Ушаков Руслан Михайлович (rafikov.ruslan@list.ru)
Студент Института прокуратуры
Саратовской государственной юридической академии
Ruslan M. Ushakov
Saratov State Academy of Law
Institute of Prosecution, Student

ТЕХНОЛОГИЯ BIG DATA КАК ВЕКТОР РАЗВИТИЯ КРИМИНАЛИСТИЧЕСКОЙ ТЕХНИКИ: ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ В КОНТЕКСТЕ ИХ ПРАВОМЕРНОСТИ

BIG DATA TECHNOLOGY AS A DIRECTION OF DEVELOPMENT OF CRIMINALISTIC TECHNIQUE: PROSPECTS FOR APPLICATION IN THE CONTEXT OF THEIR LAWFULNESS

Аннотация: В исследовательской работе рассматриваются различные аспекты применения технологии Big Data в криминалистической деятельности. На основе анализа законодательства, положений правовой доктрины и существующего опыта использования различных форм искусственного интеллекта в жизнедеятельности человека автором обозначаются возможные направления их внедрения в криминалистическую практику (прежде всего — в работу эксперта), выявляются диалектически связанные с этим риски и проблемы концептуально-правового характера. Обосновывается необходимость разработки и издания ряда правовых мер, направленных на предотвращение негативных последствий распространения технологии Big Data, в частности

— общего законодательного запрета на принятие субъектами правоприменения юридически значимых решений, основанных исключительно на выводах, полученных программными методами.

Ключевые слова: технологии, большие данные, искусственный интеллект, нейронные сети, машинное обучение, персональные данные, криминалистика, криминалистическая техника, криминалистическая регистрация, экспертиза.

Abstract: The article discusses various aspects of the application of Big Data technology in forensic activities. Based on the analysis of the legislation, provisions of the legal doctrine and the existing experience of using various forms of artificial intelligence in human life, the author identifies possible directions for their implementation in forensic practice (primarily in the work of an expert), identifies dialectically related risks and problems of a conceptual and legal nature. The necessity of taking a number of legal measures aimed at preventing the negative consequences of the dissemination of Big Data technology is substantiated, in particular, the introduction of a general legislative ban on the adoption by law enforcement entities of legally significant decisions based solely on conclusions obtained by software methods.

Key words: technology, big data, artificial intelligence, neural networks, machine learning, personal data, forensics, forensic technology, forensic registration, expertise.

Согласно емкому определению Британской энциклопедии (Encyclopædia Britannica) в наиболее общем виде

криминалистика представляет собой применение методов естественных и физических наук к вопросам уголовного и гражданского права [1], что весьма точно указывает на ее прикладной, междисциплинарный характер, отмечает адаптивность и готовность к восприятию достижений научно-технического прогресса. Конкретные технологии, прежде чем окончательно войти в инструментарий криминалистики, как правило, проходили «тернистый путь» от своего создания до апробации и широкого применения в практике. Подобное можно утверждать, в частности, в отношении судебной фотографии (вторая половина XIX в.) [2, с. 232-233] и дактилоскопии (рубеж XIX и XX вв.) [3, с. 140]. В настоящее время к данным технологиям относятся глубоко интегрированные в жизнь фото- и видеосъемка, к перспективным, ориентированным на будущее, — явления сущностно одного порядка: искусственный интеллект, нейронные сети, робототехника и др.

Текущие и возможные последствия ускоряющейся экспансии передовых технологий в механизм функционирования существующей системы общественных отношений все более дискутируются в правовой доктрине; закономерно, что они, обладая огромным потенциалом для применения в криминалистической технике, при широком внедрении в практику гипотетически позволят качественно повысить эффективность выявления, раскрытия, расследования и предупреждения преступлений. А потому следует заключить, что т.н. «цифровая криминалистика» — в высшей степени актуальное направление для современных исследований [4, с. 4-6; 5, с. 43-49].

