

ГЛАВА 2

Будущее личности, государства и персональных данных

В следующем десятилетии количество виртуальных личностей превысит население Земли. Все мы будем представлены в сети сразу несколькими аккаунтами, а значит, возникнет множество переполняемых энергией сообществ по интересам, которые и отражают, и обогащают реальный мир. В результате образуются огромные массивы информации (уже появился термин «революция данных») и люди получат невиданную раньше власть. И вот здесь необходимо сделать исключительно важное предостережение: в результате этой революции данных мы практически утратим контроль над своей персональной информацией, попадающей в виртуальное пространство, что приведет к серьезным последствиям и в реальном мире. Возможно, это затронет не каждого пользователя, но на макроуровне очень сильно изменит нашу жизнь. Перед нами стоит трудная задача: решить, на что мы готовы пойти для того, чтобы сохранить контроль над личной жизнью и безопасностью.

Сегодня наши виртуальные личности в некоторой степени влияют на наше физическое «я», но пока не доминируют над ним. То, как ведут себя пользователи в социальных сетях, и то, что они пишут, может нравиться или нет, но чаще всего по-настоящему конфиденциальная или личная информация остается скрытой от посторонних глаз. От онлайн-склок и дискредитирующих кампаний страдают в основном заметные общественные фигуры, а не обычные люди. В будущем на нашу личность в реальной жизни все большее влияние станут оказывать наша виртуальная деятельность и контакты в сети. Детально документированное прошлое начнет

определять наши перспективы, и мы утратим контроль над тем, как нас воспринимают другие. Одновременно вырастет вероятность несанкционированного доступа к персональным данным, их кражи или манипулирования ими, в частности благодаря тому, что мы все больше полагаемся на «облачные» хранилища данных. (Говоря упрощенно, «облачные» вычисления проводятся на программном обеспечении, размещенном в интернете, управляемым которым пользователь не может. А хранение документов и иного контента «в облаке» означает, что данные находятся на удаленных, а не на локальных серверах или собственном компьютере человека и доступ к ним могут получить разные пользователи и с разных устройств. «Облачные» вычисления ускоряют распространение информации и процесс работы в интернете, поскольку сокращают трафик.) Однако в силу этой уязвимости — и воображаемой, и реальной — технологическим компаниям придется прилагать все больше усилий, чтобы завоевывать доверие пользователей в области конфиденциальности и безопасности данных, иначе они столкнутся с оттоком клиентов. Отрасль высоких технологий уже озабочилась поиском новых способов снизить указанные риски, например при помощи двухфакторной идентификации, когда для доступа к своим персональным данным от вас требуется что-то, что вы знаете (предположим, пароль), имеете мобильный телефон или что вам неотъемлемо принадлежит (отпечаток пальца). Не может не радовать то, что над созданием нового поколения таких решений трудятся лучшие в мире инженеры. Как минимум в качестве более надежного, хотя и не идеального выхода будет повсеместно использоваться строгое шифрование. («Шифрованием» называется кодирование информации, при котором декодировать ее может лишь тот, кто прошел верификацию.)

Могут измениться сами основы виртуальной идентификации. Некоторые правительства, решив, что иметь тысячи анонимных, бесконтрольных и непроверенных граждан — «подполье» — слишком рискованно, захотят узнать, кто скрывается за каждым онлайн-аккаунтом, и потребуют верификации на государственном уровне для усиления контроля над виртуальным пространством. В будущем ваша виртуальная личность вряд ли будет ограничена страничкой в Facebook — скорее всего, она станет целым созвездием профилей, созданных вами в интернете, которое будет верифицироваться и даже регулироваться властями. Представьте, что все ваши аккаунты — в Facebook, Twitter, Skype, Google+, Netflix, подписка на New York Times — привязаны к одному «официальному» профилю. Рейтинг информации, связанной с верифицированными онлайн-профилями, в результатах поиска

44 НОВЫЙ ЦИФРОВОЙ МИР

окажется более высоким по сравнению с контентом без такой верификации, а это, естественно, приведет к тому, что большинство пользователей будут кликать на верхние (верифицированные) результаты. И тогда истинная цена анонимности может стать слишком высокой: даже самый увлекательный контент, созданный владельцем анонимного профиля, просто не будет виден в поисковой выдаче из-за своего чрезвычайно низкого рейтинга.

Переход от ситуации, когда личность формируется онлайн и позднее проецируется в сеть, к созданию онлайн-личности, которая затем воплощается в реальном мире, окажет огромное влияние на граждан, государства и компании. И от того, как удастся решить проблемы конфиденциальности и безопасности личных данных, будут зависеть границы человеческой свободы. На этих страницах мы хотели бы поговорить о том, что́ всеобщий доступ в сеть будет значить для граждан в будущем, как они им воспользуются и какие последствия это возымеет и для диктатур, и для демократий.

Революция данных

Революция данных принесет жителям планеты колоссальное благо. В частности, они смогут узнать, что думают и как ведут себя другие люди, каких правил придерживаются, почему их нарушают — причем не только соотечественники, но и те, что живут на других континентах. Обретенная способность получать онлайн точную и проверенную информацию по первому требованию на родном языке и в неограниченных количествах будет означать начало эпохи критического мышления в тех сообществах, которые прежде были культурно изолированы от остального мира. В странах с неразвитой инфраструктурой доступ в сеть позволит людям заниматься бизнесом, в том числе онлайн, и взаимодействовать с правительством на совершенно ином уровне.

Это будет означать наступление эры невиданных возможностей. И даже если кто-то попытается сохранить максимум индивидуальности, дистанцируясь от виртуальной жизни, другие сочтут, что открывающиеся перспективы оправдывают риск, на который приходится идти. Гражданское участие достигнет новых высот: каждый человек, имеющий мобильный телефон и доступ в интернет, сможет внести свой вклад в реализацию идеи подотчетности и прозрачности властей. И лавочник в Аддис-Абебе, и сознательный не по годам подросток в Сан-Сальвадоре станут распространять информацию о случаях вымогательства взяток и коррупции, сообщать о нарушениях избирательного законодательства — в общем,

призывать правительство к ответу. А если для того, чтобы полицейские вели себя по закону, недостаточно телефонов с функцией фотосъемки, в полицейских автомобилях можно установить видеокамеры! На самом деле развитие технологий позволит населению контролировать полицию с помощью огромного количества прежде недоступных способов, включая систему мониторинга, предназначенную для формирования рейтинга каждого полицейского в городе, в режиме реального времени. После того как основные общественные институты: системы здравоохранения, образования и судебная система — окончательно вступят в цифровую эру, они станут более эффективными, прозрачными и доступными.

