ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

УДК 342:343:347.96(73) **DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.1.1092-1109**

К. СЛОБОГИН[1]

[1] *Университет Вандербильта, США*

ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ, БАЗЫ ДАННЫХ И НАБЛЮДЕНИЕ*

Кристофер Слобогин, профессор, Школа права, Университет Вандербильта
Адрес: 131 21st Ave. South, Нэшвилл, TN 372031181, США
E-mail: christopher.slobogin@vanderbilt.edu

Цель: разработка правовых рекомендаций по доступу правоохранительных органов к базам данным.
Методы: диалектический подход к познанию социальных явлений, позволяющий проанализировать их в историческом развитии и функционировании в контексте совокупности объективных и субъективных факторов, который определил выбор следующих методов исследования: формально-юридический, сравнительно-правовой и др.
Результаты: базы данных содержат большие объемы персональной информации, которая может быть полезной в работе правоохранительных органов. Доступ государственных организаций к таким базам данных может осуществляться по пяти основаниям: «по подозреваемому», «по профилю», «по событию», «по программе» и «по инициативе». Согласно рекомендации автора работы, в дополнение к ограничениям в силу Четвертой поправки (которые в настоящее время минимальны), каждый вид доступа должен иметь собственный режим регулирования. Так, доступ «по подозреваемому» должен иметь обоснование, пропорциональное степени глубины доступа. При доступе «по профилю» также должен соблюдаться принцип пропорциональности в отношении степени прозрачности, контроля и общих ограничений. Доступ «по событию» должен ограничиваться временем и местом события. Доступ «по программе» должен регулироваться соответствующими актами, не противоречащими действующему законодательству. Информация, собираемая по инициативе различных организаций, не должна быть доступна, если только она не является необходимой для предотвращения серьезного правонарушения.
Научная новизна: в работе предложены следующие рекомендации по доступу правоохранительных органов к базам данных: а) если отделение полиции ищет непубличную информацию о конкретном человеке, оно должно предъявить подозрения в совершении им преступного деяния, пропорциональные глубине вторжения в личные данные; б) если правоохранительные органы получают доступ к информации с целью создания профиля для поиска подозреваемых, они должны убедиться, что профиль имеет необходимый коэффициент попадания на основе принципа пропорциональности, что он не содержит противоправной дискриминации и использует понятный алгоритм; в) если отделение полиции отталкивается в своем расследовании не от подозреваемого или профиля, а от самого преступления, то такое преступление должно относиться к категории тяжких преступлений, а круг лиц, по которым запрашивается информация, должен быть минимальным и соответствовать времени и месту преступления; г) сбор данных, необходимых для целей правоохранительной деятельности, должен осуществляться негосударственными организациями в пределах, соответствующих основным целям сбора информации; независимо от места сбора и хранения информации, эти процессы должны регулироваться особым законодательством и административными нормами, выработанными открыто и демократическим путем.
Практическая значимость: основные положения и выводы статьи могут быть использованы в научной и педагогической деятельности при рассмотрении вопросов, связанных с теоретическими и прикладными проблемами, связанными с выявлением, пресечением и предупреждением правонарушений.

---

* Данная статья является сокращенной версией статьи, впервые опубликованной на английском языке в журнале Criminology, Criminal Justice, Law & Society and The Western Society of Criminology Hosting by Scholastica. По вопросам коммерческого использования обратитесь в редакцию журнала Criminology, Criminal Justice, Law & Society (CCJLS) и The Western Society of Criminology: CCJLS@WesternCriminology.org

Цитирование оригинала статьи на английском: Slobogin C. Policing, databases, and surveillance // Criminology, Criminal Justice, Law & Society. 2017. Vol. 18. Is. 3. Pp. 70–84.

Адаптировано журналом Criminology, Criminal Justice, Law & Society из: Slobogin C. Policing, databases, and surveillance. In E. Luna (Ed.), Reforming criminal justice: A report of the Academy for Justice on bridging the gap between scholarship and reform. 2017. Vol. 2. Pp. 209–232. Phoenix, AZ: Academy for Justice.

Доступно на сайте: https://scholasticahq.com/criminology-criminal-iustice-law-society/

URL публикации: https://ccjls.scholasticahq.com/article/2724-policing-databases-and-surveillance

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Ключевые слова: государственный контроль; базы данных; наблюдение; Четвертая поправка; доктрина третьей стороны; реформа уголовной политики

Благодарности: Более ранняя версия статьи была опубликована в сборнике National Constitution Center's White Paper Series под названием «Деятельность полиции и облачная информация» ("Policing and the Cloud") и доступна по ссылке https://constitutioncenter.org/digital-privacy/policing-and-the-cloud. Автор поблагодарит Stephen Henderson, Wayne Logan, Scott Sunday и Robert Weisberg за комментарии к предыдущей версии статьи.

Как цитировать русскоязычную версию статьи: Слобогин К. Государственный контроль, базы данных и наблюдение // Актуальные проблемы экономики и права. 2019. Т. 13, № 1. С. 1092–1109. DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.1.1092-1109

C. SLOBOGIN[1]

[1] *Vanderbilt University, USA*

POLICING, DATABASES, AND SURVEILLANCE*

Christopher Slobogin, professor, Vanderbilt University Law School
Address: 131 21st Ave. South, Nashville, TN 37203-1181, USA
E-mail: christopher.slobogin@vanderbilt.edu

Objective: to elaborate legal recommendations concerning the access of law enforcement bodies to data bases.
Methods: dialectical approach to cognition of social phenomena, allowing to analyze them in historical development and functioning in the context of the totality of objective and subjective factors, predetermined the following research methods: formal-logical, comparative-legal, and others.
Results: Databases are full of personal information that law enforcement might find useful. Government access to these databases can be divided into five categories: suspect-driven; profile-driven; event-driven; program-driven and volunteer-driven. This chapter recommends that, in addition to any restrictions imposed by the Fourth Amendment (which currently are minimal), each type of access should be subject to its own regulatory regime. Suspect-driven access should depend on justification proportionate to the intrusion. Profile-driven access should likewise abide by a proportionality principle but should also be subject to transparency, vetting, and universality restrictions. Event-driven access should be cabined by the time and place of the event. Program-driven access should be authorized by legislation and by regulations publicly arrived-at and evenly applied. Information maintained by institutional fiduciaries should not be volunteered unless necessary to forestall an ongoing or imminent serious wrong.
Scientific novelty: the article suggests the following recommendations on the access of law enforcement bodies to data bases: a) if a policing agency seeks non-public records about an identified person, it should have to demonstrate suspicion of wrongdoing proportionate to the intrusion involved; b) if a law enforcement agency is accessing data for the purpose of executing a profile to identify suspects, it should ensure the profile produces the requisite proportionality - derived hit rate, avoids illegitimate discrimination, and uses an understandable algorithm; c) if policing agencies are relying on a crime rather than a suspect or a profile as the starting point of the investigation, the crime should be serious and the number of people investigated kept to the minimum dictated by the time and place of the crime; d) collections of data needed by law enforcement should be maintained outside of government to the extent consistent with governing needs, but wherever maintained they should be authorized by specific legislation and administrative rules transparently and democratically arrived at.

---

* Adapted version is first published in the English language by Criminology, Criminal Justice, Law & Society (CCJLS) and The Western Society of Criminology Hosting by Scholastica. For more information, please contact: CJLS@WesternCriminology.org

For original publication: Slobogin C. Policing, databases, and surveillance // Criminology, Criminal Justice, Law & Society. 2017. Vol. 18. Is. 3. Pp. 70–84.

Adapted from: Slobogin C. Policing, databases, and surveillance. In E. Luna (Ed.), Reforming criminal justice: A report of the Academy for Justice on bridging the gap between scholarship and reform. 2017. Vol. 2. Pp. 209–232. Phoenix, AZ: Academy for Justice.

Available at: https://scholasticahq.com/criminology-criminal-iustice-law-society/

Publication URL: https://ccjls.scholasticahq.com/article/2724-policing-databases-and-surveillance

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Practical significance: the main provisions and conclusions of the article can be used in scientific and educational activities while consideration the issues related to identification, suppression and prevention of crimes.

Keywords: Policing; Databases; Surveillance; Fourth Amendment; Third-party doctrine; Criminal justice policy reform

Acknowledgements: An earlier version of this paper was published in the National Constitution Center's White Paper Series, as "Policing and the Cloud," available at https://constitutioncenter.org/digital-privacy/policingand-the-cloud. The author would like to thank Stephen Henderson, Wayne Logan, Scott Sunday, and Robert Weisberg for their comments on earlier versions of this paper.

For citation of Russian version: Slobogin C. Policing, databases, and surveillance, *Actual Problems of Economics and Law*, 2019, vol. 13, No. 1, pp. 1092–1109. DOI: http://dx.doi.org/10.21202/1993-047X.13.2019.1.1092-1109.

