Список литературы

1. Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Официальный Интернет-портал правовой информации. URL: http: //www.pravo.gov.ru (дата обращения: 01.09.2022).

2. Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»» // Российская газета (федеральный выпуск). 28.04.2020.

3. Казарян Э. А. Соотношение понятий «свобода» и «права человека» // Молодой ученый. 2019. № 21. С. 337–339.

4. Курбалийя Й. Управление Интернетом / DiploFoundation, АНО «Координационный центр национального домена сети Интернет». М.: б. и., 2018. С. 198.

5. Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 96.

6. Черемисинова М. Е. Реализация законных интересов в сети Интернет // Журнал российского права. 2018. № 9 (261). С. 120.

7. Luhmann N. The Autopoiesis of social systems // Luhmann N. Essays on self-reference. New York: Columbia University Press, 1990.

Э. И. Лескина,
кандидат юридических наук, доцент кафедры информационного права
и цифровых технологий,
Саратовская государственная юридическая академия

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ BIG DATA В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Аннотация. Всеобщая цифровизация, развитие информационного общества, активное применение информационных технологий публичным и частным сектором предоставляет новые возможности правоохранительным органам. Многие преступления имеют цифровые следы, по которым противоправные деяния можно предотвратить или раскрыть. В данной статье рассматриваются возможности внедрения технологии Big Data для предотвращения и раскрытия преступлений, зарубежный опыт в этой области, направления применения аналитики больших данных для указанных целей, а также проблемы, которые могут в связи с этим возникнуть и возможные пути их решения.

Ключевые слова: большие данные (Big Data), терроризм, профилактика, профилирование, аналитика данных, преступность, цифровизация, информационное общество, информационное право

APPLICATION OF BIG DATA TECHNOLOGY IN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Abstract. General digitalization, the development of the information society, the active use of information technologies by the public and private sectors provide new opportunities for law enforcement agencies. Many crimes have digital traces by which illegal acts can be prevented or revealed. This article discusses the possibilities of introducing Big Data technology to prevent and solve crimes, foreign experience in this area, the directions for using big data analytics for these purposes, as well as the problems that may arise in connection with this and possible ways to solve them.

Keywords: Big Data, Terrorism, Prevention, Profiling, Data analytics, Crime, Digitalization, Information society, Information law

Большие данные представляют собой структурированную и неструктурированную, содержащуюся в большом количестве разнообразных источников информацию, объемы которой не позволяют обрабатывать ее вручную в разумное время [5].

Перспективы больших данных заключаются в том, что с помощью расширенного анализа можно найти дополнительную ценность в максимальном использовании существующих и/или новых массивов, казалось бы, не связанных между собой данных. Алгоритмы будут собирать скрытые под массой других данных части целого, чтобы раскрыть истинную природу объекта.

Технологии больших данных используются правоохранительными органами в различных целях при решении повседневных задач своей деятельности.

В зарубежных странах правоохранительные органы применяют большие данные для идентификации лиц, транспортных средств, отслеживания финансовых потоков [6. С. 15], прогнозирования совершения преступлений, выработки рекомендаций по мерам пресечения и условиям условно-досрочного освобождения [1. С. 19–21], выдвижения и проверки следственных версий [2. С. 3–8]. В Китае функционирует система отслеживания каждого гражданина с установлением рейтинга доверия на основе анализа 160 000 данных [7. С. 762]. А в США с 2017 г. действует платформа, которая на основе анализа больших данных рекомендует правоохранительным органам определенные действия в зависимости от анализируемой платформой ситуаций (например, когда зафиксировано, что взрослый ведет сопротивляющегося ребенка) [3. С. 112–113]. Государства (Бразилия, Великобритания) используются большие данные для мониторинга и борьбы с преступностью (даже практикуется прогнозирования места совершения преступлений, выявление налоговых преступлений, мошенничества) [9]. Правоохранительные органы используют инструменты, обеспечивающие расширенную аналитику больших данных (например, IBM Security Intelligence и Palantir), систему так называемой разведки из открытых источников (OSINT [8]) производятся прогнозы преступного поведения, адаптивных реакций на контрмеры, добываются сведения о личности преступников, их поведенческих моделях. С помощью больших данных возможно более глубокое понимание произошедших кибератак, производство непрерывного анализа рисков безопасности. Большие данные сегодня постепенно становятся од-

ним из ключевых моментов в раскрытии преступлений, совершаемых с помощью информационно-телекоммуникационных сетей.