Тем, кто хочет распространять религиозные, культурные и этнические мифы, придется кормить своими выдумками сообщество хорошо информированных слушателей. В распоряжении людей появится больше данных и способов их проверить. И тогда колдун из Малави, занимающийся врачеванием, вдруг столкнется с враждебным отношением к нему со стороны соплеменников, если они найдут в сети информацию, развенчивающую его авторитет, и поверят ей. Или, например, молодые юменцы, обнаружив, что виртуальное сообщество отрицательно относится к культивируемой в стране традиционной практике женитьбы на маленьких девочках, восстанут против нее, поскольку решат, что она бросает тень на них самих. А последователи индийского «святого» найдут способ проверить его прошлое и отвернутся от него, выяснив, что он их обманывал. Многие опасаются, что в эпоху процветания онлайн-источников у людей может усилиться психологическая склонность искать подтверждение своей позиции (когда, сознательно или нет, они обращают внимание лишь на ту информацию, которая согласуется с их сложившейся точкой зрения). Однако недавнее исследование ученых из Университета штата Огайо показало, что этот эффект слабее, чем кажется, особенно на американском политическом ландшафте. На самом деле склонность к поиску подтверждений проявляется и когда мы пассивно реагируем на информацию, и когда активно отбираем ее источники. Поэтому, когда миллионы людей выходят в интернет, у нас есть основание с оптимизмом смотреть на будущие социальные изменения.

Властям будет все труднее маневрировать по мере того, как все больше их граждан получают доступ к мобильной связи и интернету. В новую цифровую эру такие репрессивные действия, как уничтожение документов, похищения людей и уничтожение памятников, практически потеряют смысл. Ведь документы можно восстановить и сохранить «в облаке», а давление, которое способно организовать активное глобализированное

46 НОВЫЙ ЦИФРОВОЙ МИР

интернет-сообщество в ответ на беззаконие, заставит власти подумать дважды, прежде чем похищать кого-то или держать в застенках неопределенно долго. Да, некоторые режимы, вроде установленного талибами, по-прежнему смогут уничтожать памятники, как они разрушили бамианские статуи Будды*. Но такие памятники можно будет отсканировать с применением самой современной технологии, что позволит сохранить все их углы и закоулки в виртуальной памяти, а затем воссоздать — вручную или при помощи 3D-принтеров — или даже спроектировать в виде голограмических изображений. Возможно, Центр всемирного наследия ЮНЕСКО станет использовать такую практику в рамках своей деятельности по реставрации памятников. Старейшую синагогу Сирии, которая сегодня находится в музее Дамаска, можно спроектировать или реконструировать посредством 3D-печати. Активное гражданское общество, которое сегодня имеется в большинстве развитых стран, готовое проверять факты и расследовать действия властей, появится почти везде, причем в значительной степени этому будет способствовать распространение дешевых и мощных мобильных устройств. Как минимум жители всех стран смогут сравнивать себя и свой образ жизни с тем, как живет остальная часть мира. И в этом контексте варварские или устаревшие обычаи будут выглядеть особенно одиозно.

* * *

В будущем уникальная личность человека окажется его самым ценным активом, и существовать эта личность будет преимущественно в сети. Опыт жизни в режиме онлайн люди станут приобретать с самого рождения, если не ранее. При этом различные периоды человеческой жизни, «замороженные» во времени, будут легкодоступны для всеобщего обозрения. В результате придется создавать новые средства контроля информации, позволив людям самим составлять списки тех, кто может видеть их данные. Используемые нами сегодня технологии связи «инвазивны» по определению: они собирают наши фотографии, комментарии и имена друзей в огромные базы данных, по которым можно проводить поиск и которые в отсутствие внешнего регулирования становятся законной добычей для работодателей, университетских отделов по работе с персоналом и сплетников. Мы то, что мы «твиттим».

* Статуи Будды, входившие в комплекс буддийских монастырей в Бамианской долине (Афганистан), в 2001 году были разрушены талибами как памятники язычества.
Прим. ред.

В идеале все мы должны сознательно и тщательно управлять своими онлайн-личностями и виртуальными жизнями, отслеживать и корректировать их, чтобы не усложнять свою реальную жизнь, причем с самого раннего возраста. Увы, это невозможно. У детей и подростков желание делиться информацией всегда перевесит смутный отдаленный риск рассказать о себе слишком многое, несмотря на многие примеры негативных последствий. Так что к тому моменту, когда человеку исполнится сорок, в сети сложится повествование о его жизни, очень подробное и включающее все факты и вымысли, ошибки и победы. И даже слухи будут жить вечно.

В глубоко консервативных обществах, где общественное порицание значит очень многое, мы можем столкнуться со своего рода «виртуальным бесчестием» — сознательными усилиями по дискредитации онлайн-личности человека (путем приписывания ему недостойных поступков и распространения ложной информации или связывания его онлайн-личности с контентом, в котором идет речь о реальном или вымышленном преступлении). Разрушение репутации в сети может не сопровождаться физическим насилием со стороны злоумышленника, но если, скажем, такого рода обвинения будут предъявлены девушке, ее честь может оказаться запятнанной, причем, к ее несчастью, навсегда — и скрыться в таком случае невозможно. Учитывая публичность позора, все может закончиться ее гибелью от руки одного из родственников.

А что насчет роли родителей? Она нелегка, и это известно всем, у кого есть дети. Появление виртуального мира еще больше усложнило ее, но не стоит считать ситуацию безнадежной. В будущем ответственность родителей не уменьшится, но им придется еще активнее участвовать в жизни своих детей, если они хотят, чтобы те не совершили в сети ошибок, способных навредить их судьбе в реальном мире. А поскольку виртуальное развитие детей значительно опережает их физическое созревание, большинство родителей придут к пониманию того, что самый лучший способ помочь своим отпрыскам — поговорить с ними о необходимости защиты личной информации и соблюдения безопасности в сети даже раньше, чем о вопросах секса. Так что традиционный разговор с детьми по душам не утратит своей роли в их воспитании.

Школьная система тоже изменится и внесет свою лепту в развитие навыков онлайн-осмотрительности. По настоянию родительских ассоциаций наряду с уроками сексуального воспитания в школах появятся уроки защиты личной информации и основ безопасности при работе в интернете. На таких занятиях школьники научатся оптимизировать установки

48 НОВЫЙ ЦИФРОВОЙ МИР

безопасности программ и хорошо усвоят, что можно и чего нельзя делать в виртуальном мире. А учителя будут пугать их историями из реальной жизни о том, что бывает, когда не начинаешь защищать личную информацию и соблюдать безопасность в сети с самого раннего детства.

Конечно же, найдутся родители, которые в попытке обыграть систему начнут действовать еще предпримчивее. Один из примеров — выбор имени будущего ребенка. По мере роста функциональной ценности онлайн-личности роль родителей на начальном этапе жизни детей окажется критически важной. Начинаться все будет с их имен. Стивен Левитт и Стивен Дабнер в книге *Freakonomics** проанализировали, насколько популярные в определенных этнических группах имена (в частности, у афроамериканцев) могут предсказывать жизненный успех их владельцев. Дальновидные родители учтут и то, как результаты поисковой выдачи скажутся на будущем их детей. Однако истинно стратегический подход проявится не просто в заблаговременном резервировании аккаунтов социальных сетей и не в покупке соответствующих доменных имен (предположим, www.JohnDavidSmith.com), а в выборе ребенку такого имени, которое облегчит или усложнит процесс его поиска в интернете. Некоторые сознательно выберут уникальные или традиционные, но искаженно написанные имена с тем, чтобы избавить своих детей от прямой конкуренции и облегчить им задачу продвижения в виртуальном мире. Другие, напротив, остановят свой выбор на самых распространенных именах, что обеспечит их детям определенный «щит» от индексации в сети: просто еще одна «Джейн Джонс» среди тысяч подобных записей.