В настоящее время широко известно, что практически все наши действия заносятся в базы данных, часть которых находится в руках государства, а другие – в руках частных компаний. Эти базы данных – в данной статье мы для удобства называем их «Облако» – находятся на серверах Google, Netflix и Apple; в памяти телефонов, камер видеонаблюдения, смарт-автомобилей, спутников; в компьютерах государственных и коммерческих организаций. Они отслеживают широчайший спектр повседневных действий, включая использование интернета, средств коммуникации, банковские транзакции, маршруты поездок, информацию о налогах, о медицинском обслуживании, биометрические данные, а также более прозаические вещи, такие как места работы и проживания, пользование коммунальными услугами и поломки автомобиля. В данной статье мы рассмотрим вопрос, в каких ситуациях государство должно иметь доступ к этому огромному объему персональной информации в целях обеспечения правопорядка и национальной безопасности.

В Соединенных Штатах, чтобы ответить на этот вопрос, нужно изучить целый ворох законов и еще несколько решений Верховного суда. Например, если государственный орган желает получить доступ к информации, находящейся в компьютере, то по федеральным законам и законам штатов обычно требуется ордер, который выдает судья, обнаруживший вероятную причину [«вероятная причина» – юридический термин в законодательстве США. – *Прим. переводчика*], что эта информация может быть свидетельством преступления [1]. Однако если официальные лица хотят получить доступ к уже открытому документу, находящемуся на сервере, или к еще не открытому тексту, который пробыл на сервере более 180 дней, тогда они должны всего лишь показать, что он «имеет отношение» к расследованию [«имеет отношение» к расследованию – юридический термин в законодательстве США. – *Прим. переводчика*], а это гораздо менее значимо, чем вероятная причина, хотя это часто спорное утверждение, как и в случае обычной повестки в суд [2][1]. Если же информация содержится на «частном» сервере (например, принадлежащем работодателю), то никакой судебной процедуры не требуется [3].

В случае, когда правоохранительные органы ищут записи у третьих сторон, вне контекста коммуникации, может применяться широкий спектр постановлений. Обычно банковские, образовательные и даже медицинские данные можно получить по простой повестке, цель которой часто остается неизвестной, пока не будет предъявлено обвинение [4]. Во множестве иных ситуаций, таких как получение отснятого материала с камер видеонаблюдения, информации о покупках по кредитной карте или прошлых поездках, в большинстве юрисдикций от полиции не требуется выполнения каких-либо судебных процедур; правоохранительные органы могут получать любую информацию по своему усмотрению и усмотрению тех, в чьих руках находится информация [5]. Когда правоохранительные органы хотят получить информацию из баз данных других государственных структур, в отличие от баз данных частных компаний, обычно

[1] 9 февраля 2017 года палата представителей единогласно проголосовала за отмену этого положения и его замену на требование ордера; на момент написания статьи голосование в Сенате еще не состоялось.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

достаточно письменного запроса от руководителя данного органа, хотя иногда требования выше [4, p. 173].

Теоретически Конституция США, в частности Четвертая поправка, должна регулировать такие ситуации. Согласно Четвертой поправке, государство должно действовать «разумно» при «обыске» или «задержании», а суды считают, что требование разумности выполняется только при наличии ордера. Однако это требование применяется только к таким действиям правительства, которые называются «обыск». Верховный суд очень узко определяет этот термин, а именно как действия, нарушающие «разумные ожидания соблюдения приватности», а также содержащие определенные виды физического вторжения [6]. В наибольшей степени это касается тех решений Верховного суда, согласно которым конституционная защита не относится к информации, переданной третьим сторонам – будь то интернет-провайдеры, банки или телефонные компании, – поскольку мы «принимаем риск» передачи информации этими третьими сторонами государству [7, 8][2]. Как будет показано ниже, эта доктрина «третьей стороны» претерпела некоторые изменения за последние годы, однако она остается причиной того, что, за исключением вопроса доступа к содержанию коммуникации (например, [10])[3], Четвертая поправка очень слабо влияет на способность государства получать информацию из частных баз данных, даже когда в дело идут новейшие технологии.

Напротив, когда база данных создается самими правоохранительными органами, Конституция действует в полную силу. В частности, сбор информации для такой базы данных требует обоснования. Например, взятие пробы ДНК с помощью мазка слизистой является «обыском» согласно Четвертой поправке [11], а попытка заставить гражданина предоставить документы, дающие возможность обвинить его, сразу вводит в действие Пятую поправку, если только государственные органы не укажут точно, какие именно документы они запрашивают [12]. Однако в случае необходимости Четвертую поправку легко обойти, заявив, что запрос данного конкретного типа данных не обоснован, так как не соблюдается принцип «разумных требований»; в таких случаях наличие вероятной причины не обязательно [11]. При этом Пятая поправка не действует, если информация «не может служить доказательством» – как в случае с отпечатками пальцев или ДНК [13], или предоставляется «добровольно» не в целях уголовного разбирательства – как в случае возврата налогов или подачи заявки на государственные льготы [14, 15], или получена не от частного лица. Наконец, в Конституции ничего не говорится о доступе к информации со стороны правоохранительных органов в случае, если они или другие государственные организации собирают ее на законных основаниях [16].

Статутное и конституционное право часто критикуют за расплывчатость, однако наиболее популярное контрпредложение – а именно что все или большинство обращений государственных органов к облачной информации должны происходить по судебному ордеру, – также не лишено недостатков. На понятийном уровне очевидно, что во многих ситуациях требование наличия ордера для доступа к информации не обеспечивает полной гарантии, что суд имеет «вероятную причину». На практике такой порядок свяжет руки всем законным усилиям правительства в борьбе с террористами и преступностью. Вероятно, необходим более тонкий подход.

Поиски такого подхода нужно начать с оценки различных мотиваций государства при использовании облачных технологий. Доступ к облачной информации может происходить как минимум по пяти различным основаниям: «по подозреваемому», «по профилю», «по событию», «по программе» и «по инициативе». Иногда официальные органы стремятся получить как можно больше информации о лицах, подозреваемых в преступлении. В других случаях поиск начинается не с конкретного подозреваемого, а с возможного круга подозреваемых, предположительно ограниченного некими характеристиками тех, кто ранее совершал или мог бы совершить определенное пре-

[2] По делу United States v. Miller [9] было вынесено решение, что гражданин не вправе рассчитывать на сохранение в тайне банковских сведений, «даже если информация раскрывается для использования в ограниченных целях и предполагается, что третья сторона не будет раскрывать персональных данных» (p. 443). В деле Smith v. Maryland [7] было вынесено аналогичное решение в отношении телефонных номеров, по которым звонит гражданин.

[3] В деле United States v. Warshak [10] на Шестой выездной сессии суда было вынесено решение, что, согласно Четвертой поправке, для доступа к ранее полученным электронным письмам требуется ордер.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

ступление. Облачный поиск третьего типа начинается не с характеристики конкретного или возможного подозреваемого, а с события – обычно это преступление – и ставит задачей выяснить, исходя из места и обстоятельств этого события, кто мог быть к нему причастен. В рамках четвертого типа доступа государство, чтобы иметь необходимую информацию для поиска предыдущих типов, может инициировать работу специальных программ по сбору данных. И наконец, государство может полагаться на инициативу граждан, обнаруживших в Облаке инкриминирующую информацию о других гражданах.

Каждая из этих ситуаций отличается от остальных четырех. Каждая требует особого режима регулирования. Ниже описывается, как могли бы выглядеть эти режимы. Хотя разработанные в настоящей работе принципы основаны на опыте применения Четвертой поправки, они тем не менее заполняют пробел в законодательстве, поскольку современная практика правоприменения не приспособлена к работе в Облаке. Это новая область правоприменения, до сих пор мало разработанная судами.

Доступ к облачной информации «по подозреваемому» – пропорциональность

Предположим, что в полиции раздается телефонный звонок и женский голос сообщает, что Джон Слейд, учитель местной школы, является наркодилером. Для проверки этого заявления полицейским могут понадобиться записи о телефонных звонках Слейда, которые покажут, знаком ли он с известными наркодилерами, членами банд и потребителями наркотиков. Имея доступ к банковским данным Слейда, можно определить, соответствуют ли его денежные средства заработку учителя. Кроме того, полицейские могли бы выяснить по записям GPS, дронов и камер наблюдения, посещает ли Слейд те места в городе, где обычно продают наркотики.

Согласно действующей Четвертой поправке и законодательным актам, ни одно из этих действий не требует ордера или вероятной причины, а в ряде юрисдикций некоторые из них не требуют даже повестки в суд. Такому отсутствию регулирования способствуют и заявления Верховного суда о том, что неразумно ожидать соблюдения приватности в таких вопросах, когда информация предоставляется третьей стороне или деятельность происходит в публичном месте [6, 17]. Однако при опросах большинство людей высказывают противоположную точку зрения; например, доступ к банковским счетам и информации о телефонных переговорах сравнивают с обыском в спальне, а отслеживание путей перемещения – с обыском при задержании [4, 18, 19]. Рассуждая в более философском плане, исследователи говорят о том, что легкий доступ государственных органов к базам данных угрожает не только приватности, но и независимости и чувству собственного достоинства [20]. Они также заявляют об угрозе ограничения прав граждан на самовыражение и на создание объединений, что несет в себе риск злоупотреблений; в конце концов знание – сила, а Облако – это кладезь знаний [21].

