**Деанонимизация и уникализация**

Деанонимизация − процесс установления личности пользователя в сети либо подлинного места выхода в сеть. Понятие деанонимизации неотделимо от понятия анонимности. Анонимность − это возможность посещать сайты, совершать какие-либо активные действия на веб-ресурсах, например оставлять сообщения, без возможности связать ваши действия с вашей реальной личностью или местом вашего выхода в сеть. Многие приравнивают анонимность к сокрытию подлинного IP-адреса, но это очень упрощенный подход. Во-первых, злоумышленник может провести JavaScript-атаку и, используя уязвимости в веб-браузере, получить доступ к вашему устройству. Дальше, получив контроль над устройством, постараться определить владельца на основе анализа посещаемых сайтов, реального IP-адреса, документов и информации в мессенджерах. Во-вторых, через сайт можно проверить наличие у вас аккаунтов в социальных сетях, где вы авторизованы. Если вы авторизованы в Facebook и там указаны ваши реальные данные, владелец сайта сможет получить их незаметно для вас.  
Установление личности пользователя или точки выхода в сеть по IP-адресу или mac-адресу называется пассивной деанонимизацией, когда против пользователя не применяется никаких атак. Атаки на пользователя, например через сайт с вредоносным JavaScript, или фишинг − это активная деанонимизация. Важно понимать отсутствие прямой связи между IP-адресом и каким-либо пользователем. IP-адрес принадлежит точке выхода в сеть. Например, если вы подключаетесь к Wi-Fi роутеру, то получаете IP-адрес данного роутера. Все остальные пользователи, подключившись к этому роутеру, получат этот же самый IP-адрес. Проверка IP-адреса может указать только интернет-провайдера и общее место расположения, проведя сканирование, можно определить модель роутера. Провайдер интернет-связи, подключивший кабель интернета к данному роутеру, знает, на кого он оформлен и где располагается, при запросе от компетентных органов он обязан выдать эту информацию. Есть еще возможность проанализировать логи провайдера, логи роутера − обо всем этом мы расскажем в главе, посвященной деанонимизации. Злоумышленник может взломать Wi-Fi роутер и затем начать перехватывать трафик с целью найти в нем зацепки для установления личности, например аккаунты социальных сетей, либо пытаться заразить компьютер через подмену DNS или «склейку» пакетов. Все это − активная деанонимизация, о которой мы будем еще много говорить. К слову, сокрытие IP-адреса важно не только для анонимности, но и для безопасности. Как уже было сказано выше, сканируя ваш IP-адрес, злоумышленник может взломать ваш роутер или модем, если вы выходите через Wi-Fi или 3G/4G-модем, либо прямо компьютер, если он подключен непосредственно к интернет-кабелю. Подобные истории происходят слишком часто, чтобы игнорировать данную угрозу.   
  
 **Уникализация**

Уникализация - поиск и сбор уникальных идентификаторов браузера для формирования уникального отпечатка, по которому всегда можно будет узнавать данный браузер независимо от IP-адреса и предоставляемых пользователем данных. Уникализация, как правило, не несет задачи установить личность пользователя, а лишь узнавать его в любой ситуации. Уникализация пользователей сайтов происходит благодаря уникальным отпечаткам браузера, таким как Canvas fingerprint, WebGL fingerprint, Front fingerprint и др., а также благодаря использованию cookies. Для формирования уникальных отпечатков вам достаточно всего лишь один раз посетить веб-сайт. Даже если в следующий раз вы посетите сайт с другого IP-адреса, предоставите иные авторизационные данные, сайт все равно вас узнает, а если сайт подключен к какой-либо антифрод или маркетинг-системе, собирающей отпечатки пользователей, то и другие сайты-участники этой системы смогут получить информацию о вас. HWID - уникальный отпечаток «железа», уникализирует устройство пользователя. Он может быть получен только при установке на ваш компьютер программы, которая соберет данные для уникализации. Уникализация устройства возможна благодаря наличию у комплектующих вашего компьютера уникальных серийных номеров. Серийный номер материнской платы, серийный номер жесткого диска задаются производителем, и изменить их − далеко не самая простая задача. Уникальные серийные номера есть даже у монитора и клавиатуры. Даже если вы удалите программу, переустановите систему и вновь установите программу, она узнает вас по тому же HWID, сгенерированному на основе уникальных серийных номеров «железа» вашего компьютера. HWID и различные идентификаторы «железа» используются в основном для лицензирования программного обеспечения и антифрод системами приложений. Уникализация браузеров пользователей в основном используется для борьбы с мошенниками, но может быть использована для отслеживания и даже деанонимизации. Например, вы зашли на сайт, где оставили свои данные, пусть это будет интернет-магазин. Этот магазин установил у себя антифрод систему, призванную защищать от мошенников. Антифрод система получила уникальный отпечаток вашего браузера и данные о вас, указанные при заказе. Получив эту информацию, она может узнать вас на любом сайте, который вы открыли и где размещены ее скрипты, хотите вы этого или нет.  
  
