Глава 6

У нас все ходы записаны

Эта глава посвящена цифровым следам,
которые мы вольно или невольно оставляем
своим присутствием в интернете.
Мы узнаем, где и как это происходит, от каких следов
можно избавиться, а какие остаются навсегда.
И еще: нужно ли об этом беспокоиться или нет.

Во все века люди стремились оставить о себе память, след в истории. Одни творили и строили, другие, как Герострат, — наоборот, разрушали. Но, в любом случае, самого факта действия было мало — нужно, чтобы он был задокументирован и сохранен в анналах истории, иначе даже современники быстро забудут о ваших подвигах. Да и собственная память может подвести, поэтому лучше все записывать сразу, а не фантазировать потом, когда придет охота писать мемуары.

> *Писатель, поэт, журналист и общественный деятель Константин Симонов вел подробный архив, который он сам называл «Все сделанное», — сейчас это звучит как название папки в компьютере.*
>
> *«Архив Константина Михайловича огромен и по-своему сложен.... Мало ему было собственных трудов. При его разнообразной и активной деятельности на его голову буквально сыпались в невероятном количестве письма, материалы, деловые бумаги, рукописи всех жанров... Представьте себе, он ведь с шестнадцати лет хранил все присылаемые ему письма и снимал для себя копии со своих», — рассказывала Нина Павловна Гордон, бывшая в течение многих лет секретарем писателя[1].*

Чтобы вести такой архив, надо быть очень организованным человеком, и далеко не каждый на это способен. В наши дни задача сильно упростилась: интернет помнит все, хотим мы того или нет.

---

1 Из книги Бориса Панкина «Четыре Я Константина Симонова».

Интернет помнит все, хотим мы того или нет.

Каждое отправленное письмо или сообщение, каждый клик по ссылке, открытие сайта, каждый пост, лайк или комментарий в соцсети, фотография или видео, телефонный звонок или SMS, покупка в магазине (онлайн или офлайн, если по банковской карте), любая поездка (самолетом и поездом, само собой, в том числе и городским транспортом, — во время самоизоляции в Москве проехать в метро по карте «Тройка» можно было, только если она привязана к цифровому пропуску), все ваши маршруты пешком и на велосипеде или самокате — это цифровые следы, остающиеся в памяти разных компьютерных систем. Причем эти данные сохраняются практически навечно, и, откровенно говоря, у вас нет возможности полностью удалить свой цифровой след, несмотря даже на последние инициативы законодателей (об этом чуть ниже).

> ***Цифровой след*** *(или цифровой отпечаток; англ. digital footprint) — совокупность информации о посещениях и действиях пользователя во время пребывания в цифровом пространстве. Может включать в себя информацию, полученную из интернета, мобильного интернета, веб-пространства и телевидения.*

Принято разделять цифровые следы на активные и пассивные. Активные — это то, что люди делают сами, включая публикации в соцсетях, комментарии, фотографии и так далее. Своей активностью пользователь может управлять — например, выбирать, на какие темы писать, какие делать репосты, как себя вести в комментариях. То есть осознано формировать свой цифровой образ. А пассивные — это то, что компьютерные системы записывают автоматически: IP-адрес, с которого вы выходите в интернет, история посещений

сайтов, данные геолокации и прочее. Большинство людей и не подозревают о том, как много следов они оставляют в цифровом пространстве, даже если помалкивают и не ввязываются ни в какие холивары. Некоторые называют цифровые следы «цифровой тенью» — будем считать, что это одно и то же.

Большинство людей и не подозревают о том, как много следов они оставляют в цифровом пространстве.

Контролировать свои пассивные следы практически невозможно. Чтобы от них полностью избавиться, нужно совсем перестать пользоваться телефоном и компьютером, и то не факт, что это поможет. Во-первых, все важные вехи вашей жизни, от рождения до смерти, фиксируются в государственных информационных системах — учеба в школе и в институте, служба в армии, работа, свадьба, развод, участие в выборах, получение водительских прав, покупка квартиры, выезд за границу, обращение в поликлинику, — буквально каждый ваш чих оставляет цифровой след. (Это в полной мере ощутили москвичи, которых обязали пользоваться приложением «Социальный мониторинг» во время пандемии коронавируса.)

Если вы живете в большом городе, то вы каждый день попадаете в поле зрения камер видеонаблюдения. Например, в Москве в 2019 году их насчитывалось больше 170 тысяч, и мэрия планировала установить еще, обещая даже запустить систему распознавания лиц. Так что в скором времени все наши перемещения по городу будут известны, как минимум, властям, а, возможно, и хакерам, потому что абсолютно надежных систем не бывает.

Скоро все наши перемещения по городу будут известны, как минимум, властям, а, возможно, и хакерам.

Кто этому точно порадуется, так это будущие историки, которым больше не придется по крупицам собирать информацию, рассеянную в письмах и книгах, а можно будет написать один запрос к базе данных и получить исчерпывающую фактографическую информацию о перемещениях и активности своего героя. Дальше им останется только придумать, каким образом лучше ее визуализировать и каким комментарием снабдить.

> *Поэтесса Анна Ахматова не вела блог и не отмечалась в соцсетях, но тем не менее мы сейчас имеем возможность просмотреть ее цифровые следы. Хотите совершить виртуальную прогулку по ахматовским местам в Москве? Пожалуйста! Необходимые геоданные в машиночитаемом виде уже лежат на Портале открытых данных РФ.*
>
> *Загружаете эти данные в Google My Maps — сервис внутри Google Maps, позволяющий создавать свои собственные карты, и вуаля — ваша карта готова! Можно отправляться по цифровым следам любимой многими поэтессы — просто кликайте по меткам на карте. Вот здесь, во флигеле сталинской высотки на Котельнической набережной, Ахматова гостила у Фаины Раневской в 1950-е; в районе Остоженки жила в 1917-1918 годах со своим вторым мужем, ассириологом и поэтом Владимиром Шилейко; на Никитский бульвар ходила в гости к Михаилу Булгакову и его жене, которая была подругой Ахматовой, а на Поварской общалась с писателями Борисом Пильняком и Корнеем Чуковским*[1].

1 *Электронный след Анны Ахматовой. // Системный Блок{ъ}, 23 июня 2019.*

Если даже прошлое может быть оцифровано, что уж говорить о настоящем! Очевидно, что дальнейшая история человечества будет записана в цифровом формате и со все большими подробностями — вплоть до создания полной цифровой копии всей жизни каждого человека.

Риск и польза геоданных

«— Киса, — продолжал Остап, — давайте и мы увековечимся. ... У меня, кстати, и мел есть! Ей-богу, полезу сейчас и напишу: „Киса и Ося здесь были"».

Говоря современным языком, Остап Бендер таким образом решил «зачекиниться».

Когда интернета еще не было, люди оставляли информацию о посещении каких-то мест более прямолинейным способом — в виде надписи на камне, на заборе или стене. Сейчас эту функцию взяли на себя наши цифровые компаньоны, и делают это автоматически, днем и ночью, вне зависимости от того, просим мы их об этом или нет. Ведь вы же не выходите из дома без мобильного телефона, да? Он фиксирует ваше местонахождение даже без подключения к интернету. Ваш смартфон — фактически GPS-устройство. Если функция геолокации включена, его встроенный приемник получает сигналы со спутников и с высокой точностью определяет ваши координаты.

Распространено заблуждение, что спутники GPS каким-то образом следят за пользователями и знают, где те находятся. На самом деле, спутники только передают сигналы. Ни спутники, ни операторы GPS-оборудования не знают, где вы находитесь, и сколько

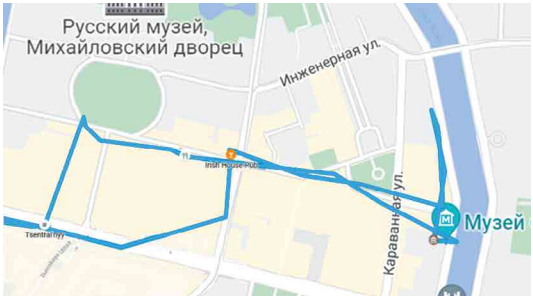
людей использует систему. Спутники — это просто маячки, по которым GPS-навигатор определяет свое местоположение.