Эти проблемы начали осознавать и в Верховном суде. Так, в деле Riley v. California [22], несмотря на многовековой прецедент, разрешающий изучение любого предмета, найденного на арестованном подозреваемом, Верховный суд потребовал ордер на обыск содержимого мобильного телефона арестованного, признав тот факт, что «мобильный телефон может содержать информацию множества различных типов: адрес, заметку, медицинский рецепт, банковский чек, видеозапись, – которая в совокупности раскрывает гораздо больше, чем любая отдельная запись» (p. 2489). В деле United States v. Jones [23] пять членов Суда вынесли заключение, что, согласно Четвертой поправке, обыск имеет место, когда полиция осуществляет «длительное» слежение за автомобилем с использованием сигналов GPS. Хотя ни в одном из этих дел не было доступа к базам данных, становится понятным направление рассуждений Суда, когда судья Sotomayor заявила в поддержку решения по делу Jones, что, «возможно, необходимо пересмотреть предпосылку, что гражданин не может ожидать приватности в отношении информации, добровольно переданной третьей стороне. Этот подход не соответствует реалиям цифровой эры, когда люди раскрывают огромное количество информации о себе третьим сторонам в повседневной жизни» [23, p. 417].

С этой точки зрения государство имеет право по своему усмотрению использовать информацию из блогов, твитов, публичных записей, которые очевидно предназначаются для публичного доступа. Однако при этом полиция не должна без достаточного обоснования иметь доступ к непубличным данным из Облака, которые люди порождают, когда занимаются

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

«повседневными делами», такими как общение с друзьями, проведение банковских операций, покупки. Также должен быть запрещен доступ без достаточного обоснования к отслеживанию данных о повседневных перемещениях, которые человек предпринимает, считая, что остается практически анонимным.

Коротко говоря, необходимо потребовать, чтобы государство могло получать персональную информацию, недоступную на публичных ресурсах, только при наличии серьезного основания. В таком случае возникает вопрос, насколько серьезным должно быть такое основание. В обычных случаях, согласно Четвертой поправке, поиск информации осуществляется на основании вероятной причины, которая сводится к «достаточной вероятности», что будет обнаружено доказательство преступления [24]. Вернемся к ситуации со Слейдом. Если бы звонившая представилась и сообщила детали о торговле Слейда наркотиками, то у полиции, возможно, появилась бы вероятная причина для полномасштабного цифрового поиска. Однако в нашем примере звонок был анонимным и сообщалось только, что Слейд продает наркотики; таким образом, нельзя исключить, что звонившая является недовольной ученицей или отвергнутой любовницей. Согласно прецедентам Верховного суда, такой звонок не может служить основанием для традиционного расследования [25].

Предположим теперь, что сообщение, хотя и было анонимным, содержало подробности следующей продажи наркотиков Слейдом. Хотя этого недостаточно для возникновения вероятной причины, но такое свойство «предсказательности» служит дополнительным показателем достоверности [26]. В этом случае полиция, возможно, имеет «разумное подозрение» [«разумное подозрение» – юридический термин в законодательстве США. – *Прим. переводчика*] – это причина более низкого уровня, но она тем не менее требует наличия четко сформулированного основания для действий [27]. В такой ситуации полиция, вероятно, все еще не имеет права изымать те значительные объемы информации, о которых шла речь выше. Но, возможно, они должны иметь право доступа к более ограниченному объему данных, например, о звонках Слейда в указанный период времени или о его перемещениях в определенном направлении.

Такой продуманный подход к получению информации из Облака основан на так называемом *принципе пропорциональности* [4]. Согласно традиционным правилам Четвертой поправки, для ареста необходима вероятная причина, а для кратковременного задержания достаточно разумного подозрения; аналогичным образом полный обыск требует вероятной причины, а обыск при задержании – только разумного подозрения [27, p. 20]. Таким же образом глубокое вторжение в личную сферу в Облаке – например, получение выписки о банковских операциях или активности в Интернете за месяц или, как предложил Верховный суд в деле Jones, *отслеживание перемещений гражданина в течение месяца,* – должно быть возможным только при наличии важной причины – такой же, как для обыска дома или машины [23, p. 403]. Однако менее глубокий доступ – например, информация об одном телефонном звонке, или одной покупке по банковской карте, или одной поездке, или определение личности по записи камеры, или отслеживание перемещения в течение нескольких часов – может осуществляться и по менее значительной причине. Такое применение принципа пропорциональности не только лучше отражает степень вторжения государственных органов в личную жизнь человека, но и помогает избежать «Уловки-22», когда от полицейских требуют предъявить вероятную причину до этапа предварительного расследования, которое и должно обнаружить эту вероятную причину.

При абстрактном рассуждении принцип пропорциональности имеет смысл. Однако при практическом применении возникает проблема разграничения. Какое основание потребуется, если полиции нужно узнать о финансовых операциях или перемещениях Слейда не за месяц, а лишь за неделю? Или если необходимо узнать, звонил ли Слейд по определенному номеру, посещал ли определенное место и помещал ли в банк крупную сумму в течение определенного месяца, но никакая другая информация за этот месяц не нужна?

Отвечая на подобные вопросы, мы неизбежно приходим к неким произвольным классификациям. Можно выделить ряд категорий, что было сделано Верховным Судом относительно обысков в домах с использованием сложных приборов тепловидения; в деле Kyllo v. United States [28] Суд постановил, что *все* такие обыски требуют наличия вероятной причины. В отношении доступа со стороны государственных органов к такой же защищенной категории

Актуальные проблемы экономики и права. 2019. Т. 13, № 1
Actual Problems of Economics and Law, 2019, vol. 13, No. 1
ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

должны быть отнесены данные, аналогичные содержимому домов, – например, частные документы, хранящиеся в Облаке, или сообщения в закрытой социальной сети [29][4].

Однако для иных данных требование доступа к личной информации исключительно по ордеру является чрезмерным; об этом свидетельствуют как решения Верховного суда, так и результаты опросов граждан [19, 30]. Один из возможных подходов состоит в дифференцировании по типам информации. Например, медицинские данные должны получить, возможно, максимальную защиту; банковская информация – меньшую степень защиты; данные по коммунальным услугам – еще меньшую [31]. В действующем федеральном законодательстве такой подход применяется в отношении средств связи, а именно данные о подписчиках имеют минимальную степень защиты, номера телефонов и электронные адреса – более сильную, записи прошлых разговоров – еще более сильную, а перехват сообщений требует вероятной причины [1–4]. Но в основе такого порядка лежит «принцип подозреваемого»: например, данные о контактах человека за один месяц могут дать больше информации, чем запись разговора; действительно, учитывая развитие технологий, «уже нельзя считать убедительной концепцию метаданных как категории информации, четко отграниченной от содержания коммуникации, а значит, подлежащей более низкой степени защиты приватности» [32, p. 92]. То же можно сказать и о других типах данных: банковские операции, операции с кредитными картами и даже счета за коммунальные услуги могут представлять собой более или менее приватную информацию в зависимости от человека и контекста.

В этих обстоятельствах подход с точки зрения принципа пропорциональности, применяемый как основной или дополнительный, может основываться на ограничениях по времени или по объему собираемой информации. Так, в деле Jones пять членов Верховного суда разграничивали понятия кратковременного и продолжительного слежения ([23, p. 430], судья Alito, в поддержку данного решения). Также суд указал, что физическое задержание до 15 минут требует разумного подозрения, более длительное задержание требует вероятной причины, а арест не может продолжаться более 48 часов без решения суда [33, 34]. Поиски непубличной информации в Облаке вне контекста жилища могут ограничиваться по тем же основаниям, исходя из положения, что чем больше известно о человеке – неважно, из какого источника, – тем выше степень вторжения в его личную жизнь. Например, для получения информации о банковских операциях Слейда в определенный день или за два дня может быть достаточно того, что эта информация «имеет отношение» к расследованию, однако если нужна информация о всех его действиях за период более 48 часов или за несколько отдельных дней, то потребуется повестка от судьи, а для получения информации за месяц необходимы вероятная причина и ордер. Такой подход на основе длительности срока также имеет недостатки с точки зрения администрирования, однако его преимущество в том, что приватность защищена при приблизительном соблюдении принципа пропорциональности, и в то же время государственные органы могут выстраивать свою работу без обязательного требования наличия вероятной причины с самого начала расследования (сравни [35] и [36]). В конце концов, применяя принцип пропорциональности при поиске «по подозреваемому», можно использовать сочетание подходов по типу данных и по агрегированной информации.

