МРНТИ 10.19.51

М.С. Бисалиев, К.Н. Шакиров

Казахский национальный университет им. аль-Фараби, Алматы, Казахстан
(E-mail: mbissaliyev@gmail.com, kshakirov@gmail.com)

Цифровые следы как фактор безопасности оборота персональных данных в сети Интернет

Аннотация. В статье рассматриваются основные подходы к использованию знаний о цифровых следах в сети Интернет как значимом факторе обеспечения безопасного оборота персональных данных в киберсреде. Сделан обзор содержащихся в доктрине цифровизации научных позиций по указанному вопросу. Представлено авторское определение цифровых следов, предложен алгоритм выявления способов посягательства на персональные данные с помощью глобальной информационной сети, показаны типичные фазы такого рода посягательства и обычные действия правонарушителя. Впервые в данной области знаний применен комплексный подход, совмещающий в себе как достижения доктрины информационного права, так и криминалистического учения о следах. В результате сделаны предложения по принятию международного либо регионального (европейского) акта, предусматривающего стандарты обращения к специальным знаниям в случае обнаружения неправомерного доступа к персональным данным, включая их «перехват» в рамках информационного обмена в сети Интернет.

Ключевые слова: информационная безопасность, киберсреда, цифровые следы, персональные данные, личная информация, криминалистическая идентификация, правовая защита.

DOI: https://doi.org/10.32523/2616-6844-2023-142-1-81-98

Введение

В связи с увеличением роста развития информационных-телекоммуникационных технологий одной из важнейшей задачей юридической науки и практики является совершенствование правового регулирования общественных отношений в сфере обеспечения информационной безопасности. Основная современная человеческая деятельность связана с ИТ-технологиями, так как они занимают ведущую роль в

различных сферах индустрии и жизнедеятельности экономических агентов (экономика, здравоохранение, промышленность, оборона, культура, образование, оборона, юриспруденция и проч.). В настоящее время не подлежит доказыванию, что развитая информационная инфраструктура способствует социальному экономическому росту и развитию, созданию новых инструментов роста капитала (в том числе человеческого).

Однако информатизация общественного развития в условиях глобализации имеет не только положительные, но и отрицательные стороны. Анализ нормативного материала (национальных доктрин информационной безопасности и иных стратегических документов) позволяет установить следующие причинно-следственные связи: государства признают рост компьютерной преступности, особенно в кредитно-финансовой сфере; ИТ-поле используется как инструмент для разжигания межнациональной и религиозной розни; наблюдаются рост милитаризации информационного пространства и наращивание гонки информационных вооружений, при этом чаще всего указанные негативные тенденции связаны с несанкционированным доступом к персональным данным граждан.

Научным сообществом выявлено, что несанкционированный доступ к персональным данным в сети Интернет оставляет так называемые «цифровые следы». Возможность исследования данных следов представляет собой важный фактор повышения безопасности оборота персональных данных в сети Интернет с точки зрения, во-первых, установления факта нарушения права на конфиденциальность и защиту персональных данных, во-вторых, для обнаружения обстоятельств, свидетельствующих, с каких устройств такой доступ был осуществлен, и, в-третьих, каким именно лицом осуществлен доступ к личной информации.

Само по себе исследование цифровых следов в процессе оборота персональных данных в сети Интернет призвано повысить безопасность оборота персональных данных, создать необходимые правовые условия для доказывания факта несанкционированного доступа к персональным данным, их изменения, уничтожения и т.п., то есть в целях доказывания в уголовном, гражданском и административном процессе фактов совершения правонарушений.

Вместе с тем в науке сегодня нет единого подхода к такого рода исследованиям, поскольку данная тематика не относится в полной мере к категории информационного права и находится частично в области интереса криминалистов в процессе раскрытия и расследования правонарушений, а в определенной части – специалистов по процессуальному праву, что обусловливает потребность в комплексном изучении данной проблематики, поскольку она еще в должной мере системно не сформировалась как самостоятельное направление научного исследования.

Для выработки эффективных мер обеспечения безопасности оборота персональных данных в сети Интернет и

их защиты необходимо, таким образом, исследовать не только теорию и практику применения законодательства о персональных данных, но и информацию о цифровых следах как одну из форм доказательной деятельности в процессе обеспечения посредством криминалистических методов проблем безопасности использования информационно-телекоммуникационной сети Интернет. Изложенные выше положения показывают актуальность избранной нами темы исследования.

Предметом исследования является проблема криминалистического анализа цифровых следов при обеспечении безопасного оборота и защите персональных данных в глобальной информационной сети.

Цель исследования - выработка посредством применения криминалистического подхода методов выявления и учета признаков и свойств цифровых следов при обеспечении безопасного оборота персональных данных в сети Интернет.

Для достижения поставленной цели предполагалось решение следующих задач: анализ, обобщение теоретических материалов с целью выявления уровня научной разработанности темы в общетеоретических и отраслевых исследованиях; рассмотрение дискуссионных положений; определение некоторых методологических задач для дальнейшего научного поиска; анализ и синтез философского, психологического, социологического, лингвистического, исторического, управленческого, юридического и прежде всего информационных и криминалистических подходов к изучению категории «цифровые следы» в правовой науке с целью их применения в процессе идентификации личности в современном обществе, национальном и международном праве.