Ни спутники, ни операторы GPS-оборудования не знают, где вы находитесь, и сколько людей использует систему.

А кто же тогда следит? Это делают приложения, установленные на телефоне. Зайдите в свой Google-аккаунт и откройте страницу **https://www.google.com/maps/timeline** — если вы никогда раньше сюда не заходили, то вас ожидает сюрприз.

> *Google помнит все ваши перемещения, все адреса и явки будут как на ладони. Можно даже посмотреть, где вы были в конкретный день.*

Теперь не скажешь «ой, где был я вчера, не найду, хоть убей, только помню, что стены с обоями». «Гугл» все помнит, и даже покажет фото, которые вы сделали в каждом месте. Допустим, вы гуляли по Невскому проспекту, заходили в музеи и кафе, прошлись по набережной, — спроси вас через год про точный маршрут, так вы и не скажете. А на карте все видно!



Хотя с позиционированием он иногда ошибается — может быть, просто «глючит», а может быть — не по своей вине. Например, довольно часто бывает, что люди гуляют около Кремля, а GPS показывает, что они во Внуково, — спецслужбы устраивают такие фокусы, чтобы запутать шпионов. То есть на точность записей Google на 100% полагаться нельзя. Разработчики это тоже знают, поэтому в приложении есть функция «Подтвердить место», где вы были, или «Удалить» его из маршрута. Вы можете отключить функцию слежения и даже стереть всю историю или подчистить отдельные места, пребывание в которых вам не хочется афишировать. Не ходи к гадалке, параноики скажут, что это ничего не значит, и что на серверах Google все равно вся информация сохранится, — и, возможно, они будут правы. Но если вы не делали ничего противозаконного, беды в этом большой нет.

Можно отключить функцию слежения, стереть всю историю или подчистить места, пребывание в которых вам не хочется афишировать.

Ну, ладно «Гугл» — ему мы все-таки доверяем. Однако на вашем телефоне могут быть шпионские приложения, которые отправляют информацию о ваших перемещениях неизвестно кому и неизвестно с какой целью. Поэтому не стоит скачивать приложения из непроверенных источников и давать им доступ к геолокации. Если это приложение для ловли покемонов, то о'кей — доступ к геоданным ему действительно нужен, иначе не поиграешь. А если это очередная модификация Тетрис, то зачем ему знать, где именно вы решили убить немного времени, укладывая падающие фигуры?

Не стоит скачивать приложения из непроверенных источников и давать им доступ к геолокации.

Вы можете подумать, что, отключив GPS на телефоне, избавитесь от отслеживания ваших перемещений. Увы! При включенном wi-fi все будет прекрасно работать, может быть, даже еще точнее. Ведь вы, скорее всего, включаете wi-fi на телефоне, когда находитесь дома или на работе, и вряд ли сразу выключаете его, выйдя за дверь. (Особо продвинутые могут настроить так, чтобы это делалось автоматически, но это требует специальных усилий.) А в городе полным-полно точек доступа, и ваш телефон будет все время пытаться подключиться к ближайшей из них, раскрывая, таким образом, ваше местоположение.

Каким же образом эта коробочка, раздающая беспроводной интернет, узнает, где она сама находится? Ведь в wi-fi-роутере нет GPS-приемника: принесли из магазина, включили и все. А происходит вот что: когда в зоне сигнала роутера появляется телефон с включенным GPS, информация об обнаруженных wi-fi сетях передается поставщику его операционной системы (например, Apple, или Google для телефонов на Android). Таким образом, геопозиция нового роутера фиксируется и заносится в базу. Потом, когда кто-то заходит в кафе или магазин, где стоит этот роутер, и подключается к wi-fi со своего телефона (пусть и с выключенным GPS), его координаты мгновенно определяются. И вовсе не обязательно логиниться в эту wi-fi-сеть — достаточно того, что ваш телефон ее увидел. Аналогичным образом работает геопозиционирование по вышкам сотовой связи — их точное местоположение хорошо известно, а точка, где вы сейчас находитесь со своим телефоном, вычисляется методом триангуляции (эти данные доступны только оператору).

Точность позиционирования по wi-fi и станциям мобильных операторов может достигать 5-15 метров, что даже выше, чем по сигналу со спутника GPS, — если вы находитесь в районе с очень плотной инфраструктурой связи. Например, в Москве одно лишь количество публичных точек доступа превышает 60 тысяч, не считая wi-fi-роутеров, установленных в квартирах. А в самой большой базе данных точек wi-fi, принадлежащей компании Combain Positioning Solutions, хранятся координаты почти 2,7 миллиардов устройств. Естественно, все они находятся в населенных пунктах или вдоль дорог — в тундре или тайге обнаружение с помощью такого метода вам не грозит.

> *В Google есть способ, позволяющий администраторам точек доступа (включая вас, если вы управляете домашним или офисным wi-fi), отказаться от внесения координат вашего роутера в глобальную базу данных. Добавьте «_nomap» в конец имени сети (например, mynetwork_nomap), и Google больше не будет отслеживать его.*

Однако Google не единственная компания, собирающая такие данные, и не все компании предоставляют столь простые способы отказаться от отслеживания. Поэтому, скорее всего, ваш wi-fi-роутер все-таки окажется в какой-то глобальной базе данных. Стоит ли по этому поводу волноваться? Пожалуй, нет. В базу попадает только уникальный номер вашего устройства (MAC-адрес), который никак не связан с вашими персональными данными. Пускай ваш роутер тоже будет одним из маячков в цифровом океане — вдруг он однажды поможет заблудившемуся путнику найти дорогу.

Что делать, если вам все-таки хочется «пропасть с радаров»? Манипуляции с настройками телефона, скорее всего, не помогут. Рас-

следование Associated Press, проведенное в 2018 году, показало, что многие службы Google на устройствах Android и iPhone хранят данные о вашем местоположении, даже если вы явно указали в настройках конфиденциальности, что запрещаете это делать[1].

Что делать, если хочется «пропасть с радаров»? Лучше всего просто выключить телефон.

Поэтому лучше всего будет выключить телефон. Но даже это не гарантирует, что он не отслеживает свои (то есть ваши) координаты, уверены параноики, и советуют для большей надежности вынуть из него батарею. Возможно, они правы, но не со всеми моделями это получится. Сначала лучше задать себе вопрос: с какой целью вы хотите стать невидимым? Ведь геотрекинг работает, скорее, на благо вашей безопасности, нежели против нее. Полиция, например, активно использует цифровые следы при раскрытии преступлений.

> *Летом 2019 года в Солт-Лейк-Сити пропала девушка, студентка местного университета. Ее тело нашли три недели спустя в 90 милях от города. В доцифровую эпоху это преступление имело бы высокие шансы остаться нераскрытым, но в наши дни все оставляют цифровые следы — и жертва, и преступник, что помогает работе полиции. Следователи проанализировали геоданные с телефона девушки (по записям оператора мобильной связи) и выяснили, что человек, подозреваемый в ее похищении и убийстве, находился неподалеку от нее в тот момент, когда ее телефон прекратил работу. Сначала подозреваемый отрицал, что знаком с потерпевшей, однако*

1 *AP Exclusive: Google tracks your movements, like it or not. // AP News, 14 августа 2018.*

на его телефоне обнаружили несколько ее фотографий, и он, кроме того, оказался подписан на ее «Инстаграм». Конечно, одних только цифровых следов было бы недостаточно, чтобы предъявить обвинение, но они очень помогли в поиске преступника. Позже полицейские обнаружили и более серьезные улики[1].*

Преступник оказался бывшим специалистом по ИТ, но это ему не помогло. «Хороший айтишник может пойти и сделать отличную работу, чтобы подчистить свои следы, но я гарантирую вам, что он не сможет сделать эту работу исчерпывающе. В продуктах и системах, которыми мы пользуемся, встроены некоторые вещи, практически исключающие полное блокирование работы полиции», — прокомментировал ситуацию частный детектив с 25-летним стажем, занимающийся расследованием подобных случаев[2].