Признавая такой подход убедительным в теории, многие считают, что в конкретном контексте национальной безопасности он неприменим, т. е. что никакие ограничения доступа к облачной информации не должны действовать в случае угрозы национальной безопасности. Однако это положение нужно воспринимать скептически. Национальная безопасность – это очень широкое понятие, и оно слишком часто использовалось как карт-бланш для злоупотреблений со стороны государства [37]. Конкретная опасность

[4] Высказывалось мнение, что зашифрованные данные должны пользоваться такой же, или даже абсолютной защитой именно по той причине, что они зашифрованы. Но, учитывая, что любые данные, включая обезличенную информацию о деловых операциях, могут быть зашифрованы, государственные органы должны, с точки зрения теории пропорциональности, иметь доступ к дешифрованию любых данных при наличии достаточной причины. Дискуссия о шифровании данных слишком обширна, чтобы разбирать ее в этой статье. См. [29] (подробно описаны практические проблемы и законодательство США и других стран в связи с различными подходами к допуску государственных организаций к дешифрованию информации).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

для страны может оправдать отход от правил, которые действуют при обычной охране правопорядка в стране; например, при явной, значительной и неизбежной угрозе требования к пропорциональному обоснованию могут быть снижены. Однако в остальных случаях Агентство по национальной безопасности и иные подобные государственные структуры должны рассматриваться наравне со всеми другими правоохранительными органами.

Доступ к облачной информации «по профилю» – коэффициент попадания

Поиск «по профилю» очень похож на поиск «по подозреваемому». Разница состоит в том, что поиск «по подозреваемому» начинается с конкретного человека, подозреваемого в причастности к преступлению, и лишь затем поиск информации продолжается в Облаке; при поиске «по профилю» у государственных органов нет конкретного подозреваемого, данные на которого ищут в Облаке. Вместо этого используется профиль с описанием возможных характеристик преступника в надежде определить его личность. Вернемся к примеру с Джоном Слейдом. Предположим, что полиция начала подозревать его не из-за анонимного звонка, а потому, что компьютерная программа, разработанная с участием криминалистов, указала на него как на потенциального наркодилера. Подобная программа могла учитывать, скажем, пять факторов, относящихся к особенностям передвижений, финансовых трат и круга общения. Или аналогично тому, как кредитные организации определяют случаи мошенничества, программа может выдать вероятное место и время продажи наркотиков, что позволит организовать наблюдение и схватить преступника. Как и имеющиеся программы для определения риска задержания и вынесения приговора по категориям граждан [38], такие программы изначально строятся на анализе характеристик и поведения наркодилеров, а затем проходят перекрестную проверку в других категориях населения и регионах.

Создание профилей с использованием облачной информации, что иногда называют «прогнозной деятельностью правоохранительных органов», находится в самом начале своего развития. Однако отделения полиции активно разрабатывают необходимые для этого инструменты [39, 40]. Разумеется, подобные профили будут полезны только в том случае, если государственные органы будут иметь доступ к информации, на которой основан профиль. Ниже мы обсудим вопрос, могут ли они иметь такой доступ (см. раздел о поисках «по программе»). Пока предположим, что такой доступ имеется.

Как и в случае поиска «по подозреваемому», при доступе к облачной информации «по профилю» должно присутствовать обоснование, пропорциональное глубине доступа. Другими словами, «коэффициент попадания» при таком доступе должен совпадать с коэффициентом достоверности, требуемым по принципу пропорциональности. Так, если коэффициент попадания при данной вероятной причине составляет 50 %, то доступ к профилю, по которому наркодилер верно определяется с 20 %-ной вероятностью, будет закрыт, но только в том случае, если в этом профиле используется большое количество источников персональных данных. Если же такой профиль содержит только данные о задержаниях, составе банд и другие открытые или квазиоткрытые данные, то этот профиль будет доступен.

При этом для большинства криминальных сценариев даже 20%-ный уровень вероятности будет невозможен; ученые, занимающиеся прогнозами в сфере правосудия, только стремятся достичь такой точности. Получены значения переменных для различных типов криминального поведения, но предсказательная сила каждой отдельной переменной или их комбинаций очень низка. В дальнейшем, вероятно, профили будет необходимо обновлять как по причине естественных изменений криминального поведения, так и потому, что информация о составе факторов в профилях станет известна преступникам. К этому следует добавить, что значительная часть облачной информации об отдельных людях недостоверна [40]. Все это говорит о том, что лишь немногие профили смогут реально помочь в поимке преступников, а значит, полиция должна будет обращать особое внимание на соблюдение принципа пропорциональности.

Предполагая, что профили с достаточно высоким коэффициентом попадания все же можно создать, мы приходим ко второму ограничению использования Облака для поиска «по профилю», а именно необходимости прозрачности информации. Профили должны быть доступны для судов и других надзорных органов, по крайней мере, «при закрытых дверях» (т. е. не в судебном заседании, в отсутствие публики).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Кроме того, прозрачность гарантирует, что факторы, использующиеся при составлении профилей, будут закрытыми, а те из них, которые противоречат закону, например, дискриминирующие по признаку расы, не будут влиять на результаты.

Процедуры такого закрытия могут представлять проблему, особенно если, как в некоторых коммерческих контекстах, профили основываются на сложных алгоритмах машинного обучения или на алгоритмах, защищенных авторскими правами [41]. Что еще более осложняет дело, такие факторы риска, как криминальная история, место жительства и работы, могут косвенно указывать на расовую и классовую принадлежность, другие характеристики, что обычно считается неприемлемым в работе полиции [42–44].

И все же эти трудности нельзя считать непреодолимыми. Например, можно запретить использовать в правоохранительных контекстах все профили, основанные на закрытых алгоритмах, независимо от их точности[5]; можно также разрабатывать профили, для которых гарантируется «соответствие законным процедурам», несмотря на использование сложных алгоритмов машинного обучения [46, pp. 637, 656–677]. Также можно принять определенные меры, если некоторые факторы риска коррелируют не только с уровнем преступности, но и с расовой принадлежностью. Например, разработчикам алгоритмов по определению возможных преступников или мест преступлений можно дать указание не учитывать данные о задержаниях по поводу легких преступлений и правонарушений, связанных с наркотиками, так как они могут отражать практику повышенного внимания полиции по признаку расовой принадлежности; вместо этого разработчики алгоритмов должны будут опираться на данные *полицейских отчетов* (для профилей мест преступлений) и данные о тяжких или имущественных преступлениях (для профилей преступников). Таким образом, будет уменьшено влияние показателей задержаний за наркотики, которые сильно коррелируют с расовой принадлежностью; аналогично можно поступать и в случае других правонарушений, коррелирующих с какими-либо характеристиками [47]. Важно также помнить, что традиционно работа полиции часто основывается на одних и тех же факторах, связанных с конкретным подозреваемым; эта работа часто интуитивна, ее трудно формализовать, а значит, открывается поле для различных злоупотреблений. Прозрачные алгоритмы могут значительно улучшить ситуацию, если дадут достаточный коэффициент попадания и не будут содержать откровенно незаконных факторов [48][6].

Чтобы еще эффективнее не дать предубежденности повлиять на расследование, нужно ввести третье правило поиска «по профилю»: все, кто подпадает под определенный профиль, должны быть в равном положении. Другими словами, если профиль наркодилера с достаточным коэффициентом попадания показывает данные 200 человек, то полиция должна не останавливаться на Слейде из нашего примера, а проверить каждого человека из профиля. Если же это невозможно, то выборочная проверка должна осуществляться по нейтральному основанию, без каких-либо предубеждений (например, проверять каждого третьего по списку). В отсутствие такого ограничения все попытки избежать противозаконной дискриминации при составлении профилей окажутся бесполезными, так как дискриминация проявится на дальнейшей стадии расследования.

Дополнительное преимущество этого третьего ограничения поиска «по профилю» состоит в том, что правоохранительные органы вынуждены применять его с большой осторожностью. Такой поиск дает огромное число ложноположительных результатов даже в случае высокого качества его проведения. Например, если предсказанный уровень попадания составляет 50 %, то половина обследованных окажутся невиновными независимо от того, будут обследованы все лица, выбранные по алгоритму, или только подгруппа, отобранная нейтральным образом. Даже если

[5] Например, Selbst и Barocas [45 (в печати)] выделяют чрезвычайно сложные подходы к построению алгоритмов, от логики «дерева решений» до «глубокого обучения» искусственного интеллекта.

[6] Goel с соавт. [48], используя данные о задержаниях и досмотрах в Нью-Йорке, создали профиль, прогнозирующий ношение оружия с вероятностью от 20 до 30 % – это значительно выше, чем коэффициент попадания Нью-Йоркского отдела полиции, который составил менее 1,3 % на пике «программы досмотров» [49]. Goel с соавт. [48] также определили, что такие факторы, как «вороватые движения», служащие стандартным обоснованием для полицейского задержания, не связаны с ношением оружия; кроме того, среди задержанных с помощью профиля белые с большей частотой имели оружие, чем черные.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

проверка результатов поиска осуществляется в условиях кабинетной работы, большой объем работы будет проделан впустую. В тех же случаях, когда проверка потребует реальных обысков или задержаний, немалое число попавших под такую проверку лиц начнут негодовать и жаловаться, как это происходило при досмотрах нью-йоркской полицией [50]. Поиск облачной информации «по профилю» – дискретный и объективный – имеет значительные преимущества по сравнению с традиционными методами поиска «по подозреваемому», однако массированный характер такого поиска может оказаться настолько неприемлемым с практической или политической точки зрения, что полиция откажется применять его.