Отраслью криминалистической техники, особенно предрасположенной к восприятию достижений науки и техники, является система уголовной (криминалистической) регистрации, назначение которой заключается в формировании системы криминалистических учетов определенных объектов — носителей информации (источники — фотоснимки, антропометрические измерения, описание по методу словесного портрета, дактилоскопические оттиски и др. [6, с. 254]), используемой для раскрытия и расследования преступлений [7]. Криминалистическая регистрация, корнями уходящая к древним способам наказания преступников в форме нанесения увечий (клеймения и калечения) — как правило, в целях последующей их идентификации — получила бурное, но во многих аспектах экстенсивное, а не интенсивное развитие в XX и XXI вв., выразившееся в значительном увеличении количества подлежащих учету объектов, а также в усовершенствовании способов и методов регистрации, внедрении автоматизированных систем (яркий пример — создание геномного учета в России в 2008 г.)[1]. В этой связи следует констатировать, что к настоящему времени криминалистическая регистрация представляет собой целостно неоднородное, сложное структурное образование, состоящее из совокупности нескольких десятков учетов [8, с. 368-385].

Исходя из того, что сущность криминалистической регистрации состоит в накоплении, систематизации и дальнейшем использовании определенных сведений о признаках объектов, попадающих в сферу судопроизводства (в

[1] О государственной геномной регистрации в Российской Федерации: федер. закон от 03.12.2008 г. № 242-ФЗ (с изм. от 17.12.2009 г.) // Собр. законодательства Рос. Федерации. 2008. № 49. Ст. 5740.

частности, о преступниках), то, безусловно, ключевым понятием, определяющим ее содержание, является информация[2]. Результативность выявления, раскрытия и расследования преступлений напрямую зависит от количества и качества доступной для анализа криминалистически значимой информации, источниками которой выступают разнообразные (материальные, идеальные и цифровые) следы преступления. По признаку значимости для следствия в науке приоритетно выделяется ее подвид — актуальная криминалистически значимая информация, понятием которой охватываются фактические сведения, данные, находящиеся в причинно-следственной связи с событием преступления и характеризующие способ его совершения, личность правонарушителя, предметы преступного посягательства, орудия преступления и т. п. [10, с. 170].

Однако, как справедливо отмечает Р.С. Белкин, криминалистически значимой может оказаться информация любой природы [11, с. 68]. Следовательно, ценность имеют все сведения, способные стать доказательствами по уголовному делу либо в целом повлиять на его разрешение. Например, информация, аккумулируемая в системе уголовных учетов, способствует действенному решению диагностических и идентификационных задач уголовного расследования, достаточности доказательственной базы. В настоящее время, что весьма значимо, в виду ускорения развития технологий роль подобной справочной, т.е. косвенной, прямо не связанной

[2] Единого понятия информации не существует в виду сложности и многоаспектности самого явления; в соответствии с диалектико-материалистической философией ее содержанием охватывается отражение предметов и явлений в сознании человека, а также явлений и процессов в друг друге, вне связи с сознанием, что соотносится с понятием следов в криминалистике [9, с. 20].

причинно-следственной связью с конкретным деянием потенциальной криминалистически значимой информации в экспертной деятельности и уголовном судопроизводстве существенно возрастает.

Обобщая, следует заключить, что поскольку из-за значительного роста объема криминалистически значимой информации соответствующих учетов становится все больше и больше [12, с. 111] (данный процесс, думается, будет продолжаться со значительным ускорением), является логичным, что система уголовной регистрации нуждается во внедрении не просто технологий автоматизированного сбора, хранения и систематизации информации (это, как следует из далее изложенного, в настоящее время уже успешно осуществляется), но и ее ресурсоемкого эффективного анализа с целью последующей выработки значимых для следствия и суда выводов, что возможно добиться с помощью внедрения различных форм искусственного интеллекта в криминалистическую практику.

В рамках данного дискурса полагаем, что определенный интерес как для развития отраслей криминалистической техники, так и для уголовного судопроизводства представляет распространение Big Data (т.н. «больших, или сложных, данных», термин был введен в зарубежной доктрине в 2008 г. [13, с. 28-29]; далее — BD) — технологии, в основе которой находится механизм сбора и обработки значительных по объему, прямо не взаимосвязанных между собой структурированных и неструктурированных массивов информации из различных источников, подверженных постоянным обновлениям, в целях повышения качества принятия решений [14, с. 60]. Исходя из данного определения,

BD понимаются в двух, составляющих единое целое, значениях: во-первых, как совокупность различных по содержанию крупных сегментов информации, во-вторых, как технология, способная ее обработать с относительно высокой скоростью (Volume, Variety, Velocity), что в совокупности обеспечивает допустимость их использования для аналитики, моделирования и прогнозирования. Структурно BD объединяют в себе в качестве методов и инструментов обработки, в частности, интеллектуальный анализ данных (Data Mining), машинное обучение (Machine Learning), искусственные нейронные сети и иные подобные технологии, моделирующие человеческое мышление [15, с. 27-31].