 **Нарушение приватности**

Немало пользователей путают приватность и анонимность, полагая, что это одно и то же или близкие понятия. На самом деле анонимность − это возможность посещать сайты, совершать какие-либо активные действия на веб-ресурсах, например оставлять сообщения, без возможности связать ваши действия с вашей реальной личностью или местом вашего выхода в сеть. А приватность − это отсутствие доступа к информации у лиц, для которых эта информация не предназначена. Например, вы общаетесь в мессенджере со своим собеседником, и за этим следит агент Джон. Если он пытается установить личности собеседников − это деанонимизация, он покушается на вашу анонимность. А вот если он читает вашу переписку − это уже нарушение вашей приватности: он получает доступ к информации, которая составляет вашу с собеседником тайну и не предназначена для третьих лиц. Самыми частыми нарушениями приватности являются чтение переписок в мессенджерах, просмотр электронной почты, прослушивание телефонов. К сожалению, спецслужбы значительно чаще хакеров и киберпреступников нарушают приватность простых пользователей сети.   
Но если спецслужбы и правоохранительные органы вашей страны нарушают вашу приватность в большинстве случаев на основании права, данного законом, то спецслужбы другой державы никакого права не имеют следить за вами. А они следят. Например, почтовый сервис Yahoo согласно данным, просочившимся в СМИ, сканировал входящие письма и передавал информацию разведке США. Эдвард Сноуден после этого скандала призвал всех удалять свои аккаунты в Yahoo, мы присоединяемся к данной рекомендации. К слову, переписки владельцев почты на Yahoo почитали, похоже, и хакеры, скомпрометировавшие по последним данным три миллиарда аккаунтов почтового сервиса. Действия Yahoo, разведки США и хакеров − грубое нарушение приватности пользователей. Бывают и менее грубые нарушения приватности. Например, почтовый сервис Gmail был замечен за анализом содержания писем своих пользователей, на основе которого выводил связанную с текстом рекламу. Это допускается пользовательским соглашением, которое вы принимаете при регистрации.