Мы предвидим пышный расцвет отрасли, связанной с защитой персональных данных и репутации. Такой бизнес существует уже сегодня: компании вроде Reputation.com используют различные методы как быстрого реагирования, так и профилактики для того, чтобы удалять из сети нежелательный для их клиентов контент или минимизировать ущерб от его появления**. По некоторым сообщениям, в ходе экономического

* Выходила на русском языке: Левитт С., Дабнер С. Фрикономика. М.: Манн, Иванов и Фербер, 2011. *Прим. ред.*

** Большинство таких методов относятся к группе инструментов поисковой оптимизации (SEO). Чаще всего, чтобы повлиять на механизм ранжирования результатов выдачи поисковых систем, используют создание позитивного контента, содержащего целевые слова (например, имя человека), многочисленных ссылок на него и частое обновление содержимого. В результате поисковые «пауки», скорее всего, будут идентифицировать этот материал как популярный и новый, тем самым сдвигая ниже в результатах поиска старые и менее релевантные материалы. На рейтинг также может

кризиса 2008 года несколько банкиров с Уолл-стрит привлекали компании, специализирующиеся на защите онлайн-репутации, чтобы те минимизировали информацию о них в виртуальном мире. Стоили такие услуги до \$10 000 в месяц. В будущем на волне растущего спроса эта отрасль существенно расширится, и услуги репутационных менеджеров станут таким же обычным делом, как брокеров и финансовых консультантов. Нормой для известных и стремящихся к известности людей будет активное управление своим онлайн-имиджем, например, получение от репутационного менеджера ежеквартальных отчетов, фиксирующих его изменение за прошедший период.

Появится новое направление страхования. Вам предложат застраховать свою онлайн-личность от кражи и взлома, ложных обвинений, злоупотреблений и несанкционированного присвоения. Родители смогут купить страховку от репутационного ущерба, который способны причинить им действия их детей в интернете. А преподаватель, скажем, захочет застраховаться от взлома студентами его профиля в Facebook и размещения на странице оскорбительной и порочащей информации. Страхование от кражи персональных данных уже существует, но в будущем страховые компании смогут предложить своим клиентам защиту и от других злоупотреблений. Такие полисы будут покупать не только те, кому они действительно нужны, но и просто параноидально настроенные люди.

Онлайн-личности возобладают столь высокой ценностью, что их — реальные или придуманные — можно будет купить на черном рынке. В этом будут заинтересованы и обычные люди, и преступники, ведь под чужой маской смогут скрыться как наркоторговцы, так и диссиденты. Такие онлайн-личности, украденные или созданные с нуля, станут продаваться в комплекте со всей необходимой исторической информацией: записями в лог-файлах интернет-провайдеров, фиктивными «френдами» и данными о покупках, то есть всем тем, благодаря чему будут выглядеть правдоподобно. И если полицейский информатор из Мексики захочет избежать мести со стороны наркокартеля, набор таких фальшивых онлайн-личностей

влиять использование популярных ключевых слов и обратных ссылок на «раскрученные» сайты. Все это вполне законно и морально приемлемо. Однако у поисковой оптимизации есть и оборотная сторона — «черная SEO», которая включает в себя попытки манипулирования рейтингом при помощи незаконных или аморальных методов, скажем, причинение вреда чужому контенту (к примеру, путем привязки его с помощью ссылок к подозрительным сайтам, в частности содержащим детскую порнографию), добавление скрытого текста или маскировка сайта (это когда поисковым роботам показывают одну его версию, а конечным пользователям — другую).

наверняка поможет членам его семьи скрыть свое прошлое и начать жизнь с чистого листа.

Естественно, что в цифровую эпоху такой способ побега представляет собой рискованное предприятие: начало новой жизни должно означать полный разрыв всех прежних связей, ведь выдать человека может малейший неверный жест вроде поискового запроса по имени кого-то из родственников. Более того, тому, кто использует фальшивую личность, следует избегать всех мест, где применяется технология распознавания лица, способная связать его со старым аккаунтом человека. Да и сам этот теневой рынок сделок с онлайн-личностями будет неспокойным местом: и покупатель, и продавец остаются анонимными благодаря зашифрованным каналам связи и расчетам в виртуальной валюте, которые очень сложно отследить. Поэтому и посредники, и покупатели столкнутся с теми же рисками, что и сегодняшние участники черного рынка, включая работу правительенных агентов «под прикрытием» и обман в ходе сделок (вероятность всего этого, скорее всего, даже повысится, учитывая анонимную природу транзакций в виртуальном мире).

* * *

Многие с восторгом отнесутся к отсутствию контроля, что предполагает всеобщий доступ в сеть с неограниченными объемами хранящихся там данных. Люди будут считать, что информация по определению должна быть доступна всем^{*} и что еще большая прозрачность сделает мир проще, безопаснее и свободнее. Пока самым заметным евангелистом этой идеи является Джюлиан Ассанж^{**}, но его ценности разделяют, поддерживая созданную им WikiLeaks, люди самых разных убеждений — от правых либертиарianцев до крайне левых либералов и аполитических энтузиастов высоких технологий. И хотя они не всегда согласны друг с другом в вопросах тактики, общей для них является вера в необходимость вечного хранения данных как основы существования общества. По мнению активистов свободного доступа к информации, отсутствие кнопки Delete в конечном счете ускорит движение человечества к полному равенству, производительности и самоопределению, несмотря на некоторые известные негативные

^{*} Считается, что впервые эту максиму сформулировал Стиоарт Брэнд, основатель и редактор Whole Earth Catalog, в ходе Первой хакерской конференции, состоявшейся в 1984 г.

^{**} Подробнее о Джюлиане Ассанже и WikiLeaks можно прочитать в книге: Ассанж Д. Неавторизованная биография. М. : Альпина Бизнес Букс, 2012.

последствия такого подхода (угроза индивидуальной безопасности, испорченные репутации и дипломатический хаос). Однако мы убеждены, что это очень опасная модель, особенно если учесть, что всегда найдутся глаупщи, готовые по недомыслию поделиться гибельной для многих людей информацией. Вот почему сохранится система государственного регулирования, которая при всем ее несовершенстве по-прежнему будет определять круг лиц, уполномоченных принимать решения о том, какие данные считать секретными, а какие — нет.

Мы встречались с Ассанжем в июне 2011 года, когда он содержался под домашним арестом в Великобритании. Какой бы ни была наша позиция, мы должны учитывать то, к чему могут стремиться активисты, выступающие за полную свободу информации, поэтому мнение Ассанжа является хорошей отправной точкой. Мы не собираемся останавливаться на том, что обсуждается сегодня (этому посвящены многие книги и статьи) и касается в основном западной реакции на WikiLeaks, содержания обнародованной переписки, степени деструктивности утечек информации и того, какое наказание должны понести причастные к этому люди. Нет, нас интересует будущее и то, что попытаются создать — или разрушить — представители следующего поколения движения за свободу информации, начиная с последователей Ассанжа, но не ограничиваясь ими. В ходе интервью Ассанж поделился с нами двумя своими главными соображениями на эту тему, причем обе посылки связаны друг с другом. Первое: человеческая цивилизация основана на всей совокупности результатов нашей интеллектуальной деятельности, следовательно, правильным является как можно более тщательно фиксировать эти результаты, чтобы обеспечить информацией следующие поколения людей. Второе: поскольку различные лица всегда будут пытаться уничтожить или скрыть часть этой общей истории в своих интересах, цель каждого человека, ценящего истину и стремящегося к ней, — фиксировать как можно больше информации, препятствовать ее уничтожению, а также делать ее максимально доступной для всех жителей планеты.