В ходе функционирования BD программному анализу подвергается вся имеющаяся информация безотносительно ее выборки и качества (формата, типа), причем в рамках данного процесса доминирует поиск корреляций, а не установление причинно-следственных связей между данными [16, с. 113]. Следовательно, содержание выводов, полученных этим способом, характеризуется высокой степенью достоверности, но лишь при условии должной подборки эмпирического материала (что, как правило, компенсируется его объемом — применительно к масштабам оперируемых данных действует т.н. закон «больших чисел»: чем более значительнее и релевантнее данные, тем точнее вывод, поскольку машина непрерывно учится на их анализе), и в большинстве случаев не может быть объяснено с позиции формальной логики, что позволяет извлекать новое знание из существующей информации на принципиально ином уровне познания и выявлять многие, ранее скрытые для логического анализа, закономерности. Это предоставляет колоссальные

возможности для оптимизации различных областей жизнедеятельности: производства, коммерции, государственного управления, медицины и, безусловно, права во всех его проявлениях как формы, опосредующей общественные отношения. Иными словами, направления использования BD не являются исчерпывающими, ибо технология имеет универсальный характер.

Вышеописанные технические аспекты BD позволяют сформировать определенное понимание множественности последствий широкого внедрения технологии в бытие человека, что особенно актуально в настоящее время в виду государственного стимулирования процессов цифровизации в России[3]. Поскольку научно-технический прогресс необратим, закономерно, что BD, в силу своих особенных свойств, представляют высокий интерес для криминалистики. Однако широкое развитие BD и подобных технологий приносит как определенные возможности для ее дальнейшего развития, так и проблемы и риски концептуального характера.

Во-первых, думается, что разрабатываемый криминалистический подход к правовому регулированию технологии BD напрямую предопределяется ее структурными особенностями. Как отмечалось выше, условно BD можно разделить на два вида: структурированные и неструктурированные. Сбор первых, осуществляемый в соответствии с установленными критериями, изначально подчинен определенной цели (что отличает их от вторых). Необходимо констатировать, что подобные структурированные BD, при условии их понимания в изначальном смысле —

[3] О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы: указ Президента РФ от 09.05.2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20. Ст. 2901.

исключительно как совокупности крупных сегментов информации, систематизированных по каким-либо признакам — относительно давно используются в криминалистической деятельности, в частности, в системе автоматизированного учета АДИС «Папилон», функционирование которой осуществляется в рамках создания электронной базы данных дактилокарт и следов в целях дальнейшего ее использования для решения ряда практических задач: 1) установления личности по отпечаткам и следам пальцев и ладоней; 2) идентификации неопознанных трупов; 3) объединения по следам преступлений, совершенных одним и тем же лицом [17, с. 20].

В этой связи следует заключить, что информатизация дактилоскопии и иных отраслей криминалистической техники — относительно давняя тенденция. Первые пробные разработки автоматизированных дактилоскопических систем были инициированы в СССР еще в конце 1950-х гг. [18, с. 69], а широкая автоматизация дактилоскопических учетов в России реализована в 2002 г.: оптимизированы более 20 млн. дактилокарт Главного информационно-аналитического центра МВД РФ. В настоящее время проверка одного следа по указанной базе данных занимает несколько десятков минут, что экономит тысячи человеко-часов рабочего времени [19]. Однако представляется, что до настоящего времени развитие криминалистической регистрации осуществлялось преимущественно в векторе улучшения способов хранения и систематизации огромных массивов криминалистически значимых данных для повышения эффективности поиска в них экспертом необходимой конкретной информации. А потому полагаем, что именно внедрение BD, способных на основе

анализа баз данных самостоятельно выявлять криминалистически значимые корреляции, делать на их основе высокоточные выводы и тем самым значительно облегчить (но не подменить и исключить) работу экспертов — наиболее перспективное направление развития системы уголовных учетов.

