные», а не «информация» наблюдалось до массового распространения кибертехнологий – в законодательных актах об обороте аналоговых, а не цифровых данных. Наиболее интересный пример этого можно найти в законодательстве США, которое, в силу своеобразного построения, некоторые учёные называют «секторальным» [10, 13]. Это означает, что законодательство распространяется не на весь круг правоотношений в сфере киберотношений и цифровых данных вообще, а на его определённые секторы и обстоятельства (например, есть Закон о защите конфиденциальности видео 1988 г., Закон о защите кабельного телевидения и конкуренции 1992 г., Закон о добросовестной кредитной отчётности, а также Закон об ответственности и переносе данных о страховании здоровья граждан 1996 г. и т.д.). Но два федеральных правовых акта направлены исключительно на оборот цифровых данных: Закон об ответственности и переносе данных о страховании здоровья граждан 1996 г. и Закон Грэмма – Лича – Блайли [14, 15]. Помимо них разработаны федеральные законы, содержащие ограничения для провайдеров цифровых услуг, имеющих доступ к персональным данным.

На данный момент в США наиболее значимым является Закон об ответственности и переносе данных о страховании здоровья граждан 1996 г., также известный как Закон Кассебаума – Кеннеди [14], и именно его нам хотелось бы привести в качестве примера, объясняющего разницу между цифровыми данными и информацией (в силу детализации практики применения этого закона). Целью действия этого закона является защита информации, поступающей в базы данных при оформлении медицинской страховки, благодаря чему все провайдеры цифровых услуг разделены на тех, кто обязан следовать нормам закона, и тех, на кого такая обязанность не возложена. Закон Кассебаума – Кеннеди обеспечивает упорядоченную процедуру ведения электронных медицинских записей и включает в себя положения о безопасности и конфиденциальности так называемых «защищённых данных о состоянии здоровья».

В их перечень включается достаточно большое количество разнообразных данных, имеющих прямое отношение к здоровью, его состоянию или же только касающихся этого, благодаря которым можно идентифицировать лицо – собственника данных (например, из данных о страховке или результатов лабораторных исследований, в том числе рентгеновских снимков, результатов анализов крови и пр.) [16]. Закон Кассебаума – Кеннеди затрагивает практически любую сферу, касающуюся конфиденциальной информации о состоянии здоровья. Он влияет на исследования в области здравоохранения, в том числе даже на те, результаты которых представлены в виде графиков и диаграмм, а тем более на исследования, связанные

с общением с пациентами, с целью отслеживания состояния здоровья и влияния процесса лечения на человеческий организм [17].

Помимо прочего, практика применения этого закона вылилась в целый перечень чётких требований и критериев технического характера, позволяющих точно установить пределы действия с данными, особенности их обработки, технологий персонализации и деперсонализации, а также извлечения информации из этих данных. Например, Amazon Web Services разработал «Белую книгу» для тех своих клиентов, кто заинтересован в сохранении конфиденциальности медицинской информации при применении оказываемых компанией услуг. «Белая книга» Amazon Web Services содержит исчерпывающие сведения о том, как, в соответствии с Законом Кассебаума – Кеннеди, этим провайдером цифровых услуг обрабатываются конфиденциальные личные данные о здоровье [18].

Всё это позволяет нам ещё раз прийти к выводу, уже сделанному в середине работы. Неточность дефинитивного аппарата в сфере регулирования цифровых и киберотношений способна привести как к частным, так и общим проблемам применения права. Особенно это важно, если государство, как, к примеру, сейчас Российская Федерация, планирует существенное реформирование законодательной сферы, которое приведёт к созданию новой отрасли права. Уже сейчас, сталкиваясь со стремительным прогрессом регулируемых отношений, мы видим, что имеющийся закон существенно отстаёт – в техническом и юридическом смыслах, а это влечёт существенные проблемы в применении даже ограниченного числа норм, что имеются сейчас.

СПИСОК ЛИТЕРАТУРЫ

1. Системы обработки информации. Термины и определения [Электронный ресурс] : Государственный стандарт СССР ГОСТ 15971-90 (утв. и введен в действие постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26 октября 1990 г. № 2698). – Режим доступа: <http://docs.cntd.ru/document/gost-15971-90>.

2. Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования [Электронный ресурс] : Государственный стандарт Союза ССР ГОСТ 27201-87 (утв. постановлением Госстандарта СССР от 28 января 1987 г. № 124) (с изм. и доп.). – Режим доступа: <http://docs.cntd.ru/document/gost-27201-87>.