Тем не менее, постоянный мониторинг ваших перемещений вполне обоснованно может вызвать раздражение и ощущение вмешательства в частную жизнь. С одной стороны, это так. Но с другой — вы же не думаете, что все это результат всемирного заговора, и что технологические мегакорпорации вместе со спецслужбами озабочены тем, чтобы вызнать про вас все подробности? Все гораздо проще: компании хотят вам что-то продать, и для этого они хотят знать ваши маршруты и любимые места — чтобы показывать вам более точную рекламу, а взамен они предоставляют вам множество

---

* *Соцсеть признана экстремистской и запрещена на территории РФ.*

1 *Body of Utah student Mackenzie Lueck recovered, identified. // FOX8 Digital Desk, 5 июля 2019.*

2 *How an alleged killer's digital footprint led to his capture. // ABC4.com, 29 июня 2019.*

полезных сервисов, таких как карты, такси, поиск друзей поблизости, ресторанов, магазинов, игры вроде покемонов, фитнес-трекеры для учета своих ЗОЖ-достижений и многое другое. Большинство из этих приложений бесплатны.

По-моему, это честная сделка. И потом: вы же хотите знать, где находится ваш ребенок и куда он вообще ходит, да? Если технологии в этом помогают, то это хорошо — для его безопасности и вашего спокойствия. Любые инсинуации про постоянную слежку и Большого Брата в данном случае будут неуместны — это ваше право и обязанность как родителя. И закон, и здравый смысл в этом вопросе на вашей стороне.

> *В июле 2019 года Госдума окончательно одобрила законопроект об упрощении поиска пропавших детей с помощью геолокации. В случае пропажи ребенка его родители (или один из них, или законные представители) смогут обратиться в органы полиции с письменным заявлением, и те в течение 24 часов должны начать поиски, в том числе с возможностью получить доступ к данным геолокации мобильных устройств ребенка — например, его телефона или планшета. При этом о начале проведения таких оперативно-розыскных мероприятий правоохранительные органы должны будут также уведомить суд, и в течение 48 часов с момента их начала получить судебное решение о проведении такого оперативно-розыскного мероприятия, либо прекратить его проведение, — говорится на сайте Думы*[1].

---

1 *Принят закон об упрощении поиска пропавших детей. // Государственная Дума, официальный сайт, 24 июля 2019.*

Председатель Государственной Думы Вячеслав Володин подчеркнул, что возможность правоохранительных органов оперативно получить доступ к данным геолокации ребенка позволит значительно ускорить его розыск. «Это время может оказаться бесценным, если, например, ребенок заблудился, потерялся или с ним случилась беда», — отметил он.

По словам председателя профильного Комитета по безопасности и противодействию коррупции Василия Пискарева, «в случае пропажи ребенка быстрое определение его местонахождения также поможет пресечь совершение в отношении него противоправных действий и не допустить наступления общественно опасных последствий, сохранить его жизнь и здоровье».

Безусловно, это здравое решение, и его можно только приветствовать — технологии могут и должны использоваться во благо. Однако на этом примере снова видно, насколько те, кто пишет законы, далеки от понимания того, как работает интернет.

В переводе с бюрократического языка на человеческий это означает, что «данные о геолокации мобильных устройств ребенка» — это данные оператора связи, который вычисляет местоположение устройства относительно вышек сотовой связи. Их действительно надо запрашивать у компании, онлайн они недоступны. Преимущество этого метода только в том, что таким образом можно получить координаты даже самого примитивного кнопочного мобильника, с которого нет доступа в интернет. Но какой подросток согласится ходить с таким гаджетом? Ведь засмеют! Да и как на нем играть? А даже самый дешевый китайский смартфон умеет выходить в Сеть и позволяет устанавливать приложения — значит, на него можно установить и приложение для обеспечения безопасности.

Даже самый дешевый смартфон выходит в Сеть и работает с приложениями — значит, на него можно установить и приложение для обеспечения безопасности.

Например, Kaspersky Safe Kids позволяет видеть на карте местоположение ребенка (точнее говоря, его телефона). При этом можно заранее задать безопасный периметр и получать уведомления о выходе ребенка за его пределы. А чтобы не впадать в панику почем зря, приложение еще сообщит вам о низком уровне заряда батареи на его устройстве и заодно не даст соврать «ой, у меня телефон разрядился», когда ребенок не хочет отвечать на ваши звонки.

На случай, когда ребенок намеренно не выходит на связь, а в это время у бабушки давление уже скакнуло под 200, тоже есть решение. Хорошо, что некоторые отцы умеют программировать. Одному из них, англичанину Нику Герберту надоело, что сын может игнорировать его сообщения и звонки, поэтому он придумал приложение Respond ASAP, которое блокирует телефон ребенка до тех пор, пока он не перезвонит родителям. Если телефон ребенка вдруг стоит на беззвучном режиме, приложение может запустить специальную сирену, чтобы звонок не остался незамеченным. Пока есть только версия для Android, над версией для iOS Ник еще работает.

Вот что он сам написал об этой истории на своем сайте **http://respondasap.co.uk/**:

> *«...У меня есть сын Бен. Когда он пошел в среднюю школу, я купил ему смартфон, чтобы иметь возможность связаться с ним, а он мог бы связаться со мной (разумеется, не во время занятий).*

Однако то, что я считал решением, превратилось в другую проблему. Поскольку телефон «умный», Бен может на нем играть в игры и смотреть видео. Поэтому он всегда держит телефон в беззвучном режиме, чтобы я об этом не знал. Когда я пытаюсь связаться с ним, он редко отвечает — либо потому, что не слышит сигнала, либо потому, что (и мне, наконец-то, пришлось признаться в этом самому себе) смущается говорить с отцом в присутствии друзей.

Иногда мне нужно передать ему сообщение, но он не может знать, насколько важен звонок или текст, который он игнорирует или не видит, а у меня нет возможности узнать, видел ли он его (я имею в виду именно видел, а не просто смахнул сообщение, чтобы продолжить игру). Существуют приложения-мессенджеры, которые сообщают вам, когда сообщение доставлено и просмотрено, но ведь оно может быть проигнорировано просто потому, что сигнал о его получении никто не слышал.

RespondASAP ® — мое решение этой проблемы.

В процессе разработки я поговорил с Беном, показал ему дизайн и концепцию приложения; идея ему понравилась, потому что, получив такое сообщение, он обязательно услышит его и поймет, что это нечто важное. Более того, у него будет возможность отправлять такие же сообщения мне. Так у нас возникает взаимопонимание, что RespondASAP® предназначено только для важных случаев, а то, что Бену нужны новые батарейки для контроллера Xbox, к таковым не относится.

Мои друзья увидели и другие «взрослые» применения этого приложения, потому что большинство из них большую часть

времени тоже держат свои телефоны в беззвучном режиме. Предложения варьировались от изменения заказа, когда друг берет вам напитки в баре, или поиска телефона, потерянного где-то дома, до рабочих ситуаций, когда нужно быстро связаться с коллегами...»

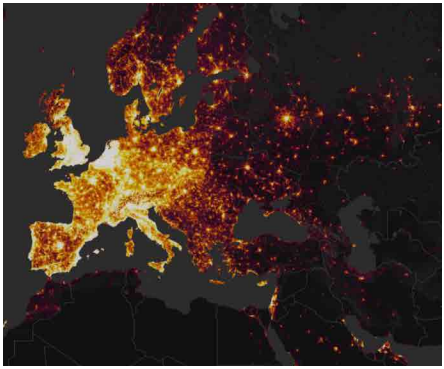
Конечно, существует риск, что злоумышленники получат контроль над вашим телефоном или доступ к вашему аккаунту с историей перемещений. Да, всякое вторжение в частную жизнь неприятно, поэтому надо предпринимать превентивные меры, чтобы такого не произошло, защищать свою информацию и не пренебрегать правилами цифровой гигиены. А еще рекомендуем иметь поменьше тайн, раскрытие которых может вам навредить.

Мы живем в прозрачном мире, где ничего нельзя абсолютно надежно спрятать.