**Трекинг**

Наверное, каждый из вас сталкивался с ситуацией, когда вы ввели в поиске какое-либо слово, затем, закрыв поиск, перешли на сайт и вам показывается реклама, связанная с недавними поисковыми запросами? Это и есть трекинг. Простейший пример трекинга − адресная реклама в рекламной сети Google. У многих сегодня есть аккаунт в Google, который по умолчанию сохраняет все ваши поисковые запросы в поисковой системе Google. Эта информация используется рекламной сетью Google для вывода потенциально интересной вам рекламы. Аналогичным образом в России работает компания Яндекс. Зачем это нужно? Google зарабатывает, когда вы кликаете на рекламное объявление. Компания заинтересована показывать актуальную вам рекламу. Поисковый гигант собирает иную информацию о вас, такую как пол, возрастная группа, язык, страна. Согласитесь, мужчину 50 лет из Магадана навряд ли заинтересует предложение покупки молодежной одежды для девушек в Лондоне. Сегодня существует масса реализаций трекинга пользователей, например, трекинг по MAC-адресу. Ваш мобильный девайс или ноутбук при активном модуле Wi-Fi постоянно посылает сигналы, содержащие техническую информацию, в том числе и уникальный MAC-адрес устройства. Благодаря этой функции вы всегда можете находить Wi-Fi сети поблизости. Отправляемые устройствами данные можно мониторить, тем самым отслеживая перемещения владельца. Данная система применяется торговыми сетями и спецслужбами для отслеживания пользователей. Известно использование данной системы для поимки преступников, например, когда известен только MAC-адрес ноутбука преступника, а также то, что он появится в одном из ресторанов в центре города. Подобная система, при достаточном ее распространении, в течение нескольких секунд обнаружит преступника после того, как он включит свой ноутбук с Wi-Fi модулем. Есть и более продвинутые технологии трекинга, например, Cross-device tracking. Технология Cross-device tracking немного похожа на 25-й кадр, только в данном случае используются звуки. Изначально технология предполагала к рекламе на ТВ добавлять специальные звуковые маячки, которые бы могли воспринимать и обрабатывать мобильные девайсы, а затем передавать в единый центр обработки информации. Например, вы смотрите рекламу по Первому каналу, в этот момент раздается звуковой маячок. Его улавливает ваш мобильный и передает информацию в центр статистики, который собирает ее и затем может сказать, сколько человек видели рекламу, какие передачи и когда смотрели. Это гораздо эффективнее обзвонов и онлайн-опросов. Технология должна была позволить проводить высокоточную аналитику ТВ-рекламы и аудитории. Но разработка пошла не туда... Согласитесь, ничто не мешает подобный сигнал издать компьютеру, владелец которого хочет оставаться анонимным. А мобильный телефон, где анонимность настроена не настолько качественно, примет этот сигнал и передаст информацию о владельце в единый центр.

**Физический доступ**

Данная угроза предполагает получение физического доступа к устройству для кражи информации или совершения каких-либо действий, способных причинить вред владельцу. Самыми распространенными атаками являются: прямая кража информации, установка вредоносного программного обеспечения и подключение внешних носителей. Приведу пример атаки с использованием физического доступа. Злоумышленник подсмотрел ваш пароль, лично или поставив миниатюрную камеру неподалеку от вашего компьютера, затем он дожидается, когда вы отойдете, и устанавливает программу для шпионажа за компьютером. Программа работает незаметно для вас, собирая всю информацию и отправляя ее злоумышленнику. Шпионская программа руками добавляется в белые списки антивирусов, потому на них рассчитывать не стоит. Программы для слежки можно приобрести абсолютно легально, и предназначены они в основном для контроля за детьми. От вредоносного программного обеспечения эти программы отличает необходимость наличия физического доступа к компьютеру. Обычный функционал такого программного обеспечения включает запись происходящего на экране, запись всех нажимаемых клавиш, контроль периметра при помощи веб-камеры и микрофона, формирование удобных отчетов об активности пользователя. Некоторые программы умеют помимо незаметного сбора информации еще и цензурировать работу пользователя, блокируя доступ к некоторым сайтам. Как защищаться от подобной угрозы? Первым делом нужно добавить в пароль ложные символы: это защитит вас от любителей подсмотреть пароль. Второе: поставить и настроить Panic Button − программу, которая защищает от несанкционированного доступа к компьютеру. Можно и на этом не останавливаться: сегодня в свободной продаже имеются и замки, и сейфы, и сигнализации для ноутбуков.   
  
