Организация Объединенных Наций A/72/540

Генеральная Ассамблея

Distr.: General
19 October 2017
Russian
Original: English

Семьдесят вторая сессия
Пункт 72(b) повестки дня
Поощрение и защита прав человека: вопросы прав человека, включая альтернативные подходы в деле содействия эффективному осуществлению прав человека и основных свобод

Право на неприкосновенность частной жизни*

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить Генеральной Ассамблее доклад Специального докладчика Совета по правам человека по вопросу о праве на неприкосновенность частной жизни г-на Джозефа А. Каннатачи, представленный в соответствии с резолюцией 28/16 Совета по правам человека.

* Настоящий доклад был представлен с опозданием в связи с необходимостью отразить в нем последние события.

17-18460 (R) 311017 021117

Доклад Специального докладчика Совета по правам человека по вопросу о праве на неприкосновенность частной жизни

Резюме

Настоящий доклад состоит из двух частей: в первой части содержится краткое деятельности, проведенной в 2016 и 2017 годах, а во второй части содержится промежуточный доклад о работе Целевой группы по вопросам использования больших объемов данных и открытых данных, которая была создана Специальным докладчиком по вопросу о праве на неприкосновенность частной жизни.

Содержание

Стр.

I. Обзор деятельности Специального докладчика по вопросу о праве на неприкосновенность частной жизни за период 2016–2017 годов . . . 3
A. Проект международно-правового документа по вопросам слежения и неприкосновенности частной жизни . . . 3
B. Письма с информацией о предполагаемых нарушениях . . . 4
C. Прочие письма: открытая информация; Япония . . . 5
D. Прочие осуществляемые инициативы, касающиеся слежения . . . 5
E. Более глубокое понимание концепции неприкосновенности частной жизни . . . 5
F. Целевая группа по вопросам конфиденциальности данных в сфере здравоохранения . . . 5
G. Использование корпорациями персональных данных . . . 5
H. Официальное посещение стран . . . 6
I. Обеспечение ресурсами . . . 6
II. Целевая группа по большим объемам данных и открытым данным . . . 6
A. Постановка вопросов . . . 7
B. Данные . . . 8
C. Большие объемы данных . . . 10
D. Углубленный анализ данных . . . 12
E. Алгоритмы . . . 13
F. Открытые данные . . . 18
G. Открытое правительство . . . 19
H. Комплексный характер больших данных . . . 20
I. Обзор нынешней ситуации: большие коммерческие данные и конфиденциальность . . . 23
J. Принципы на будущее: контроль за раскрытием данных . . . 26
III. Вспомогательная документация . . . 28
IV. Заключение . . . 29
V. Рекомендации . . . 29

I. Обзор деятельности Специального докладчика по вопросу о праве на неприкосновенность частной жизни за период 2016–2017 годов

1. Период 2016–2017 годов был особенно активным в плане осуществления мандата Специального докладчика, включая взаимодействие с гражданским обществом, правительствами, правоохранительными органами, разведывательными службами, управлениями по защите данных, разведывательными надзорными органами, академическими кругами, корпорациями и другими заинтересованными сторонами в рамках 26 мероприятий, проведенных в 15 странах на четырех континентах. В ходе этих мероприятий Специальный докладчик посетил более 30 различных городов — некоторые в Азии, Северной Африке и Центральной Америке, при этом 25 процентов мероприятий проводились в Соединенных Штатах Америки и более 50 процентов — в Европе.

A. Проект международно-правового документа по вопросам слежения и неприкосновенности частной жизни

2. Темы безопасности и слежения приобрели большое значение, в связи с чем Совет по правам человека Организации Объединенных Наций в 2015 году учредил мандата Специального докладчика по вопросу о праве на неприкосновенность частной жизни.

3. В мандате Специального докладчика по вопросу о праве на неприкосновенность частной жизни, изложенном в резолюции 28/16 Совета по правам человека, четко определена следующая обязанность: «выявлять возможные трудности, препятствующие поощрению и защите права на неприкосновенность частной жизни, выявлять и поощрять принципы и эффективную практику на национальном, региональном и международном уровнях и обмениваться ими, а также представлять в этой связи Совету по правам человека предложения и рекомендации, в том числе в отношении особых проблем, возникающих в цифровой век»[1].

4. В качестве одного из серьезных препятствий для защиты права на неприкосновенность частной жизни Специальный докладчик определил вакуум, существующий в международном праве в том, что касается слежения и неприкосновенности частной жизни в киберпространстве, что является самой сутью опубликованных Сноуденом разоблачений, и в настоящее время именно этот вопрос является предметом основной обеспокоенности Специального докладчика. Специальный докладчик считает, что не только отсутствие ключевых правовых норм препятствует укреплению и защите права на неприкосновенность частной жизни, но и отсутствие надлежащих механизмов[2].

5. В рамках своего мандата Специальный докладчик намерен настойчиво рекомендовать Совету по правам человека поддержать обсуждение и принятие в рамках Организации Объединенных Наций правового документа для достижения двух основных целей:

a) представления государствам-членам комплекса принципов и типовых положений, которые можно было бы включить в их национальное законо-

[1] A/70/53, раздел III, часть A, резолюция 28/16, пункт 4(c).

[2] Доклад Специального докладчика по вопросу о праве на неприкосновенность частной жизни в Совете по правам человека Организации Объединенных Наций, март 2017 года (предварительный неотредактированный вариант имеется онлайн, см. A/HRC/34/60).

дательство и которые закрепляли бы и обеспечивали бы соблюдение ими высших принципов в области прав человека и, в особенности, права на неприкосновенность частной жизни, когда речь идет о слежении;

b) представления государствам-членам ряда вариантов, способствующих устранению пробелов и заполнению вакуума в области международного права, в частности в связи с правом на неприкосновенность частной жизни в киберпространстве.

6. Хотя потребность в таком правовом документе очевидна, четкого представления о сфере его охвата и о его формате еще нет. Представление об основных положениях этого документа становится более конкретным благодаря текущим исследованиям и консультациям с заинтересованными сторонами, однако наилучший способ достижения указанных целей еще только предстоит определить.

7. Давно признано, что одной из немногих областей, в которых право на неприкосновенность частной жизни не может быть абсолютным, является обнаружение, предупреждение и расследование преступлений и преследование виновных, а также сфера национальной безопасности. Вместе с тем для сохранения демократии необходима система сдержек и противовесов, которая бы обеспечивала, чтобы любое слежение предпринималось исключительно для защиты свободного общества. Предварительное разрешение на слежение и последующий надзор за такой деятельностью являются ключевыми элементами правил, гарантий и средств правовой защиты, которые необходимы демократическому обществу для сохранения определяющих его свобод.

8. В датируемом мартом 2017 года вышеупомянутом докладе Специального докладчика Совету по правам человека содержатся промежуточные выводы, касающиеся правового документа, регулирующего слежение в киберпространстве и дополняющего уже существующие правовые нормы по киберпространству — например, Конвенцию о киберпреступности (Будапештская конвенция), принятую Комитетом министров Совета Европы в 2001 году. Варианты правового документа, регулирующего слежение в киберпространстве, также изучаются в рамках ранее разработанной при поддержке Европейского союза инициативы по альтернативным методам, касающимся неприкосновенности частной жизни, частной собственности и регулирования Интернета (МАППИНГ). Проект текста, который сейчас обсуждается представителями гражданского общества и международных корпораций, будет обнародован к весне 2018 года.

9. Этот процесс подробно описан во вспомогательном документе V[3].

B. Письма с информацией о предполагаемых нарушениях

10. Некоторые письма, направленные Специальным докладчиком правительствам в связи с предполагаемыми нарушениями, касающимися слежения, будут опубликованы Управлением Верховного комиссара по правам человека (УВКПЧ) вместе с докладами о сообщениях мандатариев специальных процедур.

[3] См. www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

C. Прочие письма: открытая информация; Япония

11. 18 мая 2017 года Специальный докладчик опубликовал письмо в адрес правительства Японии (см. вспомогательный документ III)[4]. В этом письме Специальный докладчик выразил обеспокоенность в связи с несовершенством предлагаемого законодательства, которое позволяет вести слежение без соблюдения необходимых гарантий и цель которого якобы заключается в том, чтобы позволить Японии ратифицировать принятую в 2000 году Конвенцию Организации Объединенных Наций против транснациональной организованной преступности. По-прежнему предпринимаются попытки наладить взаимодействие по этому вопросу, и информация об этом будет отражена в докладе Специального докладчика Совету по правам человека в марте 2018 года.

D. Прочие осуществляемые инициативы, касающиеся слежения

12. В рамках мандата идет изучение и других инициатив, касающихся слежения, безопасности и неприкосновенности частной жизни. Если это будет сочтено уместным, позже будет опубликована более подробная информация.

E. Более глубокое понимание концепции неприкосновенности частной жизни

13. Специальный докладчик анализирует неприкосновенность частной жизни в том числе как неотъемлемое право, обеспечивающее осуществление всеохватывающего и основополагающего права на свободное и беспрепятственное развитие личности. Председатель Целевой группы по вопросам неприкосновенности частной жизни и развитию личности Элизабет Кумз, бывший уполномоченный по вопросам неприкосновенности частной жизни (Новый Южный Уэльс, Австралия), любезно согласилась взять на себя эту функцию, с уделением особого внимания гендерным вопросам и вопросам неприкосновенности частной жизни.

14. Более подробная информация о деятельности Целевой группы представлена во вспомогательном документе IV[5].

F. Целевая группа по вопросам конфиденциальности данных в сфере здравоохранения

15. Целевая группа Специального докладчика по вопросам конфиденциальности данных в сфере здравоохранения приступила к работе под руководством д-ра Стива Стеффенсена (Соединенные Штаты). Консультации должны пройти весной и летом 2018 года.