О методах научного исследования цифровых следов

При работе над темой авторы методологически исходили из положений о комплексности рассматриваемой проблематики. В этой связи авторами широко использовались общенаучные, частно-научные и специальные методы исследования – философский, психологический, социологический, исторический, сравнительно-правовой и проч. Однако наибольшее внимание было уделено методу системного анализа, поскольку исследование цифровых следов, оставленных в глобальном информационном пространстве, является важным средством научно обоснованного установления факта неправомерного вторжения в информационный обмен, связанный с передачей персональных данных. С применением системного подхода предоставляется возможность комплексно, на основе применения достижений ИТ-технологий раскрыть действительные особенности криминалистической характеристики способов нарушения тайны персональной информации (цифровых следов), что, в свою очередь, позволяет более эффективно и качественно идентифицировать личность правонарушителя, неправомерно действующего в информационном

пространстве.

Однако до настоящего времени в доктрине информационного права, международном праве, да и в правовой науке в целом, мы наблюдаем явную недооценку важности «заимствования» и использования в сфере защиты персональных данных достижений криминалистической науки. В свою очередь, надо признать, и в криминалистической теории пока еще так же не в полной мере воспринимают специфику нарушений в информационном обмене в глобальной информационной сети и нередко затрудняются с разработкой методов и способов работы с цифровыми следами в информационном пространстве.

Именно с целью устранения возникающего в данном случае диссонанса нами сделана попытка применения комплексного подхода в виде обращения как к нормам информационного права, так и к достижениям криминалистической науки.

В итоге, на наш взгляд, формирование и развитие полноценных криминалистических знаний взаимосвязи цифровых следов как результата криминального доступа к персональным данным в информационном пространстве, в силу их особых признаков и свойств, позволит обеспечить разработку научно обоснованных криминалистических способов и методов их правовой защиты с целью достоверного установления факта и обстоятельств нарушения злоумышленниками прав субъектов-носителей персональных данных.

Вместе с тем необходимо отметить, что вопрос поиска и фиксации цифровых следов при обнаружении случаев доступа к персональным данным, совершенного с использованием информационно-коммуникационных технологий, в том числе технологий сети Интернет, прежде не являлся предметом комплексных исследований. При этом в криминалистике в процессе исследования механизма следообразования ещё недостаточно внимания уделяется особенностям формирования цифровых следов с учетом развития информационных технологий.

Например, в работах М.Ю. Батурина, В.Б. Вехова, Ю.В. Гаврилина, В.А. Мещерякова и других исследователей рассматривались вопросы установления факта доступа к персональным данным в сфере компьютерной информации. Вопросы характеристики противоправного поведения в области оборота персональных данных в сети Интернет поднимались в монографиях и публикациях В.А. Климова, В.А. Мещерякова. В трудах В.Ю. Агибалова, В.Б. Вехова, А.С. Вражнова, Л.Б. Красновой, В.В. Крылова, М.М. Менжега рассматривались криминалистически значимые сведения о расследовании преступлений в сфере оборота персональных данных, раскрывались проблемы расследования киберпреступлений, в том числе исследовался вопрос обоснования информационно-следовой картины доступа к персональным данным, совершенного с использованием информационно-коммуникационных технологий. Кроме того, Е.Р. Россинской, В.А. Мещеряковым, В.О. Давыдовым, Ю.В. Гаврилиным, Д.Ю. Илюшиным

уделяется внимание исследованию актуальных вопросов тактики производства отдельных проверочных действий и мероприятий при расследовании киберпреступлений. В научных же трудах Р.С. Атамановой, Д.А. Илюшина, И.Е. Мазуровой, А.Л. Осипенко, Е.С. Шевченко были предложены методические рекомендации по выявлению отдельных видов противоправного доступа к персональным данным, сопряженных с использованием сети Интернет.

Таким образом, приходится констатировать, что, к сожалению, в юридической литературе последних лет отсутствуют комплексные фундаментальные исследования указанной проблемы, существуют лишь отдельные профильные исследования, как правило, в области информационного права и криминалистического учения о следах, что свидетельствует о том, что уровень научной разработки предложенной проблематики достаточно низкий, и это служит важным аргументом для проведения более широких криминалистических исследований процессов применения цифровых следов с целью выявления фактов нарушений в сфере оборота персональных данных.

Персональные данные и возможные виды их нарушений

Обеспечение безопасности оборота персональных данных и их защиты во многом зависит от вида конкретной противоправной деятельности, посягающей на права личности в указанной сфере. Как мы указывали выше, в доктрине информационного права лишь упоминается о способах нарушения информационных прав на охрану личной (частной) жизни применительно к действиям субъектов оборота персональных данных [1] ввиду скрытого предположения о том, что более глубокие исследования должны относиться, скорее, к области специальных знаний, например, в сфере юридической науки, в частности криминалистики [2].

Международное и европейское право сегодня предусматривает в рамках регулятивных отношений значимые превентивные меры, направленные на недопущение нарушения прав субъекта персональных данных в будущем.

Так, п.1 ст.35 Регламента Европейского Парламента и Совета 2016/679 «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС (Общие правила защиты данных)» от 27 апреля 2016 года [3] указывает, что в случае, если способ обработки данных, особенно при использовании новых технологий и с учётом характера, объёма, контекста и целей обработки, может привести к высокой степени риска для прав и свобод физических лиц, то контролер перед обработкой персональных данных проводит оценку воздействия запланированной обработки на их защиту.