Другой довольно распространенный вид атаки − подключение внешних устройств, например, к вашему компьютеру незаметно подключается USB-флешка. При загрузке системы с этой USB-флешки вам загружается вредоносное программное обеспечение. На черном рынке можно найти предложения уже настроенных флешек, злоумышленнику останется просто вставить флешку . При этом далеко не всегда флешка с вирусом устанавливается злоумышленником, иногда вирус сам записывается на флешку, а ее владелец является такой же жертвой. Вредоносное программное обеспечение, попав на компьютер, нередко записывает себя на все внешние носители, которые затем будут заражать новые и новые устройства. Так распространялись и распространяются многие троянцы, включая легендарные Sality, Zeus Citadel и Zeus Gameover. Пик популярности подобного пути распространения пришелся на середину двухтысячных, сегодня он сходит на нет, так как файлы все чаще передают по сети. Разберем работу встроенных механизмов защиты, таких как Secure Boot. В рамках тестирования безопасности устройств мы с вами будем настраивать аналогичную USB-флешку для проверки защиты ваших устройств. На самом деле вариантов атак при получении физического доступа значительно больше: например, на ваш компьютер может быть установлено устройство, содержащее шпионский имплант. Это может быть простой кабель, соединяющий монитор с системным блоком, внешне он будет не отличим от оригинала, но в нем будет содержаться имплант, передающий злоумышленнику изображение с вашего экрана. RAGEMASTER Кстати, знакомьтесь, это RAGEMASTER − VGA-кабель с имплантом для шпионажа. Используется АНБ с 2008 года. Имея солидный бюджет, на черном рынке можно заказать подобное решение под любые модели мониторов. Шпионские импланты − более высокий уровень, требующий высокотехнологичных решений, обычно применяется для корпоративного и государственного шпионажа.

**Криминалистический анализ**

Криминалистический анализ − это набор технических решений и методик для извлечения ценной информации с цифровых устройств. Криминалистический анализ применяется, как правило, правоохранительными органами для поиска интересной для следствия информации на устройствах подозреваемых. Но ввиду того что техника и программное обеспечение находятся в открытом доступе, этот инструмент может получить любой злоумышленник. Криминалистический анализ можно проводить на десктопных компьютерах, ноутбуках, планшетах и смартфонах. Криминалисты прекрасно умеют работать со всеми популярными операционными системами: Windows, macOS, операционными системами на основе Linux, Android, BlackBerry и iOS. Отличием криминалистического анализа от простого физического доступа являются применяемые технологии. Криминалистический анализ большое внимание уделяет оперативной памяти устройства, где могут храниться ценные артефакты, например ключи шифрования, в некоторых случаях применяется атака DMA − получение прямого доступа к оперативной памяти, пришедшая на смену известной cold boot attack. Если кто не знает, cold boot attack − та самая атака, когда жидким азотом замораживается оперативная память, извлекается из устройства, и затем с нее считывается информация.Современная оперативная память четвертого поколения (DDR4) и старше уже не подвержена этой уязвимости. Если cold boot attack сегодня уже больше история, то файлы подкачки и гибернации − области на жестком диске, куда сохраняется информация из оперативной памяти, − не утратили свою актуальность и по-прежнему могут многое рассказать о владельце устройства. Компьютерными криминалистами довольно часто применяется восстановление данных на носителях, производимое в специальных лабораториях. Даже удаление файла не защитит его от угрозы извлечения при криминалистическом анализе. Современные методики позволяют достаточно эффективно восстанавливать удаленные файлы. Программные решения для проведения криминалистического анализа умело находят и извлекают изображения, видео, документы, переписки в мессенджерах, социальных сетях, информацию об используемых программах, резервные копии устройств, сохраненные в облачные хранилища, историю посещения сайтов − и это плохая новость.