Доступ к облачной информации «по событию» – уровень шума

Иногда правоохранительные органы осуществляют поиск облачной информации, отталкиваясь не от профиля или возможного подозреваемого, а от события – обычно криминального, – используя облачные данные с целью определить его действующих лиц или свидетелей. Вернемся к примеру с Джоном Слейдом, но теперь сделаем его жертвой, а не возможным подозреваемым. Представим, что в два часа ночи в воскресенье полицию вызывают на место убийства, на темную улицу города, где обнаруживается тело убитого Джона Слейда с разбросанными вокруг наркотиками. Медэксперт утверждает, что смерть наступила около двух часов назад, т. е. около полуночи. До развития облачных технологий полицейские, вероятно, обошли бы всех окрестных жителей, из которых некоторые утверждали бы – правдиво или нет, – что были в другом месте или ничего не видели и не слышали. Однако теперь полиция может получить данные с мобильных телефонов или автомобильных GPS-навигаторов, а также записи с камер видеонаблюдения с функцией распознавания лиц или с камер ночного видения; распознать людей и машины, находившиеся вблизи места преступления в то время, когда оно было совершено, а затем использовать технологии поиска «по подозреваемому», чтобы определить преступника [51].

Такой поиск способен показать огромное количество людей, среди которых может быть преступник или свидетель, но большинство окажутся ни при чем. В то же время все, что дает это «море информации», – что они находились в определенное время в определенном месте; согласно принципу пропорциональности, получение этой информации требует очень низкого уровня обоснования. Но даже в этом случае глубина поиска информации государственными структурами должна, вероятно, быть ограниченной, чтобы уменьшить как степень вторжения в частную жизнь, так и число людей, которых придется допрашивать. Другими словами, следует минимизировать «уровень шума», по терминологии Джейн Бамбауэр – долю невиновных людей, попадающих под полицейское расследование, цель которого – найти одного или нескольких преступников [52].

Допустимый «уровень шума» будет зависеть от вероятного числа лиц, причастных к рассматриваемому событию. Фактически попытка уменьшить «уровень шума» – это призыв ограничить поиск «по событию» релевантным местом и временем. Например, при расследовании смерти Слейда полиция должна иметь возможность установить личности и допросить прохожих и водителей машин, которые находились рядом с местом преступления незадолго до или сразу после полуночи (если считать, что заключение медэксперта верно). Возможно, придется установить, что полиция не имеет права допрашивать людей, находившихся дальше 50 метров от места преступления или тех, кто был там ранее 11:30 или позднее 12:30.

Облачная информация открывает перед правоохранительными органами большие возможности для поиска «по событию». Такие расследования могут быть очень масштабными, ограничиваясь только фантазией и приоритетами правоохранителей (поскольку они не ограничены действующим законодательством, по крайней мере, в большинстве юрисдикций). В отличие от коэффициента попадания, требуемого для поиска «по профилю», приемлемый «уровень шума» для поиска «по событию» установить нелегко; возможно, он должен зависеть от типа запрашиваемой информации и типа расследуемого преступления[7]. Что касается положений закона, которые должны применяться

[7] В аналогичной ситуации Верховный суд поддержал задержания на дороге с целью найти свидетелей ДТП, случившегося неделей ранее, когда нарушитель скрылся с места происшествия [53]. Согласно решению суда, при анализе таких ситуаций следует учитывать «степень общественной обеспокоенности из-за причины задержаний, степень влияния задержания на общественные интересы, степень вмешательства в личную свободу граждан» (p. 427).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

в данном случае, то, возможно, лучший вариант – это требовать от правоохранительных органов получать санкцию суда на поиск такого типа, поскольку суд может учесть потенциальный «уровень шума» и другие факторы при определении допустимости и глубины поиска «по событию» в каждом конкретном случае.

Доступ к облачной информации «по программе» – демократическая авторизация

Поиск облачной информации «по подозреваемому», «по профилю» и «по событию» опирается на различные степени доступа к разнообразным базам данных, от информации о телефонных звонках и передвижениях до финансовых операций и социальных контактов. С точки зрения правоохранительной деятельности держать такие базы данных отдельно друг от друга по меньшей мере неэффективно, а в случае поиска «по профилю» и вовсе фатально, поскольку профили работают только при условии одновременного охвата нескольких баз данных. Именно на основе этого факта Министерство обороны США после 11 сентября предложило программу Полной информированности (the Total Information Awareness – TIA). По задумке Министерства обороны, программа TIA должна аккумулировать огромный массив данных, который касается, в соответствии с официальным документом, деятельности «в области финансов, образования, медицины, ветеринарии [!], въезда [т. е. иммиграции и таможни], транспорта, жилья... и связи», а также всей государственной отчетности (Total Information Awareness, n.d.). Данные должны собираться, а затем изучаться с помощью специальных алгоритмов с целью выявления террористической деятельности. В 2003 году Конгресс, будучи явно не в восторге от этой идеи, отказался финансировать программу [54]. Однако, если верить Эдварду Сноудену, в настоящее время функционируют несколько подобных программ под управлением Агентства национальной безопасности и других государственных организаций [55].

Как показала реакция общества на откровения Сноудена, значительная часть граждан относится к таким программам негативно. Аккумулирование информации из разных источников в одном месте вызывает множество возражений. В первую очередь такое аккумулирование данных способствует попыткам хакерства и кражи данных, как это происходило недавно в других странах [56]. Еще одно следствие такой деятельности – «размывание задач», когда правоохранительные органы понимают, что информация, собранная с одной целью (например, для борьбы с терроризмом), может оказаться полезной и для других целей. Это легко может привести к злоупотреблениям, от незаконного сбора информации о журналистах, политиках, общественных активистах, членах определенных этнических групп до утечки информации по причине личной мести [57]. И, что самое опасное, у государства появляется соблазн на основе собранной информации создавать «портреты личности» или «цифровые досье» на каждого гражданина, что обычно ассоциируется с тоталитарными режимами [58][8].

Частично из-за реакции общества на откровения Сноудена Агентство национальной безопасности (далее – АНБ), вероятно, больше не собирает метаданные; вместо этого ему приходится получать повестки на конкретные компании, являющиеся держателями информации, в соответствии с подходами поиска «по подозреваемому» и «по профилю», которые были описаны выше [59]. Однако АНБ и другие федеральные агентства продолжают агрегировать данные иных типов [60]. Информацию собирают также различные организации на местном уровне и на уровне штатов. Например, система New York City's Domain Awareness, созданная совместно департаментом полиции города и компанией Microsoft, сводит воедино данные с тысяч камер видеонаблюдения и картографические данные с целью выявления вероятных мест преступления, а также данные систем распознавания автомобильных номеров и сигналы GPS, что позволяет отслеживать перемещения в реальном времени и в записи [61]. Многие другие города имеют крупномасштабные системы видеонаблюдения с помощью камер, а некоторые также разрабатывают систему круглосуточного наблюдения с дронов или самолетов [62, 63]. Программа другого типа, под названием «центры интеграции»,

[8] Daniel Solove популяризовал термин «цифровое досье», определяя его как собрание данных, формирующее «профиль человека с точки зрения его финансов, здоровья, психологии, убеждений, политических взглядов, интересов и стиля жизни», которое «все в большей степени переходит из частного сектора в государственный, особенно в том, что относится к правоохранительной сфере» [58, p. 1084].

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

действует более чем в половине штатов. Эти центры – по последним данным, их более 75, и в некоторых работает более 200 сотрудников – «интегрируют» информацию о финансах, аренде, коммунальных услугах, транспорте и связи из федеральных, региональных и местных баз данных, а также баз данных правоохранительных органов и частных компаний в целях следствия [64, p. 4].

Такая деятельность «по программам», которую называют всеобъемлющей, так как в ней задействуются записи об огромных массах населения, подразумевает, что большинство записей не содержит ничего криминального [65]. По этой причине такой сбор данных не может регулироваться по принципу пропорциональности в рамках подхода «по подозреваемому». Однако этого, возможно, и не требуется. Пока люди не пользуются доступом к этой информации для поиска конкретных данных, как в случае с Джоном Слейдом, никакого вторжения в личное пространство не происходит. И только когда такой доступ осуществляется, государственные органы должны предъявить причину, необходимую для поиска «по подозреваемому», «по профилю» или «по событию».

Чтобы еще более обезопасить персональные данные от вторжения со стороны государства, можно применить порядок, предложенный Конгрессом в отношении программы метаданных АНБ, а именно потребовать, чтобы все базы данных были отделены от государства. Даже поиски облачной информации «по профилю» могут осуществляться частными организациями; при этом государственные органы предоставляют профиль, а компания выдает данные только тех граждан, которые соответствуют этому профилю. И хотя такой порядок также несет риски, связанные с агрегацией данных (хакерство и прочее), он, несомненно, уменьшает потенциальные возможности для злоупотреблений со стороны государства.

В конечном итоге, однако, попытки отделить государство от баз данных безрезультатны. Многие базы данных, необходимые для поиска в Облаке – такие как данные с камер видеонаблюдения, отслеживания на дорогах, миллиарды записей о личной криминальной истории, налогах, документах о праве на собственность, сделках с недвижимостью и многие другие, – не могли бы существовать без поддержки государства. Органы исполнительной власти используют эту информацию для самых разных законных действий, включая профилактику преступности. Таким образом, нельзя запретить государству иметь и развивать такие базы данных.