Сами по себе регулятивные способы реализации в сфере информационного права достаточно подробно предусмотрены международными актами в виде обязанностей контролера и процессора,

а также иных участников оборота персональных данных. Однако в отношении правоохранительных способов (способов защиты) персональных данных международно-правовой инструментарий значительно уже. Способы же нарушения прав личности при их обороте исследованы на сегодняшний день не в достаточной степени.

В криминалистической науке способ совершения преступления большинством авторов традиционно относится к важнейшим и даже основным элементам криминалистической характеристики преступления [4], хотя ранее это понятие рассматривалось более широко и заключало в себе и способы сокрытия преступлений [5], а также некоторые типичные следственные ситуации [6], что было свойственно не только для отечественной, но и для иностранной литературы [7].

Анализ предложенных в криминалистической литературе определений способа совершения преступления (правонарушения) обычно не в полной мере отражает сущность посягательства на персональные данные, выявленную в информационном праве [8], в связи с чем они должны быть уточнены и трансформированы применительно к исследованию конкретных видов посягательств на личную информацию. Более того, данные определения представляются нам крайне сложными. Мы полагаем, в качестве исходной посылки, что способ совершения посягательств на персональные данные с использованием информационно-коммуникационных сетей, включая Интернет, – это избранная злоумышленником последовательность личных действий и операций, связанных с применением IT-технологий в противоправных целях.

Вместе с тем данное определение будет поверхностным без указания на предметную область реализации такого способа, а именно криминалистики и непосредственно её приемов, способов и методов использования в информационно-коммуникационной сети. В этой связи отметим, что злоумышленниками в качестве средства причинения вреда используется информация, которая выступает в качестве объекта указанных правоотношений. Информация вообще является объектом, который порождает общественные информационные отношения [10]. При этом национальный законодатель и международное право оперируют в этой области такими взаимосвязанными понятиями как «информация», «информационный ресурс», «информационно-телекоммуникационная сеть» и другими, что характерно и для доктрины информационного права [10], а также криминалистической и криминологической литературы [11]. Персональные данные, соответственно, рассматриваются как разновидность такой особо охраняемой законом информации.

В интересующем нас контексте с точки зрения криминалистической теории, а именно криминалистической характеристики преступлений, следует различать персональные данные как предмет правонарушения и персональные данные как средство его совершения.

Как предмет правонарушения персональные данные имеют исключительно достоверный характер. Важным характеризующим признаком персональной информации является ее внешняя форма. Личная информация обязательно должна быть связана с конкретным материальным источником - лицом. Особое место среди криминалистических признаков такой информации как предмета правонарушения служат её формализованность и её ценностнное значение. Другим важным признаком, характеризующим персональную информацию в качестве предмета правонарушения, является ее способность быть объектом регулирования общественных отношений, в том числе отношений в связи с оборотом персональных данных в сети Интернет.

Персональная информация, как уже указывалось, может выступать и средством совершения правонарушений [12]. В такой ситуации она представляет собой нелегитимный набор знаний о персональных данных граждан, специфический для совершения преступлений против личности либо интересов юридического лица. В отличие от информации-предмета информация-средство совершения правонарушений представляет собой по большей части искаженные сведения о личности, так как именно искаженная информация вызывает неопределенности в системе общественных отношений. Для персональной информации, используемой в качестве средства совершения правонарушения, характерно отсутствие у нее экономической или иной ценности [13]. Таким образом, персональная информация как средство совершения правонарушения – это преимущественно ложные (искаженные) сведения о личности, не обладающие какой-либо экономической или иной ценностью, используемые злоумышленниками с целью посягательства на объект правовой охраны.

Криминалистам в процессе расследования преступлений следует учитывать, что на практике в качестве средства совершения правонарушения либо объекта такого посягательства (противоправного интереса) выступает не какая-либо конкретная персональная информация, а информационный ресурс, содержащий персональные данные многих лиц в целом. Информационный ресурс — документ или документы, расположенные в информационных системах, которые могут создаваться пользователем или информационной системой. Доступ к информации и к информационному ресурсу возможен только посредством информационно-телекоммуникационной сети.

С точки зрения расследования преступлений, связанных с покушением на персональные данные, мы должны здесь видеть следующую схему: персональная информация, как самостоятельный набор сведений или, что чаще всего бывает в качестве некоторого массива данных на информационном ресурсе, являясь объектом правовой охраны, может выступать предметом правонарушения, которое совершается посредством противоправного воздействия на нее

(доступа к ней) «в границах» информационно-телекоммуникационной сети, которая, в свою очередь, может быть локальной (в рамках одной организации или одного органа власти) или глобальной (Интернет).

На основе анализа литературы и нормативного материала мы полагаем, что информационно-телекоммуникационной сетью является электрическая (электронная) сеть, предназначенная именно для обмена информацией - её передачи, хранения, обработки и т.п. с помощью вычислительной техники, позволяющей осуществить доступ к линиям (по линиям) связи, используемым для этих целей. Соответствующим образом (то есть с учетом данной дефиниции) мы определяем и способ противоправного посягательства на оборот персональных данных.