Свои особенности имеет использование больших данных для предотвращения и раскрытия преступлений террористического характера.

Что касается использования технологии больших данных в целях противодействия терроризму, то стоит отметить, что еще до развития технологий Big Data правоохранительные органы собирали, использовали и производили данные, использовали их для предотвращения преступления террористического характера. Террористические атаки сопровождают цифровые следы, исследуя которые возможно оптимизировать деятельность правоохранительных органов. В настоящее время мы можем наблюдать совсем иной объем данных, аккумулируемый посредством распространения Интернета, умных устройств, социальных сетей и т. д. Кроме того, указанные объекты используются террористическими группами для пропаганды, планирования преступных действий, вербовки и т. д.

Правоохранительные органы посредством больших данных могут выявлять террористические сети, например, в интернет-сообществах, информацию о планировании атак, а также признаки вербовки, радикализации сообществ. В результате становится возможным остановить террористическое, экстремистской развитие в информационном пространстве. Указанные возможности показывают новые направления в борьбе с терроризмом.

Здесь следует отметить, что в сфере национальной безопасности аналитика больших данных нацелена, по большей части, на профилактику, предотвращение (например, предотвращение на этапе подготовки, с помощью анализа коммуникаций, после покупки опасных материалов, путем выявления лиц, подверженных риску).

Возможности больших данных для предотвращения терроризма возможно использовать для:

1) прогнозирования места и времени совершения преступления террористической направленности;

2) прогнозирования рисков совершения преступлений террористической направленности конкретным лицом. Ввиду прогнозов больших данных возникает этические проблемы в желании изолировать людей, которые в соответствии с данными аналитики склонны к совершению преступлений, подвергать их проверкам для предотвращения преступления. Допустим, выявлен несовершеннолетний, который по результатам профилирования с большой вероятностью совершит преступление террористического характера. Его в целях профилактики может посещать социальный педагог, психолог, чтобы оказать помощь. Однако указанное вмешательство можно расценивать как наказание за действия, которые не были совершены;

3) выявление совершающихся преступлений террористического характера в медиапространстве. Важным направлением использования больших данных является то, что с их помощью возможно выявить тех, кто может оказаться террористом на основе аналитики массовых публикаций, комментариев, реакций в социальных сетях или поисковых запросов в Интернете. С помощью Big Data возможно отслеживать связи между людьми и отслеживать интересующих людей посредством цифровых следов.

Выявим основные направления аналитики Big Data для предотвращения терроризма.

Первое направление аналитики состоит в том, чтобы выявить образцы-данные террористической деятельности, подготовки к ней, выявить ту информацию, которая свидетельствовала бы о подготовке к преступлениям террористического характера. Сложность здесь заключается в недостатке информации различного рода, например, знаний биографий террористов, уверенность в источниках данных, которые уже отфильтрованы в качестве свидетельствующих о терроризме, различия в том, что составляет терроризм исходя из различных источников. Таким образом, прогностическая модель на основе больших данных о прошлой террористической деятельности, не является эффективной.

Второе направление аналитики Big Data в аспекте предотвращения террористической деятельности состоит в том, чтобы результаты аналитики обращали внимание на поведение, в котором потенциально прослеживается террористическая направленность.

Здесь отрицательным моментом будут алгоритмы профилирования с указанием чрезвычайно широких социально-демографических критериев, таких как возрастная группа, пол, образование или социально-экономический статус. Другими словами, чтобы поймать значительную часть террористов, мы должны также ложно идентифицировать десятки тысяч граждан.