Вместо этого необходимо перевести регулирование поиска «по программам» на политическую основу [65]. Это предложение может показаться наивным, учитывая, насколько легко Конгресс соглашается на предложения исполнительной власти о всеобщем надзоре после теракта 11 сентября. Однако законодатели могут принять меры в этом отношении, о чем свидетельствует отказ финансировать TIA и пересмотр программы метаданных АНБ [5, 66][9]. Особенно в тех случаях, когда в процессе поиска облачной информации затронуты значимые группы населения – например, представители органов законодательной власти и их наиболее влиятельных подразделений, – некоторые виды политического воздействия не только возможны, но и вероятны.

В то же время следует признать, что правоохранительные и антикриминальные лобби очень сильны как на уровне штатов, так и на федеральном уровне, и они могут оказать значительное влияние на решение этих вопросов. Важную роль в этом могли бы сыграть суды, причем в двух направлениях. В ряде случаев суды могли бы выносить решения об особой схеме сбора данных, вне рамок Четвертой поправки. Однако, учитывая узкое определение термина «обыск», данное Верховным судом для целей применения Четвертой поправки, а также его пристрастие к программам, включающим поиск различной информации (в рамках так называемого особого правосудия), такой исход вряд ли возможен в ближайшем будущем [65].

Второй способ, с помощью которого суды могли бы подвигнуть законодательные и правоохранительные органы к более сбалансированному подходу к указанной проблеме и который будет действовать независимо от Четвертой поправки, – это применять тот же «строгий» анализ, который они используют в отношении программ, создаваемых другими административными органами, например Агентством по охране окружающей среды или Администрацией по контролю за

[9] Среди других примеров – законы штатов, которые ограничивают наблюдения с использованием дронов (собрание таких законов см. [66]), и федеральные законы, ограничивающие доступ к различным типам информации (подробный список таких законов см. [5]).

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

продуктами питания и лекарствами [67]. Правоохранительные органы редко оказываются объектом этого типа судебного надзора, который вполне обычен для других ведомств; однако такой недостаток контроля – это скорее закрепленная традицией случайность, чем сознательная политика. В настоящей работе мы не рассматриваем вопрос о том, почему суды обязаны осуществлять надзор такого типа [68, 69]. Для целей нашего исследования достаточно отметить, что при всеобъемлющем сборе информации «по программе» суды должны рассматривать отделы полиции наравне с другими ведомствами, которые определяют границы законопослушного поведения граждан.

Этот вывод имеет несколько следствий. Во-первых, в рамках существующих принципов административного права ни одна ведомственная программа не может действовать, если она влияет на права и обязанности граждан; чтобы ввести в действие подобную программу, ведомство должно сослаться на законодательство, которое в идеале описывает негативное явление, которое следует устранить, категории граждан и виды деятельности, которые могут подвергнуться воздействию этого явления, и общие меры, которые могут быть приняты для его устранения. Это означает, что прежде чем такие программы, как New York City's Domain Awareness в Нью-Йорке и «центры интеграции» на уровне штатов, начнут действовать, муниципальные, региональные и местные законодательные органы должны определить, какие виды информации они могут получить и с какой целью. Подобное требование законодательной авторизации, поддержанное судами, должно обеспечить хотя бы минимальную демократическую оценку таких программ и способов их реализации.

На этом, однако, влияние принципов административного права не заканчивается. Согласно стандартной практике, когда ведомство получает одобрение на организацию какой-либо программы, оно должно разработать правила ее реализации, провести процедуру публичного обсуждения (или подобную ей) и дать письменное обоснование для окончательного варианта правил; затем эти правила рассматриваются судом, чтобы гарантировать, что они соответствуют законодательству и свободны от дискриминации по принципу групп населения или областей применения [69]. Такие процедуры для обеспечения принципов демократии и судебного надзора налагают дополнительную нагрузку на отделения полиции, что не может не повлиять на выбор способа сбора данных. Необходимость прохождения такой публичной процедуры заставит значительно сократить программы, подобные TIA, «центры интеграции» и другие масштабные практики, или, по крайней мере, применять их более сдержанно.

Требование равноценности при сборе данных, введенное для предотвращения предвзятости, приобретает особую значимость; предлагается даже усилить это требование через доктрину «равноценной защиты» [70]. Это потребует либо всеобщего, либо случайного сбора данных (как предлагалось выше в связи с поиском «по профилю»), либо обоснования того, что неравномерный сбор данных статистически оправдан. Например, согласно этому принципу, потребуется установить камеры видеонаблюдения во всех точках города или, как вариант, везде, где зафиксирован определенный уровень преступности. Тогда сбор метаданных будет осуществляться в масштабах всей страны и будет либо случайным, либо основанным на алгоритмах с высоким коэффициентом попадания. В этом случае наличие баз данных ДНК, собранных у задержанных, как было одобрено Верховным судом (см. Maryland v. King [11]), будет трудно оправдать без доказательства того, что задержанные совершают больше преступлений, чем население в среднем [71].

Один из недостатков такого публичного подхода к сбору облачной информации «по программе» состоит в том, что преступники будут знать критерии отбора данных и научатся избегать попадания в собираемые базы данных. Такое происходит и в традиционной правоохранительной практике, что признается в административно-процессуальном законодательстве, однако в случае цифровых баз данных опасения оказываются преувеличенными [72]. Дело в том, что главная цель всех масштабных правоохранительных мероприятий – предотвращение преступлений, и публичность может только способствовать ей. Кроме того, можно не раскрывать специфические детали применения такого подхода. Например, если используются камеры скрытого видеонаблюдения, то нужно раскрыть факт и основную цель такого наблюдения, но не расположение конкретных камер. Типы данных, собираемых «центрами интеграции», должны быть известны, но алгоритмы, используемые при их анализе, могут обсуждаться только в закрытых судеб-

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

ных заседаниях. И, наконец, основное возражение в ответ на подобные опасения следующее: принцип подотчетности в демократическом обществе требует, чтобы граждане знали не только о широкомасштабных возможностях полиции, но и о том, как именно они применяются.

Доступ к облачной информации «по инициативе» – фидуциарные обязательства

Все вышеописанные типы поиска облачной информации подразумевают расследования по инициативе государственных органов. В нашем исследовании мы исходим из предпосылки, что обоснование в той или иной степени необходимо при любом вмешательстве государства в личную информацию. Но что если держатель информации – банк, транспортная организация, больница – обнаруживает информацию, которая, возможно, свидетельствует о преступной деятельности, и хочет передать ее полиции? До сих пор мы обсуждали ряд причин, по которым государство не должно иметь права требовать информацию у третьих сторон без обоснования, однако ситуация совершенно меняется, если третья сторона сама проявляет инициативу.

При этом важно отметить, что не все ситуации доступа к облачной информации «по инициативе» одинаковы. В тех делах, когда Верховный суд впервые обнародовал «доктрину третьей стороны», третья сторона была лично знакома с ответчиком (Hoffa v. United States [73]; Lewis v. United States [74]). Правило, что информация, полученная от таких лиц, должна игнорироваться государством, подрывает их независимое решение о раскрытии этой информации; можно даже утверждать, что это правило подрывает их право на свободу слова, гарантированное Первой поправкой. Вспомним, например, осведомителя в нашем примере с Джоном Слейдом. Каковы бы ни были его мотивы и откуда бы он ни получил информацию, его решение раскрыть эту информацию заслуживает уважения и должно рассматриваться как легитимная основа для действий государственного органа, если имеются достаточные указания на достоверность этой информации.

Однако в недавно рассмотренных Верховным судом делах с участием третьей стороны, Miller v. United States [75] и Smith v. Maryland [7], третьей стороной выступало не физическое лицо, а организация, а именно банк и телефонная компания. Исторически корпорации не считаются самостоятельными «лицами» в большинстве контекстов и имеют меньше прав в рамках Первой поправки, чем люди (Citizens United v. Fed. Elec. Comm'n [76])[10]. Что еще важнее, в отличие от физических лиц организации имеют формальные или квазиформальные фидуциарные обязательства перед своими клиентами, поскольку, в отличие от третьей стороны в виде физического лица, они могут получать личную информацию просто потому, что предоставляют определенную услугу [4, 78]. Самый яркий пример – медицинские учреждения, которым пациент передает личную информацию, чтобы получить лечение. Даже Верховный суд отклонил заявление, что медицинское учреждение имеет право не соблюдать врачебную тайну в интересах поимки преступника (Ferguson v. City of Charleston [79]). Вероятно, такую же позицию следует занять по отношению к банкам и телефонным компаниям, которым мы передаем информацию с единственной целью осуществлять финансовые операции или пользоваться связью.

