

5. Сидоров, В. Е. Начальный этап расследования: организация, взаимодействие, тактика / В.Е. Сидоров. – М. : Рос. право, 1992. – 178 с.
6. Логвин, В. Некоторые процессуальные вопросы осмотра места происшествия / В. Логвин, Ю. Матвейчев // Судовы веснік. – 2008. – № 1. – С. 67–70.
7. Криминалистика : пособие / В. Б. Шабанов [и др.] ; под ред. В. Б. Шабанова, В. Л. Григоровича. – Минск : БГУ, 2019. – 551 с.
8. Саковец, И. Н. Тактические особенности осмотра места происшествия при расследовании нарушений уставных правил взаимоотношений между военнослужащими [Электронный ресурс] / И. Н. Саковец // Борьба с преступностью: теория и практика : тезисы докладов X Междунар. науч.-практ. конф., г. Могилев, 22 апр. 2022 г. / Министерство внутренних дел Республики Беларусь, УО «Могилевский институт Министерства внутренних дел Республики Беларусь» ; редкол.: Ю. П. Шкаплеров (отв. ред.) [и др.]. – Могилев : Могилев. институт МВД, 2022. – 1 электрон. опт. диск (CD-R). – С. 319–321.
9. Саковец, И. Н. Структура криминалистической характеристики нарушений уставных правил взаимоотношений между военнослужащими / И. Н. Саковец // Вестник Сибирского юридического института МВД России. – 2022. – № 1 (46). – С. 116–122.
10. Архив Суда Минского района за 2014 г. – Уголовное дело № 14036350003.

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ АВТОМАТИЧЕСКИХ СИСТЕМ КРИМИНАЛИСТИЧЕСКОГО РАСПОЗНАНИЯ ЛИЦ

Середа А. Е., Лузгин И. И.

*Белорусский государственный университет,
пр. Независимости, 4, 220030 Минск, Беларусь, lawcrim@bsu.by*

Исследуется правовое обеспечение обработки персональных данных автоматических систем криминалистического распознавания лиц. Делается вывод о необходимости разработки и имплементации Концепции организованной консолидации персональных данных в расследовании преступлений и правонарушений, а также унифицированной классификации баз персональных данных.

Ключевые слова: персональные данные; криминалистика; базы данных; распознавание лиц; биометрические данные; расследование преступлений; информация, система

В настоящее время развитие общественных отношений в информационной сфере и складывающаяся судебная практика предопределили формирование нового элемента структуры комплексного конституционного права на неприкосновенность частной жизни – права на защиту персональных данных. В этой связи, в Республике Беларусь был принят первый в стране Закон от 7 мая 2021 г. № 99-З «О защите персональных данных», который вступил в силу 15 ноября 2021 г., а в его развитие был издан Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных». Наряду с результатами комплексного совершенствования законодательства о персональных данных как в Республике Беларусь, так и правового регулирования за ее пределами (модернизирована Конвенция Совета Европы от 28 января

1981 г. № 108 «О защите физических лиц при автоматизированной обработке персональных данных», принят Общий регламент о защите персональных данных Европейского союза от 27 апреля 2016 г. (GDPR) (вступил в силу 25 мая 2018 г.), научный и практический интерес представляет рассмотрение института публичной ответственности за его нарушение, а также применение специальных и биометрических персональных данных в раскрытии и расследовании преступлений. На современном этапе, значимым направлением в криминалистике являются информационные и интеллектуальные технологии, которые занимают центральное место в системах криминалистического обеспечения расследования, обвинения, защиты и судебной деятельности, т.к. основным объектом криминалистического исследования в данном ключе является информационная человеческая деятельность: с одной стороны, информация о поведении преступника (как объекта познания), с другой – информация о его идентифицирующих признаках (как элементов познания) [1, с. 11].

Согласно мнению заслуженного деятеля науки Республики Беларусь, доктора юридических наук, ученого-криминалиста А.В. Дулова, криминалистика – это наука, призванная решать задачи, возникающие в борьбе с преступностью, путем изучения преступления, процессов его отражения в окружающем мире и сознании человека и содержания деятельности по расследованию в целях познания закономерностей этих процессов и связей между объектами исследований для разработки методов, средств, приемов и рекомендаций по организации тактической деятельности по выявлению, расследованию и профилактике преступлений [2, с. 16].