Помните, что мы живем в прозрачном мире, где ничего нельзя абсолютно надежно спрятать. Например, не надо выкладывать маршрут своей пробежки в интернет, если вы служите на секретном объекте, — такая курьезная история действительно произошла. Хакерам даже не потребовалось ничего ломать, достаточно было проанализировать открытые данные.

Бегают сегодня все — студенты и бизнесмены, домохозяйки и кинозвезды, пенсионеры и топ-менеджеры, любители собак (вместе с ними) и любители кошек (без них), спецагенты, солдаты и дипломаты. Поскольку все сегодня стало социальным, для бегунов есть специальные приложения, в которых они отмечают достижения, соревнуются заочно друг с другом, находят партнеров по тренировкам в реале — в общем, типичный клуб по интересам.

Вполне логично, что такие приложения записывают маршруты пробежек, чтобы вести статистику и точно подсчитывать сожженные калории, контролировать кардионагрузки и другие показатели физической активности. Разработчикам одного такого популярного приложения Strava пришла в голову мысль отобразить все пробежки своих пользователей по всему миру на тепловой карте. Надо признать, поучилось красиво!



Карту опубликовали в ноябре 2017-го, а спустя два месяца неожиданно случился конфуз. 20-летний австралийский студент Натан Русер, изучающий международные конфликты, обнаружил, что на этой карте можно увидеть и фитнес-маршруты солдат и агентов в чувствительных местах, включая американские базы в Афганистане и Сирии, авиабазу Великобритании на Фолклендских островах Маунт-Плезант, предполагаемую базу ЦРУ в Сомали и даже Район 51 (где, как говорят, американское правительство скрывает доказательства существования НЛО). Главным образом, в поле зрения

попали американские и британские войска, но также на этой карте засветились и российские базы — в том числе беговые дорожки наших дипломатов в Дамаске. В государствах, где не ведутся войны, карта окрашена примерно одинаково по всей площади, а в горячих точках она темная, за исключением мест дислокации военных.

Формально никакой утечки не произошло — данные на карте Strava обезличены, из них нельзя выяснить, кто именно бегает в этих отдаленных местах. Но сам факт повышенной физической активности в определенных районах уже позволяет делать выводы о присутствии там воинских формирований. Ну, не инопланетяне же бегают по секретной базе! Хотя кто знает...

Пентагон отреагировал быстро и объявил о новой политике, вступившей в силу немедленно: всем действующим сотрудникам Министерства обороны США запрещено использовать функции слежения на своих телефонах и устройствах в оперативных районах (в любом месте, где военные выполняют определенную миссию). Командиры могут разрешить использование в каждом конкретном случае только после проведения проверки безопасности. Обязательное обучение кибербезопасности теперь будет включать информацию о фитнес-трекерах и других технологиях, способных к геолокации.

Министерство обороны России запретило военнослужащим включать на смартфонах геолокацию вскоре после публикации об открытии австралийского студента.

Учитывая сказанное выше про возможности геолокации, эти меры нельзя признать достаточными. На самом деле у военных есть только один выход: полностью отказаться от использования потребительских

смартфонов, если они хотят сохранить режим секретности. Обычным же законопослушным гражданам не о чем беспокоиться: им можно бегать по утрам и вечерам там, где заблагорассудится, и спокойно делиться своими маршрутами с товарищами по этому увлечению.

Стоит ли бояться своей цифровой тени?

«Человек без тени — ведь это одна из самых печальных сказок на свете», — писал Евгений Шварц в одной из своих самых известных пьес (по мотивам сказки Г. Х. Андерсена). Мы добавим, что в наше время человек, не имеющей цифровой тени, — то есть тот, о ком в Сети нет никакой информации или она крайне скудная, — не выглядит реально существующим. Он становится призраком, если не оставляет цифровых следов. Получается как в пьесе Шварца: когда Ученый опрометчиво отправил свою тень к принцессе, он сразу упал в обморок и все всполошились: «Беги за доктором! Доктор уложит дурака в кровать недели на две, а тем временем у него вырастет новая тень», — говорит один из персонажей.

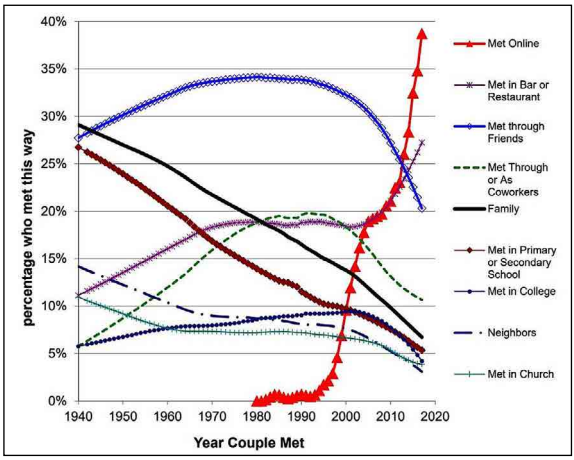
Не теряйте свою цифровую тень и следите за ее здоровьем: кормите хорошей информацией и водите гулять в интересные места.

Так что не теряйте свою цифровую тень и следите за ее здоровьем: кормите хорошей информацией, водите гулять в интересные места, — когда ваш принц или принцесса захотят с вами познакомиться, им будет легче понять, что вы за человек.

Опросы показывают, что 7 из 10 молодых людей в Великобритании проверяют интернет-профили человека перед тем, как отправить-

ся на свидание со своим визави, и 40% из них с подозрением относятся к людям, о которых сложно найти информацию в интернете. Только один из двадцати (5%) юношей и девушек в возрасте от 18 до 24 лет говорят, что они никогда этого не делают[1].

Интернет сегодня становится основным местом, где люди находят себе пару. Все остальные способы знакомства остались в прошлом веке. Просто примите это как факт. Встречают теперь не по одежке, а по аватарке и цифровому следу.



Michael Rosenfeld et al., Stanford University, Reuben J. Thomas, University of New Mexico, Sonia Hausen, Stanford University. Disintermediating your friends: How Online Dating in the United States displaces other ways of meeting. // Published in 2019 in the Proceedings of the National Academy of Sciences, Volume 116, issue 36, https://doi.org/10.1073/pnas.1908630116

---

1 *Would you go on a date with someone who didn't have a digital footprint? // YouGov, 2018.*

Выращивать правильную цифровую тень полезно не только из романтических соображений. Это влияет и на такие более прозаические и насущные стороны нашей жизни, как, например, поиск работы или обращение за кредитом в банк. Современный человек без адекватной цифровой тени вызовет много вопросов у любой службы безопасности. Поэтому не торопитесь уходить в полный цифровой детокс на веки вечные. Будет лучше, если вы научитесь с этим жить.

Воздействие цифрового следа на жизнь пользователей возрастает с каждым годом: к примеру, опросы показывают, что если в 2006 году только 11% работодателей проверяли социальные сети соискателя на работу, то в 2017-м это делали уже 70% компаний (по данным Career Builder, США, 2017). Едва ли в России ситуация принципиально отличается[1].

Но удивительное дело: насколько же много в интернете публикаций на тему того, как удалить свои цифровые следы! Почему-то людей это очень беспокоит. Авторы советов по «выпиливанию» себя из интернета, как правило, не озабочены тем, зачем это делать и каковы будут последствия. Они одержимы лишь одной идеей — стать цифровыми невидимками, чтобы скрыться от всевидящего ока государства.

Авторы советов по «выпиливанию» себя из интернета, как правило, не озабочены тем, зачем это делать и каковы будут последствия.

В большинстве случаев их советы, по меньшей мере, наивны, потому что у правительств есть свои механизмы отслеживания граж-

1 *70% of employers are snooping candidates' social media profiles. // Career Builder, 15 июня 2017.*

дан. Кроме того, цифровых следов сегодня так много и системы стали настолько сложными, что никакие рекомендации не будут исчерпывающими и надежными. И если уж вы что-то такое натворили, то цифровой след где-то все равно останется, — там, где вам и в голову не придет искать.