Цифровые следы как объекты-носители информации о нарушении персональных данных

Криминалистам при анализе информационного пространства с целью расследования компьютерных преступлений следует иметь в виду, что сама по себе информационно-телекоммуникационная сеть – это лишь область (цепь) электрических соединений разной модальности и последовательности, трансформирующихся в информацию как раз вследствие различий в характере соединений и последовательности соединений (главным образом, второго). Следовательно, некоторые сведения (в виде цифровых следов), свидетельствующие о действиях злоумышленника и таким образом о совершенном им правонарушении, изначально, до их поступления в распоряжение заинтересованных лиц, могут отображаться в самой информационно-телекоммуникационной сети; на устройствах, относящихся к компьютерной технике, с помощью которых осуществляется вход в сеть, подразумевающий последующий или одновременный доступ к персональной информации посредством передачи, хранения, обработки (например, шифрование или иная криптографическая обработка, архивирование особого типа) персональной информации и получения персональной информации.

Именно эти сведения (логи) можно считать «цифровыми следами», представляющими при расследовании преступлений наибольший научный и практический интерес. Следы, как об этом известно в криминалистике, - это всегда материальное отображение чего-то в пространстве.

Полагаем, что информация о возможности нахождения сведений, свидетельствующих о совершенном или готовящемся правонарушении в отношении персональных данных в самой информационно-телекоммуникационной сети, помимо соответствующего компьютерного устройства, доступна даже в ситуации, когда эта персональная информация уже относительно безвозвратно удалена с устройств ее отправителя и получателя. Её хранение в информационно-телекоммуникационной сети, представляющей собой цепь (последовательность, схему)

соединенных (соединившихся) между собой устройств, возможно лишь в условиях наличия некоторого материального носителя для хранения информации в «машинном виде», например, в форме двузначных и прочих кодов. Это утверждение верно даже в той ситуации, когда информация хранится в «облаке» какой-либо системы электронной почты, в хранилище информации на автономном сервере, куда у сторон имеется лишь ключ доступа и т.п.

Такого рода следы и представляют предмет нашего исследования как цифровые. Разделяются этапы следообразования цифровых следов на различных объектах-носителях.

В первую очередь, необходимо обратиться к специальной сфере криминалистики – трасологии. Необходимо отметить, что категория «след» понимается в трасологии неоднозначно: обычно под следом понимается отображение (отпечаток, оттиск) одного предмета на другом, возникающее в результате контакта между ними, хотя в теории трасологии как отрасли криминалистических знаний встречались и другие определения «следа» [14]. Поэтому следы в криминалистике (в узком смысле слова) – это только лишь следы, изучаемые в трасологии, то есть материальные отпечатки [15]. При этом криминалисты отмечают, что такого рода «классическое» понятие следа распространяется лишь на трасологическую морфологию, то есть в процессе трасологической идентификации следы изначально должны рассматриваться с разных позиций [16], а их круг, с очевидностью, шире привычного и общепринятого [17], представленного, например, Г.Л. Грановским [18].

Следует упомянуть и о том, что «традиционной» криминалистикой под следами в трасологическом значении подразумеваются материальные отображения на каких-то предметах признаков внешнего строения материальных объектов, контактно взаимодействовавших с первыми, то есть распространено мнение о «контактном принципе» следообразования и, следовательно, и определения следов как последствий контакта, что предполагает и выделение особых групп следов [19], к которым, исходя из предложенных авторами характеристик, цифровые следы (как предмет нашего исследования) относятся не в полной мере [20].

В то же время в литературе подчеркивается, что след именно потому признается следом, что он определенным образом изменяет объективную действительность [21]. Кроме того, сегодня в криминалистике широко распространено мнение о том, что категория «след» изначально должна быть пригодна для использования не только в криминалистических, но и в других областях научных знаний [22], в том числе в информационном праве в сфере обеспечения безопасного оборота персональных данных [23].

Такой подход перспективен и полностью соответствует современным реалиям оборота персональных данных, включая их трансграничную передачу. В криминалистике XXI века высказано правильное, на наш взгляд, мнение о том, что след – это любое материальное отображение свойств вещей и явлений,

позволяющее судить об их свойствах и использовать их отражение для решения диагностических, классификационных, идентификационных и интеграционных (ситуалогических) задач [24]. При этом выделяется и след электромагнитного воздействия [25], хотя такого рода определение в предложенном контексте и представляется нам более широким, чем определение понятия «цифровые следы» в понимании настоящего исследования.

Как мы указывали выше, цифровые следы могут отражаться либо на конкретных устройствах, участвовавших в информационном обмене персональными данными или иной работе с персональной информацией, либо в виде исключения в самой информационно-телекоммуникационной сети. Для того чтобы быть воспринятыми каким-либо лицом эти цифровые следы должны быть отображены в свойствах некоторого обособленного объекта материального мира, условно называемого в науке материальным носителем [26].

С точки зрения этимологии, материальный носитель – это документ, содержащий данные с записанной на нем информацией, предназначенный для ее передачи во времени и пространстве. По сути же, это объективированный в пространстве носитель информации, а значит – любой материальный объект (или среда), содержащий информацию, способный достаточно длительное время сохранять в своей структуре занесенные в него сведения, к примеру, в том числе электромагнитное излучение. В процессе генезиса человечества для создания документов применяются различные материальные объекты-носители (бумага, различные технические накопители и проч.), которые служат для закрепления и хранения на них различной информации: речевой, звуковой, рукописной и проч. Информатизация и компьютеризация общества способствовала появлению документов на небумажных носителях информации, поиск и воспроизведение которых требуют применения специальных технических устройств.