Ассанж не сражается с секретностью как таковой: по его словам, «есть множество причин, по которым неправительственные организации могут хранить секреты, и, на мой взгляд, это их законное право: они нуждаются в этом, потому что не обладают иной властью». Он борется с секретностью, прикрывающей действия, которые идут вразрез с интересами общества. «Почему правительственные организации стремятся к секретности?» — задает он риторический вопрос. И сам отвечает на него: потому что их планы, стань они известными широкой публике, встретили бы отпор,

52 НОВЫЙ ЦИФРОВОЙ МИР

а секретность помогает им воплотить их. Тот, чьи планы не противоречат интересам общества, не встречает противодействия, и ему нечего скрывать, добавляет он. По словам Ассанжа, в этом противостоянии в конечном счете верх возьмут те, кто обладает реальной поддержкой людей. Так что раскрытие информации «позитивно для организаций, ведущих деятельность, которую поддерживает общество, и негативно для организаций, занятых делами, которые общество не одобряет».

Мы возразили, что в этом случае не желающие огласки организации просто начнут скрывать свою деятельность, но Ассанж выразил уверенность, что его движение способно этому воспрепятствовать. Он считает, что полная секретность невозможна — серьезные структуры всегда оставляют бумажные следы: «Понимаете, в системную несправедливость обычно вовлечено множество людей». Не у всех из них есть полный доступ ко всем планам, но каждый знает достаточно для того, чтобы выполнять свою работу. «Если перестаешь фиксировать информацию на бумаге, если решишь не оставлять ни электронных, ни бумажных следов, любые институты приходят в упадок, — говорит он. — Вот почему у всех серьезных организаций существует строгая система документирования на бумаге всех решений, в том числе самого высшего руководства». Бумажные следы дают уверенность в том, что команды выполняются должным образом, поэтому, по словам Ассанжа, «если организация настолько “балканизирована” внутри, что утечки невозможны, то это означает резкое снижение ее эффективности». А неэффективность означает слабость.

С другой стороны, Ассанж считает, что открытость может создать проблемы для самих искателей истины: «Открытость затрудняет нам жизнь, поскольку люди начинают скрывать свои плохие поступки, искусственно усложняя систему». В качестве очевидных примеров он привел бюрократическую демагогию и офшорный финансовый сектор. Технически это открытые системы, но по сути своей — непрозрачные: к ним трудно пристряться, но еще труднее использовать эффективно. Бороться со сложной, сознательно запутанной, хотя и законной системой, призванной скрывать темные делишки, гораздо труднее, чем с простой цензурой.

К сожалению, такие люди, как Ассанж, и организации вроде WikiLeaks легко смогут воспользоваться возможностями, которые сулят грядущие перемены. И даже тем, кто их поддерживает, не так-то просто дать однозначную оценку применяемых ими методов и последствий прозвучавших разоблачений, особенно если проецировать то, что происходит, в будущее. И здесь одним из самых трудных является вопрос о том, кто будет решать,

какую информацию можно обнародовать без купюр, а что нужно хотя бы временно публиковать выборочно? Почему, в частности, именно Джулиан Ассанж определяет, какие материалы представляют собой общественный интерес? И что будет, если человек, принимающий решения о раскрытии информации, готов смириться с неизбежным вредом, который оно причинит ни в чем не повинным людям? Большинство из нас согласится с тем, что для того, чтобы такие платформы приносили обществу пользу, над ними нужен некоторый контроль, но никто не даст гарантий возможности такого контроля (это подтверждает безжалостность хакеров*, выкладывающих в сети огромные массивы персональных данных множества людей).

Если решения о раскрытии информации принимаются централизованно, то их должно принимать очень ограниченное количество людей, а людям свойственно иметь предрассудки и отстаивать собственные идеи. И пока этим миром правим мы, представители человеческой расы, а не компьютеры, останется проблема субъективности человеческого суждения независимо от того, насколько прозрачны или технически совершенны используемые нами инструменты.

В будущем на волне все большей доступности интернета можно ожидать всплеск активности платформ, аналогичных WikiLeaks. По мере роста количества пользователей и объемов секретной и конфиденциальной информации появятся десятки более мелких сайтов, стремящихся воспользоваться увеличением спроса и предложения и делающих тайное явным. Мысль убедительная и пугающая, но ошибочная. Рост количества сайтов, публикующих секретные материалы, ограничен естественным образом, в том числе внешними факторами, которые не позволяют успешно существовать множеству аналогичных платформ. Каким бы ни было ваше отношение к WikiLeaks, только подумайте о том, как много факторов способствовали ее превращению в глобальный бренд: несколько крупномасштабных утечек мирового значения, способных привлечь внимание международной общественности; стабильная публикация информации, что доказывает приверженность организации своим идеям, вызывает общественное доверие и стимулирует новых информаторов, показывая им, что WikiLeaks способна их защитить; харизматическая фигура лидера, олицетворяющая организацию и служащая ее «детонатором» (так называет себя Ассанж); постоянное обнародование новых утечек, часто большими блоками, что

* Хотя в программистском сообществе термин «хакер» означает человека, создающего что-то быстро и спонтанно, мы используем здесь это слово в его привычном значении — «взломщик компьютерных систем».

позволяет организации оставаться на виду; а также, что немаловажно, распределенная и технически совершенная цифровая платформа для работы с рассекреченными документами, которой пользуются информаторы, сотрудники организации и посетители (при этом оставаясь анонимными) и которая благополучно обходит попытки ее блокировки властями множества стран. Такую сложную и гибкую систему построить непросто и в силу технических проблем, и из-за того, что ценность одних ее компонентов напрямую зависит от остальных (кому нужна продвинутая платформа без мотивированных информаторов или огромный массив секретных данных без системы их непрерывной обработки и распространения?). WikiLeaks потребовалось годы на то, чтобы сбалансировать общественный интерес, энтузиазм информаторов и техническую защищенность системы, и поэтому сложно вообразить, что в будущем какие-то вновь созданные, отпочковавшиеся или конкурирующие команды смогут создать аналогичную платформу и выстроить схожий по силе бренд быстрее, чем это удалось сделать Ассанжу, особенно учитывая то, что сейчас все правительства хорошо понимают угрозу, исходящую от таких организаций.