В Мидлтауне, штат Огайо, в сентябре 2016 года сгорел дом 58-летнего Росса Комптона. К счастью, хозяин успел выбраться через окно, но его кошка погибла в огне. Сгорело все: дом площадью 2000 квадратных футов с четырьмя спальнями и тремя ванными комнатами стоимостью 179 тысяч долларов вместе со всем имуществом. Страховая компания оценила общий урон в 400 тысяч долларов.

Вроде бы обычное дело — пожар: загорелась электропроводка или коротнуло что-нибудь. Тем не менее, департамент пожарной охраны начал расследование — порядок есть порядок. Об умышленном поджоге сначала никто не думал: трудно поверить, что человек подожжет дом и оставит своего питомца умирать в огне. Но эксперты обнаружили, что очагов возгорания было несколько, да и сам погорелец путался в показаниях. Однако всего этого было недостаточно, чтобы сделать вывод о мошенничестве. Понятно же: у человека стресс, а ко всему прочему оказалось, что у него «искусственное сердце» — то есть он пользуется кардиостимулятором.

«Ага!» — сказали следователи и запросили ордер на получение медицинских данных с кардиостимулятора Комптона. Они хотели знать, каков был его пульс до, во время и после пожара. В судебных документах говорится: «Кардиолог, проверивший данные, определил: очень маловероятно, что г-н

Комптон смог собрать, упаковать и вынести такое количество вещей из дома, выбраться через окно своей спальни и оттащить многочисленные большие и тяжелые предметы в сторону за столь короткий промежуток времени при наличии имеющихся у него заболеваний»[1].

То есть налицо было очевидное вранье. В этом деле полиция впервые использовала данные кардиостимулятора, которые оказались отличным средством расследования и помогли выдвинуть обвинение в поджоге с целью получения страховки.

Даже продвинутые хакеры оставляют следы, по которым их находят. Обычным же пользователям лучше учиться ответственному поведению в цифровой среде и не впадать в цифровой анархизм.

«Многие очень опасаются трансформации общества и тотального контроля за обществом, вроде того, что описаны в книгах Хаксли или Оруэлла, — пишет на своей странице в соцсети учитель истории Александр Гулин. — Я всегда парирую цитатой из Джона Леннона «Каждому есть что скрывать, кроме меня и моей обезьянки»[2]*. До 30 лет я вообще ничего нигде не терял и не забывал, держал все на контроле. Но возраст берет свое: часто, решая рабочие вопросы, отключаешь блок, связанный с контролем себя самого. (Обычно все происходит из-за банальной спешки.) В прошлом году я забыл на остановке сумку со всеми документами (доб-рые люди на следующий день меня нашли*

---

1 *Cops use pacemaker data to charge homeowner with arson, insurance fraud. // CSO Online, 30 января 2017.*

2 *Everybody's Got Something to Hide Except Me and My Monkey — песня The Beatles из «Белого альбома», написанная Джоном Ленноном.*

и вернули). Зимой оставил макбук в такси (благодаря приложению, водитель привез его мне на следующий день). В пятницу в каршеринге выпал чехол от AirPods (ну очень торопился подписать какие-то документы). «Делимобиль» пытался найти мои вещи, но безрезультатно. И тут в воскресенье вечером мне пришло письмо от Belka Car — отчет о поездке в пятницу (я дважды ездил на «Делимобиле» и один раз на «Белке»): по цифровым следам машины они нашли человека, который пользовался ею после меня. Естественно, он им сообщил, что нашел мои наушники, и завтра с утра я могу забрать их на пункте охраны. Технологии не хорошие и не плохие; они упрощают нашу жизнь — на моем примере видно, что из-за цифровых следов я вернул намного больше, чем мог потерять. И вообще, хороших людей больше, чем плохих, — Джон Леннон это знал...»

Каждый клик — в истории

История посещения веб-сайтов и отдельных страниц — один из богатейших и ценнейших источников цифрового следа, оставляемого человеком. Маленькие дети, «дорвавшись» до компьютера, совершенно не задумываются о том, что каждый их клик сохраняется в истории браузера, и что потом будет неудобно, когда мама увидит, какие «интересные» ролики смотрел ее сын на YouTube. Он-то на голубом глазу будет все отрицать, — дескать, он только играл в игру, которую ему открыли. Но предатель-браузер быстро выведет врунишку на чистую воду.

(В принципе, ничего драматичного в этом нет. Ну, посмотрел и посмотрел. Тему про «недетский» контент и ограничение доступа

к нему мы разберем в другой главе; сейчас наше внимание сосредоточено на технике.)

> *История браузера хороша тем, что наглядно показывает, насколько дотошно фиксируются в интернете все действия пользователей, и как легко попасть в неловкую ситуацию, когда вы думаете, что делаете что-то втайне, а на самом деле это видно всем.*

Хорошо будет выучить этот урок с детства, потому что во взрослой жизни все точно также: на работе ваш системный администратор видит, какие сайты вы открывали и сколько времени вы там сидели, и если дело дойдет до конфликта с руководством, то эти данные запросто лягут на стол вашему начальнику, и крыть будет нечем.

Более-менее продвинутый ребенок уже знает об этом коварстве со стороны браузера и умеет чистить историю, благо это совсем не сложно: достаточно нажать «Ctrl-H», и появится список посещенных веб-страниц с точным временем посещения. Если ваша рука сразу тянется к кнопке «Очистить историю» — не спешите. Вездесущий «Гугл» уже запомнил все ваши блуждания по сайтам и настроил свои алгоритмы показа рекламы, так что локальная чистка в браузере ничем не поможет. Зато если вы вдруг закрыли страницу с какой-то важной информацией и забыли название сайта, то можно будет его найти в истории, — согласитесь, это весьма полезно.

> *Кроме истории, есть еще кэш браузера — место, где он хранит временные файлы. Когда вы в первый раз открываете веб-страницу, то сначала все картинки и тексты с нее скачиваются на ваш компьютер (или телефон), а потом уже показываются на экране.*

Причем, когда вы закрываете страницу и даже удаляете из истории запись о том, что вы ее смотрели, в кэше все равно остается ее копия. Это делается для того, чтобы ускорить его работу, — когда вы в следующий раз зайдете на ту же страницу, картинки не будут скачиваться заново, и вы увидите ее быстрее. Удобно? Конечно! Как водится, за все удобства надо платить. В данном случае плата невысока, всего лишь место на диске и цифровой след, отображающий ваши интересы.

Пока вы пользуетесь интернетом с личных устройств, про кэш браузера можно не беспокоиться — разве что иногда почистить, если возникли какие-то сбои с отображением некоторых страниц, а вот когда приходится пользоваться публичными компьютерами, об этом следует помнить. Например, вам нужно зайти в почту и переслать письмо с копией паспорта и другими документами вашему турагенту, чтобы оформить поездку в отпуск. Вы открыли письмо — и сканы паспортов попали в кэш. Поэтому, закончив свои дела, не забудьте очистить историю браузера и удалить сохраненные данные. В браузере Chrome для этого надо нажать "Ctrl-Shift-Del", и откроется окно «Очистить историю», в других браузерах есть аналогичная команда.

Закончив работать на публичном компьютере, не забудьте очистить историю браузера и удалить сохраненные данные.

Простые методы, описанные выше, защитят вас от чьих-то слишком любопытных обычных глаз, но не от профессионалов. В большинстве случаев этого будет достаточно, и не стоит пренебрегать такими мерами предосторожности, но помните — есть и более продвинутые инструменты: такие, как, например, HstEx — утилита из арсенала компьютерной криминалистики,

которая создана и разработана для восстановления удаленной истории и кэша браузера. Предположим, человек захотел что-то утаить, удалив свои следы, — в таком случае программа HstEx поможет их извлечь из недр жесткого диска[1].

> *Разумно не пользоваться публичными компьютерами и чужими устройствами для любых операций, требующих ввода личной информации: просмотра почты, платежей через интернет-банк, подключения или отключения услуг в личном кабинете мобильного оператора или чего-то подобного.*

Кстати, если вы используете домашний компьютер в коллективном режиме (один на всех), то будет лучше завести для каждого члена семьи отдельный аккаунт. В этом случае и история браузера тоже будет у каждого своя, и тогда среди недавно просмотренных роликов у вас не окажутся сплошь стримы «Майнкрафта» и популярные ютьюберы. Также верно и обратное: если вы сами решите вечером посмотреть какое-то кино для взрослых, ребенок не увидит эту ссылку на стартовой странице, когда ему будет позволено посмотреть мультики.