Разумеется, в процессе расследования существуют исключения, когда следовую информацию можно получить непосредственно из сети (опять-таки с подключением соответствующего вычислительного устройства и входа в сеть), минуя устройства, с которого была передана персональная информация и устройства, на которую она была получена, а также устройства ее хранения (серверы провайдеров и т.п.). Например, можно говорить в этой связи о следах, оставленных при осуществлении записи в информационной системе, построенной по типу распределенных систем (например, блокчейн) [27]), когда совершенное в системе действие автоматически отражается у всех других участников системы, не имеющих отношение к произведенным юридически значимым действиям, причем эти отображения абсолютно равнозначны технически и имеют равную юридическую силу. Теоретически, с точки зрения физики, можно говорить и о такой ситуации, когда сложный электронный импульс, содержащий те или иные сведения, пытаясь проникнуть на какое-либо устройство, по сути, «живет» в

информационно-телекоммуникационной сети до момента его «затухания» в силу закона сохранения энергии [28].

Вместе с тем указанные случаи являются в большей степени исключениями; чаще всего следы противоправных действий в отношении персональных данных в информационно-телекоммуникационной сети остаются на тех или иных вычислительных устройствах, участвовавших в информационном обмене, связанном с направлением, передачей, получением, хранением, обработкой соответствующей персональной информации, то есть здесь уже следует говорить об «информации об информации». Данные следы, называемые «цифровыми», хранятся на этих устройствах и отображают сведения, как минимум, о самом устройстве, посредством которого совершены определенные действия, и о самих действиях (в той или иной степени), совершенных с использованием указанных устройств.

Таким образом, что особенно значимо для поисковой и познавательной деятельности в указанной сфере, в таких цифровых следах совмещаются воедино сами действия и устройства, с помощью которых они были совершены. Потенциально в процессе расследования преступлений устройства могут «указать» на лицо, совершившее противоправные действия, а характер совершенных им действий – свидетельствовать о наиболее важных признаках способа совершения посягательства в процессе криминалистического установления киберпреступления.

В криминалистической теории надо иметь в виду, что цифровые следы всегда образуются и модифицируются в результате воздействия компьютерных программ (приложений). Специфика этих следов проявляется в том, что они не имеют ни цвета, ни запаха, ни иных характеристик, которые традиционно рассматриваются трасологией, и в которых могли бы отразиться отдельные черты злоумышленника, на основании которых можно было бы достоверно идентифицировать его личность [29].

Заключение

По результатам исследования мы приходим к следующим основным выводам и положениям.

Прежде всего, мы определяем способ нарушения прав на персональные данные с помощью информационно-коммуникационных технологий как избранную злоумышленником последовательность личных действий и операций, связанную с использованием информационно-коммуникационных сетей в противоправных целях.

Персональная информация о физическом лице как самостоятельный набор сведений или, что чаще всего бывает, в качестве некоторого массива данных на информационном ресурсе, являясь объектом правовой охраны, может выступать предметом посягательства, которое совершается посредством противоправного воздействия на нее (доступа к ней) «в границах» информационно-телекоммуникационной сети, которая, в свою очередь, может быть локальной (в рамках одной организации или одного

органа власти) или глобальной, всеобщей (сеть Интернет).

Таким образом, с точки зрения криминалистики способ нарушения прав на персональные данные с помощью информационно-коммуникационных технологий – это избранная злоумышленником последовательность личных действий и операций на этапе подготовки, совершения и сокрытия своего вмешательства в оборот персональных данных, сопряженная с применением компьютерной (вычислительной) техники, позволяющей осуществлять доступ к персональной информации, включая ее отправление, получение и передачу посредством использования линий электрической (электронной) связи.

Способ нарушения прав на персональные данные с помощью информационно-коммуникационных технологий, с точки зрения криминалистического расследования преступления, тесно связан с механизмом следообразования. В данном случае, цифровой след образуется ввиду самого факта участия субъектов в информационном обмене посредством использования информационно-телекоммуникационной сети.

Криминалистам следует учитывать, что цифровые следы имеют значительную специфику относительно «обычных» следов, исследуемых трасологией, указанную нами выше, которая во многом обусловлена свойствами как самой информации, так и информационно-телекоммуникационной сети Интернет. Злоумышленники могут оставить цифровой след в условиях доступа в сеть, когда имеет место целенаправленный поиск информации или соответствующих сегментов сети, «пригодных», по мнению нарушителя, для ее распространения (следует помнить, что иногда достаточно включения электропитания устройства злоумышленника, что подразумевает не только его «обнаружение» в сети, но и посредством кэш-информации и файлов-куки облегченный доступ к интересовавшей злоумышленника ранее персональной информации); вследствие целенаправленных действий злоумышленника в сети (что в ряде ситуаций не исключает и непредвиденных злоумышленником случайных соединений между устройствами, находящимися в информационно-телекоммуникационной сети).

Мы полагаем, что для цифрового следа свойственны следующие характеристики: это особая информация, которая выражена в электронном виде в форме учетной записи, представляющей собой машинный код; образуется в результате участия в информационном обмене посредством информационно-телекоммуникационной сети; представляет собой сведения об устройстве (адресе устройства), с которого был осуществлен доступ в сеть и (или), о действиях, предпринятых в сети посредством данного устройства, может быть обнаружена на одном из устройств, участвовавших в информационном обмене, в той ее части, в которой данное устройство участвовало в этом обмене (было источником или получателем информации, ее хранителем или передающим звеном и т.п.).

Понимание способов нарушения прав на персональные данные с помощью информационно-

коммуникационной сети Интернет в международном информационном праве шире, чем их уголовно-правовое или криминалистическое понимание в юридической науке.