G. Использование корпорациями персональных данных

16. Специальный докладчик продолжает изучать бизнес-модели, касающиеся неприкосновенности частной жизни в контексте использования корпорациями персональных данных; эту работу он ведет как самостоятельно, так и в рамках проекта МАППИНГ в преддверии создания Целевой группы Специального до-

[4] См. www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.
[5] См. www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

кладчика по данному вопросу в сроки, о которых было объявлено на веб-сайте Специального докладчика (https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx).

H. Официальное посещение стран

17. Были осуществлены или планируются следующие поездки в страны: Соединенные Штаты Америки (с 19 по 28 июня 2017 года)[6], Франция (подтвержденные сроки — с 13 по 17 ноября 2017 года); Соединенное Королевство Великобритании и Северной Ирландии (подтвержденные сроки — с 11 по 17 декабря 2017 года); Германия (подтвержденные сроки — с 29 января по 2 февраля 2018 года); и Республика Корея (подтвержденные сроки — с 3 по 15 июля 2018 года).

I. Обеспечение ресурсами

18. Из бюджета, выделенного на выполнение Специальным докладчиком своего мандата и находящегося в ведении УВКПЧ, финансировались только официальный визит в Соединенные Штаты и поездка Специального докладчика и других выступающих в Гонконг, Китай, где проходили Международная конференция комиссаров по вопросам защиты данных и неприкосновенности частной жизни и дискуссии по вопросам неприкосновенности частной жизни, развития личности и информационных потоков в Азии. Остальные поездки финансировались из внешних источников, главным образом организаторами соответствующих мероприятий.

II. Целевая группа по большим объемам данных и открытым данным

19. Учрежденную Специальным докладчиком Целевую группу по большим объемам данных и открытым данным возглавляет Дэвид Уоттс[7]. Ведущие авторы настоящего доклада — Дэвид Уоттс и Ванесса Тиг[8]. К членам Целевой группы, многие из которых также внесли свой вклад в подготовку текста доклада, относятся Кристиан д'Кунья (Уполномоченный Европейского союза по защите данных), Алекс Хаббард (Управление комиссара Соединенного Королевства по вопросам информации), профессор Вольфганг Нейдль (Ганноверский университет, Германия), Марти Эбрамс (Фонд по вопросам ответственного использования информации, Соединенные Штаты Америки) и Мари Жорж (Франция). Также в подготовку доклада внесли свой вклад Шон МакЛафлан, Элизабет Кумз и Джоу Каннатачи.

[6] Заключительный доклад в связи с официальным визитом в США будет опубликован приблизительно весной 2018 года. С заявлением, сделанным по итогам этого визита, можно ознакомиться на сайте www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx.

[7] Дэвид Уоттс, адъюнкт-профессор права в университетах Ла Троба и Дикина. До 31 августа 2017 года он занимал должность комиссара по вопросам неприкосновенности частной жизни и защите данных в штате Виктория, Австралия.

[8] Ванесса Тиг, старший лектор на кафедре компьютерных и информационных систем в Мельбурнском университете, Австралия.

20. С более подробной информацией о процессе подготовки доклада по большим объемам данных и открытым данным можно ознакомиться во вспомогательном документе VII[9].

A. Постановка вопросов

21. Одна из наиболее трудных задач, стоящих перед информационными обществами в XXI веке, заключается в нахождении баланса между общественными благами, предоставляемыми новыми информационно-коммуникационными технологиями, и защитой основополагающих прав, таких как право на неприкосновенность частной жизни. Эти новые технологии могут помогать государствам в обеспечении соблюдения и выполнения их обязательств в области прав человека, но в то же время могут подрывать осуществление некоторых прав человека, в частности права на неприкосновенность частной жизни.

22. Новые методы сбора и анализа данных — явление «больших объемов данных» — и растущее желание правительств во всем мире публиковать личную информацию, которой они располагают, пусть даже в обезличенном формате, с тем чтобы стимулировать экономический рост и научную исследовательскую деятельность, — явление «открытых данных» — ставят под вопрос многие предположения, лежащие в основе нашего понятия о том, что такое неприкосновенность частной жизни, что она под собой подразумевает и как эффективнее всего ее защищать.

23. С учетом того, что Совет по правам человека признал право на неприкосновенность частной жизни в качестве императивного права, обеспечение которого крайне важно в контексте соблюдения права на достойную жизнь и свободное и беспрепятственное развитие личности (см. резолюцию 34/7 Совета по правам человека от 23 марта 2017 года), проблемы, связанные с большими объемами данных и открытыми данными, приобретают все большие масштабы.

24. Некоторые заявления относительно больших объемов данных и открытых данных называют «утопическими»[10]. В таких заявлениях утверждается, что большие объемы данных открывают возможности для получения уникальной информации о трудноразрешимых вопросах в сфере государственной политики, таких, как изменение климата, угроза терроризма и общественное здравоохранение. С другой стороны, есть те, кто придерживается антиутопической точки зрения и обеспокоен расширением масштабов слежения со стороны государственных и негосударственных субъектов, неоправданным вторжением в частную сферу жизни и ослаблением механизмов защиты неприкосновенности частной жизни.

25. Одна из основных трудностей, возникших при подготовке настоящего доклада, заключалась в том, чтобы разобраться в заявлениях этих и других заинтересованных сторон, участвующих в непростых обсуждениях вопросов о больших объемах данных и открытых данных, а также оценить заявления различных заинтересованных сторон. Хотя оба вопроса породили значительный объем комментариев и научных исследований, наше понимание технологий и последствий их дальнейшего применения остается неполным: как ни парадок-

[9] См. www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

[10] Danah Boyd and Kate Crawford, “Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon”, *Information, Communication and Society*, vol. 15, No. 5.

сально, такое отсутствие данных затрудняет наше понимание потенциальных благ и возможного ущерба, связанных с большими объемами данных и открытыми данными.

B. Данные

26. Каждый день в результате нашей цифровой деятельности накапливается около 2,5 квинтлн байтов данных[11]. Речь идет о таком количестве байтов данных, при котором за числом 2,5 следует 18 нулей[12]. Для сравнения: в романе среднего объема в триста страниц количество байтов данных таково, что за числом 3 следует пять нулей. Девяносто процентов всего мирового объема данных было накоплено за последние два года[13], и скорость, с которой идет накопление этих данных, продолжает увеличиваться.

27. В условиях нынешней глобальной взаимосвязанности генерация данных — это распространенное и повсеместное явление. Всякий раз, когда мы пользуемся компьютером, смартфоном или даже повседневными устройствами, в которые встроены датчики, способные записывать информацию, в качестве побочного продукта генерируются данные. Они принимают форму знаков или символов, которые в конечном счете перекодируются вычислительными устройствами в двоичный код, который затем обрабатывается, сохраняется и передается в качестве электронных сигналов.

28. Источники данных в контексте больших объемов данных столь же разнообразны, как и деятельность, осуществляемая в сети Интернет:

> «Данные поступают из многочисленных и различных источников, в том числе из приборов для научных исследований, медицинских приборов, телескопов, микроскопов, спутников; цифровых средств массовой информации, в том числе текстовых, видео- и аудиозаписей, электронной почты, Интернет-блогов, «Твиттера», коллекций изображений, посещаемых сайтов и финансовых операций; динамических сенсорных, социальных и иных видов сетей; научных симулирующих приборов, моделей и исследований; или компьютерного анализа данных наблюдений. Данные могут иметь временной, пространственный или динамический характер; быть структурированными и неструктурированными; информация и знания, получаемые из данных, могут различаться в плане представленности, сложности, степени детализации, контекста, происхождения, достоверности, надежности и охвата. Также может различаться скорость, с которой происходит генерация данных и с которой к ним можно получить доступ»[14].

29. Некоторые из получаемых данных не связаны с частными лицами. Это данные, полученные в результате такой деятельности, как анализ погодных условий, исследование космоса, научные испытания материалов или структур или анализ рисков, связанных с ценными бумагами на финансовых рынках. Вместе с тем значительная часть данных создается либо нами самими, либо о нас. Основное внимание в этом докладе уделяется именно этой категории дан-

[11] См. https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

[12] Это шкала, которая используется в Соединенных Штатах. В Соединенном Королевстве Великобритании и Северной Ирландии используется другая шкала, по которой в данном случае за числом 1 следует 30 нулей.

[13] См. www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

[14] United States, National Science Foundation, Critical techniques and technologies for advancing big data science and engineering (BIGDATA)", Program Solicitation NSF 14-543, URL: https://www.nsf.gov/pubs/2014/nsf14543/nsf14543.pdf at p3.

ных — персональной информации, будь то в контексте ее представления, изучения, получения или выведения на ее основе заключений[15].

30. Личные данные отражают нашу индивидуальность. Именно эта возможность установления личности любого человека обуславливает такую ценность информации личного характера.

31. Данные, которые мы создаем сами, связаны с нашей собственной деятельностью. К ним относятся сообщения электронной почты и текстовые сообщения, а также изображения и видеоматериалы, которые мы создаем и распространяем. Другой тип данных о нас создается третьими сторонами, но при таких обстоятельствах, при которых в их генерации были задействованы — по крайней мере в какой-то степени — мы сами, например в случае создания электронных медицинских карт или осуществления электронной торговли.

32. Вместе с тем остальные данные о нас создаются не совсем очевидным образом, поскольку речь идет о закулисном процессе, проводимом в условиях, которые нам неясны, в значительной степени неизвестны и не могут быть известны. Этот процесс включает в себя понятие «цифровых хлебных шек»[16] — «электронных артефактов» и других «электронных следов», которые мы оставляем за собой в качестве продукта нашей деятельности в Интернете и в реальной жизни. Такие данные могут включать в себя информацию о времени и месте подключения наших мобильных устройств к вышкам сотовой связи или спутникам Глобальной системы определения координат (GPS), информацию о посещаемых нами веб-сайтах или изображения, полученные при помощи цифровых систем видеонаблюдения. Эти «цифровые хлебные крошки», которые мы оставляем после себя и которые, по всей вероятности, навечно останутся на компьютерных серверах, помогают распознать нас и узнать, чем мы занимаемся и чего хотим. Таким образом, персональные данные — данные о частных лицах — становятся чрезвычайно ценными как в контексте общественных благ, так и для частных компаний»[17].