По определению советского и российского криминалиста, доктора юридических наук, заслуженного деятеля науки РСФСР Р. С. Белкина, криминалистика – это наука о закономерностях механизма преступления, возникновения информации о преступлении и его участниках, исследования, оценки и использования доказательств, основанных на познании этих закономерностей, специальных средствах и методах судебного исследования и предотвращения преступления [1, с. 10].

В своих работах белорусский ученый, доктор юридических наук В. Б. Шабанов утверждает, что в центре внимания криминалистики находятся не только следы, но и человек, который их оставляет. «Криминалистика, в том числе наука, информативно-центрированная на личность, определившая механизмы совершения, раскрытия преступлений, закономерности расследования, обвинения и защиты по уголовным делам». В связи с этим целесообразно иметь необходимое тактическое и стратегическое средство – систему технологий, составляющих композицию криминалистического обеспечения оперативно-розыскной деятельности, расследования обвинения, защиты и судебной деятельности [1, с. 11].

Природа криминалистики в значительной степени интегративна – с позиции некоторых ученых, это позволяет дополнить ее определение положением о том, что «это наука о системном изучении и познании закономерностей механизма преступления, возникновения информации о преступлении и его участниках, изучении и познании этих закономерностей, исследования, оценки и использования доказательств, создании и использовании системных специальных средств и методов судебного исследования и предотвращения преступлений» [3, с. 185].

Дополнение, не изменяя содержания определения, расширяет и углубляет его смысл.

Автоматическое распознавание лиц как процесс представляет собой цифровую визуальную регистрацию характерных особенностей элементов внешности, в данном случае лица человека, с последующим конструированием уникальной системы признаков, обладающей достаточным набором характеристик, которые в совокупности предоставляют возможность для точной криминалистической идентификации (система автоматического распознавания лиц. С целью фиксации особенностей лица человека, технология производит их «оцифровку» – т.е. математизирует, моделирует биометрические признаки и создает шаблон для последующего сравнения с образцами, загруженными в базу данных. В криминалистике, ручные и автоматизированные биометрические методы могут быть использованы для анализа и интерпретации биометрических следов в следующих трех аспектах расследования преступлений: 1) продемонстрировать наличие преступления; 2) расследовать преступление; 3) идентифицировать преступника [4, с. 733]. В криминалистической трактовке следы – это прежде всего то, что оставляют преступники на месте происшествия. Следы это то, что ищут и изучают оперативные работники, следователи, эксперты, судьи, познают по ним, что требуется выявить и доказать. Все, кто занимается этим, практически «следоведы». В связи с тем, что системы автоматического распознавания лиц оперируют биометрическими данными, то речь идет о роли и использовании персональных данных в раскрытии и расследовании преступлений.

Персональные данные – это любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано (как определено п. 9 ст. 1 Закона № 99-3) [5]. К понятию «Персональные данные» можно отнести любые данные, если с их помощью можно идентифицировать физическое лицо, так как законодательством не установлен перечень «иных данных». Определить физическое лицо можно, в частности, через: Ф.И.О.; дату рождения; идентификационный номер; через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности (п. 9, ст. 17 Закона № 99-3) [5]. Любое действие или совокупность действий, совершаемые с персональными данными, включая сбор, систематизацию, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление персональных данных называется обработкой персональных данных (п. 6 ст. 1 Закона № 99-3) [5]. Субъектом персональных данных может быть только физическое лицо, в отношении которого осуществляется обработка персональных данных (п. 13 ст. 1 Закона № 99-3) [5]. Юридические лица и иные организации не являются субъектами персональных данных. Гражданство физического лица не имеет значения, если на обработку персональных данных этого лица распространяется действие Закона № 99-3.

Согласно ст. 1 Закона № 99-3 биометрические персональные данные являются разновидностью персональных данных и представляют собой информацию, характеризующую физиологические и биологические особенности человека, ко-

торая используется для его уникальной идентификации [5]. Идентификация имеет схожие смыслы в различных областях науки:

- 1) признание тождественности, отождествление объектов;
- 2) установление тождества объекта или личности по совокупности общих и частных признаков (криминалистика);
- 3) процесс эмоционального и иного самоотождествления личности с другим человеком, группой, образцом;
- 4) установление соответствия распознаваемого предмета своему образу (знаку) (технические и точные науки);
- 5) установление тождества неизвестного химического соединения с известным путем сравнения их физических и химических свойств (химия).