Значение способа вмешательства в правомерный оборот персональных данных с использованием информационно-телекоммуникационной сети Интернет для организации работы по профилактической защите этого оборота, в том числе техническими средствами, а также для установления факта вмешательства в оборот персональных данных в глобальной информационной сети (его документирования и доказывания), выбора стратегии и тактики обеспечения безопасности персональной информации и ее защиты достаточно велико. А на первоначальной стадии (при установлении несанкционированного доступа к персональной информации), - даже определяющее, поскольку от установленного с той или иной долей вероятности способа использования информационно-телекоммуникационной сети с целью получения доступа к персональной информации зависит установление того, какие именно доказательства должны быть собраны, какие исследовательские действия и в какой последовательности (очередности) должны быть проведены, определение путей и пределов использования специальных знаний, в том числе в части назначения криминалистических экспертиз, привлечения к участию в этих действиях специалистов и проч.

Среди категорий объектов, являющихся носителями практически значимой для раскрытия и расследования информации, по нашему мнению, следует выделять: устройства для хранения информации; устройства для ввода и вывода информации; устройства для обработки информации; устройства для передачи информации по каналам (шлюзам) связи; информационные системы. Указанные объекты могут заключать в себе определенную значимую информацию, представляющую доказательственный интерес.

Исходя из анализа следовой картины незаконного вмешательства в правомерный оборот персональных данных, компьютерная система может выступать в качестве: средства осуществления такого вмешательства; носителя следов противоправной деятельности; предмета посягательства (неправомерного доступа к персональным данным) и носителя иной значимой информации.

С точки зрения механизма следообразования в компьютерных системах, в криминалистике наиболее продуктивно установить в качестве критерия деления уровень воздействия пользователя на компьютерную систему, на основании чего выделять следы непосредственные и опосредованные. Под непосредственными следами мы предлагаем называть цифровые следы, которые предполагают прямую связь с причиной (целью) воздействия пользователя на компьютерную систему. Например, такими следами будут компьютерные данные:

- образованные или измененные пользователем посредством устройств ввода (клавиатура, микрофон и проч.);

- скопированные или перемещенные;

- почтовые (e-mail) отправления;

- переписки с использованием мессенджеров;

- истории запросов Интернет-браузера;

- записи в базах данных и проч.

Опосредованными следами мы предлагаем называть любые цифровые следы, которые пусть и не имеют прямой связи с причиной (целью) воздействия пользователя на компьютерную систему, но инициированы этим воздействием. Например, такими следами могут быть:

- записи в файлах журналирования системных событий (логи);

- файлы реестра операционной системы;

- метаданные информационных ресурсов;

- записи служебных баз данных и проч.

Принадлежность цифрового следа к непосредственным или опосредованным может предоставлять как информативность данного цифрового следа, так и уровень применения специальных знаний и техники, необходимых для его обнаружения и дальнейшей идентификации.

Таким образом, рассмотренные нами теоретические положения показывают, что цифровые следы могут и должны рассматриваться как самостоятельный фактор посредством их применения в процессе раскрытия и расследования возможных нарушений оборота персональных данных и обеспечения их безопасности. Однако в криминалистической науке необходимо повышать уровень теоретической разработки предложенной проблематики, что послужит важной основой для проведения более широких криминалистических исследований процессов применения цифровых следов с целью эффективного расследования фактов нарушений в сфере оборота персональных данных.

Список литературы

1. Рассолов И.М. Защита частной жизни в сетях международного информационного обмена // Актуальные проблемы российского права. 2015. № 2. - С. 48 - 53.

2. Сорокин Д.В. Проблемы правового обеспечения информационной безопасности России в условиях глобализации информационного пространства. Авто-реф.дисс.канд.юр.наук. Спб., 2006. – 28 с.

3. Регламент (ЕС) 2016/679 Европейского Парламента и Совета «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС» (Общие правила защиты данных) от 27 апреля 2016 года.

4. Криминалистическая методика расследования отдельных видов преступлений: учебник: в 2 ч. / под ред. А. П. Резвана, М. В. Субботиной. М., 2020. Ч. 1. – 480 с.

5. Лузгин И.М. Некоторые аспекты криминалистической характеристики и место в ней данных о сокрытии преступлений. М., 1984. – 340 с.

6. Пантелеев И.Ф. Методика расследования преступлений. М., 1975. – 280 с.

7. Doak J., McGourlay C. Evidence in Context. London, New York : Routledge, 2012. 365 p.

8. Адеев П.Г. Институциональное развитие правового обеспечения информационной безопасности в российском информационном праве. Екатеринбург. 2012. – 170 с.

9. Бачило И.Л. Компьютерное право. Методология и практика // Безопасность информационных технологий. 2017. Вып.2. – С.70-81.

10. Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. 2015. № 8. - С. 100 – 109.

11. Яшков С.А. Информация как предмет преступления: дис. ... канд. юрид. наук. Екатеринбург, 2020. - 196 с.

12. Российское уголовное право. Особенная часть. Учебник для вузов / Под ред. В.П. Коняхина и М.Л. Прохоровой. М., 2019. – 680 с.

13. Коняхин В.П., Асланян Р.Г. Информация как предмет и средство совершения преступлений в сфере экономической деятельности // Российский следователь. 2016. № 8. - С. 24 – 27.

14. Ищенко Е.П., Топорков А.А. Криминалистика. Учебник. 3-е издание, испр. и доп. М.: Деловой двор, 2017. – 578 с.