33. В мире, захлестнутом данными и охваченном процессами электронной обработки данных и мгновенной цифровой связи, возникают вопросы относительно обеспечения прав на неприкосновенность частной жизни ввиду новых технологий, которые позволяют собирать, обрабатывать и анализировать личную информацию таким образом, который был немыслим в то время, когда разрабатывались Всеобщая декларация прав человека 1948 года и Международный пакт о гражданских и политических правах 1966 года.

34. В результате повсеместного использования компьютера практически все аспекты мира приобретают новое символическое измерение на фоне того, как события, объекты, процессы и сами люди становятся заметными и узнаваемыми, а информация о них передается другим лицам. Мир переживает второе рождение в условиях, когда данные и электронные сообщения становятся универсальными как по своим масштабам, так и по своему охвату[18].

35. То, каким образом информационно-коммуникационные технологии позволяют частным лицам становиться узнаваемыми за счет анализа их данных,

[15] Martin Abrams, “The origins of personal data and its implications for governance”, URL: http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf.

[16] Evan Schwartz, ”Finding our way with digital bread crumbs”, *MIT Technology Review*, 18 August 2010. URL: https://www.technologyreview.com/s/420277/finding-our-way-with-digital-bread-crumbs/.

[17] Julie Lane and others, eds., *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (New York, Cambridge University Press, 2014).

[18] Shoshana Zuboff, “Big other: surveillance capitalism and the prospects of an information civilization”, *Journal of Information Technology*, vol. 30, No. 1 (March 2015).

предполагает, в частности, «восприятие природы того или иного человека исключительно на основе информации об этом человеке»[19]. Явление, которое способствует этому, широко известно под названием «большие объемы данных».

C. Большие объемы данных

36. Термин «большие объемы данных» обычно используется для описания большого и увеличивающегося объема данных и методов углубленного анализа, применяемых в контексте поиска, сопоставления, анализа этих данных и выведения заключений на их основе.

37. Общепринятого определения термина «большие объемы данных» нет. Национальный институт стандартов и технологии Соединенных Штатов описывает это явление как неспособность традиционных систем данных эффективно обрабатывать новые массивы данных. К характеристикам «больших объемов данных», которые способствуют возникновению новых структур данных, относятся:

a) объем (т. е. размер массива данных);

b) разнообразие (т. е. данные, полученные из различных хранилищ и областей, или разные типы данных);

c) скорость (т. е. скорость потока данных);

d) изменчивость (т. е. изменения других характеристик).

38. Эти характеристики — объем, разнообразие, скорость и изменчивость — известны в просторечье как “Vs” (от англ. Volume, Variety, Velocity, Variability) «больших объемов данных»[20].

39. Описание, предложенное Национальным институтом, а также многочисленные другие попытки дать определение такому явлению, как «большие объемы данных», например заявление Европейского союза, согласно которому «термин “большие объемы данных”[21] относится к крупным массивам данных, которые весьма быстро генерируются большим числом различных источников», обращают внимание на совокупность технологий, позволяющих превратить сбор, обработку и анализ больших объемов данных в повседневную реальность. Вместе с тем высокий уровень обобщения, свойственный этим определениям, а также преимущественный акцент в них на технологиях не позволяют адекватно объяснить явление «больших объемов данных».

40. Ряд экспертов предприняли попытку сформулировать исчерпывающее определение «больших объемов данных», которое не ограничивается лишь четырьмя “V”. Ценным и более подробным определением понятия «больших объемов данных» является следующее:

a) это данные большого объема, которые состоят из терабайтов и петабайтов информации;

b) они передаются на высоких скоростях и генерируются в реальном или близком к реальному времени;

---

[19] Luciano Floridi, “Four challenges for a theory of informational privacy”, *Ethics and Information Technology*, vol. 8, No. 3 (July 2006).

[20] Им приписывают и другие характеристики, но эти четыре являются ключевыми. См. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1.pdf.

[21] См. https://ec.europa.eu/digital-single-market/en/policies/big-data.

c) отличаются разнообразием и обладают структурированным и неструктурированным характером;

d) являются исчерпывающими по своему масштабу, пытаясь охватить все население или системы;

e) это данные высокого разрешения, которым присвоен уникальный индекс идентификации;

f) это данные, относительные по своей природе и обладающие общими характеристиками, которые позволяют объединять различные массивы данных;

g) это данные гибкой структуры, которые позволяют с легкостью добавлять новые характеристики и быстро расширять масштабы[22].

41. Не всегда в каждом конкретном случае большие объемы данных обладают всеми этими характеристиками.

42. В рамках других подходов большие объемы данных представляются как нечто большее, нежели технологическое явление:

> «Мы определяем “большие объемы данных” как культурное, технологическое и научное явления, которое обусловлено взаимодействием:
>
> a) технологии — достижение максимальной мощности в расчетах и точности алгоритмов для сбора, анализа, увязки и сопоставления больших массивов данных;
>
> b) анализа — использование больших массивов данных для выявления тенденций, с тем чтобы формулировать выводы в экономической, социальной, технической и юридической сферах;
>
> c) мифологии — широко распространенное мнение о том, что большие массивы данных способствуют развитию более высокого уровня интеллекта и знаний, за счет чего могут генерироваться ранее немыслимые идеи, которые приобретают ореол правдивости, объективности и точности»[23].

43. Один из основных доводов сторонников использования больших объемов данных заключается в том, что такие данные могут устранить ограничения в области исследований, вызванные отсутствием эмпирических данных, т. е. нехваткой данных, и представить нам объективную истину относительно каких-либо обстоятельств или явлений. Эти теоретические доводы, в которых, как правило, большие объемы данных возводятся в ранг некой новой формы научного метода, являются основным предметом обеспокоенности, выражаемой многими лицами по поводу ограничений и рисков, связанных с большими объемами данных.

44. Существует широкий консенсус в отношении того, что большие объемы данных могут создавать общественные блага, включая предоставление индивидуализированных услуг, расширение доступа к услугам, улучшение состояния здоровья людей, технологический прогресс и облегчение доступа[24]. Евро-

[22] Rob Kitchin, “Big data, new epistemologies and paradigm shifts”, *Big Data and Society*, vol. 1, No. 1 (April–June 2014).

[23] Boyd and Crawford, “Critical questions for big data”.

[24] Вместе с тем существуют и противоположные взгляды. Например, в заявлении Рабочей группы Европейского союза по защите данных, сделанном 16 сентября 2014 года в соответствии со статьей 29 относительно последствий генерации больших объемов данных для защиты частных лиц в контексте обработки персональных данных в Европейском Союзе, говорится: «Несмотря на то, что реальная ценность больших объемов данных еще не доказана, согласно прогнозам, их производство приведет к созданию

пейская комиссия заявляет, что «необходимость разобраться с понятием «больших объемов данных» способствует инновациям в технологической сфере, разработке новых инструментов и развитию новых навыков»[25].

45. Европейская комиссия рассматривает информацию как один из экономических активов, являющихся столь же важным для общества, как труд и капитал[26]. Важно отметить, что на этом рынке доминирует небольшое число крупных технологических фирм, удельный вес продукции которых на рынке зависит от использования данных.

D. Углубленный анализ данных

46. Важнейшим изменением стало масштабное использование данных для выработки алгоритмов, поведение которых зависит от данных, к которым они получают доступ.

> «Термин «машинное обучение» подразумевает автоматическое выявление в данных значимых закономерностей. За несколько десятилетий машинное обучение стало общепринятым методом, применяемым в контексте практически любой задачи, которая требует извлечения информации из больших массивов данных.
>
> Одной характерной чертой использования алгоритмов является то, что — в отличие от более традиционных компьютерных методов — в этих случаях, в силу сложности выявляемых закономерностей, программист не может дать четких и пошаговых инструкций для выполнения таких задач... Инструменты машинного обучения наделяют программы способностью самообучаться и адаптироваться»[27].

47. Основным различием между современными и прежними методами является автономный и полуавтономный характер новых методов.

48. Одним из наиболее широко используемых аналитических методов является «интеллектуальный анализ данных». Это процесс, в рамках которого из крупных массивов данных извлекаются данные, которые затем анализируются на предмет наличия каких-либо закономерностей или корреляции. Интеллектуальный анализ данных способствует упрощению и обобщению большого объема необработанных данных[28] и позволяет получать знания на основе выявленных закономерностей.

49. В основе таких методов и инструментов лежит алгоритм.

многочисленных индивидуальных и коллективных благ. Разумеется, Рабочая группа будет поддерживать на уровне Европейского Союза и национальном уровне действенные усилия, которые направлены на получение жителями Европейского Союза — будь то в индивидуальном или коллективном порядке — этих благ». См. https://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf .

[25] См. https://ec.europa.eu/digital-single-market/en/making-big-data-work-europe.

[26] Ibid.

[27] Shai Shalev-Shwartz and Shai Ben-David, *Understanding Machine Learning* (New York, Cambridge University Press, 2014).

[28] Данные, которые относятся только к одному лицу.

E. Алгоритмы

50. Алгоритмы — изобретение отнюдь не новое. Они «существовали испокон веков, задолго до того, как для них был придуман специальный термин»[29].

51. Применение алгоритмов не ограничивается лишь сферой математики… Жители Вавилона использовали их для принятия решений по вопросам права, преподаватели латыни использовали их для проверки грамматики; кроме того, алгоритмы применялись и до сих пор применяются во всех культурах для прогнозирования будущего, при принятии решений относительно того или иного курса лечения или при приготовлении пищи. Сегодня каждый из нас использует тот или иной вид алгоритмов, причем зачастую это происходит неосознанно — будь то при приготовлении пищи по рецепту или при воспроизведении рисунка в процессе вязания, или в процессе использования домашней бытовой техники[30].