Однако даже если кому-то и удастся запустить конкурирующие сайты, одновременно сможет существовать лишь горстка подобных платформ. На это есть несколько причин. Во-первых, для успеха даже самым «сочным» утечкам требуется последующая «раскрутка» в СМИ. А если сайтов, на которых публикуется рассекреченная информация, станет слишком много, СМИ не смогут уследить за всеми существующими платформами и публикуемыми материалами, да и уровень доверия к ним упадет. Во-вторых, информаторы предпочтут организации, которые, по их мнению, с одной стороны, обеспечат максимальное общественное внимание к их информации, а с другой — максимальную защиту. Новые сайты будут конкурировать за информаторов, обещая им еще большую известность и лучшую защиту, но очевидно, что потенциальный источник информации скорее последует примеру своих успешных предшественников и воспользуется той же платформой. С какой стати ему рисковать представившимся шансом и самой жизнью, полагаясь на непроверенный сайт? А те организации, которые не смогут стablyно предлагать миру качественные утечки информации, лишатся общественного интереса и финансирования, в результате чего медленно, но верно захиреют. Ассанж считает, что для его организации это вполне благоприятная ситуация и что доверие к WikiLeaks точно позволит ей продолжать свою деятельность. «Информаторы голосуют ногами, — заметил он, — рынок дисциплинировал нас».

Судьба сайтов, специализирующихся на публикации секретных материалов, будет сильно зависеть от того, на какие регионы они ориентированы. На Западе и правительственные структуры, и корпорации в большинстве своем хорошо представляют себе риски, связанные с недостаточной степенью безопасности компьютерных систем. В их системы и так невозможно проникнуть, однако и в государственный, и в частный секторы по-прежнему инвестируются значительные ресурсы для еще более качественной защиты записей, пользовательских данных и инфраструктуры. О большинстве развивающихся стран такого не скажешь, и, поскольку можно ожидать, что в ближайшие десять лет их население получит доступ в интернет, многие государства столкнутся со своей версией WikiLeaks: там появятся информаторы, имеющие доступ к цифровым данным и готовые организовать их утечку в политических целях. Последующие за этим бури, пусть и ограниченные одной страной или регионом, будут иметь для них разрушительные последствия. И даже могут привести к революции. Следует ожидать, что для борьбы с такими сайтами власти станут применять похожие методы (даже если сами организации и их серверы расположены за пределами страны): фильтрация, прямые атаки, финансовая блокада и судебное преследование.

В конце концов технологии, используемые при создании таких платформ, станут настолько совершенными, что блокировать их будет практически невозможно. Когда в 2010 году WikiLeaks в результате DDoS-атак и давления провайдера, предоставлявшего хостинг, утратила контроль над своим основным сайтом WikiLeaks.org, сторонники организации немедленно создали свыше тысячи зеркальных сайтов (копий оригинального сайта, расположенных в разных местах) с такими адресами, как WikiLeaks.fi (в Финляндии), WikiLeaks.ca (в Канаде) и WikiLeaks.info. В ходе DDoS-атак — атак типа «отказ в обслуживании» — к сайту-мишени обращается одновременно большое количество зараженных компьютеров, засыпая его информационными запросами и приводя к перегрузке системы, в результате чего сайт перестает обслуживать обычных пользователей. WikiLeaks изначально проектировалась как распределенная система: ее деятельность не концентрируется в рамках одного хаба, а распределяется между множеством различных компьютеров, так что отключить такую платформу значительно труднее, чем представляется большинству дилетантов. В будущем организации, специализирующиеся на публикации секретных материалов, наверняка пойдут гораздо дальше создания сайтов-зеркал (простых копий существующих сайтов) и станут использовать новые методы для репликации и сокрытия своих операций, чтобы защититься от действий властей.

56 НОВЫЙ ЦИФРОВОЙ МИР

Одним из инструментов может быть такая система хранения, в рамках которой в различных местах находится множество копий фрагментов файлов. В случае уничтожения какой-то директории с информацией файлы можно будет собрать заново из этих фрагментов. Создатели подобных платформ придумают новые способы сохранения анонимности потенциальных информаторов: WikiLeaks, к слову, постоянно совершенствует методы передачи информации и призывает не пользоваться устаревшими криптографическими инструментами, как только выясняется их уязвимость (допустим, протоколом SSL и скрытыми сервисами Тор), а переходить на Тор-сеть с высоким уровнем шифрования.

А что можно сказать о лидерах этого движения? В будущем появятся новые «ассанжи», но сторонников у них будет по-прежнему не очень много. Наибольшую пользу принесут те, кто последует примеру людей вроде Алексея Навального, блогера и борца с коррупцией из России, пользующегося большой симпатией на Западе.

Разочаровавшись в российских оппозиционных партиях, этот специализирующийся на недвижимости юрист начал вести собственный блог, посвященный разоблачению коррупции в крупнейших компаниях России. Поначалу он получал материалы, покупая небольшие пакеты акций этих компаний и используя права акционера на получение информации об их деятельности. Позднее он стал применять краудсорсинг и предложил своим сторонникам использовать те же методы, причем небезуспешно. В конечном счете его блог превратился в полноценную платформу по публикации секретных материалов, посетители которой могут делать пожертвования на ведение ее операционной деятельности посредством PayPal. Известность Навальногоросла по мере того, как пополнялась коллекция его разоблачений, в частности после обнародования им в 2010 году документов о злоупотреблениях в государственной компании «Транснефть», операторе магистральных нефтепроводов, на сумму \$4 млрд. К концу 2011 года благодаря своей популярности Навальный оказался в эпицентре общественных протестов, связанных с выборами, а придуманное им прозвище для возглавляемой Владимиром Путиным партии «Единая Россия» — «Партия жуликов и воров» — мгновенно разнеслось по стране.

Характерно, что при всей своей принципиальности Навальный не использовал в качестве мишени самого Путина, по крайней мере поначалу. Его целью были преимущественно коммерческие организации, хотя, учитывая,

что в России частный и государственный сектор разделить непросто, опубликованная информация нередко затрагивала и некоторых чиновников. Более того, несмотря на оказываемое на него давление — Навального задерживали, помещали под арест, устраивали за ним слежку, возбуждали уголовные дела, — он все эти годы остается на свободе. Критики могут называть его лгуном, лицемером или марионеткой ЦРУ, тем не менее Навальный не уезжает из России (в отличие от многих других известных оппонентов Кремля), а блог его продолжает работать.

Некоторые наблюдатели считают, что Навальный не представляет особой угрозы режиму: знают о нем в стране по-прежнему мало, хотя его сторонники объясняют это тем, что невысокие цифры поддержки скорее отражают факт недостаточного распространения интернета и наличие жесткой цензуры в государственных СМИ (Навального запрещено показывать на федеральных телеканалах). Но есть более интересная точка зрения: Навальный, по крайней мере какое-то время, ухитрялся не выходить за рамки борьбы с коррупцией и четко знал, какие — и чьи — секреты раскрывать, а какие — нет. В отличие от других известных критиков Путина, вроде отбывающего тюремный срок миллиардера Михаила Ходорковского и находившегося в добровольном изгнании олигарха Бориса Березовского, Алексей Навальный, похоже, нашел способ бросить вызов Кремлю, борясь с коррупцией, но не заходя на слишком чувствительную для режима территорию, что могло бы быть для него смертельно опасным. (За исключением плохо смонтированной фотографии, появившейся в прокремлевских СМИ, на которой Навальный, смеясь, беседует с Березовским, нет никаких свидетельств об их связи.) Кажется, что до июля 2012 года власть терпела его, но затем использовала для его дискредитации все возможные средства, предъявив Алексею официальные обвинения в злоупотреблениях, связанных с продажей принадлежавших государственной компании лесоматериалов в бытность его советником губернатора Кировской области. Эти обвинения в преступлении, максимальное наказание за которое — десять лет тюремного заключения, отражают угрозу, которую несут для режима непрекращающиеся антиправительственные протесты. Мир продолжает следить за судьбами таких фигур, как Навальный, чтобы понять, поможет ли его подход обеспечить цифровым активистам защиту от давления властей.