15. Ищенко Е.П. Актуальные проблемы и направления развития криминалистики // Актуальные вопросы криминалистики и уголовно-процессуального права. Киров, 2018. - С. 9-10.

16. Зинин А.М., Майлис Н.П. Судебная экспертиза. Учебник. М., 2020. – 560 с.

17. Койсин А.А. Современные методы исследования запаховых следов (образований) // Эксперт-криминалист. 2011. № 2. - С. 44-50.

18. Грановский Г.Л. Основы трасологии. 2-е изд. М.: Наука, 2016. – 230 с.

19. Майлис Н.П. Введение в судебную экспертизу. М., 2020. – 192 с.

20. Сухарев А.Г. Трасология и трасологическая экспертиза: Учебник. Саратов, 2018. – 492 с.

21. Криминалистика: Учебник для среднего профессионального образования / Под ред. А. А. Закатова, Б. П. Смагоринского. Волгоград, 2019. – 680 с.

22. Степанов Г.Н., Бронников А.И. Трасология: Справочник криминалиста. Т.2. Механоскопия. Волгоград, 2020. – 210 с.

23. Computer Forensics: investigation procedures and response. 2nd ed. EC-Council Press, 2017. 172 p.

24. Грановский Г.Л. Основы трасологии. М.: Деловой двор, 2018. – 212 с.

25. Максуров А.А. Исследование следов. Актуальные проблемы трасологии - Mauritius: Palmarium Academic Publishing. 2020. – 128 с.

26. Vinson D.E. Jury trials: the psychology of winning strategy. Michie Co., 1986. 244 p.

27. Максуров А.А. Технология блокчейн – новое информационное и экономико-правовое явление // Актуальные проблемы современного российского государства и права: материалы ежегодной всероссийской научно-практической конференции / отв. ред. к.ю.н., доц. С.А. Старостина. Калининград: Калининградский филиал СПбУ МВД России, 2018. - С.132-143.

28. Saferstein R. Criminalistics: an Introduction to Forensic Science. 12th ed. New Jersey: Pearson, 2017. 576 p.

29. Volonino L., Anzaldua R., Godwin J. Computer forensics: principles and practices. New Jersey: Pearson / Prentice Hall, 2007. 534 p.

М.С. Бисалиев, К.Н. Шакиров

Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан

Цифрлық іздер Интернет желісіндегі дербес деректер айналымының қауіпсіздік факторы ретінде

Аңдатпа. Мақалада кибер ортадағы дербес деректердің қауіпсіз айналымын қамтамасыз етудің маңызды факторы ретінде Интернеттегі цифрлық іздер туралы білімді пайдаланудың негізгі тәсілдері қарастырылады. Аталған мәселе бойынша цифрландыру доктринасындағы ғылыми ұстанымдарға шолу жасалды. Цифрлық іздердің авторлық анықтамасы берілген, жаһандық ақпараттық желіні пайдалана отырып, дербес деректерге қол сұғу тәсілдерін анықтау алгоритмі ұсынылады, сонымен қатар мұндай бұзушылықтың типтік фазалары мен құқық бұзушының әдеттегі әрекеттері көрсетілген. Бұл білім саласында алғаш рет ақпараттық құқық доктринасының жетістіктерін де, іздер туралы сот-медициналық ілімдерді де біріктіретін кешенді тәсіл қолданылды. Нәтижесінде дербес деректерге заңсыз қол жеткізу, оның ішінде оларды Интернетте ақпарат алмасу шеңберінде оларды «ұстау» анықталған жағдайда арнайы білімге жүгіну стандарттарын көздейтін халықаралық немесе өңірлік (еуропалық) акт қабылдау жөнінде ұсыныстар жасалды.

Түйін сөздер: ақпараттық қауіпсіздік, кибер орта, IT-технологиялар, цифрлық іздер, жеке деректер, жеке ақпарат, сәйкестендіру, құқықтық қорғау

M.S. Bissaliyev, K.N. Shakirov

Al-Farabi Kazakh National University, Almaty, Kazakhstan

Digital footprints as a factor in the security of personal data trafficking on the Internet

Abstract. The article discusses the main approaches to the use of knowledge about digital footprints on the Internet as a significant factor in ensuring the safe circulation of personal data in the cyber environment. The authors have made a review of the positions contained in the doctrine on this issue. The article contains definitions of digital traces, an algorithm for methods of encroaching on personal data using a global information network, and typical phases of such encroachment and the usual actions of the offender. For the first time in this field of knowledge, an integrated approach has been applied, combining both the achievements of the doctrine of information law and the forensic doctrine of traces. As a result, the authors have made proposals to adopt an international or regional (European) act providing standards for accessing special knowledge in case of detection of illegal access to personal data, including their "interception" as part of information exchange on the Internet.

Keywords: information, cyber environment, Internet, digital traces, personal data,

personal information, identification, legal protection

References

1. Rassolov I.M. Zashchita chastnoj zhizni v setyah mezhdunarodnogo informacionnogo obmena // Aktual'nye problemy rossijskogo prava. 2015. № 2. - S. 48 - 53.

2. Sorokin D.V. Problemy pravovogo obespecheniya informacionnoj bezopasnosti Rossii v usloviyah globalizacii informacionnogo prostranstva. Avtoref.diss.kand.yur.nauk. Spb., 2006. – 28 s.

3. Regulation (EU) 2016/679 of The European Parliament and of the Council 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).