**Последствия физического доступа**

Последствия физического доступа могут быть самыми разными, они зависят от задач, преследуемых недоброжелателем. Это может быть отец, желающий установить на компьютер сына программу для кибершпионажа (так называемое скрытое ПО для контроля за детьми), в результате успеха подобной атаки отец узнает, какое порно предпочитает его сын и какую ересь он пишет девочкам вместо любовных писем. Для начальника, чья секретарша задумала похитить корпоративную информацию в интересах конкурента или, купившись на предложения хакеров из Даркнета, решила занести в корпоративную сеть вредоносный софт, все закончится еще печальнее, как и для его компании. Владельцу онлайн-магазина наркотиков, к которому пожаловали через форточку представители правоохранительных органов, физический доступ к его компьютеру обернется заслуженными годами за решеткой, как создателю Silk Road Россу Ульбрихту, отбывающему пожизненное заключение в американской тюрьме. Но есть еще несколько последствий физического доступа, которыми я, возможно, смогу вас удивить. Во-первых, вам могут подбросить цифровые доказательства: запрещенную литературу, экстремистские материалы, детскую порнографию или что-то другое. Во-вторых, у вас могут похитить криптовалюту, и это может быть главной целью визита к вам недоброжелателей. В один из дней представители Службы безопасности Украины с двумя понятыми пришли к основателю русскоязычного криптовалютного журнала ForkLog Анатолию Каплану и, предъявив судебный ордер, изъяли у него всю технику. Обыск проводился в рамках уголовного дела, к которому проект ForkLog имел косвенное отношение, так как с помощью него подозреваемые якобы меняли криптовалюту. В целом основатель ForkLog мог быть просто вызван как свидетель, и визит с арестом техники явно лишний шаг. Что побудило на него органы? У Анатолия имелась криптовалюта... По словам адвоката, уже в процессе обыска сотрудники СБУ предпринимали попытки перевести себе биткоины, а на следующий день хранимые на изъятых у Анатолия кошельках Ethereum средства были переведены на неизвестный кошелек. Стоит взять на заметку: если вы владелец криптовалюты, защита от физического доступа для вас должна быть на первом месте. Помимо этого, настоятельно рекомендую познакомиться с секретами безопасных паролей, способами тайного хранения данных и методами маскировки криптоконтейнеров. В-третьих, вашу технику могут уничтожить. Сейчас я вам расскажу одну интересную историю. Мы часто слышим, что пользователи в России и ряде других стран получают штрафы и даже реальные или условные сроки за лайки, комментарии и репосты в социальных сетях. Но немногие из вас знают, что штраф иногда не самое страшное в подобных историях, когда суд признает компьютер орудием совершения преступления с последующим его уничтожением. Так, в Свердловской области слушалось дело об экстремизме. Обвиняемый Владимир скачал и выложил в публичный доступ ролики, которые были признаны экстремистскими. Обычная история, коими нынче не удивить, однако интересен приговор, в рамках которого, кроме штрафа, суд постановил уничтожить компьютер Владимира. На дворе был 2011 год, и после этого аналогичные меры в отношении компьютеров и ноутбуков принимались еще не раз. Самый громкий подобный случай в России произошел с матерью-одиночкой Екатериной Вологжениновой, которая за репосты на свою страничку картинок в поддержку Украины была приговорена к 320 часам исправительных работ, а ее компьютер и мышку суд постановил уничтожить как орудие совершения преступления. Честно говоря, познакомившись с содержанием картинок, я так и не смог понять, где там этот самый экстремизм, но Суду виднее. Хороший компьютер или ноутбук стоит более $2000, на нем может храниться ценная информация, резервных копий которой не сделано, потому, даже совершив ошибку с лайком или репостом, желательно не допустить кого-либо к своему компьютеру. Ведь чтобы доказать, что конкретный компьютер использовался для публикации сообщений, нужно получить доступ и провести криминалистический анализ активности в социальных сетях.  
  
