Правовые аспекты управления Big Data в странах БРИКС и ШОС

И.Н. Федулов,
Югорский государственный университет

Что такое «большие данные»?

- Большие массивы «обезличенных данных», как структурированных, так и неструктурированных, которые нельзя сопоставить с конкретным пользователем без привлечения дополнительной информации, но которые тем не менее могут содержать о нем некоторую уникальную информацию, доступную после соответствующего анализа (***IP-адреса посещенных страниц, информация о действиях на посещаемых страницах, запросы в поисковых системах и соцсетях, прочая информация из соцсетей, камер видеонаблюдения, данные геопозиции и т.п.***)
- Результат статистической обработки и анализа указанных массивов данных

Необходимость правового регулирования в сфере «больших данных» с точки зрения государства

- Необходимость «информационного суверенитета» государства
- Повышение эффективности средства контроля и управления обществом включение Big Data в правовую систему государства

Необходимость правового регулирования в сфере «больших данных» с точки зрения пользователей

- Ограниченные возможности воздействия рядовых пользователей на крупные корпорации в вопросе сохранности и конфиденциальности персональных данных
- Опасения «диктатуры данных» (дискриминации на основании результатов статистического анализа Big Data)
- «Эффект охлаждения» (искусственное сдерживание развития Интернет-сервисов из-за опасения пользователей оставить «цифровые следы»)
- «Эффект информационных пузырей» (побочный эффект фильтрации контента на основе статистического анализа Big Data, приводящий к однобокому, подсознательно желаемому освещению событий, игнорирующему альтернативные точки зрения)[I, с. 32-34]

Бразилия

- Закон No.13,709, of August 14, 2018 «Provides for the protection of personal data»[1]
- Поправки к закону No. 12,965, of April 23, 2014(the “Brazilian Internet Law”)[1]
  - правовые основания для обработки персональных данных
  - принципы обработки персональных данных
  - права субъектов данных
  - коммуникация и объединение данных
  - международная передача данных
  - обязанности акторов
  - административные санкции

Бразилия

Особенности законодательства о персональных данных

- Подразделение пользовательских данных на два множества: ***персональные*** и ***анонимизированные*** по принципу возможности идентификации субъекта данных существующими техническими средствами
- Выделение подмножества ***конфиденциальных персональных данных,*** в которое включаются сведения о расовом или этническом происхождении, религиозных и политических убеждениях, членстве в профсоюзах или религиозных, философских или политических организациях, данные, касающиеся здоровья или половой жизни, генетические или биометрические данные, когда они связаны с физическим лицом
- Широкие права субъекта данных (имеет право требовать доступа к данным, исправления неполных, неточных или устаревших данных, анонимизации, блокирования или удаления ненужных или чрезмерных данных)

Китай

- Big Data — технологическая основы системы социального рейтинга китайских граждан (система «социального кредита»)
- До последнего времени отсутствовал специальный закон, регулирующий оборот персональных данных, подобный европейскому GDPR
- В сфере защиты данных в настоящий момент действуют
  - Решение Постоянного комитета Национального Народного Конгресса об усилении защиты сетевой информации (National People’s Congress Standing Committee Decision concerning Strengthening Network Information Protection) от 28 декабря 2012 года[2]
  - Закон о кибербезопасности (China’s Cybersecurity Law), вступил в силу 1 июня 2017 года[3]
  - Национальный стандарт по защите персональной информации (GB/T 35273-2017 Information Technology – Personal Information Security Specification), вступил в силу 1 мая 2018 года[4]