Если применительно к структурированным BD проблем их правового регулирования видится незначительное количество (существует именно недостаток фактического характера: развитие этой группы данных зависит преимущественно от отставания внедрения достижений научно-технического прогресса в криминалистическую практику), то в отношении неструктурированных BD можно констатировать обратное. Неструктурированные BD, к которым относятся, в частности, мультимедиа (комбинированное сочетание видео, звуков, текста), передаваемые операторами сотовой и интернет-связи [20, с. 166-167], также могут быть использованы в экспертной, оперативно-розыскной и следственной деятельности, поскольку существует вероятность, что в них содержится потенциальная криминалистически значимая информация.

Сбор и обработка неструктурированных данных на первоначальном этапе осуществляются безотносительно целей и интересов правоохранительных органов. Но в случае возникновения необходимости их можно использовать для анализа поведения отдельных людей и их групп, выявления и отслеживания перемещения преступника, его действий [21, с. 105]. Биометрия, опирающаяся на технологию BD и нацеленная на распознавание и идентификацию людей по их физическим и поведенческим чертам, все более внедряется в криминалистическую деятельность [22, с. 27-31]. В целом, как

следует из анализа существующей практики, неструктурированные BD применяются различными, как частными, так и публичными субъектами в процессе профайлинга — сбора информации о физических лицах (персональных данных) в целях ее дальнейшего использования (в том числе коммерческого) [23, с. 63-65], при этом зачастую данные действия осуществляются без выяснения согласия исследуемого лица.

Необходимо констатировать, что процесс цифровизации выявил глубокий конфликт между требованиями о защите личной информации и фактической невозможностью их соблюдения в случае ее попадания в открытый доступ. Как справедливо отмечает Э.В. Талапина, происходит нарастание противоречий между частными и публичными началами в праве, открытостью и закрытостью информации, транспарентностью и тайной частной жизни [24, с. 145]. А потому закономерно, что вышеописанные способы использования BD обусловливают возникновение и обострение конфликта между интересами физических лиц и государства (а также различных организаций), использующего технологию в своей деятельности, в аспекте возможного нарушения фундаментального конституционного права конкретных индивидов на неприкосновенность частной жизни (и производного от него права на защиту персональных данных), что особенно актуально применительно к неструктурированным BD, которые нередко собираются без ведома лица и могут быть использованы в криминалистической деятельности.

Действительно, неограниченные сбор и обработка информации о личности технологией BD в сущности

противоречат ключевым принципам Федерального закона «О защите персональных данных»[4]. В частности, BD несовместимы с принципом ограничения обработки персональных данных заранее определенными целями, установленным в вышеуказанном законе (ст. 5), так как при их применении, ввиду технических свойств и самого назначения технологии, как правило, подвергается обработке вся имеющаяся у государства или организации информация о личности, в том числе собранная ранее для иных целей. А следовательно, BD также находятся в противоречии с концепцией информированного, конкретного и сознательного согласия как главного основания легитимации обработки персональных данных, поскольку ее ключевой элемент — информированность — состоит в предоставлении и понимании исчерпывающего перечня целей, для которых будет использована информация, полученная в результате действия технологии, что сложно обеспечить на практике. Наконец, обезличивание персональных данных не является гарантией их анонимности в эпоху современных технологий, ибо BD позволяют с высокой долей вероятности идентифицировать личность конкретного лица посредством установления корреляций между фрагментами данных различного характера (при этом нет необходимости знать, например, имя, дату рождения и подобную по значимости информацию) [25].

Таким образом, неконтролируемое, не ограниченное законом применение данной технологии как в общественной практике в целом, так и в криминалистической деятельности в

[4] О персональных данных: федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 31.12.2017 г.) (с изм. и доп., вст. в силу с 30.06.2018. г.) // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. I). Ст. 3451; 2018. № 1 (ч. I). Ст. 82.

частности приносит определенные угрозы для прав и свобод человека, что обусловливает необходимость опережающей разработки соответствующего нормативно-правового регулирования.