4. Kriminalisticheskaya metodika rassledovaniya otdel'nyh vidov prestuplenij: uchebnik: v 2 ch. / pod red. A. P. Rezvana, M. V. Subbotinoj. M., 2020. CH. 1. – 480 s.

5. Luzgin I.M. Nekotorye aspekty kriminalisticheskoj harakteristiki i mesto v nej dannyh o sokrytii prestuplenij. M., 1984. – 340 s.

6. Panteleev I.F. Metodika rassledovaniya prestuplenij. M., 1975. – 280 s.

7. Doak J., McGourlay C. Evidence in Context. London, New York: Routledge, 2012. 365 p.

8. Adeev P.G. Institucional'noe razvitie pravovogo obespecheniya informacionnoj bezopasnosti v rossijskom informacionnom prave. Ekaterinburg. 2012. – 170 s.

9. Bachilo I.L. Komp'yuternoe pravo. Metodologiya i praktika // Bezopasnost' informacionnyh tekhnologij. 2017. – Vyp.2. – S.70-81.

10. Tereshchenko L.K., Tiunov O.I. Informacionnaya bezopasnost' organov ispolnitel'noj vlasti na sovremennom etape // ZHurnal rossijskogo prava. 2015. № 8. - S. 100 – 109.

11. Yashkov S.A. Informaciya kak predmet prestupleniya: Dis. ... kand. yurid. nauk. Ekaterinburg, 2020. - 196 s.

12. Rossijskoe ugolovnoe pravo. Osobennaya chast': Uchebnik dlya vuzov / Pod red. V.P. Konyahina i M.L. Prohorovoj. M., 2019. – 680 s.

13. Konyahin V.P., Aslanyan R.G. Informaciya kak predmet i sredstvo sovershenija prestuplenij v sfere ekonomicheskoj deyatel'nosti // Rossijskij sledovatel'. 2016. № 8. - S. 24 – 27.

14. Ishchenko E.P., Toporkov A.A. Kriminalistika: Uchebnik. 3-e izdanie, ispr. i dop. M.: Delovoj dvor, 2017. – 578 s.

15. Ishchenko E.P. Aktual'nye problemy i napravleniya razvitiya kriminalistiki // Aktual'nye voprosy kriminalistiki i ugolovno-processual'nogo prava. Kirov, 2018. - S. 9-10

16. Zinin A.M., Majlis N.P. Sudebnaya ekspertiza: Uchebnik. M., 2020. – 560 s.

17. Kojsin A.A. Sovremennye metody issledovaniya zapahovyh sledov (obrazovanij) // Ekspert-kriminalist. 2011. № 2. - S. 44-50.

18. Granovskij G.L. Osnovy trasologii. 2-e izd. M.: Nauka, 2016. – 230 s.

19. Majlis N.P. Vvedenie v sudebnuyu ekspertizu. M., 2020. – 192 s.

20. Sukharev A.G. Trasologiya i trasologicheskaya ekspertiza: Uchebnik. Saratov, 2018. – 492 s.

21. Kriminalistika: Uchebnik dlya srednego professional'nogo obrazo¬vaniya / Pod red. A. A. Zakatova, B. P. Smagorinskogo. Volgograd, 2019. – 680 s.

22. Stepanov G.N., Bronnikov A.I. Trasologiya: Spravochnik kriminalista. T.2. Mekhanoskopiya. Volgograd, 2020. – 210 s.

23. Computer Forensics: investigation procedures and response. 2nd ed. EC-Council Press, 2017. 172 p.

24. Granovskij G.L. Osnovy trasologii. M.: Delovoj dvor, 2018. – 212 s.

25. Maksurov A.A. Issledovanie sledov. Aktual'nye problemy trasologii - Mauritius: Palmarium Academic Publishing. 2020. – 128 s.

26. Vinson D.E. Jury trials: the psychology of winning strategy. Michie Co., 1986. 244 p.

27. Maksurov A.A. Tekhnologiya blokchejn – novoe informacionnoe i ekonomiko-pravovoe yavlenie // Aktual'nye problemy sovremennogo rossijskogo gosudarstva i prava: materialy ezhegodnoj vserossijskoj nauchno-prakticheskoj konferencii / otv. red. k.yu.n., doc. S.A. Starostina. Kaliningrad: Kaliningradskij filial SPbU MVD Rossii, 2018. - S.132-143.

28. Saferstein R. Criminalistics: an Introduction to Forensic Science. 12th ed. New Jersey: Pearson, 2017. 576 p.

29. Volonino L., Anzaldua R., Godwin J. Computer forensics: principles and practices. New Jersey: Pearson / Prentice Hall, 2007. 534 p.

Сведения об авторах:

Бисалиев М.С. - докторант 2-го курса кафедры международного права, Казахский национальный университет им. аль-Фараби, пр. аль-Фараби, 71, Алматы, Казахстан.

Шакиров К.Н. - д.ю.н., профессор кафедры международного права, Казахский национальный университет им. аль-Фараби, пр. аль-Фараби, 71, Алматы, Казахстан.

Bissaliyev M. – The 2nd year Ph.D. student, Department of International Law, Al-Farabi Kazakh National University, 71 Al-Farabi ave., Almaty, Kazakhstan.

Shakirov K. – Doctor of Law, professor, Department of International Law, Al-Farabi Kazakh National University, Al-Farabi ave. 71, Almaty, Kazakhstan.