52. Как и в случае с другими элементами больших объемов данных, «крайне сложно подобрать точное определение алгоритму»[31]. Для целей настоящего доклада выбрано следующее удобное рабочее определение:

> «... конкретный набор инструкций для выполнения какой-либо процедуры или решения какой-либо проблемы, как правило, с требованием прекращения данной процедуры в тот или иной момент. Конкретные алгоритмы именуются также методом, процедурой или приемом… Процесс применения алгоритма к исходным данным данных в целях получения некоего результата называется вычислением»[32].

53. Алгоритм, используемый для выпечки пирога, отличается от алгоритма, оценивающего кредитоспособность какого-либо лица, только степенью автоматизации, своим автономным и нелинейным характером и объемом обрабатываемых данных.

54. Все чаще наше понимание нас самих и наше отношение к миру формируются через призму алгоритмов. Сегодня алгоритмы являются важнейшим элементом информационного общества, все чаще регулируя «проведение каких-либо операций, принятие решений и осуществление выбора, что раньше было уделом людей»[33], рекомендуя подходящих партнеров на сайтах знакомств[34], определяя оптимальный маршрут поездки[35] и оценивая нашу благонадежность при получении кредита[36]. Они используются для формирования «психологического портрета» — выявления личных качеств и особенностей поведения для составления персональных прогнозов, например относительно товаров или услуг, которые мы, возможно, будем склонны приобрести. Они определяют, каким образом следует толковать данные и какие действия следует

[29] Jean-Luc Chabert, ed., *A History of Algorithms: From the Pebble to the Microchip* (Berlin, Springer-Verlag, Berlin, Heidelberg, 1999).

[30] Ibid.

[31] Felicitas Kraemer, Kees van Overveld and Martin Peterson, “Is there an ethics of algorithms?”, *Ethics and Information Technology*, vol. 13, No. 3 (September 2011).

[32] См. https://mathworld.wolfram.com/Algorithm.html.

[33] Brent Mittelstadt and others, “The ethics of algorithms: mapping the debate”, *Big Data and Society*, vol. 3, No. 2 (July–December 2016).

[34] См., например, Rebecca Harrington, “Dating services tinker with the algorithms of love”, *Scientific American*, 13 February 2015. URL: www.scientificamerican.com/article/dating-services-tinker-with-the-algorithms-of-love/.

[35] See, https://motherboard.vice.com/en_us/article/4x3pp9/the-simple-elegant-algorithm-that-makes-google-maps-possible.

[36] См. Michael Byrne, “The simple, elegant algorithm that makes Google Maps possible”, 22 March 2015. URL: http://mitsloan.mit.edu/media/Lo_ConsumerCreditRiskModels.pdf.

в результате предпринимать. Они «опосредствуют социальные процессы, коммерческие операции и правительственные решения, а также то, как мы воспринимаем и понимаем окружающую действительность, и как мы взаимодействуем друг с другом и с окружающим миром»[37].

55. С точки зрения неискушенного человека, рекомендации и решения, являющиеся результатом алгоритмической обработки, будто бы появляются из непроницаемого и неизвестного черного ящика — своего рода дельфийского оракула современности, который, как кажется, выступает с неоспоримыми и авторитетными пророчествами, не имеющими ничего общего с человеческой деятельностью. Понять действие различных механизмов алгоритмической обработки данных и, следовательно, оценить риски, которые с ними сопряжены, — явление непростое, и с этим связано множество вопросов, которые необходимо решить. Эти сложности подрывают нашу способность понять, каким образом функционируют алгоритмы и как они влияют на нашу жизнь.

56. Появляется все больше литературы, посвященной проблемам, которые могут быть вызваны алгоритмами, и призывающей проявлять осторожность, прежде чем устремляться в «алгоритмическое» будущее, не подумав о гарантиях, которые нам нужны для управления рисками.

1. В основе алгоритмов лежат ценностные суждения

57. Несмотря на заложенную в алгоритмы арифметическую структуру, которая придает им видимость объективности, в основе алгоритмов «в любом случае лежат ценностные суждения»[38]. Те ценности, которые они воплощают, часто отражают культурные или иные суждения инженеров программного обеспечения, которые разрабатывают алгоритмы и встраивают их в логическую структуру алгоритмов.

58. Например, алгоритм оценки кредитоспособности может быть разработан таким образом, чтобы выяснять место рождения того или иного человека, название школы, в которой он учился, и его статус занятости. Выбор этих косвенных показателей означает наличие в алгоритме оценочного суждения, согласно которому ответы на вышеперечисленные вопросы имеют отношение к оценке того, следует ли данному лицу предоставлять кредит и, если следует, то на каких условиях. В любом случае лицо, обращающееся за кредитом, зачастую не имеет возможности узнать причину принятия конкретного решения по кредиту и не может определить, какие оценочные суждения были заложены в алгоритм.

59. Хотя в ряде обществ эти косвенные показатели и могут иметь отношение к оценке кредитоспособности, в других обществах они окажутся в лучшем случае бесполезными отвлекающими факторами, а в худшем — нанесут ущерб. Например, использование таких косвенных показателей в некоторых развивающихся странах, где значительная часть населения может не иметь постоянного адреса проживания, практически не иметь формального образования и заниматься индивидуальной трудовой деятельностью, навсегда лишило бы этих людей доступа к кредитам.

60. С другой стороны, алгоритмы, анализирующие нетрадиционные формы данных, могут показать, что лицо, не обладающее привычной кредитной исто-

[37] Mittelstadt and others, “The ethics of algorithms”.
[38] Ibid.

рией, тем не менее, может быть надежным кредитополучателем, что способствовало бы развитию человеческого потенциала[39].

2. Проблема несовершенства данных

61. «Сырьевым материалом» алгоритмов являются данные, однако не все данные отличаются точностью, необходимой полнотой, актуальностью и достоверностью[40]. Происхождение некоторых данных, например, налоговых отчетов, как правило, можно легко установить, однако точность самих данных может варьироваться от одного налогового органа к другому в пределах одного государства и между государствами. Другие данные могут быть заимствоваться из устаревших баз данных, которые никогда не чистились, или из незащищенных источников, или же из источников, в которые данные вводятся ненадлежащим образом и для которых характерны низкие стандарты учета данных.

62. Роль алгоритмов заключается в обработке данных, и поэтому им «свойственен тот же недостаток, что всем видам обработки данных, а именно: данные на выходе никогда не могут быть более качественными, чем вводные данные»[41]. Действует принцип «каковы исходные данные, таков и результат».

3. Выбор данных

63. Риск, связанный с выбором, данных аналогичен тому, о котором говорилось в пункте 62 выше. Точно так же как недостаток данных приводит к плохим результатам, выбор неподходящих или не имеющих отношения к делу данных приводит к результатам, которые могут быть ненадежными и/или вводить в заблуждение.

64. Значительное число процессов алгоритмической обработки предполагает формирование индуктивных суждений и выявление корреляции между явно разнородными наборами данных. В случае использования неподходящих данных любые вынесенные на их основе рекомендации или решения будут неверными.

4. Предвзятость, дискриминация и ухудшение невыгодного положения

65. Хотя некоторые эксперты и проводят различие между предвзятостью и дискриминацией[42], связанные с ними риски в контексте больших объемов данных достаточно схожи и поэтому обсуждаются в одном разделе.

66. Алгоритмы могут использоваться для формирования «психологического портрета», т. е. «определения корреляции и прогнозирования поведения лиц на уровне группы, пусть и таких групп (или характеристик), которые постоянно меняются и пересматриваются в результате используемого в алгоритмах принципа машинного обучения:

---

[39] United States, Federal Trade Commission, “Big data: a tool for inclusion or exclusion — understanding the issues” (2016). URL: www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

[40] Так, например, группы меньшинств, которые недостаточно представлены в конкретном массиве данных, могут впоследствии пострадать от принятых на основе этих данных решений и прогнозов.

[41] Mittelstadt and others, “The ethics of algorithms”.

[42] Предубеждением считается постоянное или неоднократное выражение конкретных предпочтений применительно к решениям, ценностям или убеждениям. Дискриминация является неблагоприятным и несоразмерным последствием принятия решений на основе алгоритмов.

> «В алгоритмах и с динамической, и со статической структурой данных восприятие того или иного лица зависит от его связей с другими лицами, а не от его реального поведения. Предпочтения того или иного лица структурируются в соответствии с информацией о данной группе. Формирование «психологического портрета» может непроизвольно воспроизвести факты, которые могут привести к дискриминации»[43].

67. Некоторые эксперты утверждают, что такие методы углубленного анализа, как формирование «психологического портрета», лишь ухудшат невыгодное положение. В качестве примера можно привести предсказуемое полицейское патрулирование, в основе которого лежит принцип использования статистических данных о преступности и алгоритмического анализа в целях прогнозирования очагов преступности и акцентирования на них внимания правоохранительных органов[44]. Поскольку такие очаги преступности подвергаются более активному полицейскому патрулированию и зачастую находятся в социально неблагополучных районах, а не в районах, где преобладают должностные преступления, более активное патрулирование, как правило, приводит к арестам и вынесению обвинительных приговоров именно в таких местах, что, в свою очередь, служит основанием для последующего отнесения таких криминогенных районов к числу криминогенных, вследствие чего возникает замкнутый круг. Таким образом, лица, и без того находящиеся в неблагоприятном положении, подвергаются еще более высокому риску ареста и наказания в соответствии с уголовным законодательством.

68. Возможное использование правительствами таких методов для того, чтобы контролировать и выбирать в качестве мишени определенные общины или причинять им иной ущерб, также вызывает обеспокоенность[45].

5. Ответственность и подотчетность

69. Ущерб, причиняемый в результате алгоритмической обработки данных, в целом обусловлен трудностями, связанными с обработкой большого объема разнородных массивов данных, а также с разработкой и применением используемых для обработки данных алгоритмов. Поскольку в этом процессе задействовано множество переменных факторов, определить, кто несет ответственность за причинение ущерба в том или ином случае, нелегко. Зачастую анализ больших объемов данных основывается на принципах обнаружения и исследования, а не тестирования конкретной гипотезы, в связи с чем на самом раннем этапе бывает трудно предсказать (а для физических лиц — сформулировать) конечную цель использования данных.