3. Евдокимов, К. Н. Вопросы уголовно-правовой квалификации неправомерного доступа к компьютерной информации и его отграничения от смежных составов преступлений // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2009. – № 2 (10). – С. 42–46.

4. Вехов, В. Б. Преступления, связанные с неправомерным использованием баз данных и содержащейся в них компьютерной информации // Защита информации. Инсайд. – 2008. – № 2 (20). – С. 76–82.
5. Старичков, М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института Министерства внутренних дел России. – 2014. – № 1 (68). – С. 16–20.
6. Апелляционное постановление Свердловского областного суда от 18 декабря 2017 г. по делу № 22-9487/2017 [Электронный ресурс]. – Режим доступа: http://ekbobsud.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=14762698&delo_id=4&new=4&text_number=1.
7. Шкиль, Д. А. К вопросу о видах ответственности работников, допустивших распространение охраняемой законом информации / Д. А. Шкиль, А. В. Китаева // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе : материалы международной научной конференции адъюнктов, аспирантов, курсантов и студентов. Т. 1. – Самара, 2018. – С. 179–181.
8. Кучина, Я. О. Правовое регулирование облачных технологий (вычислений) / Я. О. Кучина. – М. : Юрлитинформ, 2018. – 168 с.
9. Privacy and legal issues in cloud computing. Elgar law, technology and society / ed. by R. H. Weber, A. Cheng. – London : Edward Elgar Pub, 2015. – XIV, 290, 14 p.
10. International compendium of data privacy laws [Электронный ресурс] / compil. T. J. Kobus, G. S. Zeballos. – Baker Hostetler, 2015. – Режим доступа: <https://www.lexology.com/library/detail.aspx?g=347b9a58-5b45-474b-9395-7a52abe5ba7a>.
11. DLA Piper. Data Protection Laws of the World [Электронный ресурс]. – Режим доступа: <https://www.dlapiperdataprotection.com/#handbook/world-map-section>.
12. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных [Электронный ресурс] : Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г. – Режим доступа: <https://pd.rkn.gov.ru/law/>.
13. Schriver R. You cheated, you lied: the safe harbor agreement and its enforcement by the Federal Trade Commission // Fordham Law Review. – 2002. – Vol. 70, iss. 6. – P. 2777–2818.
14. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub. L. 104–191, 110 Stat. 1936, August 21, 1996, (U.S.) [Электронный ресурс]. – Режим доступа: <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>.
15. The Gramm–Leach–Bliley Act (Financial Services Modernization Act of 1999), Pub. L. 106–102, 113 Stat. 1338, November 12, 1999 (U.S.) [Электронный ресурс]. –

Режим доступа: <https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>.

16. Armstrong, D. Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome / D. Armstrong, E. Kline-Rogers, S. Jani, E. Goldman // *Archives of Internal Medicine*. – 2005. – Vol. 165, iss. 10. – P. 1125–1129.

17. Privacy and Anonymity in the Digital Era / guest ed. S. Gritzalis. – Bradford, GBR : Emerald Group Publishing Ltd, 2006. – 112 p. – (Internet Research ; vol. 16, no. 6).

18. Architecting for HIPAA Security and Compliance on Amazon Web Services. Amazon Web Services, December 2015 [Электронный ресурс]. – Режим доступа: https://www.examineus.com/EducationFiles/AWS_HIPAA_Compliance_Whitepaper.pdf.

REFERENCES

1. *USSR State Standard GOST 15971-90 «Information processing systems. Terms and definitions» (approved and enacted by the decision of the USSR State Committee for Product Quality Management and Standards of October 26, 1990 No. 2698)*. Available at: <http://docs.cntd.ru/document/gost-15971-90> (accessed 18 May 2018). (In Russian).

2. *USSR State Standard GOST 27201-87 «Personal electronic computers. Types, basic parameters, general technical requirements» (approved by the State Standard of the USSR on January 28, 1987 No. 124) (with changes and additions)*. Available at: <http://docs.cntd.ru/document/gost-27201-87> (accessed 18 May 2018). (In Russian).