Важно также отметить, что когда третьей стороной является организация, то степень «добровольной» передачи информации государству может быть очень разной. В некоторых случаях государство *отдает команду* третьим сторонам предоставить имеющуюся у них информацию автоматически и без какого-либо судебного ордера. Например, банки должны сообщать обо всех вкладах свыше 10 тысяч долларов независимо от обстоятельств [80]. Такой приказ может считаться обоснованным, только если он исходит от законодательного органа и применяется для всех без исключения (что в случае с вкладами соответствует действительности). Чаще государство прибегает к более тонким рычагам давления на третью сторону для получения от нее информации. В самом очевидном случае некоторые держатели информации, хотя и являются частными компаниями и не зависят от правительства, но во многом рассматривают государство в качестве клиента [81]; другие компании, завися от

[10] Решение Верховного Суда по делу Citizen's United [76] фокусировалось на праве корпораций на политические выступления, что не рассматривается в данном контексте. Кроме того, в рамках Пятой поправки корпорации до сих пор не считаются «лицами», а в рамках Четвертой поправки имеют очень мало прав [8, 77].

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

щедрости государства, стремятся доказать свою полезность [82]. Если поиск «по инициативе» не получит четкого определения, то он может в конечном итоге свести на нет все усилия по передаче максимального объема данных в руки частных компаний, на что направлены, например, недавно принятые законы АНБ. Это явление вызывает тревогу, поскольку граждане должны быть уверены, что частные организации, которым они доверяют самые основы своей жизни, не передадут информацию государству.

В то же время следует признать, что фидуциарные обязательства и опасения по поводу двуличности корпораций не должны всегда ставиться выше свободы слова и заботы об общественной безопасности. Например, и медики, и юристы признают свою обязанность раскрывать информацию, способную остановить или предотвратить тяжкое преступление (например, [83, 84, Правило 1.6 (b) (1)]). Если применить эту норму к облачной информации, то третьи стороны будут иметь право раскрывать, а государство – использовать информацию, способную предотвратить тяжкое преступление в ближайшем будущем. Однако спорным остается вопрос, следует ли применять эту норму в полной мере, если в ситуациях доступа «по инициативе» третьей стороной выступают организации, без которых в современном мире мы не можем обойтись[11].

Рекомендации

Базы данных содержат информацию, которая может помочь правоохранительным органам успешнее бороться с преступностью и терроризмом. Однако, учитывая персональный характер большей части такой информации, государство не должно иметь возможности получать, просматривать или использовать такую информацию бесконтрольно. На основе проведенного исследования были разработаны следующие рекомендации относительно доступа правоохранительных органов к базам данных:

Если отделение полиции ищет непубличную информацию о конкретном человеке, оно должно предъявить подозрения о совершении им преступного деяния, пропорциональные глубине вторжения в личные данные. Независимо от того, будут ли суды модифицировать действующий закон о Четвертой поправке для регулирования такого доступа, законодательные органы должны требовать строгого обоснования в отношении типа данных, их объема или обоих этих параметров.

Напротив, если правоохранительные органы получают доступ к информации с целью создания профиля для поиска подозреваемых, они должны убедиться, что профиль имеет необходимый коэффициент попадания на основе принципа пропорциональности, что он не содержит противоправной дискриминации и использует понятный алгоритм. Суды должны давать оценку профилю в закрытом заседании, если это необходимо, чтобы гарантировать их валидность и отсутствие предвзятости в выделении факторов риска. Если профиль используется для идентификации подозреваемых, то у полиции не должно быть возможности выбирать, кто из подозреваемых подлежит дальнейшему расследованию; расследование должно проводиться в отношении всех лиц из профиля или, если это невозможно, в отношении подмножества профиля, отобранного на нейтральной основе.

Если отделение полиции отталкивается в своем расследовании не от подозреваемого или профиля, а от самого преступления, то такое преступление должно быть достаточно тяжелым, а круг лиц, по которым запрашивается информация, должен быть минимальным и соответствовать времени и месту преступления. Если очевидно, что расследование будет масштабным, то определять необходимость и масштабы доступа к информации должен суд.

Сбор данных, необходимых для целей правоохранительной деятельности, должен осуществляться негосударственными организациями в пределах, соответствующих основным целям сбора информации; независимо от места сбора и хранения информации, эти процессы должны регулироваться особым законодательством и административными нормами, выработанными открыто и демократическим путем. Методы получения данных должны быть универсальными, основанными на случайной выборке или статистически обоснованными. Суды должны обеспечивать выполнение этих норм через административные меры или принцип равной защиты.

[11] Конгресс принял аналогичный закон, запрещающий интернет-провайдерам предоставлять правоохранительным органам информацию о коммуникациях, за исключением критических ситуаций, могущих повлечь смерть или тяжкое телесное повреждение, и некоторых технических ситуаций [85].

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

Частные организации должны иметь право предлагать государственным органам информацию о лицах, по отношению к которым у них есть фактические фидуциарные обязательства, только в том случае, если у этих организаций имеются веские основания считать, что это предотвратит совершающееся или готовящееся тяжкое преступление. Суды должны тщательно изучать все финансовые или иные меры, которые применяют государственные органы для побуждения к передаче им информации, обычно имеющей ограничения сбора и доступа. Эти правила, подкрепленные адекватными механизмами подотчетности, чтобы обеспечить обнаружение их нарушения и наказание за него[12], позволят государству использовать потенциал облачных технологий для раскрытия преступлений, ограничив при этом возможности для злоупотреблений [4].

Список литературы / References

1. 18 U.S.C. §§ 2511 & 2518.
2. 18 U.S.C. § 2703(a), (b)(1)(B).
3. 18 U.S.C. § 2711(2).
4. Slobogin C. *Privacy at risk: The new government surveillance and the Fourth Amendment*, University of Chicago, IL, Chicago Press, 2007.
5. Murphy E. The politics of privacy in the criminal justice system: Information disclosure, the Fourth Amendment, and statutory law enforcement exemptions, *Michigan Law Review*, 2013, Vol. 111, No. 4, pp. 485–546.
6. Florida v. Jardines, 569 U.S. 1 (2013).
7. Smith v. Maryland, 442 U.S. 735 (1979).
8. United States v. Morton Salt Co., 338 U.S. 632 (1950).
9. United States v. Miller, 425 U.S. 435 (1976).
10. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
11. Maryland v. King, 133 S. Ct. 1958 (2013).
12. United States v. Hubbell, 530 U.S. 27 (2000).
13. Wilson v. Collins, 517 F.3d 421 (6th Cir. 2008).
14. Garner v. United States, 424 U.S. 648 (1976).
15. Baltimore Dep't of Soc. Serv. v. Bouknight, 493 U.S. 549 (1990).
16. Murphy E. DNA in the criminal justice system: A congressional research service report, *UCLA Law Review Discourse*, 2016, Vol. 64, pp. 340–371.
17. United States v. Knotts, 460 U.S. 276 (1983).
18. Blumenthal J. E., Adya M., Mogle J. The multiple dimensions of privacy: Testing "lay" expectations of privacy, *Pennsylvania Journal of Constitutional Law*, 2009, Vol. 11, pp. 331–373.
19. Scott-Hayward C. S., Fradella H. F., Fischer R. G. Does privacy require secrecy: Societal expectations of privacy in the digital age, *American Journal of Criminal Law*, 2015, Vol. 43, pp. 19–60.
20. Lametti D. The Cloud: Boundless digital potential or enclosure 3.0?, *Virginia Journal of Law and Technology*, 2012, Vol. 17, pp. 190–243.
21. Solove D. J. Privacy and power: Computer databases and metaphors for information privacy, *Stanford Law Review**, 2001, Vol. 53, pp. 1393–1462.
22. Riley v. California, 134 S. Ct. 2473 (2014).
23. United States v. Jones, 565 U.S. 400 (2012).
24. LaFave W. R., Israel J. H., King N. J., Kerr O. S. *Criminal procedure*, 3rd ed., Eagan, MN, Thomson/West Group, 2007.
25. Florida v. J. L., 529 U.S. 266 (2000).
26. Illinois v. Gates, 462 U.S. 213 (1983).
27. Terry v. Ohio, 392 U.S. 1 (1968).