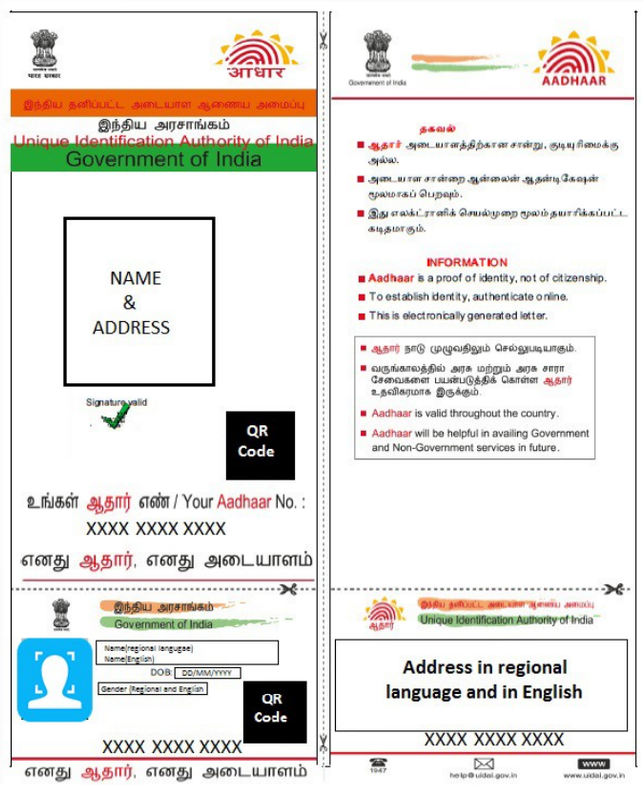
Китай

Особенности законодательства о персональных данных

- Поставщики цифровых услуг должны в обязательном порядке указывать ***цель, методы и возможности*** сбора информации, обязаны получать согласие лица, чьи данные собираются, а также публиковать свои правила сбора и использования личной информации[2]
- Перед тем, как получить от провайдера услуги доступа, пользователи обязаны предоставить ***реальную информацию о личности***[2]
- Прямой запрет провайдеру отправлять коммерческую электронную информацию (в т.ч. рекламу) конечному пользователю без его согласия[2]
- Подход к определению «конфиденциальной личной информации» отличается от принятого в Европе: таковой считаются не просто данные определённого типа, а ***любая личная информация***, «которая, в случае утери или ненадлежащего использования может подвергнуть опасности людей или имущество, нанести вред личной репутации и психическому и физическому здоровью или привести к дискриминационному обращению (например, национальные идентификационные номера, учётные данные, банковские и кредитные реквизиты, точное местоположение человека, информацию о владении недвижимостью и информацию о несовершеннолетнем (младше 14 лет))»[II]
- К «личной информации» относятся: ***аппаратные серийные коды устройства, IP-адреса, записи отслеживания веб-сайта и уникальные идентификаторы устройства***[II]
- Отказ пользователя от предоставления дополнительной информации может служить основанием для отказа провайдера предоставлять дополнительные услуги, но не может служить основанием для отказа от предоставления основных бизнес-продуктов[II] (согласно поправкам, внесенным в Стандарт в январе 2019 года, предлагается исключить «исполнение контракта» из существующих исключений для требования о согласии[III])
- Существует требование, сходное с «принципом ограничения цели» GDPR: все виды использования информации, включая вторичное использование, должны быть разумно связаны с первоначальной целью сбора данных и должны быть повторно авторизованы в других случаях[II]
- Право на удаление данных реализовано без исключений, характерных для GDPR, что, например, позволяет отклонить запросы на удаление в интересах свободы выражения мнений и информации или научных исследований, однако может входить в конфликт с другими нормами законодательства[II]
- Право на переносимость данных возникает в более широком диапазоне ситуаций, но ограничивается определенной информацией, такой как информация о здоровье, образовании или профессии[II]
- Требуется предварительное уведомление и согласие отдельных лиц на передачу или совместное использование их данных (в отличие от GDPR, где подобное согласие не требуется)[II]

Индия

- 2005 — Закон о праве на информацию (Right to Information Act)
- 2010 - Закон об UIDAI (Unique Identification Authority of India) - системе идентификации граждан и резидентов Индии, вводящей AADHAAR (биометрический аутентификационный номер)
- 2011 - «Правила информационных технологий (разумные методы и процедуры безопасности и конфиденциальные личные данные или информация)»[5]
- 2016 - The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, (“Aadhaar Act”), Aadhaar (Data Security) Regulations (“Aadhaar DS Regulations”), Aadhaar (Sharing of Information) Regulations (“Sharing Regulations”)