 **Системы массовой слежки**

Даже если вы не сделаете ничего плохого, за вами все равно будут следить. Эдвард Сноуден Системы массовой слежки − не новое явление для мира, и если в прошлом главной задачей был перехват звонков и телеграмм, то в цифровую эпоху основной собираемой информацией стал сбор данных об активности и коммуникациях в сети Интернет и сотовых сетях. В большинстве случаев системы массовой слежки осуществляют легальный сбор данных по различным каналам связи. Это сбор и хранение звонков, координат совершения этих звонков, так называемый биллинг, и, конечно, сбор и хранение интернет-трафика. Пользователи осведомлены о сборе данных, по крайней мере, существование таких систем не секрет для общества. Разумеется, встречается и незаконный сбор данных, например, проект RAMPART-A, о котором стало известно из разоблачений Эдварда Сноудена. Согласно опубликованной информации АНБ США заключило договор с 33 странами в Западной и Восточной Европе, Азии и Африке и вело сбор информации через оптоволоконные кабели, проходящие по их территориям. Почти в каждой стране есть своя система массового сбора информации: в России это СОРМ, в Канаде, Австралии, Новой Зеландии, США и Великобритании − ECHELON, Frenchelon во Франции, Золотой щит в Китае. Прогресс не стоит на месте, и эти системы периодически совершенствуются, появляются новые решения, позволяющие хранить больше информации в меньшем пространстве, тратить на это меньше денег или эффективнее осуществлять поиск нужной информации в собранных данных. Например, относительно новое явление − поиск по отпечатку голоса. Если у правительства есть запись вашего голоса, они всегда смогут найти ваши звонки, с какого бы номера вы их ни совершали. Подобные решения стоят немалых денег и имеются в арсенале спецслужб далеко не каждой страны. И в дополнение к сказанному выше вот вам фотография. Возможно, вы уже видели это здание. Это центр АНБ в штате Юта, где, вероятно, хранятся все ваши звонки, переписки в мессенджерах и социальных сетях, электронные письма за последние годы.