70. Алгоритмы отнюдь не всегда являются непрозрачными; технически на каждом этапе обработки существует возможность сохранения использованных данных и результатов применения алгоритма.

6. Факторы, ограничивающие неприкосновенность частной жизни

71. Организация экономического сотрудничества и развития (ОЭСР) опубликовала в 1980 году свои «Директивы в отношении охраны тайны и трансграничных потоков персональных данных»[46]. Восемь принципов, закрепленных в

[43] Mittelstadt and others, “The ethics of algorithms”.

[44] См., например, www.predpol.com/how-predpol-works/.

[45] Lee Rainie and Janna Anderson, “Code-dependent: pros and cons of the algorithm age”, Pew Research Center, 8 February 2017. URL: www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/.

[46] Organization for Economic Cooperation and Development (OECD), “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”. URL:

Директивах ОЭСР, а также аналогичные принципы, содержащиеся в принятой в 1981 году Советом Европы Конвенции о защите физических лиц при обработке персональных данных (Конвенция о защите данных) и в принятых в 1990 году Руководящих принципах регламентации компьютеризированных картотек, содержащих данные личного характера, принятых Генеральной Ассамблеей в ее резолюции 45/95 от 14 декабря 1990 года, легли в основу законов о неразглашении личной информации во всем мире.

72. Основополагающим принципом в Директивах ОЭСР и Конвенции о защите данных является принцип ограничения сбора информации, согласно которому личная информация должна собираться только законным и честным образом, только в тех случаях, когда это уместно, и с ведома и согласия соответствующего лица[47]. Принцип «указания цели» предусматривает объявление цели сбора личной информации на момент ее сбора и ограничение последующего использования этой информации вышеупомянутой целью или сопоставимой с нею целью, а также конкретизацию целей в случае внесения в них каких-либо изменений[48]. Принцип «ограничения применения» запрещает раскрытие личной информации для несопоставимых целей, за исключением тех случаев, когда на это дает согласие либо само лицо, либо соответствующий правовой орган[49]. Соблюдение принципа «качества данных» усложняется сбором огромного объема данных и требованием обрабатывать лишь те данные, которые являются достаточными, актуальными и неизбыточными. Руководящие принципы регламентации компьютеризированных картотек, содержащих данные личного характера, принятые Организацией Объединенных Наций в 1990 году, содержат принцип соразмерности, применяемый при хранении данных для целей обработки данных.

73. Большие объемы затрудняют осуществление этих принципов, и в то же время порождают этические проблемы и социальные дилеммы, связанные с недостаточно продуманным применением алгоритмов. Вместо того чтобы способствовать решению вопросов государственной политики, использование больших объемов данных может иметь непредвиденные последствия, подрывающие такие права человека, как свобода от всех форм дискриминации, в том числе в отношении женщин, инвалидов и других лиц.

74. В то же время появляются признаки изменения парадигмы мышления, используемой при разработке алгоритмов, что позволяет улучшить алгоритмические решения для алгоритмов, предназначенных для обработки больших объемов данных. В качестве примера здесь можно привести инициативу Ассоциации по стандартам при Институте инженеров по электронике и радиоэлектронике, касающуюся разработки алгоритмов в соответствии с этическими принципами[50].

75. Что касается частной жизни, то в соответствующих международных документах значение права на неприкосновенность частной жизни шире значения прав на неразглашение личной информации, которые находятся в центре внимания принципов, закрепленных в Директивах ОЭСР и Конвенции о защи-

---

www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[47] См. Принципы ОЭСР, касающиеся обеспечения конфиденциальности. URL: http://oecdprivacy.org/.

[48] Там же.

[49] Там же.

[50] Institute of Electrical and Electronics Engineers (IEEE), IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems, *Ethically Aligned Design: A Vision for Prioritizing Wellbeing with Artificial Intelligence and Autonomous Systems*, ver. 1 (IEEE Press, 2016). URL: http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf.

те данных. С учетом признания права на неприкосновенность частной жизни в качестве императивного права, имеющего большое значение для осуществления других прав человека, а также в качестве права, тесно связанного с понятиями человеческого достоинства и свободного и беспрепятственного развития личности (см. резолюцию 34/7 Совета по правам человека, угроза, которую большие объемы данных представляют для неприкосновенности частной жизни, затрагивает и многие другие права человека. Тенденция «вторжения» больших объемов данных в жизнь людей, в результате чего их личная информация становится известной до мельчайших подробностей тем, кто занимается сбором и анализом их данных, в корне противоречит праву на неприкосновенность частной жизни и принципам, направленным на защиту этого права.

76. Нормативно-правовые последствия столь же значительны, как и изменения, происходящие в контексте эволюционирующей промышленной и государственной практики.

F. Открытые данные

77. Открытые данные — это понятие, которое приобрело популярность на фоне разработки методов углубленного анализа. Цель открытых данных заключается в том, чтобы призвать частный и государственный секторы публиковать данные в открытом доступе в целях содействия транспарентности и открытости, особенно в правительственных учреждениях.

78. Открытые данные определяются как

> «… данные, которые могут бесплатно и повторно использоваться и передаваться кем бы то ни было только при условии указания авторства и распространения на тех же условиях»[51].

79. Открытые данные могут включать в себя практически любую категорию данных. Фонд открытых знаний характеризует эти данные следующим образом:

a) культура: данные о культурных произведениях и артефактах — например, названия и авторы, — которые обычно собираются и хранятся в галереях, библиотеках, архивах и музеях;

b) наука: данные, которые производятся в рамках научных исследований, начиная с астрономии и заканчивая зоологией;

c) финансы: такие данные, как правительственные счета (расходы и доходы), а также информация о финансовых рынках (капитал, акции, облигации и т.д.);

d) статистика: данные, подготовленные статистическими органами, такие как данные переписи населения и основные социально-экономические показатели;

e) погодные условия: многочисленные виды информации, используемой для понимания и прогнозирования погодных и климатических условий;

f) окружающая среда: информация, касающаяся природной среды, например наличия и уровня загрязняющих веществ, качества воды и рек и морей.[52]

[51] See http://opendatahandbook.org/guide/en/what-is-open-data/.
[52] See https://okfn.org/opendata/.

80. Для того чтобы соответствовать требованиям определения открытых данных, открытые данные нередко распространяются по лицензиям организации «Криэйтив коммонз». Лицензия «Криэйтив Коммонз» CC BY 4.0 разрешает неограниченное копирование, распространение и адаптацию (в том числе в коммерческих целях) лицензированного материала с учетом соблюдения требований об указании авторства[53].

81. Имеющиеся в распоряжении правительства данные о гражданах не подпадают ни под одну из этих категорий. Открытые данные и открытое правительство призваны предоставлять доступ к данным о самом правительстве и мире, в котором мы живем. Они не должны включать данные, которые правительства собирают о своих гражданах. С учетом этого некоторые страны полностью исключают из открытых данных «персональные данные» и другие категории информации, например, как коммерческую и конфиденциальную информацию правительства[54]. Несмотря на широкое применение таких терминов, как «совместное использование данных» и «связность», мы не должны упускать из виду обратный процесс, суть которого состоит в том, что правительства вместо того, чтобы публиковать данные о работе правительства, которые общественность может использовать для обеспечения его подотчетности, публикуют данные о своих гражданах.

G. Открытое правительство

82. Одним из первых указов администрации Обамы был президентский указ о поощрении практики опубликования правительственной информации, с тем чтобы повысить транспарентность, расширить участие граждан в политической жизни и укрепить сотрудничество[55].

83. После этого было сформировано партнерство «Открытое правительство». В сентябре 2011 года Партнерство опубликовало Декларацию об открытом правительстве[56]. В Декларации основное внимание уделяется предоставлению лицам более подробной информации о деятельности правительства и подчеркивается необходимость более активного участия гражданского общества и повышения транспарентности государственного управления, а также борьбы с коррупцией, расширения прав и возможностей граждан и использования «мощного потенциала новых технологий для повышения эффективности и подотчетности правительства».

84. Декларация об открытом правительстве обязывает подписавших ее членов:

a) расширять доступ к информации о деятельности правительства;

b) поддерживать участие гражданского общества;

c) применять в администрации самые высокие стандарты профессиональной этики;

[53] See https://creativecommons.org/licenses/by/4.0/.

[54] Australia, New South Wales Government, Open Data Policy, Department of Finance & Services, 2013.

[55] President Obama, “Transparency and Open Government”, 21 January 2009, memorandum for the Heads of Executive Departments and Agencies. URL: https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government.

[56] See https://www.opengovpartnership.org/open-government-declaration.

d) расширить доступ к новым технологиям в интересах повышения уровня открытости и подотчетности[57].

85. За первым президентским указом последовал еще один президентский указ, опубликованный 9 мая 2013 года, цель которого заключалась в том, чтобы по определению сделать всю информацию правительства Соединенных Штатов Америки открытой и машиносчитываемой[58]. Акцент в этом указе был иным, чем в указе 2009 года. В новом указе говорилось, что открытые правительственные данные «способствуют предоставлению общественности эффективных и необходимых услуг и содействуют экономическому росту. В качестве одного из крайне важных преимуществ открытого правительства является то, что упрощение поиска информационных ресурсов, а также их доступность и полезность могут активизировать предпринимательскую и инновационную деятельность и способствовать научным открытиям, что повысит уровень жизни американцев и будет в значительной степени способствовать созданию рабочих мест»[59].

86. За последующие годы практика использования открытых данных изменилась до такой степени, что в 2017 году цель уже не ограничивалась публикацией в открытом доступе данных, которые ни раньше, ни сейчас не извлекались из личной информации, а уже заключается в опубликовании обезличенных персональных данных. Сторонники этого подхода подчеркивают, что в правительственных базах данных или других информационных хранилищах содержится много ценнейшей информации и что ее обнародование будет только способствовать проведению исследований и стимулировать рост экономики знаний.