Однако существует опасная возможность появления сайтов, созданных людьми, которые скопируют внешний вид и устройство известных платформ для публикации секретных материалов, но не будут разделять их мотивы. И тогда вместо убежища для информаторов они станут местом

хранения и распространения всевозможного ворованного контента: информации о ведущихся военных операциях, взломанных банковских счетах, украденных паролей и домашних адресов, — не связанного никакой особенной идеей, кроме идеи анархии. И такими сайтами будут управлять не идеологические или политические активисты, а агенты хаоса. Пока хакеры и прочие информационные преступники публикуют свою незаконно полученную добычу совершенно бессистемно: например, в 2011 году с одного из торрентов все желающие могли загрузить себе персональные данные 150 тысяч пользователей Sony, украденные хакерской группировкой LulzSec. Однако если появится централизованная платформа, сравнимая по безопасности и известности с WikiLeaks, это может стать настоящей проблемой. Очевидно, что на таких сайтах информация будет размещаться бесконтрольно, никто не станет заниматься ее редактированием и проверкой, а также обеспечением безопасности информаторов, в отличие от WikiLeaks и его медиапартнеров (Ассанж сказал нам, что на самом деле редактирует материалы лишь для того, чтобы снизить международное давление на организацию, которое ставит ее в трудное финансовое положение, и что предпочел бы вовсе не заниматься этим). Необдуманная публикация некоторых секретных данных вполне может привести к гибели людей. Компьютерные преступники почти наверняка будут организовывать масштабные утечки, чтобы вызвать наибольший ущерб. Выбор и обнародование определенной секретной информации отражает конкретную цель того, кто это делает, а размещение ее без разбора — пренебрежение к чужим секретам в целом.

Большое значение имеет и контекст. Насколько иной была бы реакция, в частности, западных политических лидеров, если бы на сайте WikiLeaks публиковались похищенные секретные материалы таких режимов, как венесуэльский, северокорейский или иранский? А если бы Брэдли Мэннинг (считается, что он предоставил WikiLeaks американские военные и дипломатические документы) был пограничником из Северной Кореи или дезертиром иранского «Корпуса стражей исламской революции», насколько иначе относились бы к нему политики и правоохранительные органы США? Появись сайты, посвященные разоблачению злоупотреблений в *тех* странах, тонластной элиты Запада, конечно же, был бы иным. Принимая во внимание прецедент, установленный президентом Бараком Обамой во время его первого срока — явную «нулевую терпимость» к несанкционированным утечкам секретной информации, допущенным официальными лицами американской администрации, — следует ожидать,

что в будущем правительства западных стран придут к двойным стандартам в отношении раскрытия информации в электронных СМИ, поощряя такие действия за рубежом в отношении враждебных стран и яростно борясь с ними у себя дома.

Кризис средств массовой информации

В будущем на нашу жизнь будет сильно влиять то, какими источниками информации мы пользуемся и каким доверяем. Содержание новостей в интернет-эпоху по-прежнему останется ключевым фактором успеха; кроме того, продолжится борьба за монетизацию и синдикацию контента, которую мы наблюдаем сегодня. Но как изменится привычный медиапейзаж в результате развития технологии, понижающего входные барьеры во всех отраслях экономики?

Абсолютно ясно, что ведущие мировые СМИ будут все чаще уступать в скорости сообщения новостей. Такие организации в эру всеобщего доступа в сеть просто не в состоянии угнаться за интернетом, и неважно, насколько талантливы их журналисты и корреспонденты и сколько у них источников. Основные мировые новости можно будет узнать в первую очередь благодаря таким платформам, как Twitter: открытым сетям, позволяющим распространять информацию мгновенно, глобально и очень просто. Когда у каждого человека на планете появится телефон с функцией передачи данных или доступ к нему — а это не столь отдаленное будущее, — тогда возможность сообщить миру «горячую новость» будет зависеть от везения и случая, что подтверждает пример одного жителя Абботтабада, ставшего известным после своих твитов, в которых он в режиме реального времени сообщил об операции по уничтожению Усамы бен Ладена*.

В конечном счете этот лаг между событием и моментом, когда о нем узнают традиционные СМИ, приведет к снижению лояльности их аудитории, поскольку читатели и зрители стремятся иметь более оперативные способы получения информации. Каждое следующее поколение землян будет производить и потреблять больше новостей, чем предыдущее, так что люди перестанут пользоваться средствами массовой информации, отстающими от жизни. Такие СМИ смогут удержать свою аудиторию только за счет анализа и прогноза, а также, что еще важнее, доверия к ним. Их аудитория будет

* Вот один из твитов, которые написал в Twitter пакистанский ИТ-консультант Сохаиб Атхар в ночь операции по уничтожению бен Ладена: «Над Абботтабадом в час ночи летает вертолет (такое нечасто бывает)».

60 НОВЫЙ ЦИФРОВОЙ МИР

доверять полученной информации, точности анализа и умению правильно расставлять приоритеты при отборе новостей. Иными словами, некоторые люди будут, с одной стороны, лояльны к новым платформам за скорость сообщения новостей, а с другой — к традиционным средствам массовой информации за последующую их трактовку.

Новостные СМИ сохранят за собой важную роль во многих аспектах жизни общества, но некоторые из них перестанут существовать в нынешнем виде, а выжившие изменят свои цели, методы и организационную структуру для того, чтобы лучше отвечать требованиям новой глобальной аудитории. По мере исчезновения языковых барьеров и повсеместного строительства вышек сотовой связи появятся новые авторы, потенциальные источники информации, гражданские журналисты и фотографы-любители, готовые внести свой вклад в массмедиа. И это кстати: на фоне сворачивания деятельности множества новостных СМИ, особенно на международной арене, свежие голоса окажутся востребованными. Выигрывает и аудитория, которая получит доступ к большему диапазону мнений и точек зрения. Появление огромного количества новых действующих лиц, объединившихся вокруг различных онлайн-платформ в огромную хаотичную медиасистему, приведет к тому, что крупнейшие традиционные СМИ будут не столько сообщать, сколько подтверждать новости.