Идентификационная карта AADHAAR

Индия

Особенности законодательства о персональных данных

- Биометрическая информация считается конфиденциальной личной информацией (раздел 30 «Aadhaar Act» 2016)
- Запрещается передавать третьим лицам по любой причине основную биометрическую информацию, собранную или созданную в соответствии с Законом об AADHAAR, или использоваться для каких-либо целей, кроме генерации номеров AADHAAR и аутентификации в соответствии с Законом об AADHAAR (раздел 29)
- Информация, упомянутая в разделах 28 и 29, может быть раскрыта в случае *вынесения постановления суда*, не уступающего решению окружного судьи; *или в интересах национальной безопасности,* следуя указаниям офицера, не ниже чина Совместного секретаря правительства Индии, специально уполномоченного на это от имени распоряжения центрального правительства
- Любое физическое лицо, агентство или организация, которая собирает номер AADHAAR, или любой документ, содержащий номер AADHAAR, должны: (a) собирать, хранить и использовать номер AADHAAR в законных целях; (b) информировать владельца номера AADHAAR о цели, для которой собирается информация, является ли предоставление номера AADHAAR или его подтверждение для этой цели обязательным или добровольным, (с предоставлением обязывающего правового положения, при необходимости, альтернативами представлению номера AADHAAR или документа, содержащего номер AADHAAR, если таковые имеются; (c) получить согласие владельца номера AADHAAR на сбор, хранение и использование его номера AADHAAR для указанных целей. Такое физическое лицо, агентство или организация не должны использовать номер AADHAAR для каких-либо целей, кроме тех, которые указаны держателю номера Aadhaar в момент получения его согласия, и не должны делиться номером AADHAAR с любым лицом без согласия владельца номера AADHAAR (раздел 5 «Sharing Regulation 2016»)[IV, с. 32-33]
- Защита данных AADHAAR оставляет желать лучшего. Известны случаи оформления номеров AADHAAR на другое имя, на несуществующих лиц, даже богов и домашних животных[V]

ЮАР

- Section 14 of the Constitution of the Republic of South Africa (1996) (право на неприкосновенность частной жизни включает право на «тайну переписки» - защиту от незаконного сбора, хранения, распространения и использования личной информации)[6]
- Protection of Personal Information Act (2013)[7]

ЮАР

Особенности законодательства о персональных данных

- Чрезвычайно расширенная трактовка понятия «персональные данные»: помимо традиционного содержания оно содержит информацию о сексуальных предпочтениях, беременности, психическом здоровье, а также мнения о человеке, принадлежащие другим людям
- Виды информации, обычно относимые к Big Data (IP- и MAC-адреса, информация о местоположении, онлайн-идентификаторы), специальным образом не выделяются из персональных данных
- Субъект данных имеет право установить, владеет ли ответственная сторона личной информацией данного субъекта данных, и запросить доступ к своей личной информации, запрашивать, при необходимости, исправление, уничтожение или удаление личной информации, на разумных основаниях возражать против обработки своей личной информации
- Особый порядок обработки персональных данных для журналистских, литературных или художественных целей

Казахстан

- Закон РК № 94-V «О персональных данных и их защите» от от 21 мая 2013 года (с изменениями и дополнениями по состоянию на 28 декабря 2017 г.)[8]
- Проект Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» от 11 октября 2018[9]

Казахстан

Особенности законодательства о персональных данных

- Закон о персональных данных, несмотря на то, что содержит понятия «биометрические данные», «обезличенные данные»[8], не содержит понятия «большие данные» (Big Data)
- Права субъекта данных в отношении собственных персональных данных чётко не прописаны (отсутствует соответствующая статья, присутствующая в законодательстве о персональных данных других стран)
- Субъект или его законный представитель ***не может отозвать согласие на сбор, обработку персональных данных*** в случаях, если это противоречит законам Республики Казахстан, либо при наличии неисполненного обязательства.
- ***Допускается сбор и обработка персональных данных без согласия субъекта*** при реализации международных договоров, ратифицированных Республикой Казахстан
- Субъект данных не может требовать уничтожения данных о себе
- Основная цель работы с большими данными – это ***получение на их основании ценных аналитических выводов для практического применения***[9]
- Признается необходимым построение единой справочной системы с обязательным хранением всей исторической информации государственных органов, кроме того, деперсонализация данных для использования в системах и сервисах, не принадлежащих государственным органам[9]

Кыргызстан

- Закон КР «Об информации персонального характера» от 14 апреля 2008 года № 58 (в редакции Закона КР от 20 июля 2017 года № 129)[10]
  - Весьма широкое определение термина «персональные данные» («информация персонального характера»), допускающее вольную интерпретацию
  - Анонимизированные данные не упоминаются
  - «Большие данные» как таковые также не упомянуты; информация, относимая к Big Data, по факту включена в состав персональных данных

Таджикистан

- Закон РТ «О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ» (принят Постановлением МН МОРТ от 8 июня 2018 года, No1115, одобрен Постановлением ММ МОРТ от 2 августа 2018 года, No561)[11]
  - Упомянуты (даются определения) «биометрические данные», «обезличенные данные»
  - Big Data как таковые в тексте закона отдельно не упоминаются
  - Для сбора персональных данных согласие субъекта данных ***не требуется***