87. В этой связи открытые данные, извлекаемые из личной информации, полностью зависят от эффективности процессов «обезличивания», необходимых для того, чтобы предотвратить повторную идентификацию какого-либо лица и, соответственно, увязывание этой информации с лицом, от которого она была изначально получена. Дискуссии о том, может ли процесс обезличивания обеспечить защиту неприкосновенности частной жизни и в то же время предоставить «полезные для исследования» данные, оказались весьма жаркими.

H. Комплексный характер больших данных

88. В 2015 году австралийский журналист Уилл Окенден опубликовал свои телекоммуникационные метаданные в сети Интернет и попросил людей рассказать ему, какие выводы они могут сделать о его жизни на их основе. Метаданные включали точное время всех телефонных звонков и смс-сообщений, а также информацию о расположении ближайшей телефонной вышки. Хотя журналист и заменил номера телефонов на псевдонимы, на вопросы типа «где живет моя мать?» он получил правильные ответы, которые были с легкостью найдены лишь на основании закономерностей в данных о разговорах и местоположениях. Сделать это было несложно — аудитория просто догадалась (верно), что его мать живет в том месте, в котором он находился в день Рождества.

89. Тот факт, что имеющиеся закономерности в данных, без имен, номеров телефонов или других очевидных идентификаторов, могут быть использованы

[57] https://www.opengovpartnership.org/open-government-declaration.

[58] President Obama, executive order of 9 May 2013, on “Making open and machine readable the new default for Government information”. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government.

[59] Ibid.

для установления личности человека и, следовательно, для получения более подробной информации о нем на основе этих данных, является одной из ключевых тем исследований по вопросу о конфиденциальности. Этот метод получения информации особенно эффективен в тех случаях, когда имеющиеся закономерности в данных могут использоваться для объединения различных наборов данных в целях создания более полного портрета того или иного человека.

90. Некоторые данные неизбежно становятся известными. Телефонным компаниям известно, какие номера набирает каждый клиент, а врачи знают результаты анализов своих пациентов. Соответственно, возникают разногласия по поводу раскрытия этих данных для других, например корпораций или исследователей, а также по поводу того, каким образом правительства могут использовать информацию и влиять на осуществление прав человека своих граждан.

91. Другие данные собираются целенаправленно, зачастую без ведома или без согласия людей. Исследователи фонда «Электронные границы» опубликовали результаты эксперимента «Паноптиклик», доказавшего возможность идентификации веб-браузера того или иного человека на основе таких простых характеристик, как плагины и шрифты[60]. Исследователи предупредили о том, что просмотр страниц в Интернете может быть не конфиденциальным, если не установить ограничения на хранение таких идентификационных меток и их связей с историей просмотра страниц в Интернете. Никаких изменений по существу в соответствующую политику внесено не было. В 2017 году конфиденциальность при просмотре страниц в Интернете не обеспечивается. Многие компании регулярно и целенаправленно отслеживают людей, как правило, в коммерческих целях. В настоящее время система отслеживания в сети Интернет применяется практически повсеместно, и обойти ее можно только с большим трудом.

92. Во многом экономика современного Интернета зависит от сбора комплексных данных о потенциальных клиентах для продажи им товаров, и эта практика известна под названием «капитализм наблюдения»[61]. Однако наблюдение, как представляется, является не более оправданным для эффективности, основанной на фактических данных, чем детский труд для экономики промышленно развитой страны. Единственное, наблюдение — это самый удобный и простой способ использования информации. Оно не является одним из основных прав, в отличие от права на неприкосновенность частной жизни. Собственно, экономика, основанная на данных, могла бы выжить и процветать, если бы благодаря минимальным стандартам и усовершенствованным технологиям корпорации и правительства были вынуждены функционировать в мире, в котором обычные люди имели бы гораздо больший контроль над своими собственными данными[62].

93. Правительства смогли бы также внедрять новые методы на более легитимной основе. От уровня доверия общества к правительству во многом зависит оценка людьми потенциальных последствий инициатив «Открытые данные» и «Открытое правительство». Те, кто доверяют правительству, с гораздо

[60] Peter Eckersley, “How unique is your web browser?” in *Privacy Enhancing Technologies*, Mikhail Atallah and Nicholas Hopper, eds. (Berlin, Springer-Verlag, 2010).

[61] Shoshana Zuboff, “Big other: surveillance capitalism and the prospects of an information civilization”, *Journal of Information Technology*, vol. 30, No. 1 (March 2015). .

[62] Корпорации и правительства не обязательно должны обеспечивать защиту личных данных. Примеры этических подходов, применяемых компаниями, см. документ Управления уполномоченного по вопросам информации “Big data, artificial intelligence, machine learning and data protection”, ver. 2.2 (2017). URL: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

большей вероятностью будут считать, что инициатива «Открытые данные» имеет преимущества[63]. Исследования показывают, что в основном люди не возражают, когда их правительство размещает данные об их общинах в сети Интернет, однако, когда речь заходит о данных, касающихся непосредственно их, они начинают испытывать тревогу. Степень обеспокоенности граждан варьируется в зависимости от того, о какой части сбора данных идет речь[64].

94. Большинство законов о конфиденциальности личных данных регулируют сбор и обработку информации личного характера: если информация не является «личной», она не подпадает под действие этих законов. Во многих из этих законов признается, что личные данные могут быть деидентифицированы для их использования или обработки в таких целях, как исследования в интересах всего общества, если при этом не нарушаются права людей на конфиденциальность личных данных. Правительства и другие субъекты пытаются сохранить доверие тех, чьи данные они собирают, заверяя их в деидентификации данных.

95. В связи с этим возникает важный вопрос: «не нарушает ли права людей на конфиденциальность личных данных информация, полученная в результате процессов деидентификации?».

96. Простые виды данных, например агрегированные статистические данные, позволяют применять методы подлинной защиты конфиденциальности, в том числе метод дифференциальной конфиденциальности. Алгоритмы дифференциальной конфиденциальности наиболее эффективно проявляют себя в крупных масштабах и применяются в анализах коммерческих данных. Случайные алгоритмы, применяемые для обеспечения дифференциальной конфиденциальности, являются ценным инструментом защиты информации, однако они не дают возможность полностью деидентифицировать высокосложные наборы данных в формате индивидуальных записей[65] о частных лицах. Примером использования дифференциальной конфиденциальности в крупных масштабах является применение этого метода корпорацией «Эппл» в 2016 году[66].

97. Многомерные данные в формате индивидуальных записей о частных лицах не могут быть надежно деидентифицированы без существенного уменьшения их полезности. Эти данные собираются в результате продолжительного отслеживания истории болезни человека, его маршрутов передвижения, истории поиска в Интернете и т. д. Во вспомогательном документе I[67] содержится краткая информация об инструментах деидентификации и связанных с ними спорных вопросах.

Данные в рамках инициативы «Открытое правительство»

98. Существует множество примеров успешной реидентификации лиц на основе данных, публикуемых правительствами[68]. Такая «публичная реидентифи-

[63] John Horrigan and Lee Rainie, “Americans’ views on open Government data”, Pew Research Center, 21 April 2015.

[64] Ibid.

[65] Записи, составляемые в отношении только одного лица.

[66] Andy Greenberg, “Apple’s ‘differential privacy’ is about collecting your data — but not your data”, 13 June 2016. URL: https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/https://techcrunch.com/2016/06/14/differential-privacy/ https://arxiv.org/abs/1709.02753.

[67] См. www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

[68] Выступая в Консультативном комитете по вопросам конфиденциальности и неприкосновенности личных данных Министерства внутренней безопасности 15 июня 2005 года, Суини заявила, что в 1997 году она «смогла продемонстрировать, каким образом можно было реидентифицировать медицинскую карту Уильяма Уэлда, занимавшего на тот момент пост губернатора штата Массачусетс, исключительно на

кация» является публичной по двум причинам: во-первых, результаты становятся достоянием общественности, а, во-вторых, для реидентификации используется лишь общедоступная вспомогательная информация.

99. Чем больше имеется вспомогательной информации, тем легче на ее основе реидентифицировать большее количество лиц. По мере увеличения числа связанных между собой наборов данных уменьшается количество дополнительной информации, необходимой для обратной идентификации людей. Обнародование и объединение наборов данных позволяют собирать значительные объемы вспомогательной информации об отдельных лицах в одном и том же месте, что значительно облегчает реидентификацию любых данных, касающихся этих людей.

100. Реидентифицируемость открытых данных является лишь одним из признаков гораздо более серьезной проблемы — реидентифицируемости деидентифицированных наборов коммерческих данных, которые, как правило, продаются и распространяются.

101. В эпоху больших и открытых данных праву на неприкосновенность частной жизни противостоят мощные силы. Скорее всего, наиболее предпочтительным с финансовой точки зрения вариантом для всех, кто занимается данными, будь то в коммерческих или иных целях, вероятно, является самая незначительная степень деидентификации из всех возможных, и на правительства оказывается давление не только в связи с открытием доступа к данным об отдельных лицах, но и в связи с регулированием этого процесса.

102. Неправительственные организации выражают свою обеспокоенность по поводу роста объемов больших данных без должного учета самих людей, а также этических и правовых вопросов, возникающих в связи с ненадлежащим управлением личными данными людей, и необходимости обеспечения надлежащего регулирования[69]. Неправительственные организации будут и впредь выступать за обеспечение необходимой защиты и принятие соответствующих мер.