По мнению некоторых ученых, идентификация может быть групповой (установление принадлежности объекта к определенному роду и виду объектов) и индивидуальной (установление индивидуального тождества). При установлении личности человека на основе его персональных данных речь идет об индивидуальной идентификации.

С 15 ноября 2021 г. Законом № 99-3 выделяется особая категория персональных данных – специальные персональные данные (п. 12 ст. 1), которая включает в себя данные о [5]:

- 1) расовой или национальной принадлежности;
- 2) политических взглядах;
- 3) членстве в профессиональных союзах;
- 4) религиозных или других убеждениях;
- 5) здоровье или половой жизни;
- 6) привлечении к административной или уголовной ответственности;
- 7) физиологических и биологических особенностях человека (следы пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображения и другое), которые используются для его уникальной идентификации (биометрические персональные данные – п. 2 ст. 1 Закона № 99-3) [5].

Выделяются также общедоступные персональные данные, которые распространяются самим субъектом персональных данных либо с его согласия или распространены в соответствии с требованиями законодательных актов [5]. В данной связи, выделяют прямую идентификацию – возможность прямо идентифицировать лицо и косвенную идентификацию – возможность при неизвестности характеристик физического лица выделить его из группы других лиц по некоторым известным фактам (к примеру, по имени и месту работы). В данном контексте имеется ввиду прямая и косвенная идентификация не в ее криминалистическом, а в оперативно-розыскном значении. Содержание действий, подпадающих под этот аспект данного понятия, как раскрывают характер, так и конфликтуют с исходным его содержанием.

Часть 3 ст. 8 вышеупомянутого Закона предусматривает, что в отношении специальных персональных данных государство предоставляет дополнительные гарантии: осуществление их обработки допускается лишь при условии принятия комплекса мер, направленных на предупреждение рисков, которые могут возникнуть при этом для прав и свобод субъектов персональных данных [5].

Ст. 10-13, 15 указывают на то, что субъект персональных данных имеет право: на отзыв согласия; доступ и получение информации об обработке персональных данных; изменение персональных данных; получение информации о передаче данных; прекращение обработки данных (их удаление); обжалования действий (бездействия) оператора [5].

В отношении субъектов, обрабатывающих персональные данные, Закон № 99-3 выделяет 2 категории лиц: оператор и уполномоченное лицо [5]. Под оператором понимается государственный орган, юридическое лицо, иная организация, физическое лицо, в том числе индивидуальный предприниматель, самостоятельно или совместно с иными указанными лицами организующие и (или) осуществляющие обработку персональных данных; под уполномоченным лицом – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, которые в соответствии с актом законодательства, решением государственного органа, являющегося оператором, либо на основании договора с оператором осуществляют обработку персональных данных от имени оператора или в его интересах. Обязанности оператора и уполномоченного лица различаются тем, что уполномоченное лицо не обязано получать согласие субъекта персональных данных, такая обязанность лежит на операторе; ответственность перед субъектом персональных данных за действия уполномоченного лица несет оператор, уполномоченное лицо несет ответственность перед оператором. В остальном обязанности оператора и уполномоченного лица совпадают. Операторами, в частности, могут являться: наниматель при обработке персональных данных своих работников; учреждение образования при оказании образовательных услуг учащимся; учреждение здравоохранения при оказании медицинской помощи пациентам; страховщик по отношению к застрахованным лицам и т.п.