Но этого мало: еще нужно будет приучить всех заходить только под своим аккаунтом и обязательно выходить из него, закончив играть или работать. Эта полезная привычка не раз сослужит вам хорошую службу, когда придется пользоваться чужими компьютерами. Например, школьники после занятий очень часто оставляют свои сессии открытыми, и кто угодно может получить доступ к их данным.

---

1 HstEx: **http://www.spy-soft.net/hstex/**

Нужно приучить всех заходить только под своим аккаунтом и обязательно выходить из него, закончив играть или работать.

Если по каким-то причинам вам не хочется оставлять следов в браузере, то можно воспользоваться режимом, когда функция отслеживания выключена. В браузере Chrome это называется режим «инкогнито», в Firefox — приватное окно, в Microsoft Edge — режим InPrivate; аналогичные режимы есть и в других браузерах. В таком режиме не сохраняются файлы cookie, данные сайтов и история просмотров, а также информация, которую вы вводите в формы. Когда это может вам понадобиться? Например, когда нужно что-то быстро посмотреть с чужого компьютера или телефона.

Но не стоит обольщаться насчет секретности в этом режиме: ваши действия в приватном окне видны системному администратору и интернет-провайдеру, а также доступны веб-сайтам, которые вы посещаете. Использование режима «инкогнито» скорее можно отнести к правилам цифрового этикета, нежели к средствам обеспечения безопасности. Приличный человек не оставляет за собой мусор, в том числе и цифровой.

Приличный человек не оставляет за собой мусор, в том числе и цифровой.

Перечитайте предыдущий абзац внимательно: даже в приватном режиме действия пользователя в браузере видны внешнему наблюдателю. Теперь представьте ситуацию: какой-то не слишком знакомый вам человек, случайно оказавшийся в компании, просит вас одолжить телефон — дескать, ему надо срочно зайти в свою почту и ответить на письмо. Надеюсь, вы понимаете, что все его

действия для провайдера, а, следовательно, и для правоохранительных органов будут выглядеть как ваши?

> *Иногда лучше показаться невежливым, чем потом доказывать, что это были не вы. В Англии даже есть поговорка «Не пиши в интернете то, чего не можешь сказать полицейскому».*

Право на забвение и эффект Стрейзанд

«Что написано пером, того не вырубишь топором». Европейские, а следом за ними и российские законодатели решили оспорить эту народную мудрость и приняли ряд актов, которые условно называют «законом о забвении». Причина его возникновения ясна: она в том, что возник конфликт между правом человека на тайну частной жизни и свойством интернета помнить все. Действительно, нельзя же всю жизнь тыкать человека носом в ошибки молодости или в какие-то другие факты его биографии, которые давно утратили актуальность, но неизбежно всплывут в поисковой выдаче, как только новый работодатель или деловой партнер захочет просмотреть его цифровые следы.

> *В мае 2014 года Европейский суд рассматривал дело испанского гражданина Марио Костеха Гонсалеса против корпорации Google. В 2010 году Гонсалес обратился в Национальное агентство по защите данных с требованием удалить электронную версию статьи 1998 года в архиве газеты La Vanguardia о продаже его дома на аукционе в счет уплаты долга, который был впоследствии им погашен, а также ссылки на эту статью.*

В итоге дело дошло до Европейского суда, который вынес решение, что ссылки на Гонсалеса надо удалить, но только с испанского сайта Google.es, а материалы газеты оставить как есть. В первый же день вступления этого решения в силу Google получил 12 тысяч запросов на удаление персональных данных из своей поисковой системы («Википедия»).

Это решение было воспринято как крайне неоднозначное — особенно в США и Великобритании, где свобода слова имеет приоритет над правом на конфиденциальность. По мнению противников «закона о забвении», он может привести к цензуре и переписыванию истории. «Кто контролирует прошлое, контролирует будущее», — писал Оруэлл и, несомненно, был прав. К тому же вызывает вопросы техническая реализация закона. В частности, редактор британского журнала Index on Censorship заявил The Guardian, что право на забвение выглядит как «план людей, не знающих, как работает интернет»[1].

Похоже, что это действительно так. Формально поисковики подчинились и разместили на своих сайтах специальную форму, где нужно указать адреса страниц, которые вы требуете удалить из поисковой выдачи, и убедительно аргументировать, почему это нужно сделать. Все обращения рассматриваются вручную, и при наличии объективных причин вашу заявку удовлетворят (но это неточно).

Предположим, вам удалось реализовать свое право на забвение, и раздражающая вас статья исчезла из индекса поисковика. А как быть с тем, что она осталась на сайте издания, которое ее опубликовало?

---

1 *Google to fight Spanish privacy battle. // The Guardian, 16 января 2011.*

Законодателей это не волнует. Видимо, они считают, что люди не умеют пользоваться другими инструментами поиска, кроме Google, Bing или Yandex. На самом деле в мире существует большое количество поисковиков, далеко не все из которых подчиняются правилам конкретной юрисдикции. Как мы видели из дела Костеха, даже Google нашел паллиативное решение, удалив ссылку только с испаноязычного домена.

Достиг ли Марио Костеха Гонсалес своей цели? В интервью 2014 года он выражал полное удовлетворение решением Европейского суда. Действительно, ссылку на ту злополучную статью удалили из поиска. Зато его имя стало нарицательным, и теперь уж точно никто не забудет, что в 1998 году он испытывал финансовые трудности, а потом судился с Google. В его случае мы видим действие эффекта Стрейзанд[1] во всей красе — когда кто-то пытается изъять информацию из общественного доступа, это приводит к ее большему распространению. В общем, на чужой роток не накинешь платок. Странно, что люди этого не понимают.

Попытки изъять информацию из общественного доступа приводят к ее большему распространению.

В Англии сформировалась другая культура по отношению к информации. Если в вашей биографии был какой-то нели-

1 *Эффект Стрейзанд (англ. Streisand effect) — социальный феномен, выражающийся в том, что попытка изъять определенную информацию из публичного доступа (цензура) приводит лишь к ее более широкому распространению (обычно посредством интернета). Термин получил распространение в 2003 году, когда Барбра Стрейзанд обратилась в суд с требованием взыскать с фотографа Кеннета Адельмана и сайта Pictopia.com 50 миллионов долларов США, так как фотография ее дома была доступна среди более 12 200 других фотографий побережья Калифорнии.*

цеприятный факт, то надо быть готовым, что это в любой момент может быть опубликовано, а потому иметь заготовленный разумный ответ, вместо того чтобы пытаться заткнуть рот говорящему.

Лучше иметь заготовленный разумный ответ, чем пытаться заткнуть рот говорящему.

Вот, например, Ричард Брэнсон в автобиографии «К черту все! Берись и делай!» со всей откровенностью рассказывает, как в 1971 году он попал под арест по обвинению в продаже в магазинах Virgin пластинок, которые декларировались как экспортные товары. Тогда таможня согласилась отказаться от уголовного преследования и уладить дело без суда, но весь ущерб ему пришлось возместить. А ведь мог бы умолчать про эту историю и потребовать права на забвение, чтобы никто ее не раскопал.

Британский подход к проблеме в целом выглядит более здравым, особенно в контексте современных технологий, когда гарантировать полное удаление какой-то информации практически невозможно — для этого нужно также уничтожить все ее копии, которых может быть сколько угодно и в самых разных местах.

Но законодателям Италии, Германии, Франции, Аргентины и ряда других стран пример Испании понравился, невзирая на технические сложности и эфемерность результатов. В результате граждане, которые тоже не особо разбираются в том, как устроен интернет, завалили главный европейский поисковик заявлениями об удалении разной информации о себе. Возможно, европейцы просто не знают, что в «Яндексе» «найдется все» — в том числе все, что удалено из «Гугла».