Во-вторых, что является продолжением вышеизложенного, гипотетически может являться противоправным не только сбор и обработка информации, прямо или косвенно касающейся личности (в том числе потенциальной криминалистически значимой). Вполне очевидно, что в силу технических особенностей BD на практике возможно принятие неверных и противозаконных юридически значимых решений, основанных исключительно на логически неподтвержденных выводах, полученных в результате применения технологии, или злоупотребление их использованием, что нарушает общеправовой принцип формального равенства. Поскольку профайлинг на базе выявления характерных ассоциаций в отношении конкретного лица позволяет прогнозировать его поведение, теоретически существует угроза ущемления конституционных прав, свобод и законных интересов граждан на основе высокоточных предположений об их прошлом или будущем поведении, полученных в результате использования BD. Высказывается мнение, что при наличии определенной политической воли возможно как путем профилактических правовых средств не допустить потенциально возможное противоправное деяние (что в целом является прогрессивным способом использования технологии), так и до его совершения превентивно привлечь к юридической ответственности, то есть наказать соответствующее лицо за еще несовершенное правонарушение [16, с. 118], что недопустимо с правовой точки зрения.

В деятельности государственных органов в целом позитивное использование технологии BD, понимаемой в полном собственном значении (одновременно как совокупности больших массивов данных и инструментов, способных их обработать), в настоящее время уже осуществляется. В источниках приводятся данные об использовании профайлинга в зарубежной практике (США) для предварительной оценки угрозы, которую представляет каждый отдельный человек как потенциальный правонарушитель в рамках осуществления прогностического полицейского контроля [26]. Цель отечественной Автоматизированной централизованной базы персональных данных о пассажирах и персонале (экипаже) транспортных средств [27] заключается в выявлении пассажиров, в отношении которых следует провести проверку и при необходимости не допустить к поездке для обеспечения безопасности.

Вместе с тем следует помнить, что в рамках публичных отношений, основанных на императивных началах, сфера диспозитивности, свободного усмотрения индивида значительно ограничена, что уменьшает круг возможностей последнего в случае возникновения произвола со стороны правоприменителя, а потому, на наш взгляд, процесс распространения BD и иных подобных технологий в практике эксперта и в судопроизводстве, основывающемся на его выводах, требует научно обоснованного, взвешенного подхода.

В-третьих, следует заключить, что пробы технологий искусственного интеллекта с целью сбора и обработки BD для принятия решений в рамках экспертной практики уже осуществляются и демонстрируют существенные результаты. В частности, как отмечает Д.В. Бахтеев, на кафедре

криминалистики Уральского государственного юридического университета реализуется проект, направленный на создание искусственной нейронной сети, осуществляющей предварительный анализ почеркового материала (что, думается, потенциально может быть применено к распознаванию иных объектов) в целях выявления признаков подлога подписей, выполненных без использования технических средств [21, с. 106], т. е. в данном случае следует констатировать о разработке самой возможности принятия высокоточных решений, сходных принимаемым экспертами. Разработанная модель, как отмечалось выше, основана на использовании искусственных нейронных сетей, воспроизводящих работу мозга человека, в силу чего возможен переход от линейности традиционных математических алгоритмов к адаптивности, эвристическому характеру принятых программой решений. Создание и настройка функционирования системы BD, построенной на данных исходных посылках, состоит из трех последовательных этапов:

1) сбор необходимого материала (оцифрованных экспериментальных образцов подписей и их рукописных подложных копий);

2) подбор и настройка параметров, в соответствии с которыми будет осуществляться сравнение объектов при обучении сети (в качестве которых выступают отдельные общие и частные признаки почерка, соотношение углов наклонов штрихов, их протяженность по горизонтали и вертикали и др., при отклонении от установленных нормально возможных величин подпись считается подложной);

3) обучение сети и проверка ее работоспособности (предъявляется пара образцов подписей, одна из которых

всегда подлинная, другая — подлинная либо ложная, при этом системе заранее известно качество подписи, данная операция повторяется несколько сотен тысяч раз).

В итоге система выучивает и опознает вариационные особенности подписей, выполненных одним человеком, и отличия, проявляющиеся между оригинальными и подложными подписями. На заключительном этапе проверка функционирования сети осуществляется путем предъявления ей двух образцов подписи, один из которых подлинный, а подлинность второго неизвестна, что приближает ее работу к реальным условиям и соответствует потребностям практики [21, с. 106]. Тем самым с высокой точностью выявляются соответствующие признаки, разграничивающие подлинные и поддельные подписи, а также характеризующие лицо, выполнившее их, — при условии, что исходные параметры были выбраны верно.