Посредством кластеризации также может быть определено аномальное поведение. Один из подходов состоит в том, чтобы начать с метода кластеризации, сначала сортируя базовые аспекты для различных типов поведения. Нейронные сети особенно хорошо умеют автоматически формировать и проверять гипотезы о закономерностях с помощью машинного обучения. Это исключает из цикла множество субъективных, культурных и просто ошибочных предположений, теорий и классификаций. Однако как террористические, так и нетеррористические виды поведения чрезвычайно разнообразны, а это означает, что нет способа определить степень пересечения между «ненормальным» и «террористическим» множествами.

Выходом может быть следующая аналитическая стратегия. Если анализ больших данных направлен на поиск сетей или связей между людьми, он быстро сталкивается с проблемой определения. Когда отправитель, получатель, время, продолжительность разговоров и частота сообщений вводятся в алгоритм, можно использовать различные типы статистических методов сетевого анализа, которые в сочетании с теорией социальной психологии могут выявить роль отдельных лиц в группе в пределах разумной погрешности. Правильный способ начать процесс с использованием «больших данных» – получить доступ к большим объемам массовых коммуникаций и попытаться идентифицировать «темные сети», которые имеют общие характеристики, не разделяемые большинством пользователей телекоммуникационных услуг (в основном, время разговора, продолжительность и локализация, тенденция к низкой плотности связей, меньшему количеству контактов между членами). Проблема этой аналитической стратегии состоит в том, что нет общего определения и входных данных в отношении законности так называемых темных сетей. Это могут быть политические диссиденты, но не террористы.

Сам процесс аналитики при применении больших данных для предотвращения терроризма начинается с анализа малых данных, с аналитики данных конкретного человека, признанного террористом. Надежность, достоверность таких малых данных является важным фундаментом для всей системы на основе Big Data. Посредством малых данных впоследствии сужается группа населения, которой следует уделять дополнительное внимание со стороны правоохранительных органов. При наличии достаточного количества данных, случайность корреляции переменных быстро увеличивается; корреляции фактически становятся многочисленными.

Негативным моментом формирования больших данных является то, что источники данных находятся под сильным влиянием культуры, политической ориентации на отдельные группы населения. Независимо от того, поступают ли исходные данные от правоохранительных органов, средств массовой информации или социальных сетей, арабское, мусульманское население будут непропорционально включены в любую базу данных, что, в свою очередь, дискриминационно смещает модели в сторону одних и тех же групп населения.

Отчеты правоохранительных органов содержат большую часть информации, включенной в базы больших данных, особенно это касается конфиденциальных баз данных, используемых организациями национальной безопасности. Это создает цикл обратной связи, в котором данные добываются теми, кто их создает, результаты включаются в базу данных, а затем повторно анализируются.

Помимо проблем, связанных с неправильной идентификацией людей, можно было бы включить аспекты, которые выражаются в массовом наблюдении. Исследования показали, что наблюдение изменяет способ нашего самовыражения, даже если мы убеждены, что нам «нечего скрывать» [11]. Другими словами, наблюдение, даже без последующего вмешательства, в значительной мере влияет на наше чувство автономии от государственного аппарата, например, на способность и, по сути, желание говорить свободно.

Аналитика больших данных основана на алгоритмах: это роботизированное наблюдение. Эта форма машинного наблюдения часто представлялась как свободная от потенциального злоупотребления или другого незаконного использования возможностей наблюдения людьми. Это может нейтрализовать любую изначальную предвзятость, заложенную на этапе программирования, такую как этническое профилирование, если она не соответствует данным. Однако, большинство баз данных, связанных с терроризмом, с самого начала имеют фундаментальную предвзятость. В той степени, в которой роботы «учатся» на этих данных, они могут экспоненциально усилить эффект изначальной предвзятости.

Защита при мониторинге, конфиденциальность при машинном наблюдении являются основным аспектом в области обеспечения безопасности при применении больших данных в области противодействия терроризму.