При этом обязанности сообщать новости будут распределены намного шире, чем сейчас, что означает покрытие большего количества тем, но, возможно, с более низким качеством. Трансформируется роль традиционных СМИ: они станут в первую очередь собирать, хранить и проверять информацию, превратившись в своеобразный фильтр доверия, просеивающий все материалы и помечающий то, чему можно верить, а чему — нет, что стоит, а что не стоит читать и обдумывать. Такая проверка, а также способность убедительно анализировать происходящее критически важна представителям элиты — руководителям компаний, политикам и интеллектуалам, полагающимся на устоявшиеся, мощные СМИ. Элита может отдать предпочтение как раз *им* вследствие массового появления в сети низкокачественных новостей и непроверенной информации. В твиттере шансы наткнуться на глубокий анализ не выше, чем у обезьяны набрать на пишущей машинке собрание сочинений Шекспира (хотя они и повышаются в случае обмена твитами двух умных, авторитетных собеседников), но сила открытых, никем не регулируемых платформ для обмена информацией заключается в их скорости реагирования на события, а не в глубине или проницательности анализа.

Трудной задачей, которую придется решать традиционным СМИ, явится интеграция всех новых голосов из всех уголков планеты. В идеале журналисты должны будут не столько сами находить информацию, сколько сотрудничать с ее источниками: например, в статье о наводнении в Бангкоке нужно не просто процитировать представителя тайландинской компании — оператора речных круизов, но и дать ссылку на собственный новостной блог или Twitter этого человека. Естественно, при включении в материалы информации от необученных новичков повышается вероятность ошибок, поэтому многие уважаемые журналисты сегодня считают, что такое поощрение непрофессиональных репортеров гибельно для профессии. И эти опасения не назовешь беспочвенными.

Благодаря глобальному распространению интернета в цепочке формирования контента добавятся новые звенья. Одним из них станет сеть местных специалистов-шифровальщиков, имеющих дело исключительно с ключами для шифрования данных. И хотя они не являются источниками информации и не создают контент, их ценность для журналистов будет заключаться в создании необходимых механизмов конфиденциального общения сторон. Ведь диссиденты в странах с репрессивными режимами, таких как нынешние Беларусь и Зимбабве, всегда с большей готовностью делятся своими историями, если знают, что могут сделать это анонимно и безопасно. Потенциально такую технологию могут предложить многие, но местные независимые специалисты по шифрованию особенно ценятся. Это происходит уже сегодня: мы видим, что на Ближнем Востоке наряду с другими запрещенными товарами большим успехом пользуются услуги операторов виртуальных частных сетей (VPN), которые предлагают защищенный доступ диссидентам и группам бунтарски настроенной молодежи. Средства массовой информации будут полагаться на эти сети и специалистов по шифрованию данных, как полагаются сейчас при подготовке новостных материалов на независимых корреспондентов — стрингеров.

Что касается самих стрингеров, то в будущем появится новый их подвид. Сейчас это, как правило, малоизвестный журналист из другой страны, часто с нестабильной внутриполитической ситуацией, которому газета платит за репортажи с места событий. Нередко стрингер рискует жизнью, чтобы получить доступ к определенным источникам или оказаться в опасном месте, куда профессиональный журналист иногда не может или не хочет ехать. Может возникнуть отдельная категория стрингеров, имеющих дело исключительно с цифровым контентом и онлайн-источниками информации. Вместо того чтобы подвергать себя опасности в реальном мире, они,

62 НОВЫЙ ЦИФРОВОЙ МИР

пользуясь глобальным распространением интернета, будут получать материалы от источников, с которыми знакомы только заочно. То есть они, как и сегодня, выступят посредниками между журналистами и источниками информации. Однако, учитывая увеличение дистанции и повышение вероятности путаницы, характерных для виртуального мира, СМИ придется уделять еще большее внимание качеству переработки текста, а также проверке сведений и этической стороны репортажей.

Представьте себе, что известные актеры решают создать собственный новостной онлайн-портал, посвященный некоему взрывавшему их по тем или иным причинам этническому конфликту. Возможно, они считают, что традиционные СМИ недостаточно активно или не вполне объективно освещают его. И вот принято решение избавиться от привычных посредников и начать информировать общество напрямую, организовав, скажем, новостное агентство «Бранжелина Ньюс». Актеры направляют собственных корреспондентов для работы непосредственно в зоне конфликта и ежедневно публикуют посредством онлайн-платформы полученную от них информацию, которую сотрудники редакции облекают в форму новостей. Издержки такого агентства будут низкими — существенно ниже, чем у его традиционных крупных конкурентов: возможно, стрингерам и журналистам даже не понадобится платить — кому-то достаточно шанса получить известность. И вот за короткое время «Бранжелина Ньюс» становится главным источником информации и новостей об этом конфликте: во-первых, благодаря публичности его владельцев, а во-вторых, потому что своей работой заслужило доверие и воспринимается аудиторией вполне серьезно.

В будущем традиционные СМИ столкнутся с такого рода соперничеством, а не только с конкурентами в лице непрофессионалов, пишущих в Twitter и в собственные блоги, и это будет означать заметное усложнение медийной среды. Конечно, как мы уже отметили, многие люди отдадут предпочтение давно существующим агентствам новостей в силу привычки или веры в устоявшиеся институты, и серьезная работа — журналистские расследования, интервью с высокопоставленными людьми, анализ сложных событий с учетом широкого контекста, — как и раньше, останется уделом традиционных средств массовой информации. Для остальных диверсификация источников информации предоставит возможность выбора между серьезными СМИ и изданиями, созданными «знаменитостями». Учитывая, по всей видимости, непреодолимую любовь жителей многих стран (США,

Великобритании, да и других) к таблоидам, многие потребители, скорее всего, предпочтут новости от своих кумиров. То есть причиной популярности таких изданий будет не последовательность позиции и не качество контента, а «звездный» статус их владельцев.

И точно так же, как это уже происходит с благотворительными фондами и бизнес-проектами, известные люди начнут создавать собственные средства массовой информации в качестве логичного «расширения» собственного бренда. (Здесь мы пользуемся термином «известные люди» в максимально широком смысле, имея в виду заметные, публичные фигуры, а сегодня это может быть кто угодно — от звезд телевизионных реалити-шоу до популярных проповедников.) Конечно же, некоторые новые СМИ будут честной попыткой внести свой вклад в общественный дискурс, но многие окажутся скучным и практически лишенным содержания проектом с целью продвижения собственной персоны или получения коммерческой выгоды.

Мы застанем времена, когда новостные порталы известных людей будут привлекать толпы посетителей по причине их новизны или моды. И эту аудиторию не смутит тот факт, что содержание ресурса окажется несравненно хуже, а профессионализм его авторов — ниже, чем в традиционных СМИ. Критики станут ругать происходящие изменения и оплакивать смерть журналистики. Но не стоит спешить: если меняется аудитория, то должны перераспределиться и источники ее информирования. Люди сами разочаруются в СМИ знаменитостей из-за недостаточного количества новостей или постоянных ошибок журналистов. В случае средств массовой информации лояльность аудитории — вещь непостоянная, и чем сильнее становится конкуренция, тем заметнее это проявляется. А если доверия читателей и зрителей лишится достаточно большое количество подобных новых СМИ, это приведет к оттоку их аудитории в пользу профессиональных новостных ресурсов, которым, однако, тоже предстоит пережить трансформацию (обеспечить сбор новостей, расширить диапазон тем, сократить время реагирования на события). Не все ушедшие вернутся обратно, да и изначально не все недовольные традиционными СМИ отвергнут их и переключатся на новые модные платформы. В общем, посмотрим, насколько новые средства массовой информации, созданные известными людьми, изменят облик журналистики в долгосрочной перспективе, а вот их появление и участие в привлечении читателей, зрителей и рекламодателей, вне всякого сомнения, вызовет много шума.