I. Обзор нынешней ситуации: большие коммерческие данные и конфиденциальность

103. Экспоненциальный рост объемов собираемых данных и стремление подключить практически любое устройство к Интернету без должного учета необходимости обеспечить безопасность данных создают риски для частных лиц и групп. Чтобы заверить потребителей и лиц в безопасности идентифицирующей их информации, был введен ряд понятий. Например, понятие высокосложных

основе его даты рождения, пола и почтового индекса. В сущности, лишь на основе даты рождения (месяца, дня и года), пола и пятизначного почтового индекса можно идентифицировать 87 процентов населения Соединенных Штатов. Иными словами, данные, которые могут выглядеть анонимным, не обязательно являются таковыми». См. http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf; см. также Latanya Sweeney, “Matching known patients to health records in Washington state data”, Harvard University, 2012. URL: http://dataprivacylab.org/projects/wa/1089-1.pdf и http://dataprivacylab.org/index.html; Latanya Sweeney, “Achieving k-anonymity privacy protection using generalization and suppression”, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, No. 5 (2002).

[69] См. https://www.privacyinternational.org/node/8.

«обезличенных» данных культивируется отраслью, которой выгодно ошибочное понимание пользователями анонимности[70].

104. Значительная часть данных обычных пользователей собирается без их ведома или согласия. Эти данные могут продаваться и увязываться с данными из других источников для получения более полной информации, отражающей многие аспекты жизни человека. Эта информация используется в различных целях, включая политический контроль, как показало непреднамеренное раскрытие одной из политических организаций в Соединенных Штатах информации из одной базы данных[71]. Эта база содержала личные данные почти 200 миллионов избирателей Соединенных Штатов, а также поразительные данные — собранные или оценочные — об их политических убеждениях. В Китае есть «проект социального кредитования», который предназначен для оценки не только финансовой кредитоспособности граждан, но и для отслеживания их социального поведения и, возможно, политических убеждений. В рамках проекта используются данные из различных источников, собиравшиеся главным образом из Интернета в течение определенного времени[72].

105. Так называемые «брокеры данных» — компании, которые занимаются сбором личной информации потребителей, перепродают ее или делятся ею с другими, — являются важными участниками экономики больших данных. В процессе разработки своей продукции брокеры данных получают значительный объем подробной и конкретной информации о потребителях из различных источников[73]; анализируют ее, делая выводы в отношении потребителей, причем некоторая информация может быть конфиденциальной; и предоставляют ее своим клиентам в различных отраслях. Вся эта деятельность осуществляется без ведома потребителей[74].

106. Хотя продукция брокеров данных способствует предотвращению мошенничества, улучшению коммерческого предложения и оказанию персонализированных услуг, многие цели, ради которых брокеры данных собирают и используют их, сопряжены с рисками для потребителей. Обеспокоенность вызывают отсутствие транспарентности, сбор данных о несовершеннолетних, бессрочное хранение данных, а также использование этих данных для целей принятия решений о соответствии критериям или для незаконных дискриминационных целей[75].

---

[70] Даже если данные обезличены, это не означает отмену принципов конфиденциальности и таких понятий, как «согласие».

[71] Sam Biddle, “Republican data-mining firm exposed personal information for virtually every American voter”, *The Intercept*, 19 June 2017. URL: https://theintercept.com/2017/06/19/republican-data-mining-firm-exposed-personal-information-for-virtually-every-american-voter/.

[72] “China invents the digital totalitarian state”, *The Economist*, 17 December 2016. URL: https://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian; Lucy Hornby, “China changes tack on ‘social credit’ scheme plan”, *Financial Times*, 4 July 2017. URL: https://www.ft.com/content/f772a9ce-60c4-11e7-91a7-502f7ee26895.

[73] Сообщается о множестве примеров крупномасштабного сбора коммерческих данных при помощи электротехники, например телевизоров, «интимных устройств», детских игрушек и приложений для совместных поездок на «зарегистрированных автомобилях».

[74] United States Senate Committee on Commerce, Science and Transportation, “A review of the data broker industry: collection, use, and sale of consumer data for marketing purposes”, staff report, 18 December 2013. URL: http://educationnewyork.com/files/rockefeller_databroker.pdf.

[75] United States Federal Trade Commission, “Data brokers: a call for transparency and accountability”, May 2014. URL: www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

107. В недавно принятом Европейским парламентом проекте доклада о регламенте Европейского союза по вопросам конфиденциальности рекомендуется предлагать «конечным пользователям несколько вариантов установок, касающихся конфиденциальности: от высокого (например, «никогда не принимать файлы cookie») до низкого уровня защиты (например, «всегда принимать и файлы cookie»), включая также средний вариант…»[76].

108. Все более широко обсуждается вопрос о необходимости усиления контроля за конфиденциальностью в Интернете со стороны самих пользователей. Люди пользуются своими устройствами и данными для получения необходимой им информации, например о картах и маршрутах, а также для просмотра интересующей их рекламы. В этой связи возникает существенно важный вопрос: «Технологии, позволяющие усилить контроль со стороны конечного пользователя важны, но в какой степени люди могут обеспечивать достаточно всеобъемлющий контроль в целях защиты?». Применению этих инструментов в настоящее время противостоят экономические силы, формирующие Интернет[77]. Отведена ли правительствам какая-либо роль в разработке и принятии этих инструментов?

Технологии контроля за сбором данных

109. Контроль (включая прекращение) сбора данных важен для данных, которыми люди не хотят делиться. В случае со «старыми» технологиями этот вопрос не ставился, поскольку пользователи неизбежно контролировали свои данные, так как технологии других вариантов не допускали: камеры были оснащены затворными устройствами, также существовала возможность вручную отключать интернет-соединения на базе ethernet. В настоящее же время используются встроенное оборудование для беспроводной сети и камеры без затвора. В телевизоры встроены микрофоны, которые нельзя отключить. Функция отключения вручную исчезла, но все же существуют технологии, препятствующие сбору данных[78]. Благодаря успешной кампании “TLS Everywhere” на данный момент шифруется бóльшая часть интернет-трафика, что снижает вероятность сбора передаваемых данных субъектом, неизвестным пользователю. Такие технологии имеют преимущества, требующие дальнейшего изучения и поддержки.

110. Идея сокрытия информации о том, кем вы являетесь и что вы делаете, также не нова, если учесть борьбу между проводимой некоторыми социальными сетями политикой регистрации под настоящими именами и усилиями тех, кто отстаивает свое право регистрироваться под псевдонимами. Для сокрытия настоящего имени необходимы инструменты, позволяющие пользователям

[76] Marju Lauristin, “Draft report on the proposal for a regulation of the European Parliament and of the European Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC”, European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2017.

[77] Например, программа AdNauseum позволяет нейтрализовать отслеживание посредством открытия всех рекламных объявлений, появляющихся на экране пользователя, чтобы скрыть, какие он действительно читает. Эта функция заблокирована в браузере Chrome. Другие веб-сайты выявляют и блокируют пользователей, которые посещают их с установленной функцией блокировки рекламы. См. Daniel Howe and Helen Nissenbaum, “Engineering privacy and protest: a case study of AdNauseam”. URL: https://adnauseam.io/.

[78] Маршрутизатор компании Tor позволяет скрывать информацию о том, кто с кем общается (т. е. телекоммуникационные метаданные), однако не имеет широкого применения. В некоторых браузерах (например, Firefox и Brave) имеется режим «частного просмотра», не позволяющий собирать данные. Программы “Privacy Badger” фонда «Электронные границы» и “TrackMeNot” Нью-Йоркского университета весьма эффективны, но не имеют широкого распространения.

иметь «запасной» профиль и отделять его от других профилей, которые они решают открыть.

111. Исследования неизменно показывают, что, если люди обеспокоены тем, как организации, с которыми они работают, обращаются с их личными данными, они с большей долей вероятности укажут неточную или неполную информацию[79]. Поскольку конфиденциальность и защита данных порождают доверие, они положительно влияют на качество данных и на их анализ. Уверенность пользователей в конфиденциальности данных имеет также важное значение для стабильности и точности работы алгоритмов машинного обучения. Преднамеренно вводимые ошибочные данные могут оказывать серьезное влияние на стандартное машинное обучение[80]. Что произойдет, если большое количество людей преднамеренно будут использовать инструменты для сокрытия личных данных, будучи обеспокоенными обеспечением их конфиденциальности?

112. Упрощенный подход к большим и открытым данным, не учитывающий сложные взаимосвязи между выявленными методами управления конфиденциальностью, доверием к принципу невмешательства в личную жизнь и поведением людей, не будет способствовать развитию «больших данных», а приведет к тому, что принимаемые решения будут ошибочными и неэффективными.

J. Принципы на будущее: контроль за раскрытием данных

113. Законы о конфиденциальности, как правило, основываются на принципах, предусматривающих достаточную гибкость, позволяющую устранять риски, связанные с конфиденциальностью, по мере их изменения. Следует рассмотреть вопрос о том, необходимы ли, помимо существующих принципов конфиденциальности, дополнительные принципы для защиты личных данных от вторжений в частную жизнь при помощи технологий.

114. В рамках одного из вариантов осуществления контроля предлагается семь принципов обмена данными[81]:

1. Перенос алгоритмов в массивы данных: обмен результатами, а не непосредственно самими данными.

2. Открытые алгоритмы: проведение открытого обзора всех алгоритмов и осуществление общественного контроля за ними для обмена данными и защиты конфиденциальности в целях выявления и устранения ошибок или недостатков.

3. Использование данных на основе разрешений: использование данных при условии имеющегося на то (прямого или косвенного) разрешения или соблюдение принципа «контекстуальной неприкосновенности данных»[82]. В медицине в рамках интерфейса dynamic

[79] Office of the Australian Information Commissioner, Australian community attitudes to privacy survey, 2017 and 2013; Deloitte, “Trust starts from within: Deloitte Australian privacy index 2017”, 2017.

[80] Ian Goodfellow, Jonathon Shlens and Christian Szegedy, “Explaining and harnessing adversarial examples”, ArXiv preprint, 2014.

[81] Alex Pentland and others, “Towards an Internet of trusted data: a new framework for identity and data sharing”, 2016.

[82] Под конфиденциальностью понимается «требование относительно того, чтобы информация о людях («личная информация») распространялась адекватным образом, при этом адекватность означает «в соответствии с информационными нормами»… В основе такого толкования конфиденциальности лежат социальные условия…». См. Solon Barocas

consent («Динамичное согласие») предусматривается возможность официального отзыва согласия[83].