Европейцы просто не знают, что в «Яндексе» «найдется все» — в том числе все, что удалено из «Гугла».

Все та же газета La Vanguardia, получившая мировую известность в связи с первым делом по закону о забвении, по прошествии пяти лет подвела итоги его применения. С 2014 года по начало мая 2019 года Google получила в Европе 802 259 запросов на удаление данных, затрагивающих 3 127 986 веб-страниц, из которых 1 199 955 было удалено — 44,5% запросов. Из них 88,6% были выдвинуты частными лицами, а остальные — несовершеннолетними, юридическими лицами, политиками и людьми, занимающими общественные или другие должности[1].

Получается, что законодатели, действуя из лучших побуждений, на самом деле только подняли волну достаточно бессмысленной активности, направленной почти исключительно против корпорации Google. Пользователи «вошли во вкус» и захотели добиться большего успеха, чем Марио Костеха Гонсалес, — чтобы о них забыли не только в родной стране, но и вообще везде.

Чтобы не доводить ситуацию до полного абсурда, Европейский суд в начале 2019 года вынес решение о том, что «право быть забытым» не должно иметь обязательной юридической силы во всем мире. Дело возникло после того, как Национальная комиссия Франции по информационным технологиям и гражданским свободам (CNIL) оштрафовала Google на 100 тысяч евро за неспособность удалить информацию о человеке из всех его

1 *Cinco años de una sentencia pionera "para olvidar". // La Vanguardia, 11 мая 2019.*

доменов в интернете. Google обратился в суд с просьбой аннулировать штраф и выиграл спор[1].

Но это все взрослые дела. А как насчет детей?

> *В январе 2015 года в штате Калифорния вступил в силу закон, который неофициально называют 'Online Eraser Law for Minors' — «закон об онлайн-ластике для несовершеннолетних», если перевести буквально. Согласно этому закону, веб-сайты и другие операторы интернета обязаны удалять по требованию любой контент, опубликованный несовершеннолетними. Закон также запрещает передавать данные несовершеннолетних третьим лицам в целях маркетингового продвижения товаров и услуг. Но его действие не распространяется на контент, опубликованный третьими лицами, в котором присутствует информация о ребенке или подростке[2].*

В принципе, подход здравый: взрослый человек должен думать головой, прежде чем публиковать в интернете всякие глупости и отвечать за возможные последствия. Например, если вы выкладываете свои фото с чумовой вечеринки с друзьями, а потом вас не приглашают на серьезную работу, то это целиком ваша проблема. Для несовершеннолетних же закон делает исключение: ну, пошалили — и хватит! Детские выходки стираем, и добро пожаловать во взрослую жизнь.

---

1 *'Right to be forgotten' by Google should apply only in EU, says court opinion. // The Guardian, 10 января 2019.*

2 *How does California's Erasure Law stack up against the EU's right to be forgotten. // IAPP.org, 17 апреля 2018.*

У нас в России детские неразумные публикации могут обернуться вполне взрослыми проблемами — ведь в интернете «все ходы записаны». Это знают, в том числе, и сотрудники правоохранительных органов.

> *В июле 2019 года произошло два похожих случая: суд оштрафовал на 2 тысячи рублей молодых жителей Ульяновска и Владимира по статье 20.29 КоАП РФ — Производство и распространение экстремистских материалов — за посты «ВКонтакте», размещенные ими в 2010 году, когда одному из них было 12 лет и другому примерно столько же. Оба они запостили какие-то песни, которые, наверное, тогда казались им крутыми, а потом были признаны экстремистскими, — вот вам и административное правонарушение. Не то, чтобы пятно на всю жизнь, но неприятно*[1].

Поэтому нелишним будет объяснить подростку, что надо бы произвести ревизию своих музыкальных пристрастий и генеральную уборку на своей странице «ВКонтакте». И не только музыкальных.

Но как это сделать? В Федеральном Перечне экстремистских материалов сегодня почти 5 тысяч позиций. Дать ребенку полный список — только возбудить лишнее любопытство. Да и как технически сопоставить содержимое его страницы с перечнем?

В России аналогичный «закон о забвении» появился в 2016 году[2]. Согласно ему, операторы поисковых систем должны по запро-

---

1 *Двух россиян оштрафовали по статье об экстремизме из-за постов «ВКонтакте» девятилетней давности. // МБХ медиа, 18 июля 2019.*

2 *Федеральный закон от 13 июля 2015 г. № 264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации».*

су граждан изымать из выдачи ссылки на материалы, которые, по мнению заявителей, являются недостоверными или неактуальными. При этом закон во вступившей в силу редакции не распространяется на внутренний поиск по соцсетям.

Только за три первых месяца после вступления закона в силу Google, по ее данным, получила свыше 1,4 тысячи запросов на удаление ссылок, а «Яндекс» — более 3,5 тысяч. При этом обе компании удалили более четверти запрошенных ссылок[1].

Чтобы воспользоваться своим правом быть забытым, нужно заполнить специальную форму в каждом из популярных поисковиков:

- **Google**
  https://support.google.com/legal/troubleshooter/1114905
  https://support.google.com/legal/contact/lr_rudpa?product=websearch&uraw=

- **Яндекс**
  https://yandex.ru/support/abuse/troubleshooting/oblivion.html

- **Mail.ru**
  https://go.mail.ru/support/oblivion/

В форме понадобится указать адреса страниц, которые вы хотите изъять, и пояснить, какое отношение они имеют к вам, и почему не должны появляться в результатах поиска. Чем больше аргументов вы при этом приведете, тем больше шансов, что за-

1 *Конституционный суд не усомнился в «праве на забвение» // Газета «Коммерсантъ», 20 апреля 2019.*

прос удовлетворят: запросы рассматриваются вручную, и решение по каждому случаю принимается индивидуально. К форме нужно будет приложить копию паспорта или другого документа, удостоверяющего личность: их сверят, чтобы избежать ошибок.

> *Решение принимает администрация сервиса, которая может и отказать. Не всякая информация подлежит удалению по желанию гражданина, а лишь признанная недостоверной или неактуальной.*

Если вы не согласны с решением и хотите настоять на удалении каких-то сведений о себе, то можете обратиться в суд. Только помните об эффекте Стрейзанд: пока вы общаетесь с поисковиком, это ваше частное дело, — поисковики не публикуют информацию о запросах на удаление данных. А вот идти в суд, чтобы отстоять свое право быть забытым, — лучший способ достичь обратного эффекта. Так случалось уже не раз, однако граждане этого упорно не понимают и продолжают наступать на одни и те же грабли, приобретая все более широкую известность. Эффект Стрейзанд работает в интернете неумолимо. Это испытал на себе, в частности, продюсер Евгений Пригожин, который в итоге отозвал свой иск к «Яндекс», и авторитет Сергей Михайлов, известный как «Михась»: суд он, правда, выиграл, но тем самым напомнил о своих прошлых делах всем, кто давно уже о них забыл.

Право на забвение у вас есть, но пользоваться им нужно аккуратно.

Короче говоря, право на забвение у вас есть, но пользоваться им нужно аккуратно, с пониманием того, как работают технологии и как распространяется информация в Сети.

Заметаем цифровые следы самостоятельно

Как мы с вами выяснили, иметь цифровые следы — нормально, даже для ребенка. В целом пользы от них больше, чем вреда. Однако бывают ситуации, когда свою цифровую историю нужно основательно почистить. При этом едва ли стоит впадать в крайность и пытаться удалить все следы своего присутствия онлайн — на самом деле, обычному человеку это не под силу, даже хакеры и спецслужбы не всегда справляются с такой задачей. Но кое-что можно сделать для уменьшения будущих рисков.

> *Прежде всего, стоит удалить все аккаунты, которыми вы не пользуетесь, а, стало быть, не меняете пароли к ним и вообще не следите за их безопасностью. О'кей, хорошая мысль, но как их все найти?*

Довольно часто учетные записи привязываются к почте, и если у вас почтовый ящик на Gmail, то можно воспользоваться сервисом **deseat.me**, который найдет все ваши активные и давно забытые аккаунты в соцсетях и на других сайтах, чтобы провести ревизию и решить, что оставить, а от чего пора избавиться.