В Законе № 99-3 согласие на обработку является базовым основанием для обработки (ч. 3 ст. 4) [5]. Однако законодатель учел разнообразие ситуаций, при которых могут собираться и обрабатываться персональные данные, указав случаи, при которых обработка персональных данных будет законной и без получения на это согласия. Перечень таких случаев достаточно широкий и в основном связан с деятельностью государственных структур при осуществлении ими своих функций, как указано в ст. 6 Закона № 99-3 [5]. Однако некоторые изъятия важны и непосредственно применимы в деятельности субъектов хозяйствования. К примеру, согласие на обработку персональных данных не требуется при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности субъекта в случаях, предусмотренных законодательством (п. 8 ст. 6). Также отдельное согласие не требуется? если оператор получает персональные данные на основании договора, заключенного (заключаемого) с субъектом персональных данных, в целях совершения действий, предусмотренных этим договором (п. 15 ст. 6) [5]. Случай, когда физическое лицо указывает на персональные данные в документе, подписанном им и адресованном оператору (запрос, заявление, обращение и т.п.), также подпадает под изъятие (п. 16 ст. 6) [5].

Общественная опасность незаконных действий в отношении персональных данных значительно повышается, когда они сопровождаются последующим при-

чинением существенного вреда правам, свободам и законным интересам граждан, имущественными преступлениями и преступлениями на почве ненависти. Зачастую необратимый характер таких последствий (например, это может быть связано с затруднениями в ограничении доступа к персональным данным, уже распространенным в сети Интернет, вынужденным изменением места жительства, работы и др.) и необходимость усиления информационной безопасности личности посредством предупреждения и пресечения новых общественно опасных посягательств в целом послужило основой закрепления в главе 23 УК двух составов преступлений [6]:

«Статья 203. Незаконные действия в отношении информации о частной жизни и персональных данных»;

«Статья 203. Несоблюдение мер обеспечения защиты персональных данных».

Как уже было отмечено, обработка персональных данных – это любое действие или совокупность действий, совершаемые с персональными данными (сбор, систематизация, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление и т.д.). Системы автоматического распознавания лиц не могут осуществлять свои функции без четко сконструированных баз данных, в которых содержится информация, или, в соответствии с определением в Законе № 99-3, персональные данные граждан. Ранее была предложена классификация баз данных подобных систем, выделяя корпоративные, ведомственные и глобальные базы данных как составляющие этой классификации [4].

Согласно ст. 6 Закона № 99-3, согласие субъекта персональных данных на обработку персональных данных, за исключением специальных персональных данных, порядок обработки которых установлен статьей 8 вышеупомянутого Закона, не требуется: для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности; для осуществления правосудия, исполнения судебных постановлений и иных исполнительных документов; в целях осуществления контроля (надзора) в соответствии с законодательными актами; при реализации норм законодательства в области национальной безопасности, о борьбе с коррупцией, о предотвращении легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения; для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно; в случаях, когда обработка персональных данных является необходимой для выполнения обязанностей (полномочий), предусмотренных законодательными актами [5].

Помимо этого, статья 15 Закона Республики Беларусь «Об оперативно-розыскной деятельности» от 15 июля 2015 г. № 307-3 позволяет органам, осуществляющим ОРД, «создавать и (или) использовать базы данных (учеты), информационные системы, средства негласного получения (фиксации) информации и иные средства в соответствии с настоящим Законом и иными актами законодательства ... в целях получения сведений, необходимых для выполнения задач оперативно-розыскной деятельности...» [7]. Объем и характер этих «сведений»

не уточняется. Однако анализ иных положений Закона об ОРД, как утверждает белорусский ученый А.М. Хлус, позволяет сделать вывод, что к числу данных сведений относится также информация «о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела». По существу, рассуждает А.М. Хлус, речь идет о сборе, накоплении и анализе информации о «частной жизни физического лица и его персональных данных» [8, с. 375].

В заключение отметим, что мы считаем, что большое значение в раскрытии и расследовании преступлений также следует придавать классификации и правовому обеспечению баз данных для систем автоматического распознавания лиц в криминалистике. В общем виде, эти базы данных могут быть разделены на три крупные категории – это базы данных: глобальные (социальные сети, международные реестры и платформы, предоставляющие материал для сравнения и идентификации), корпоративные (базы данных корпоративных сотрудников предприятий и корпораций) и ведомственные (для использования правоохранительными и административными органами). Помимо этого, Указом Президента республики Беларусь от 28 октября 2021 г. установлено, что базы данных также могут быть классифицированы на базы данных, содержащие: 1) общедоступные персональные данные; 2) специальные персональные данные (кроме биометрических и генетических персональных данных); 3) биометрические и генетические персональные данные; 4) персональные данные, не являющиеся общедоступными или специальными [9].