Узбекистан

- Проект Закона «О персональных данных» (планируемый срок вступления в законную силу 1 января 2019 г.)[12]
  - Упомянуты (даются определения) «биометрические данные», «обезличенные данные»
  - Big Data как таковые в тексте закона отдельно не упоминаются
  - Субъект в течение десяти рабочих дней со дня включения его персональных данных в базу персональных данных ***должен быть уведомлен о его правах***, определенных настоящим Законом, цели сбора данных и третьих лицах, которым передаются его персональные данные, исключительно в письменной форме; Уведомление не производится, если персональные данные собираются из общедоступных источников
  - ***Допускается платный доступ третьих лиц*** к базе персональных данных

Пакистан

- National Database and Registration Authority (NADRA)[VI] — одна из крупнейших в мире баз мультибиометрических данных (121 млн фотографий и 503 млн отпечатков пальцев на середину 2015 года)[VII]. Закон о NADRA был принят в 2000 году (The National Database and Registration Authority Ordinance, 2000)[13]
- По своим функциональным возможностям и назначению NADRA в целом соответствует индийской UIDAI, однако ее возможности несколько шире (например, NADRA может обрабатывать информацию о движущихся объектах в режиме реального времени)
- Идентификационный номер NADRA необходим при открытии банковских счетов и получении пособий и субсидий
- NADRA — коммерческая структура, функционирующая на принципах самоокупаемости. Стоимость запроса на идентификацию личности составляет приблизительно $0.35
- Какие-либо механизмы влияния граждан на оборот личной информации законом ***не предусмотрены***

Необходимо ли особое законодательство для Big Data?

- В большинстве стран инициативы в области больших данных рассматриваются в соответствии с действующим законодательством в отношении персональных данных. Однако ***Big Data не вполне укладывается в текущие нормы законодательства о персональных данных***
- Новые концепции и парадигмы, такие как облачные вычисления или большие данные, не должны снижать или подрывать текущие уровни защиты данных как основного права человека и должны отвечать фундаментальные принципы права (законность, справедливость, соразмерность) и права субъектов данных
- Права людей на информационное самоопределение, а также прочие их права и законные интересы должны быть краеугольным камнем в современном информационном обществе
- Отчётливо видна тенденция использования Big Data для новых и неожиданных целей, которые могут ***противоречить принципу ограничения цели***. Большие данные, как правило, используют «все данные», что может ***противоречить принципу минимизации данных***
- В силу того, что результат статистической обработки больших данных может содержать информацию, неизвестную субъекту данных, но с большой долей вероятности релевантно отражающую особенности его личности, он ***не подпадает под определение «личной тайны»*** и, соответственно не может охраняться законодательством (в России это статья 23 Конституции РФ). Поэтому существующее определение «личной тайны» нуждается в пересмотре с учётом возможностей больших данных

Ссылки

- [1] - https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf
- [2] - http://www.law.hku.hk/cprivacy/archives/189
- [3] - http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm
- [4] - http://std.sacinfo.org.cn/gnoc/queryInfo?id=5765F72B812F670F1571443FF09C12D2
- [5] - Ministry of Communications and Information Technology, THE GAZETTE OF INDIA, EXTRAORDINARY, Part II, Section 3, Sub-section (i), 11 April 2011.
- [6] - https://www.gov.za/sites/default/files/images/a108-96.pdf
- [7] - http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf
- [8] - https://online.zakon.kz/Document/?doc_id=31396226#pos=3;-155
- [9] - https://legalacts.egov.kz/npa/view?id=1992299
- [10] - http://cbd.minjust.gov.kg/act/view/ru-ru/202269
- [11] - https://s2.siteapi.org/3d454be12a3d41d/docs/6gj8mt6118g04840owwosc40gwcs8o
- [12] - https://programms.gov.uz/ru/documents/2350
- [13] - http://nasirlawsite.com/laws/nadra.htm

Ссылки

- [I] - *Bart van der Sloot, Sascha van Schendel* International and comparative legal study on Big Data. WRR, The Hague, 2016. ISBN 978-94-90186-29-6
- [II] - https://www.insideprivacy.com/international/china/china-issues-new-personal-information-protection-standard/
- [III] - https://iapp.org/news/a/more-positive-progress-on-chinese-data-protection-regime-in-2019/
- [IV] - Data Protection & Privacy Issues in India. ECONOMIC. LAWS. PRACTICE. (https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf)
- [V] - https://www.huffingtonpost.in/2018/09/25/uidais-aadhaar-has-caused-many-problems-here-are-some-of-its-biggest-fails_a_23530870/
- [VI] - https://www.nadra.gov.pk/
- [VII] - http://www.cnews.ru/articles/bolshie_dannye_v_gossektore_opyt_pakistana