

Проблемы цифровой безопасности для населения

Проблемы цифровой безопасности для населения

Ответы на вопросы

Как быть с "запрещенным контентом"?

Можно ли осудить пользователя за распространение запрещенного контента?

Как гос органы могут помешать распространению запрещенного контента?

Можно ли найти автора какого - то контента

Как ваша система защищает "персональные данные"

Авторское право как защитить в системе "корни"?

Что значит нельзя определить "как определить объект защиты?" авторского права?

Тема "пиратского контента", как система регулирует это?

Возможен ли новый "Джулиан Асанж"?

Определения

Решение через проект "корни"

- Во время санкций люди увидели бесчестность бизнесов владеющих облаками. Людей начали отключать от сервисов по политическим причинам. в некоторых странах облака переставали работать и блокироваться. Больше это никого не устраивает.
- Данные доступные людям могут быть перестать им быть доступны, возможности тоже. Это принципиальный недостаток существующей системы. (В системе корни такое исключено - если есть доступ к каким-то данным - то будет всегда)
- Должностные лица государств блокируют некоторые ресурсы, которые частично полезны людям, под разными предлогами даже если это не в интересах граждан. Частное лицо с большим трудом вынуждено обходить эти ограничения, государство принимает решения за людей, якобы в их интересах. (В интересах человека самостоятельно принимать такие решения(и особенно юр лиц, физ лиц итд))
- Корпорации собирают отчужденную поведенческую информацию и миллиардов людей. с помощью этих данных (принадлежащих людям) корпорации строят big data, к которой люди полноценного доступа не имеют, а корпорации "почему - то" имеют. BigData корпорации используют чтобы строить алгоритмы искусственного интеллекта, который работает для их благо на данных предоставленных пользователями - все это делается за счёт пользователей. Пользователи же не имеют возможности сделать то же самое в своих интересах

- Корпорации составляют так называемые "обезличенные" наборы данных из персональной информации людей - пользователей и продают их друг другу и государству. считается что эта обезличенность описывает группы лиц, однако на практике эти данные настолько полны, что каждая "группа лиц" так мала что включает лишь одного человека - т.е. это по сути идентификация и составление "цифрового портрета" человека. Это даже более персональная информация чем обычно описывается в законах. т.е. корпорации торгуют нашей персональной информацией - это прямое нарушение как прав человека так и закона.
- Владельцы облаков постоянно совершенствуют методы манипуляции и рекламы и применяют их к людям, все это они делают за счёт и с помощью пользователей. Выгоду от этого пользователи не получают, а являются цифровым топливом и объектом манипуляций.
- Под предлогом защиты и слежки за террористами бизнесом и государством (совместно) лоббируются и принимаются законы и поправки по которым можно следить за людьми. Эти системы секретны и проследить их полезность невозможно, однако в результате "презунция невинности" перестаёт действовать поскольку при желании можно в действиях каждого найти задним числом какие-то нарушения и привлечь к ответственности. Это увеличивает и коррупцию и усиливает диктатуру государства (и корумпированных частных лиц, вероятно преступных) и создаёт предосылки для заклёванного человечеством фашизма в нашей родной стране. Это даже усложняет контроль законности прокуратурой и спецслужбами т.к. и они сами могут быть объектом шантажа и манипуляций и коррупции. Это нарушает "выстраданную" систему "сдержек и противовесов. Все это за счёт налогоплательщиков.
- Технические средства мониторинга сети отнимают очень много ресурсов у операторов связи, заставляя их объединяться для некоторых функций... это приводит к монополизации.
- Из-за конкурентной борьбы между облаками пользователи постоянно переплачивают т.к. конкуренция и борьба оплачивается из их кармана. Специалисты вынуждены постоянно многократно решать одни и те же задачи на разных конкурирующих между собой заказчиков - это не назвать продуктивной экономикой и счастливой творческой жизнью.
- Государства оказались не способны обеспечить суверенность некоторых функций, которые ранее выполняли корпорации, государства оказались уязвимы. Государства, как и простые люди нуждаются в большей независимости от произвола корпораций в интернете.

<https://www.youtube.com/watch?v=ehu0zbWe-YU> телеком сфера. «Пакет Яровой»:

Ярослав Дубовиков +7(499)37-11-777

- пакет Яровой (Яровая Озеров Пушкив Герасимова) это не конкретный закон с требованиями - это пакет поправок в двух законах касательно многих других актов
- 2016 год - год принятия. существенное расширение полномочий для правоохранительных органов; требования к операторам связи, организаторы "распространения информации" ОРИО ; миссионерская деятельность;
- ори - любой сайт в интернете, где происходит распространения информации. есть "реестр" ори - не особо много кто туда вступает, иногда туда насильно включают, выйти оттуда почти нереально, в результате получаешь требования.
- "оператор связи".
 - суть: это только юридическое лицо, частное лицо не может такие услуги оказывать.
 - задолго до пакета яровой в законе о оперативно розыскной деятельности в разделе в орм - оперативно розыскные мероприятия были изложены почти эти же элементы. уже был контроль за почтой, телеграфом, интернет переписка. итд. это было но было жестко регламентировано.
 - операторам связи выдвинулись требования. прослушивание всех телефонных разговоров. пакетные сообщения ... можно хранить и анализировать. СОПМЗ - работает быстрее. обычно оператор связи отвечает за 30 дней, сормЗ - позволяет в реальном времени видеть биллинг.
 - с пакетом яровой появились возможности 44 , 43 + пакет яровой.
 - теперь "правоохранители" могут получать данные без санкций суда , напрямую у "оператора связи" или ОРИ.
 - любой договор связи может быть расторгнут по желанию любого правоохранителя. (была целая компания по подтверждению так называемых персональных данных в мобильных договорах). Симки отключают, раскручивают телефонный номер по 15 лет и могут подставить (случайно или нет) и отключить, достаточно подозрения.