4. Отправка ответов исключительно в «безопасном» режиме: дифференциальная конфиденциальность на практике.

5. Размещение данных исключительно в зашифрованном виде: доступ к зашифрованным данным могут получать только те, кто знает шифровальный код[84].

6. Использование сетевого взаимодействия и технологии блокчейн для процессов ревизии и отчетности.

7. Социальные и экономические стимулы.

115. Эти принципы не обязательно являются полноценными решениями сами по себе, поскольку они, в свою очередь, вызывают дополнительные вопросы. Например, особенно сложно обеспечивать транспарентность в тех случаях, когда средства, используемые для защиты конфиденциальности, являются настолько сложными, что понимать их может лишь небольшое количество людей. Важным первым шагом является принцип «открытых алгоритмов», однако определить на практике, какие конкретные алгоритмы используются и каковы их последствия, все же будет сложно.

116. Предлагались и другие варианты «принципов», например «активные меры» и «транспарентность», при этом принцип «активные меры» предусматривает, в частности, право на внесение изменений в данные, частичное сокрытие данных или пробное использование фильтров[85]. Исходная динамика заключается в расширении прав и возможностей людей и в регулировании правомочий компаний, которые хранят данные, и пользователей. Другие же предлагают принципы, позволяющие скрывать информацию, предотвращать ее сбор или отказываться от него.

117. В целом, весьма важными являются принципы транспарентности и контроля со стороны пользователей, с тем чтобы пользователи могли выбирать, какие данные они раскрывают без нанесения необоснованного ущерба механизмам или услугам.

118. Кроме того, попытки разработать принципы для больших и открытых данных в целях обеспечения конфиденциальности являются полезной отправ-

---

and Helen Nissenbaum, “Big data’s end run around anonymity and consent”, in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Julia Lane and others, eds. (Cambridge University Press, 2014).

[83] Jane Kaye and others, “Dynamic consent: a patient interface for twenty-first century research networks”, *European Journal of Human Genetics*, vol. 23, No. 2 (2014).

[84] Последние достижения в области криптографии позволяют нескольким сторонам совместно рассчитывать функцию частного ввода данных, а затем раскрывать только однозначно установленные результаты. Существуют инструменты весьма общего характера, основанные на совместном расчете функции (см., например, Ivan Damgård and others, “Multiparty computation from somewhat homomorphic encryption”, *Advances in Cryptology — CRYPTO*, vol. 7417 (2012); и гомоморфном шифровании: https://www.microsoft.com/en-us/research/project/homomorphic-encryption/#). Большинство из них не работает достаточно быстро с большими наборами данных, однако, возможно, в будущем появятся упрощенные варианты. Существует множество специальных протоколов, позволяющих решать конкретные проблемы в рамках больших наборов данных. Общее понятие вычисления зашифрованных данных весьма эффективно в отношении простых расчетов одного набора данных, но может применяться и к сложным расчетам или наборам данных, размещенных в нескольких местах.

[85] Andreas Weigend, *Data for the People: How to Make our Post-Privacy Economy Work for You* (New York, Basic Books, 2017).

ной точкой для дискуссии. Независимо от того, какие принципы будут приняты, необходимо проводить надлежащие консультации между заинтересованными сторонами, включая организации гражданского общества, с целью обеспечить адекватность любых таких принципов.

119. В связи с претворением в жизнь этих принципов возникают вопросы о роли правительства, а также о видах стимулов и правовых норм, которые будут способствовать защите неприкосновенности частной жизни и других прав человека и оценке «их сравнительного воздействия на этические и политические ценности, такие как беспристрастность, справедливость, свобода, самостоятельность и благополучие, а также другие ценности, более характерные для каждой конкретной ситуации»[86].

120. Возможно, если бы правительства и корпорации реально придерживались строгих норм приобретения, распространения и контролирования данных людей, новаторская информационная экономика получала бы более широкую общественную поддержку.

III. Вспомогательная документация

121. С документами, на основе которых был подготовлен настоящий доклад, можно ознакомиться на веб-сайте Специального докладчика[87]:

I. Understanding history: de-identification tools and controversies (Экскурс в историю: инструменты деидентификации и спорные вопросы);

II. Engagements by the Special Rapporteur in Africa, America, Asia and Europe (Участие Специального докладчика в мероприятиях, проходивших в Африке, Америке, Азии и Европе);

III. Background on the open letter to the Government of Japan (Информация, связанная с открытым письмом правительству Японии);

IV. Activities of the Task Force Privacy and Personality (Деятельность Целевой группы по вопросам конфиденциальности и неприкосновенности частной жизни);

V. Description of the process for the draft legal instrument on surveillance (Описание процесса разработки проекта правового документа по вопросам наблюдения);

VI. Acknowledging assistance (Выражение благодарности за оказанную помощь);

VII. Procedural clarifications on the thematic report on Big Data and Open Data (Разъяснения процедурных вопросов, касающихся тематического доклада о больших и открытых данных).

[86] Solon Barocas and Helen Nissenbaum, “Big data's end run around anonymity and consent”, in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Julia Lane and others, eds. (Cambridge University Press, 2014).

[87] См. http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx; see also www.ohchr.org/Documents/Issues/Privacy/A-72-Slot-43103.docx.

IV. Заключение

122. **Вопросы, изложенные в настоящем докладе, не ограничиваются конкретными странами. Наличие обширных новых наборов данных позволяет людям, корпорациям и государствам во всем мире принимать более обоснованные решения, однако нерациональное управление конфиденциальностью ставит под угрозу их потенциальную ценность.**

123. **Необходимо четко понимать и успешно преодолевать риски для конфиденциальности, других связанных с этим прав человека и этической и политической ценности самостоятельности и беспристрастности.**

124. **Данные являются и будут оставаться одними из ключевых экономических активов, подобно капиталу и труду. Конфиденциальность и инновации могут и должны идти рука об руку. Понять, каким образом можно эффективно использовать большие данные и делиться их преимуществами на справедливой основе, не нарушая права человека, будет трудно, но в конечном итоге это целесообразно.**

V. Рекомендации

125. **В ожидании мнений, которые будут высказаны в процессе консультаций, заканчивающихся в марте 2018 года и результатов текущих расследований, а также с учетом направленных правительствам писем относительно предполагаемых нарушений заявлениями, Специальный докладчик рассматривает возможность вынесения следующих рекомендаций для включения в обновленный варианта настоящего доклада, который будет опубликован в 2018 году или позднее.**

126. **Политика в отношении открытых данных требует четких ограничений на использование персональной информации, основанных на международных стандартах и принципах, включая категорию, на которую распространяется изъятие из правила о конфиденциальности личной информации, и обязательства, касающиеся обеспечения надежности процессов деидентификации для публикации этой информации в качестве открытых данных, а также требует внедрения эффективных правоприменительных механизмов.**

127. **Любая инициатива в русле «открытого правительства», касающаяся личной информации, независимо от того, была ли она деидентифицирована или нет, требует тщательного общественно-научного анализа механизмов защиты личных данных, включая оценку влияния на принцип неприкосновенности частной жизни.**

128. **Конфиденциальные многомерные личные данные людей не должны публиковаться в Интернете или распространяться, если нет обоснованных доказательств того, что была проведена надежная деидентификация, которая будет защищена от потенциальной реидентификации.**

129. **Необходимо создать механизмы, позволяющие регулировать риски получения исследователями доступа к конфиденциальным данным.**

130. **Правительства и корпорации должны активно поддерживать разработку и применение технологий, направленных на более эффективное обеспечение конфиденциальности.**

131. **При работе с большими данными предлагается рассмотреть возможность использования следующих вариантов действий:**

Управление

a) ответственность: определение обязанностей, создание процесса принятия решений и, в соответствующих случаях, определение лиц, ответственных за принятие решений;

b) транспарентность: понимание того, что, когда и каким образом происходит с личными данными до того, как они станут достоянием общественности и будут использованы; в частности, речь идет об «открытых алгоритмах»;

c) качество: минимальные гарантии качества данных и их обработки;

d) предсказуемость: необходимость обеспечить предсказуемость результатов в случае использования программ машинного обучения;

e) безопасность: необходимость принятия соответствующих мер для предотвращения несанкционированного использования входных данных и алгоритмов;

f) разработка новых инструментов для выявления рисков и обозначение необходимости снижения рисков;

g) поддержка: обучение (и в соответствующих случаях аккредитация) персонала по вопросам правовых, политических и административных требований в отношении личных данных;

Нормативно-правовая база

h) принятие мер для определения четких приоритетов, обязанностей и полномочий регулирующих органов, которым поручена защита данных граждан;

i) полномочия регулирующих органов должны соответствовать новым вызовам, связанным с большими данными, в частности способность регулирующих органов тщательно изучать аналитический процесс и его результаты;

j) обзор законов о конфиденциальности личных данных на предмет их соответствия проблемам, возникающим в связи с техническим прогрессом и касающимся, например, персональной информации, генерируемой компьютерами, и таких методов анализа данных, как деидентификация;

Внедрение механизмов обратной связи

k) формальное закрепление консультационных механизмов, в том числе комитетов по этике, среди профессиональных, общественных и иных организаций и граждан в целях предотвращения нарушения прав и определения рациональных методов работы;

l) проведение широких консультаций по рекомендациям и вопросам, содержащимся в настоящем докладе, например относительно необходимости запрета на распространение данных, имеющихся в распоряжении у государственных органов;

Научные исследования

m) технические вопросы: изучение относительно новых технических методов, таких как дифференциальная конфиденциальность и гомоморфное шифрование, на предмет того, обеспечивают ли связанные с ними процессы и результаты конфиденциальность надлежащим образом;

n) оценка осведомленности граждан о деятельности государственных органов и частных компаний, касающейся данных, об использовании личной информации, в том числе для исследований, и о технических механизмах, позволяющих повысить индивидуальный контроль за персональными данными и укрепить способность граждан использовать их для удовлетворения своих потребностей.