[12] Такие механизмы могут включать как минимум: (1) процедуры аудита, показывающие, кто, когда и с какой целью запрашивал данные; (2) индивидуализированное (в случае поиска «по подозреваемому») или общее (в других случаях) уведомление, описывающее детали доступа к облачной информации; (3) правила, ограничивающие хранение данных государственными организациями или третьими сторонами, и (4) гражданские и уголовные санкции за неправомерный сбор данных или доступ к ним.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

28. Kyllo v. United States, 533 U.S. 27 (2001).
29. McCarthy H. J. Decoding the decryption debate: Why legislating to restrict strong encryption will not resolve the "going dark" problem, *Journal of Internet Law*, 2016, Vol. 20, No. 3, pp. 1/18–39.
30. Slobogin C. Government data mining and the Fourth Amendment, *University of Chicago Law Review*, 2008, Vol. 75, No. 1, pp. 317–341.
31. *ABA Standards for criminal justice: Law enforcement access to third part records*, American Bar Association, 2013, available at: https://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf
32. Bellovin S. M., Blaze M., Landau S., Pell S. K. It's too complicated: How the internet upends Katz, Smith, and electronic surveillance law, *Harvard Journal of Law and Technology*, 2016, Vol. 30, No. 1, pp. 1–101.
33. County of Riverside v. McLaughlin U. S.
34. United States v. Sharpe, 470 U.S. 675 (1985).
35. Kerr O. S. The mosaic theory of the Fourth Amendment, *Michigan Law Review*, 2011, Vol. 111, No. 3, pp. 311–354.
36. Slobogin C. Making the most of United States v. Jones in a surveillance society: A statutory implementation of mosaic theory, *Duke Journal of Constitutional Law and Public Policy*, 2012, No. 8, pp. 1–37.
37. Yamamoto E. K. White (house) lies: Why the public must compel the courts to hold the President accountable for national security abuses, *Law and Contemporary Problems*, 2005, Vol. 68, No. 2, pp. 285–339.
38. Lowenkamp C. T., Whetzel J. The development of an actuarial risk assessment instrument for U.S. pretrial services, *Federal Probation*, 2009, Vol. 73, No. 3, pp. 33–36.
39. Fagan J. Race and the new policing, *Reforming criminal justice: A report of the Academy for Justice on bridging the gap between scholarship and reform*, ed. Luna E., Phoenix, AZ, Academy for Justice, 2017, pp. 83–116.
40. Ferguson A. G. Big data and predictive reasonable suspicion, *University of Pennsylvania Law Review*, 2015, Vol. 163, No. 2, pp. 327–410.
41. Rich M. L. Machine learning, automated algorithms, and the Fourth Amendment, *University of Pennsylvania Law Review*, 2016, Vol. 164, pp. 871–929.
42. Barocas S., Selbst A. D. Big data's disparate impact, *California Law Review*, 2016, Vol. 104, pp. 671–732.
43. Carbado D. W. Race and the Fourth Amendment, *Reforming criminal justice: A report of the Academy for Justice on bridging the gap between scholarship and reform*, ed. Luna E., Phoenix, AZ, Academy for Justice, 2017, pp. 153–184.
44. Harris D. A. Racial profiling, *Reforming criminal justice: A report of the Academy for Justice on bridging the gap between scholarship and reform*, ed. Luna E., Phoenix, AZ, Academy for Justice, 2017, pp. 117–152.
45. Selbst A. D., Barocas S. *Regulating inscrutable systems* (in press), available at: http://www.werobot2017.com/wpcontent/uploads/2017/03/Selbst-and-Barocas-Regulating-Inscrutable-Systems-1.pdf
46. Kroll J. A., Huey J., Barocas S., Felten E. W., Reidenberg J. R., Robinson D. G., Yu H. Accountable algorithms, *University of Pennsylvania Law Review*, 2017, Vol. 165, pp. 633–705.
47. Feldman M., Friedler S., Moeller J., Scheidegger C., Venkatasubramanian S. Certifying and removing disparate impact, *Proceedings of the 21st ACM SIGKDD International Conference of Knowledge Discover and Data Mining*, Sydney, NSW, Australia, The Association for Computing Machinery, 2015, pp. 259–268.
48. Goel S., Perelman. M., Shroff R., Sklansky D. A. Combatting police discrimination in the age of big data, *New Criminal Law Review*, 2017, Vol. 20, No. 2, pp. 181–232.
49. Jones-Brown D., Stoudt B. G., Johnston B., Moran K. *Stop, question, & frisk policing practices in New York City: A primer* (revised ed.), 2013, available at: http://www.atlanticphilanthropies.org/app/uploads/2015/09/SQF_Primer_July_013.pdf
50. White M. D., Fradella H. F. *Stop and frisk: The use and abuse of a controversial policing tactic*, New York, NY, New York University Press, 2016.
51. Reel M. Secret cameras recording Baltimore's every move from above, *Bloomberg Businessweek*, 2016, available at: https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/
52. Bambauer J. Hassle, *Michigan Law Review*, 2015, Vol. 113, No. 4, pp. 461–511.
53. Illinois v. Lidster, 540 U.S. 419 (2004).
54. 149 Cong. Rec. S1379-02, S1416 (Jan 23, 2003).
55. Greenwald G. ZKeyscore: NSA tool collects "nearly everything a user does on the internet", *The Guardian*, 2013, available at: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
56. Perlroth N., Gelles D. Russian hackers amass over a billion internet passwords, *New York Times*, 2014, available at: https://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-abillion-stolen-internet-credentials.html
57. Sloan R. H., Warner R. The self, the Stasi, and the NSA: Privacy, knowledge, and complicity in the surveillance state, *Minnesota Journal of Law, Science, and Technology*, 2016, Vol. 17, No. 1, pp. 347–408.
58. Solove D. J. Digital dossiers and the dissipation of Fourth Amendment privacy, *Southern California Law Review*, 2004, Vol. 75, pp. 1083–1167.

ISSN 1993-047X (Print) / ISSN 2410-0390 (Online)

59. USA Freedom Act of 2015. (2015). Pub. L. No. 114–23, § 101, 129 Stat. 268, 269–71 [amending 50 U.S.C. §§ 1861(b)(2) & (c)(2)].

60. Whittaker Z. Freedom Act will kill only one of NSA's programs (and not even one of its worst), *Zero Day*, 2014, May 4, available at: http://www.zdnet.com/article/freedom-actmetadata-phone-records-prism/

61. Long C. NYPD, Microsoft create crime-fighting tech system, *NBC New York*, 2013, February 20, available at: http://www.nbcnewyork.com/news/local/NYPDMicrosoft-Crime-Fighting-Tech-System-192157481.html

62. Blitz M. J., Grimsley J., Henderson S. E., Thai J. Regulating drones under the First and Fourth Amendments, *William and Mary Law Review*, 2015, Vol. 57, No. 1, pp. 49–142.

63. Sengupta S. Privacy fears grow as cities increase surveillance, *New York Times*, 2013, October 13, available at: http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-incities.html?mcubz=0

64. *The Constitution Project*. Recommendations for fusion centers: Preserving privacy and civil liberties while protecting against crime and terrorism, 2012, available at: https://constitutionproject.org/wpcontent/uploads/2012/10/fusioncenterreport.pdf

65. Slobogin C. Panvasive surveillance, political process theory, and the nondelegation doctrine, *The Georgetown Law Journal*, 2014, Vol. 102, pp. 1721–1776.

66. Smith M. L. Regulating law enforcement's use of drones: The need for state legislation, *Harvard Journal on Legislation*, 2015, Vol. 52, pp. 423–454.

67. Garry P. M. Judicial review and the "hard look" doctrine, *Nevada Law Journal*, 2006, Vol. 7, pp. 151–170.

68. Ponomarenko M., Friedman B. Democratic accountability and policing, *Reforming criminal justice: A report of the Academy for Justice on bridging the gap between scholarship and reform*, ed. Luna E, Phoenix, AZ, Academy for Justice, 2017, pp. 5–26.

69. Slobogin C. Policing as administration, *University of Pennsylvania Law Review*, 2016, Vol. 165, pp. 91–152.

70. Friedman B., Stein C. B. Redefining what's "reasonable": The protections for policing, *George Washington Law Review*. 2016, Vol. 84, pp. 281–353.

71. Roth A. Maryland v. King and the wonderful, horrible DNA revolution in law enforcement, *Ohio State Journal of Criminal Law*, 2013, Vol. 11, pp. 295–309.

72. 5 U.S.C. § 552(b)(7)(E).

73. Hoffa v. United States, 385 U.S. 293 (1966).

74. Lewis v. United States, 385 U.S. 206 (1966).

75. Miller v. United States, 425 U.S. 435 (1976).

76. Citizens United v. Fed. Elec. Comm'n, 558 U.S. 310 (2010).

77. Hale v. Henkel, 210 U.S. 43 (1906).

78. Brennan-Marquez K. Fourth Amendment fiduciaries, *Fordham Law Review*, 2015, Vol. 84, No. 2, pp. 611–659.

79. Ferguson v. City of Charleston, 532 U.S. 67 (2001).

80. 31 U.S.C. § 5313(a).

81. Hoofnagle C. J. Big brother's little helpers: How ChoicePoint and other commercial data brokers collect and package your data for law enforcement, *North Carolina Journal of International Law and Commercial Regulation*, 2004, Vol. 29, pp. 595–637.

82. Cover A. Y. Corporate avatars and the erosion of the populist Fourth Amendment, *Iowa Law Review*, 2015, Vol. 100, pp. 1441–1502.

83. Florida Stat. Ann. § 394.4615(3)(a).

84. *Model Rules of Professional Conduct*, American Bar Association,1983, available at: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html

85. 18 U.S.C. § 2702(c).

86. Total Information Awareness. (n.d.), Wikipedia, July 14, 2017, available at: https://en.wikipedia.org/wiki/Total_Information_Awareness

87. Slobogin C. Policing, databases, and surveillance, *Criminology, Criminal Justice, Law & Society*, 2017, Vol. 18, Is. 3, pp. 70–84.

---

* Принадлежит нежелательной организации в РФ / Belongs to an undesirable organization in the Russian Federation.

Дата поступления / Received 05.01.2019
Дата принятия в печать / Accepted 03.03.2019
Дата онлайн-размещения / Available online 25.03.2019