3. Evdokimov K.N. Voprosy ugolovno-pravovoi kvalifikatsii nepravomernogo dostupa k komp'yuternoi informatsii i ego otgranicheniya ot smezhnykh sostavov prestuplenii [Issues of criminal law qualification of unauthorized access to computer information and its delimitation from related offenses]. *Vestnik Akademii General'noi prokuratury Rossiiskoi Federatsii*, 2009, no. 2 (10), pp. 42–46.

4. Vekhov V.B. Prestupleniya, svyazannye s nepravomernym ispol'zovaniem baz dannykh i sodержashcheisya v nikh komp'yuternoi informatsii [Crimes related to the misuse of databases and the computer information contained in them]. *Zashchita informatsii. Insaid*, 2008, no. 2 (20), pp. 76–82.

5. Starichkov M.V. Ponyatie «komp'yuternaya informatsiya» v rossiiskom ugolovnom prave [The concept of «computer information» in Russian criminal law]. *Vestnik Vostochno-Sibirskogo instituta Ministerstva vnutrennikh del Rossii*, 2014, no. 1 (68), pp. 16–20.

6. *The appeal decision of the Sverdlovsk regional court dated December 18, 2017 in case No. 22-9487/2017*. Available at: http://ekbobljud.ru/modules.php?name=sud_de&lo&srv_num=1&name_op=doc&number=14762698&delo_id=4&new=4&text_number=1 (accessed 20 May 2018). (In Russian).

7. Shkil' D.A., Kitaeva A.V. K voprosu o vidakh otvetstvennosti rabotnikov, dopustivshikh rasprostraneniye okhranyaemoy zakonom informatsii [On the issue of the types of workers' responsibility that allowed the dissemination of information protected by law]. *Problemy i perspektivy razvitiya ugolovno-ispolnitel'noi sistemy Rossii na sovremennom etape. Materialy Mezhdunarodnoi nauchnoi konferentsii ad'yunktov, aspirantov, kursantov i studentov* [Problems and prospects of development of the penitentiary system of Russia at the present stage. Materials of the International Scientific Conference of adjuncts, graduate students, cadets and students]. Vol. 1. Samara, 2018, pp. 179–181.
8. Kuchina Y.O. *Pravovoe regulirovaniye oblachnykh tekhnologii (vychislenii)* [Legal regulation of cloud technologies (computing)]. Moscow: Yurlitinform Publ., 2018. 168 p.
9. Cheung A., Weber R. (eds). *Privacy and Legal Issues in Cloud Computing*. Elgar Law, Technology and Society. London: Edward Elgar Pub, 2015. XIV, 290, 14 p.
10. Kobus T. J., Zeballos G. S. (compil.). *International Compendium of Data Privacy Laws*. Baker Hostetler, 2015. Available at: <https://www.lexology.com/library/detail.aspx?g=347b9a58-5b45-474b-9395-7a52abe5ba7a> (accessed 11 May 2018).
11. *DLA Piper. Data Protection Laws of the World*. Available at: <https://www.dlapiperdataprotection.com/#handbook/world-map-section> (accessed 11 May 2018).
12. *Directive 95/46 / EC of the European Parliament and of the Council of October 24, 1995 On the protection of individuals during the processing of personal data and on the free circulation of such data*. Available at: <https://pd.rkn.gov.ru/law/> (accessed 11 May 2018) (In Russian).
13. Schriver R. You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission. *Fordham Law Review*, 2002, vol. 70, iss. 6, pp. 2777–2818.
14. *The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub. L. 104–191, 110 Stat. 1936, August 21, 1996, (U.S.)*. Available at: <https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf> (accessed 12 May 2018).
15. *The Gramm–Leach–Bliley Act (Financial Services Modernization Act of 1999), Pub. L. 106–102, 113 Stat. 1338, November 12, 1999 (U.S.)*. Available at: <https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf> (accessed 12 May 2018).
16. Armstrong D., Kline-Rogers E., Jani S., Goldman E. Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome. *Archives of Internal Medicine*, 2005, vol. 165, iss. 10, p. 1125–1129.
17. Gritzalis S. (guest ed.). *Privacy and Anonymity in the Digital Era*. Bradford, GBR: Emerald Group Publishing Ltd, 2006. 112 p. (Internet Research; vol. 16, no. 6).
18. *Architecting for HIPAA Security and Compliance on Amazon Web Services. Amazon Web Services, December 2015*. Available at: https://www.examineus.com/EducationFiles/AWS_HIPAA_Compliance_Whitepaper.pdf (accessed 12 May 2018).