* * *

Распространение интернета означает не только новые вызовы существующим СМИ, но и новые возможности прессы в целом, особенно в тех странах, где сейчас ее не назовешь свободной. Одна из причин, по которой коррумпированные чиновники, могущественные представители преступного мира и прочие темные силы могут продолжать преступать закон без страха наказания, заключается в том, что они контролируют местные информационные ресурсы: или непосредственно — в качестве владельца или издателя, или косвенно — посредством давления, подкупа, запугивания или насилия. Это касается и тех стран, где значительная доля СМИ принадлежит государству, как в России, и тех, где власть над огромными территориями удерживают криминальные синдикаты, как в Мексике. В результате недостаточной независимости журналистов растет безнаказанность преступников и снижается вероятность того, что широкая огласка приведет к давлению на политиков и заставит их принять меры к пресечению и расследованию незаконных действий.

Всеобщий доступ в сеть может сдвинуть баланс в пользу общества по многим причинам, и одной из наиболее интересных является возможность цифрового шифрования данных, расширяющего возможности подпольных или нелояльных режиму средств массовой информации. Возьмем международную некоммерческую организацию (НКО), миссия которой заключается в конфиденциальном сборе информации в местах, труднодоступных или опасных для журналистов. Что сегодня отличает такие организации от других, скажем, от групп наблюдателей или негосударственных медийных ресурсов, так это использование шифрования в их платформах. Принцип работы таких платформ оригинален, но довольно прост. Чтобы сохранить имена журналистов в тайне (а именно они всегда рискуют больше других), каждому репортеру информационного агентства в системе присваивается уникальный код. Код скрывает их имена, номера мобильных телефонов и прочие идентификационные данные, при этом получить доступ к расшифрованным данным могут только ключевые сотрудники в штаб-квартире НКО, которая, что очень важно, располагается за пределами страны. А в самой стране корреспондентов знают только по их уникальному коду, который используется и для отправки репортажей, и при взаимодействии с источниками информации и местными редакторами. Скажем, если кто-то из корреспондентов сообщит о нарушениях на выборах в Венесуэле (а таких сообщений в ходе президентских выборов в октябре 2012 года было много, хотя и не анонимных), подручные президента, ответственные за выполнение «грязной» работы,

не смогут его «вычислить», не имея доступа к его персональным данным: даже редакторы не знают, кто он на самом деле. При этом корпункты как таковые в стране также отсутствуют, чтобы не оказаться мишенью. Конечно, изначально СМИ придется проверять своих репортеров, но после того, как журналист получит доступ к системе, его «прикрепляют» к новому редактору (незнакомому с ним), а его персональные данные надежно скрываются во внутренних файлах платформы.

Так что НКО, находящаяся за пределами страны, будет управлять работой своей информационной платформы на безопасном расстоянии, позволяя различным ее пользователям без опаски взаимодействовать под покровом секретности. Сама по себе идея относиться к журналистам так же, как к источникам конфиденциальной информации (защищая их персональные данные и содержание материалов), не нова, но только сегодня становится возможным шифровать то, что позволяет их идентифицировать, и использовать онлайн-платформы для организации анонимного сбора новостей. Присылаемые журналистами статьи и другие важные материалы лучше хранить на серверах, расположенных в тех странах, где данные находятся под надежной защитой закона: так меньше риска. Вначале НКО может создать бесплатную платформу и предоставлять ее различным новостным ресурсам, которые получают финансирование из независимых источников. А затем объединить все в одну суперплатформу, представляющую «засекреченные» журналистов со всего мира. Мы не являемся сторонниками усилившейся в последнее время тенденции в сторону анонимности, но считаем, что если безопасность под угрозой, а режим репрессивный, то анонимность становится вынужденной мерой, актом отчаяния. Тогда редактор в Нью-Йорке сможет войти в систему под своим логином и паролем, задать поиск по журналистам из Украины и найти кого-то подходящего с длинной историей публикаций и даже рекомендациями от своих коллег, работавших с ним раньше. После чего редактор, даже не зная настоящего имени журналиста и полагаясь исключительно на качество его прежних статей и доверие к платформе в целом, сможет решить, стоит ли начинать сотрудничать с этим человеком. А затем сделать зашифрованный звонок посредством все той же платформы, чтобы познакомиться и пообщаться с ним.

Создать и поддерживать такого рода распределенную, взаимно анонимную систему сбора новостей будет совсем нетрудно, а благодаря шифрованию персональных данных корреспондентов (да и их редакторов) и хранению репортажей на удаленных серверах к ним не дотянутся руки тех, кто выступает против независимой журналистики. Что сделают

66 НОВЫЙ ЦИФРОВОЙ МИР

оны с цифровой платформой, особенно в эпоху, когда у любого человека есть доступ к новостям прямо с мобильного устройства? Конечно, пока доступ в сеть там, где сегодня отсутствуют свободные СМИ, затруднен, но по мере изменения ситуации местные журналисты смогут сообщать о происходящих в их странах событиях все более широкой аудитории — по сути, выйти на международный уровень. Таким образом, две эти тенденции — повышение безопасности для тех, кто пишет репортажи, за счет шифрования данных и рост их аудитории за счет повсеместного доступа в сеть — дают уверенность в том, что, даже если судебная система страны слишком коррумпирована или слаба для того, чтобы должным образом наказать нарушителей закона, их можно публично обвинить в преступлениях в онлайн-СМИ. Возможно, не всех полевых командиров из Восточного Конго удастся предать Международному уголовному суду, но их жизнь осложнится, если каждый их шаг будет фиксироваться независимыми анонимными журналистами, а статьи об их преступлениях станут разлетаться по всему интернету. Как минимум их потенциальных сообщников отпугнет такая «цифровая радиоактивность»: если человек слишком заметен и находится под пристальным наблюдением общественности, он не может считаться надежным партнером по преступному «бизнесу».

Тайна частной жизни: каждый понимает ее по-своему

Обязанности по защите конфиденциальных данных и охране тайны частной жизни лежат на всех: на самих пользователях, на бизнесе и на общественных институтах. Предполагается, что такие компании, как Google, Apple, Amazon и Facebook, будут оберегать данные, защищать свои информационные системы от взлома и обеспечивать пользователей наиболее эффективными средствами для максимально полного контроля над сохранением тайны их частной жизни и личной безопасностью. Но то, как применять эти средства, зависит лишь от самих пользователей. Желая упростить себе жизнь, мы подвергаемся риску утечки конфиденциальной информации, а ведь ее объемы растут ежедневно. И не стоит полагаться на клавишу Delete! Возможность «удалить» данные — не более чем иллюзия: удаленные файлы, сообщения электронной почты и текстовые сообщения легко восстанавливаются. Очень редко данные стираются из физической памяти компьютера: как правило, операционная система лишь удаляет файл из списка во внутренней директории, сохраняя при