Эффективность автоматических систем распознавания лиц в раскрытии и расследовании преступлений напрямую зависит от эффективного взаимодействия действующих баз данных (как локальных, так и международных) с алгоритмом распознавания.

В целях усовершенствования и повышения эффективности правового обеспечения обработки персональных данных автоматических систем криминалистического распознавания лиц, считаем целесообразным разработку и имплементацию на законодательном уровне Концепции организованной консолидации данных в расследовании преступлений и административных правонарушений. Концепция в общих чертах подразумевает консолидацию персональных данных посредством создания и регистрации центрального звена, или центрального аппарата персональных данных, который соединяет базы данных действующих операторов внутри страны и за рубежом. Задача центрального аппарата заключается в передаче запросов и ответных сигналов от операторов баз персональных данных уполномоченным органам и обеспечение безопасности передаваемой информации посредством криптографической защиты. Разработка концепции и утверждение ее на законодательном уровне позволит упорядочить процесс обработки персональных данных, способствовать повышению уровня обеспечения безопасности обработки персональных данных и оптимизации обмена данными между операторами и уполномоченными лицами и государственными органами.

Библиографический список

1. Шабанов, В. Б. Особенности информационно-криминалистических технологий / В. Б. Шабанов // Криминалистическое обеспечение расследования преступлений: проблемы, перспективы и инновации: материалы Междунар. науч.-практ. конф., посвящ. 45-летию каф. криминалистики юрид. фак. БГУ, Минск, 12-13 окт. 2017 г. / БГУ ; редкол.: В. Б. Шабанов (отв. ред.) [и др.]. – Минск : Изд. Центр БГУ, 2017 – С. 10–11.
2. Криминалистика: учеб. пособие / А.В. Дулов [и др.] ; под ред. А. В. Дулова. – Минск: Экоперспектива, 1998. – 416 с.
3. Лузгин, И. И. О дополнении определения криминалистики / И. И. Лузгин // Актуальные вопросы современной правовой науки: материалы междунар. науч. конф., Минск, 4–5 ноября 2011 г. / Изд. центр БГУ; редкол. О. И. Чуприс [и др.]. – Минск, 2012. – С. 184–185.
4. Веренчиков, И. Р. Особенности криминалистического распознавания лиц: проблемы и перспективы / И. Р. Веренчиков, А. Е. Середа // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь ; редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск : Колорград, 2022. – Вып. 17. – С. 733–742.
5. О защите персональных данных [Электронный ресурс] : Закон Респ. Беларусь от 7 мая 2021 г. № 99-3 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.
6. Уголовный кодекс Республики Беларусь [Электронный ресурс] : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Республики Беларусь от 09.03.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.
7. Об оперативно-розыскной деятельности [Электронный ресурс] : Закон Респ. Беларусь, 15 июля 2015 г. № 307-3 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.
8. Хлус, А. М. Конституционные принципы оперативно-розыскной деятельности и их соблюдение / А. М. Хлус, П. А. Гуцко // Криминалистические чтения, посвященные памяти Заслуженного юриста Республики Беларусь Г. И. Грамовича : м-лы Междунар. науч.-практ. конф., г. Минск, 21 дек. 2012 г. / М-во внутр. дел Респ. Беларусь, УО «Акад. М-ва внутр. дел Респ. Беларусь» ; ред. кол. : В.Б. Шабанов (отв. ред.) [и др.]. – Минск : Акад. МВД, 2012. – С. 372-375.
9. О мерах по совершенствованию защиты персональных данных [Электронный ресурс] : Указ Президента Респ. Беларусь, 28 окт. 2021 г., № 422 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

О ПОНЯТИИ КОРРУПЦИИ И ЕЕ ПРЕДУПРЕЖДЕНИИ

Скаков А. Б.

*Костанайская академия Министерства внутренних дел Республики Казахстан
имени Ш. Кабылбаева, пр. Абая, 11, 110005, г. Костанай, Республика Казахстан,
odo@kostacademy.edu.kz*

В данной статье автором предпринята попытка проанализировать причину проникновения коррупции во все структуры социальной жизни общества. Это позволило ему сформулировать новое понятие коррупции, предусматривающее расширение круга субъ-