Вы наверняка уже слышали о методах защиты от массовой слежки, подобные инструкции активно распространяют в сети правозащитные организации и активисты. Согласно им для защиты от массовой слежки достаточно шифровать свои коммуникации, а еще лучше использовать VPN для комплексного шифрования всего интернет-трафика. И ведь разумно пишут: ну как следить, когда трафик зашифрован? VPN действительно шифрует весь интернет-трафик до VPN-сервера, и система перехвата данных на уровне вашего интернет-провайдера получит только зашифрованный трафик. Но вот на VPN-сервере трафик будет расшифрован и в лучшем случае останется зашифрованное соединение до сайта (HTTPS), которое не является непреодолимой преградой для спецслужб.  
Если в стране, где размещен ваш VPN-сервер, нет системы массового сбора данных (хотя мне не известны такие страны), то она может стоять где-нибудь на протяжении дальнейшего пути до сайта. Но если и VPN-сервер, и сервер сайта, к которому вы подключаетесь, находятся в одном датацентре и между ними нет системы массового сбора данных, то остаются только зашифрованные данные, собранные вашим интернет-провайдером или иной стороной в любом другом месте на пути к серверу VPN. Хотя нет, есть еще одно условие: VPN должен быть настроен правильно, иначе возможны утечки данных вплоть до передачи незащищенной информации в обход зашифрованного туннеля. Многие эксперты утверждают, что шифрование решает проблему тотальной слежки. К сожалению, это не совсем так. Действительно, если используется надежный алгоритм шифрования, а программное обеспечение не содержит закладок, зашифрованные данные в настоящий момент с высокой долей вероятности не расшифруют. Но прогресс не стоит на месте, и многие алгоритмы шифрования, 10 лет назад считавшиеся надежными, сегодня уже таковыми не являются. За примерами далеко ходить не надо: RSA с длиной ключа 768 бит активно использовался государственными органами, крупными компаниями и даже в оборонной сфере, пока в 2009 группа ученых не взломала его и всем было предложено прейти на 1024-битные ключи. Прошло еще время, и в 2018 году пользователям рекомендуется использовать уже ключи от 2048 бит. А на горизонте маячит квантовый компьютер, который сможет расшифровывать все зашифрованные сегодня данные. Вам придется смириться с мыслью, что шифрование − это лишь временная защита, но не панацея. Все ваши переписки, звонки, интернет-трафик со временем можно будет расшифровать, а пока их можно просто собрать и сохранить. Есть немало случаев, когда правоохранительные органы изымали зашифрованные носители информации, но не могли их расшифровать. Например, Даниель Данташ − арестованный в Рио-де-Жанейро бразильский банкир, которого бразильские власти подозревали в мошенничестве. Его диски больше года пытались взломать Национальный институт криминалистики Бразилии и ФБР, но не смогли. Возможно, придет время и они все-таки посмотрят их содержимое. А может, используемое шифрование уже ненадежно… Вы же не рассчитываете, что спецслужбы, найдя способ расшифровывать зашифрованные коммуникации, выступят с официальным заявлением и скажут: «Многоуважаемые пользователи, мы нашли способ расшифровывать данные, зашифрованные алгоритмом N, пожалуйста, перейдите на более безопасные решения»? Современные алгоритмы хорошо изучены, и вероятность этого невелика, но она не нулевая и совсем исключать ее мы не можем, тем более, подобные примеры еще свежи в памяти. Например, компания RSA Security с 2004 предлагала клиентам заведомо ненадежный алгоритм генерации псевдослучайных чисел Dual EC DRBG, позволяющий АНБ в любой момент получить доступ к зашифрованным данным. Работали эти парни не за идею, а за 10 млн долларов, заплаченные им АНБ. А что специалисты? Подозрения о наличии уязвимостей в Dual EC DRBG возникли еще в 2007, но они не вышли за пределы узкого круга экспертов до тех пор, пока в 2013 Эдвард Сноуден не раскрыл миру правду. И только тогда сообщество забило тревогу, призывая отказываться от ненадежного алгоритма. Уязвимым решением многие годы пользовались тысячи клиентов, включая таких гигантов, как Adobe, Oracle, Sony и Nintendo. Как вы поняли, о вас собирают довольно много данных и, вероятнее всего, с развитием технологий делать это будут еще активнее, а хранить данные еще дольше. Кто и как воспользуется затем этими данными? Хочется ли вам, чтобы кто-то мог узнать, что вы писали в восемнадцать лет? Какие видео вы смотрели? Какие сайты посещали? Не станут ли заблуждения молодости компроматом, который сломает вам жизнь через много лет? Кто даст гарантию, что данные не утекут в третьи руки или государство не использует их для давления на вас? Все эти вопросы делают массовый сбор данных серьезной угрозой нашего века. Вы думаете, это утопия? К сожалению, нет. В Китае уже используется система социального рейтинга, при которой каждый гражданин имеет рейтинг, и в соответствии с ним определенные привилегии и ограничения. Получить баллы, повышающие социальный рейтинг, можно за общественную работу, помощь родителям, полезную деятельность на благо партии и другие положительные действия, например своевременную выплату кредита. В данный момент система только внедряется, и этот список, насколько мне известно, еще в процессе проработки. Понижается социальный рейтинг за критику в интернете власти и сложившихся порядков, в том числе социальных сетях, личных переписках, переписках по электронной почте (в Китае переписки в мессенджерах и электронной почте анализируются системами массового контроля интернет-трафика и в случае наличия подозрительных слов передаются на изучение живым людям), в случае доносов соседей, нарушения ПДД, законов и других действий, большинство из которых, справедливости ради, наносит вред обществу. Граждане с низким социальным рейтингом не могут совершать поездки на транспорте дальнего следования и авиаперелеты. По данным Global Times, только к апрелю 2018 года низкий социальный рейтинг стал причиной отмены более 11 млн авиаперелетов. Они будут лишены или частично ограничены в возможности работать в госучреждениях, получать социальное обеспечение, брать кредиты в банках, открывать коммерческие организации, обучать детей в дорогих частных школах, останавливаться в премиальных отелях, выезжать за границу – и все это только начало, гайки будут закручивать. Если ты против власти – ты изгой, если ты говоришь, что думаешь, и это не считается правильным – ты изгой, и искать таких смелых вольнодумцев будут системы массовой слежки. В то же время законопослушные и лояльные к власти граждане КНР получают от государства различные бонусы - преимущество при устройстве на хорошую работу, обслуживание в государственных учреждениях, возможность использовать гражданские права свободного человека.