В целом, возможные сложности, которые могут возникнуть у правоохранительных органов при внедрении технологий Big Data в целях противодействия терроризму заключаются в следующих аспектах:

1) технологическая оснащенность. Эта проблема может выражается в отсутствии необходимых хранилищ. Разнообразие цифровых следов, возникающих

в связи с террористическими атаками, усложняет алгоритмы и машинное обучение в целом;

2) недостаток кадров со специальными навыками в области ИТ. Прежде всего, это касается навыков и умений самих сотрудников правоохранительных органов. Необходимо изменение мышления должностных лиц, не готовых активно внедрять инновации в свою деятельность, а также наличие образовательных программ, в том числе дополнительных образовательных программ в области аналитики данных;

3) доступности самих данных как с организационной, так и с правовой точки зрения. Анализируемые данные могут быть персональными, подпадать под юрисдикцию других государств, могут присутствовать и иные проблемы;

4) специфики данных, аккумулируемых для деятельности по борьбе с терроризмом. Такие данные, в отличие от данных, необходимых для профилактики иных преступлений, обладают гораздо большим разнообразием. Поэтому если для профилактики иных преступлений бывает достаточно именно большого объема, в случаях с преступлениями террористической направленности аналитика зачастую не может предоставить конкретный результат. Уникальность данных террористических атак приводит к неточности алгоритмов.

Ученые вследствие уникальности данных говорят о следующей триаде: проклятие размерности, дисбаланс классов и ложность корреляций [10].

«Проклятие соразмерности» заключается в том, что для обучения необходимо многообразие данных, полученных из террористических атак, но чем более разнообразны и массивны наборы данных, тем менее точны полученные в результате аналитики результаты. То есть для алгоритмов необходимо объединить большие наборы данных различного характера, в частности цифровые следы террористов в области подготовки, вербовки, необходимо использование различных побуждений (религиозных, психологических, политических и т. д.). Такое большое количество признаков увеличивает размерность наборов, и алгоритмы машинного обучения будут находить взаимосвязь между такими данными. Но такое увеличение размерности требует все более обширные наборы данных, все больше цифровых следов террористических атак, тогда как количество подтвержденных атак не так велико.

Дисбаланс классов заключается в неоднородности, разнообразии входных данных, на основании которых происходит обучение. Машинное обучение должно исходить из равных долей правомерного и «террористического» поведения. Но «террористических» данных не так много, а уменьшая «нетеррористические данные», больших объемов не достичь. Многообразие признаков террористических атак и здесь приводит к изменчивости следов, различию подмножеств, т. е. дисбалансу классов. Поэтому наборы данных с такой спецификой трудно сбалансировать, страдает точность алгоритмов.

Что касается ложности корреляций, то это вытекает из многомерности данных, аккумулируемых для сферы национальной безопасности. В результате формируются корреляции, не обладающие причинно-следственной связью, но засоряющие алгоритм, вызывая его «переоснащение». Например, это может быть корреляция между вероятностью того, совершит ли человек террористический акт, и цветом его волос или размером одежды.

Многие из выше указанных проблем носят технологический характер. Их решение видится в содействии развития разработке информационных технологий в государстве, стимулировании лиц обучаться в сфере ИТ, создавать новые продукты и совершенствовать имеющиеся. Это могут быть как экономические, социальные (примером могут быть льготы и гарантии, содержащиеся в Указе Президента РФ от 02.03.2022 № 83 [4]), а также образовательные. Можно увеличить количество бюджетных мест в каждом регионе для получения высшего образования в области ИТ, кроме того, бесплатного второго высшего образования в сфере ИТ с обязанностью в таком случае определенный срок работать в пределах Российской Федерации.

Итак, правоохранительные органы активно используют общедоступную информацию, открытые данные, информацию из социальных сетей, интернет-сообществ и т. д., в том числе для предотвращения терроризма. Применение технологий Big Data в настоящее время сопровождается многими проблемами правового, социально-экономического, кадрового, технологического характера. Однако решение указанных проблем позволит государствам противостоять угрозам терроризма.