Думается, подобные инструменты в перспективе могут быть использованы в криминалистическом исследовании документов в целом (не только в почерковедении, но и, например, в автороведческой экспертизе [28]), в криминалистической регистрации (на основе программного анализа структурированных баз данных можно делать криминалистически значимые выводы), в габитоскопии, трасологии и иных отраслях криминалистической техники, поскольку в данном случае также возникает необходимость с помощью построения математических моделей установить имплицитные закономерности и корреляции, наиболее эффективно выявить и исследовать которые способны именно BD, функционирование которых основано на применении компьютерного зрения и искусственных нейронных сетей,

опосредующих процесс распознавания и последующего анализа образов из доступного и, как правило, неструктурированного эмпирического криминалистического материала.

Таким образом, следует констатировать, что внедрение технологии BD в криминалистическую деятельность имеет колоссальные перспективы для развития, поскольку гипотетически позволит повысить релевантность приобретаемой и обрабатываемой криминалистически значимой информации, а следовательно, существенно увеличит шансы на выявление, раскрытие, расследование и предупреждение преступления.

Представляется, что необходимо продолжить разработку соответствующей нормативно-правовой базы, регулирующей отношения, складывающиеся в сфере использования BD, причем приоритетным направлением правовой политики должно являться именно устранение ряда проблем и рисков, обозначенных выше. На наш взгляд, следует законодательно зафиксировать общий запрет на принятие решений субъектами правоприменения, порождающих юридические последствия для граждан, которые основаны исключительно на автоматизированной обработке данных, поскольку даже высокоразвитая модель, воспроизводящая человеческое мышление, способна с незначительной вероятностью совершить ошибку. В этой связи считаем справедливым согласиться с позицией, высказанной в правовой доктрине, что в ряде ситуаций, которые могут возникнуть на практике, возможно, необходимо будет ввести требование обязательного установления причинно-следственных связей, не выявленных

при программном анализе, и доказывания сделанных выводов с помощью логического обоснования [16, с. 121].

Перечисленное, однако, явно не может служить исчерпывающим решением всех проблем правового регулирования BD, что требует дальнейшего научного поиска в векторе нахождения баланса между решением, принимаемым в полностью автоматическом режиме, и решением, принимаемым человеком. Безусловно, в обозримом будущем анализируемая технология не может и не должна заменить субъекта правоприменения, полностью определять его юридически значимые решения. Ее предназначение — служить особым инструментом эксперта, способным самостоятельно генерировать криминалистически значимые выводы, что позволит ему, с учетом иных имеющихся данных, существенно облегчить принятие итогового решения. А потому при позитивном развитии BD можно говорить об оптимизации скорости и качества работы эксперта, и в конечном счете — об уменьшении негативного влияния человеческого фактора в криминалистической практике за счет передачи части преимущественно «механических» функций эксперта информационной системе, что уже к настоящему времени, как следует из вышеизложенного, имеет несколько конкретных форм выражения.

Библиографический список

1. Forensic science // Encyclopedia Britannica. URL: https://www.britannica.com/science/forensic-science#ref1246174 (дата обращения: 08.01.2020 г.).

2. Булкина Н.В., Пацкевич А.П. История возникновения и развития криминалистической фотографии. Вестник Полоцкого государственного университета. Серия D: Экономические и юридические науки. 2006. № 8. С 231–234.
3. Авраменко О.И. История развития дактилоскопии как метода идентификации личности и ее современное состояние в России // Концепт. 2019. № 11. С. 138–144.
4. Бахтеев Д.В. О сущности и перспективах использования искусственных нейронных сетей в раскрытии и расследовании преступлений. Вопросы российской юстиции. 2016. № 3 (3). С. 4–6.
5. Бахтеев Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: Образование. Практика. Наука. 2018. № 2 (104). С. 43–49.
6. Трегубов С.Н. Основы уголовной техники, научно-технические приемы расследования преступлений. – М.: ЛексЭст, 2002. – 336 с.
7. Челышева О.В. Криминалистика: учебник. 2017. URL: http://be5.biz/pravo/k043/9.html (дата обращения: 12.01.2020 г.).
8. Криминалистика: учебник / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Российская; под ред. Р.С. Белкина. – М.: Норма, 2001. – 990 с.
9. Трусов А.И. Судебное доказывание в свете идей кибернетики // Вопросы кибернетики и права. – М.: Наука, 1967. – С. 20–35.
10. Криминалистика: учебник / под ред. А. Г. Филиппова, А. Ф. Волынского. – М.: Спарк, 1998. – 543 с.
11. Белкин Р.С. Криминалистическая энциклопедия. – М.: Мегатрон XXI, 2000. – 333 с.