Если у вас другая почта, то придется удалять свои учетные записи вручную. Вспомнить, где вы регистрировались, поможет менеджер паролей — специальное приложение или сервис в браузере. Идем методично по списку и «пропалываем» наши цифровые грядки. Иногда бывает так, что владельцы интернет-ресурсов не хотят расставаться со своими пользователями и прячут функции удаления аккаунта поглубже. В этом случае воспользуйтесь советом сайта Justdelete.me (**https://backgroundchecks.org/justdeleteme/ru.html**), который сразу перенаправит вас на нужные страницы или объяснит, почему удаление невозможно.

Не рубите сгоряча, может быть, вам еще пригодится ваша история — вдруг надумаете мемуары писать?

Многие ресурсы — например, «ВКонтакте», почти все сервисы Google и другие — дают возможность выгрузить все свои посты, фотографии и документы в виде архива и сохранить у себя на компьютере. Не всегда эта функция на виду, но если поискать, то найдется. Не рубите сгоряча, может быть, вам еще пригодится ваша история — вдруг надумаете мемуары писать? Но помните, что если уж «рукописи не горят», то цифровая информация и подавно, — где-то копия все равно останется.

Мы уже не раз говорили, что в интернете почти ничего не исчезает. Но где же это все лежит, если мы этого не видим? Вот, например, написал человек сгоряча какой-то твит, а потом подумал и удалил. Или компания решила полностью переделать веб-сайт, где были, в том числе, и ваши посты в форуме — а в новой версии его вообще не оказалось. Бывает, что издание опубликовало какую-то новость, а она оказалась недостоверной, и пришлось ее убрать. Неужели все это исчезло навсегда? Вовсе не обязательно. Есть множество вариантов для путешествия в цифровое прошлое.

Во-первых, есть Wayback Machine — всемирный архив интернета с поисковым сервисом, позволяющим увидеть нужный веб-сайт таким, каким он был на определенный момент в прошлом. Вводите адрес, выбираете время — и готово! Проект ведет некоммерческая организация Internet Archive, которая с 1996 года создает цифровую библиотеку интернет-сайтов и других культурных артефактов в цифровой форме. Там хранятся копии веб-страниц, книги, газеты и журналы, телепрограммы, аудио и видеозаписи.

Во-вторых, кэш Google — поисковик сохраняет тексты всех проиндексированных им страниц, чтобы люди могли их просмотреть в случае недоступности сайта. Для этого в результатах поиска после адреса страницы нажмите кнопку со стрелкой вниз и выберите Cached — вам откроется сохраненная копия искомой страницы. Обычно информация хранится в кэше несколько дней, в зависимости от частоты переиндексирования сайта. Или можно воспользоваться специальным сервисом ***http://cachedview.com/****, который ищет сразу по кэшу.*

Аналогичным образом работают кэш «Яндекса» и других поисковых машин. Имеют архивные копии своих ресурсов все социальные сети, интернет-магазины, онлайн-библиотеки и другие провайдеры. Если вам понадобилось сохранить какую-то страницу, то для этого есть специальный сервис Archive.is: просто вводите адрес — и все, вы приняли участие в сохранении цифрового наследия.

Теперь вы понимаете, насколько трудно полностью уничтожить информацию после того, как она попала в интернет? Здесь все многократно копируется и архивируется, плотность записи все время повышается, а стоимость носителей падает, так что в обозримой перспективе процесс будет продолжаться. Поэтому лучше хорошенько подумать, прежде чем выкладывать что-либо в Сеть.

Как случайно попасть в «Википедию»

Чтобы удостоиться персональной статьи во Всемирной онлайн-энциклопедии, надо быть известным человеком. Таким, например,

как Олег Тиньков, про которого, естественно, есть статья. Из нее можно узнать, что, кроме всего прочего, он увлекается велоспортом и создал команду «Тинькофф», которая участвует в престижных международных велогонках.

> *В 2015 году на Джиро д'Италия Олег Тиньков участвовал в тренировках наравне со своими спортсменами и проехал всю дистанцию — неофициально. Естественно, это привлекло внимание прессы, и фото известного банкира на велосипеде пополнило его досье в «Википедии». Но, кроме самого Олега Юрьевича, в кадр попала пользовательница одной из соцсетей Юлия Барышева, которая просто приехала в Италию посмотреть велогонку. Позже фотографию увидели ее коллеги и рассказали ей. Юлия сама увлекается велосипедным спортом и работает в банковской сфере, так что история получилась сугубо позитивная. «За спиной сильного мужчины всегда должна стоять красивая женщина!» — пошутила она на своей странице в соцсети, обнаружив себя в «Википедии».*

Но давайте посмотрим шире: мы ежедневно попадаем в объективы чьих-то камер и не можем никак этого избежать. Это не только камеры наблюдения, про которые мы уже говорили.

> *Фотографируют сегодня все: наши друзья, туристы, случайные прохожие, блогеры и профессиональные журналисты. И все это с высокой степенью вероятности попадает в интернет, потому что все фото нынче цифровые.*

Это тоже часть цифрового следа, на которую очень трудно влиять. Поиск по изображениям и технология распознавания лиц скоро сделают такие фото источником информации о вас. Да и сейчас,

если вы публикуете фотографии в соцсетях, они сразу предлагают отметить на фото людей из числа ваших знакомых, — но вы же понимаете, что распознал-то он всех, да?

Едва ли имеет смысл этого бояться — надо просто учитывать, что мир действительно прозрачен. Если вы куда-то направляетесь по секрету и даже оставили свой телефон, чтобы вас не отслеживал Google, вы можете просто встретить на пути группу китайских туристов, которые запечатлеют вас в летний день на фоне Эрмитажа — а вы на работе сказали, что страшно больны и не можете выйти из дома. Получится неудобно.

По крайней мере, попробуйте не усугублять ситуацию — когда фотографируете что-либо сами, старайтесь, чтобы в кадр не попадали случайные люди. Это тоже часть современного цифрового этикета.

Когда фотографируете что-либо сами, старайтесь, чтобы в кадр не попадали случайные люди.

К тому же изображение частного лица защищает закон. В России это статья 152.1 Гражданского кодекса, которая гласит, что обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. К счастью, для любителей фотографии есть ряд исключений: согласие не требуется, если съемка производится в общественных местах и на публичных мероприятиях, или если гражданин позировал за плату (чем промышляют «живые статуи» в туристических местах).

В Европе с 2018 года действует GDPR, в котором есть аналогичная статья, запрещающая публикацию изображений третьих лиц без их ведома, но с такими же оговорками насчет публичных мест. Так что не надо безуспешно ждать, пока толпа перед «Моной Лизой» рассосется, чтобы, не дай бог, не нарушить право на конфиденциальность какого-нибудь европейца. Если вы не занимаетесь коммерческой фотографией, то вам не стоит бояться баснословных штрафов за это. Максимум, что может произойти, если кто-то из жителей Евросоюза увидит себя на вашей странице в «Фейсбуке»*, — он или она потребуют это фото удалить, и вам придется это сделать, потому что закон будет на их стороне.

- *Учитесь вести себя так, чтобы не было стыдно за свои цифровые следы.*

В общем, стоит помнить: любое наше действие в виртуальном мире и почти каждое в реальном оставляет цифровой след. И мы не всегда имеем возможность управлять этим. Учитесь вести себя так, чтобы не было стыдно за свои цифровые следы.

Контрольные вопросы

1. Что такое цифровой след?
2. Чем отличаются активные и пассивные цифровые следы?
3. Как местоположение отслеживается по wi-fi?

---

* *Соцсеть признана экстремистской и запрещена на территории РФ.*

4. Почему не стоит удалять все свои цифровые следы?

5. Когда нужно использовать режим «инкогнито» в браузере?

6. Что такое кэш браузера? Как его очистить?

7. Что такое «право на забвение»? Как это работает?

8. Что такое кэш Google? Можно ли его очистить?

9. Как увидеть, как выглядел какой-то сайт в прошлом?