Список литературы

1. Барчуков В. К. Использование искусственного интеллекта в деятельности правоохранительных органов зарубежных стран // Международное публичное и частное право. 2020. № 5. С. 19–21.

2. Гаврилин Ю. В. Технологии обработки больших объемов данных в решении задач криминалистического обеспечения правоохранительной деятельности // Российский следователь. 2019. № 7. С. 3–8.

3. Ларина Е. С., Овчинский В. С. Искусственный интеллект. Большие данные. Преступность. Москва: Книжный мир, 2018. С. 112–113.

4. О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации: Указ Президента РФ от 02.03.2022 № 83. URL: http://publication.pravo.gov.ru/Document/View/0001202203020001 (дата обращения: 01.07.2022).

5. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203. URL: http://publication.pravo.gov.ru/Document/View/0001201705100002 (дата обращения: 01.07.2022).

6. Обзор отдельных вопросов в области больших данных и искусственного интеллекта. Вып. III. Москва: ГИАЦ МВД России, 2020. С. 15.

7. Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 753–766.

8. Akhgar B., Bayerl S., Saathoff G. Application of Big Data for National Security, A Practitioner's Guide to Emerging Technologies. London: Elsevier, 2015. URL: http://store.elsevier.com/Application-of-Big-Data-for-National-Security/Babak-Akhgar/isbn-9780128019672/ (дата обращения: 03.04.2022).

9. Jani K., Soni A. Promise and Perils of Big Data Science for Intelligence Community. 2018. URL: https://www.researchgate.net/publication/323849529_

Promise_and_Perils_of_Big_Data_Science_for_Intelligence_Community/citation/download (дата обращения: 03.04.2022).

10. L'Heureux A., Grolinger K., Elyamany H. F., Capretz M. A. M. Machine learning with big data: Challenges and approaches // IEEE Access. 2017. Vol. 5. Pp. 7776–7797. URL: https://doi.org/10.1109/ACCESS.2017.2696365 (дата обращения: 03.04.2022).

11. Penney, Jonathon. Chilling Effects: Online Surveillance and Wikipedia Use // Berkeley Technology Law Journal. 2016. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645. (дата обращения: 03.04.2022).

А. С. Лолаева,
кандидат юридических наук, доцент,
Горский государственный аграрный университет

ЭЛЕКТРОННАЯ ДЕМОКРАТИЯ КАК БАЗОВЫЙ ЭЛЕМЕНТ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Аннотация. Целью проведенного исследования является определение электронной демократии как базового инструмента информационного общества. Информационное общество рассматривается в качестве постиндустриального общества, где информация становится системообразующим звеном в механизме правового регулирования общественных отношений. Электронная демократия как составная часть информационного общества на данный момент представляется наименее разработанной. Автором подчеркнуто, что процесс информатизации демократии является серьезным испытанием для современного общества. Сделан вывод о том, что для России использование информационных технологий имеет лучшие перспективы не для перехода к прямой демократии, как это предлагается на Западе, а для дальнейшего расширения возможностей существующей системы представительной демократии и развития процессов ее демократизации. Использование интернет-технологий имеет значение для достижения следующих целей: расширение доступа избирателей и СМИ к законотворческой деятельности; повышение эффективности обратных связей между избирателями и их представителями в законодательных органах власти.

Ключевые слова: цифровые технологии, электронная демократия, непосредственная демократия, представительная демократия, информационное общество, информатизация, цифровизация, интернет-технологии

ELECTRONIC DEMOCRACY AS A BASIC ELEMENT OF THE INFORMATION SOCIETY

Abstract. The purpose of this study is to define electronic democracy as a basic tool of information society. The information society is considered as a post-industrial society, where information becomes a systemic link in the mechanism of legal regulation of social relations. Electronic democracy as a component of the information society is currently the least developed. The author emphasizes that the process of informatization of democracy