12. Койсин А.А. История становления и развития уголовной (криминалистической) регистрации // Сибирский юридический вестник. 2018. № 2. С. 104–115.
13. Lynch C. Big data: How do your data grow? // Nature. 2008. Vol. 455. №. 7209. pp. 28–29.
14. Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный). – М.: Статут, 2015. – 320 с.
15. Big data: The next frontier for innovation, competition, and productivity / Manyika J., Chui M., Brown B. et al. – McKinsey Global Institute, 2011. – 146 p.
16. Чаннов С.Е. Большие данные в государственном управлении: возможности и угрозы // Журнал российского права. 2018. № 10 (262). С. 111–122.
17. Зайцев П.А. Практические вопросы выбора эффективной автоматизированной дактилоскопической идентификационной системы (АДИС) // Эксперт-криминалист. 2008. Вып. 2. С. 20–22.
18. Репин А.В., Лобойко Ю.Д., Зырянов В.В. Современное состояние и проблемы использования АДИС «Папилон» в деятельности Управления ФСКН России по Красноярскому краю // Вестник Сибирского юридического института МВД России. 2012. № 2 (11). С. 68–71.
19. Автоматизация дактилоскопических учётов // Википедия. URL: https://ru.wikipedia.org/wiki/Автоматизация_дактилоскопических_учётов#cite_note-6 (дата обращения: 19.01.2020 г.).
20. Мещеряков В.А., Хорунжий С.Н. Влияние концепции «Больших данных» на криминалистическую теорию

причинности // Причинность в криминалистике: сб. науч.-практ. статей / под общ. ред. И.М. Комарова. – М.: Юрлитинформ, 2018. – С. 164–168.

21. Бахтеев Д.В. Большие данные и искусственный интеллект в следственной и экспертной деятельности // Актуальные проблемы криминалистики и судебной экспертизы: материалы Международной научно-практической конференции. – Иркутск: Восточно-Сибирский институт МВД России, 2019. – С. 104–107.
22. Барковская Е.Г. Криминалистика и биометрия: проблемы интеграции научного знания // Философия права. 2011. № 3 (46). С. 27–31.
23. Ларионова В.А. Информационный брокер как новый субъект информационного права в эпоху Big Data // Право в сфере Интернета: Сборник статей / отв. ред. М.А. Рожкова. – М.: Статут, 2018. – С. 62–103.
24. Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в Европейском контексте // Труды Института государства и права РАН. 2018. № 5. С. 117–150.
25. Santos J. The Myth of Anonymization: Has Big Data Killed Anonymity? URL: https://docplayer.net/14450176-The-myth-of-anonymization-has-big-data-killed-anonymity-white-paper-by-jessica-santos-ph-d-march-2015.html (дата обращения: 25.01.2020 г.).
26. Thompson T. Crime Software May Help Police Predict Violent Offences // The Guardian. 2010. July 25. URL: http://www.theguardian.com/uk/2010/jul/25/police-software-crime-prediction (дата обращения: 11.02.2020 г.).

27. База персональных данных о пассажирах и экипаже автобусов (АЦБПДП) // Северное межрегиональное управление государственного автодорожного надзора Федеральной службы по надзору в сфере транспорта. URL: https://smugadn.tu.rostransnadzor.ru/poleznaya-informacziya/baza-personal-nyx-dannyx-o-passazhi (дата обращения: 15.01.2020 г.).
28. Шаталов А.А. Модели и методы выявления закономерностей в информационном потоке на примере рукописного текста с целью установления его авторства: дис … канд. техн. наук. – Тамбов, 2015. – 170 с.