- 3 года "оператор связи" хранит логи, 6 мес звонки и сообщения, 30 дней передача информации (+15% в год)
- для ОРИ
 - 1 год логи, 6 мес все данные, и передача ключей шифрования площадка должна предоставлять (дело о блокировке телеграмм)
- Сложность реализации пакета яровой:
 - с момента принятия прошло 2 года пока начали что - то делать. все это ложится по стоимости на плечи пользователей.
 - до 2020 года операторы жили в подвешенном состоянии , не было оборудования, не было сертификации, но операторов штрафовали (либо за отсутствие решений либо за отсутствие сертификатов)
 - операторы (особенно мелкие) стали объединяться и монополизироваться, совместно финансироваться. (1 год выручки нужно оператору потратить на это, не прибыли, а выручки!) общая оценка затрат : 10 трн рублей / ... 69т.р. на каждого абонента... где деньги? штрафы очень большие (25% от выручки)
 - требования закона яровой : все на российских компонентах. ростелеком все датацентры скупает. цитадель - 60% рынка, лишь у усманов один из первых получил сертификацию и начал окупать тему. конкуренция очень не интересная и слабая, все загнивает.
- мораль пакета:
 - в 2016 году все юристы говорили "мы начали жить в другой реальности",
 - "официальная слежка за гражданами это то что мы получили с принятием пакета яровой".
 - очень много утечек данных коорые фиксируются везде: операторы, системы каршеринга, сервисы, гос сервисы ... все кто как то хранит какие то данные все стали сильно рисковать и сталкиваться с этой проблемой.
 - "отсутствие у вас судимости это не ваша заслуга а наша недоработка"

- очень серьезные противоречия с конституцией: вся частная жизнь которая раньше была частной, сейчас она хранится не понятно у кого и доступ к ней имеется фиг знает кто, непонятные коррупционеры и откровенно криминальные структуры, но не граждане.
- Правоохранители , которые должны нас защищать и огромное кол-во преступлений коорые могут и должны предотвращаться с использованием этой системы сорм это необходимость, понять цели можно, ... но границы частной жизни не должны переходится. и данные о частной жизни хранятся у операторов и используются в их целях - это создаёт различия между людьми.
- отмена презумпции невиновности, раньше данные прикладывали в порядке текущего добытия, то сейчас можно покопаться в прошлом и нарыть что угодно задним числом. это отмена статьи 49 Конституции РФ. это запись всех граждан рф в подозреваемые, в потенциально неблагонадежные субъекты. автоматический статус подозреваемого...
- помогает сормм или нет ? статистика по этому закрыта. разглашение орм что проводится и как это противозаконно. (не официальная информация: оно не работает... только если есть знакомые на пульте (потенциал для коррупции?))
- ~~vpn , настоящий, который не показывает трафик, он может позволять видеть трафик инноагентам (организаторам vpn) но может не позволять видеть его нашим спецслужбам~~
- сейчас оно реализовано в варианте более жестком чем у китайцев. надежды на раздолбайство нет -- нуу ... у нас админы и безопасники очень сильные ребята в России.

Бандиты и террористы воспользуются отдельными решениями и будут 100% все шифровать. Это организованные группы и глупо думать, что они открыто пишут в интернете свои планы.

Ответы на вопросы

Как быть с "запрещенным контентом"?

нет в этой системе больше такого понятия. если я получил доступ к каким-то данным - то я могу их изучать. Это мое право изучать то, что хранится на моём компьютере.

Никто не вправе запрещать мне читать "мои книги" и "читать мои файлы", "ознакамливаться" с любыми данными на моем оборудовании поскольку они уже мои - это моя собственность.

я могу изучать данные на своём компьютере даже отключившись от сети.

Можно ли осудить пользователя за распространение запрещенного контента?

в этой системе нельзя осудить пользователя за распространение контента (любого вида) т.к. нет фактов самого распространения:

- нет как такового публичного ресурса на котором данный контент размещен (адреса, да и самого ресурса)
- якобы "распространяющий" - просто пассивно декларирует возможность доступа к каким-то данным, некоторые из них понятно, что он создал, другие понятно, что создал кто-то другой. но кто их создал и что это за данные понять не возможно, пока их не получишь.
- пользователи сами скачивают данные, проявляя самостоятельную активность.

это нельзя назвать "распространением": грубо говоря, я лишь показываю, что у меня есть какие-то данные, синхронизирующие программы запущенные получателями, забирают те данные, которых у них не хватает. Получатели не имеют умысла прочитать что-то не законное и запрещённое. если они что-то и получают - то не преднамеренно.

Просмотр уже своих данных пользователи-получатели осуществляют со своих компьютеров, могут их удалить или пометить "экстремистскими" (на сколько сами посчитают - они не эксперты по этим вопросам), чтобы следующие получатели могли видеть эти пометки, но удаление сведений из такой сети не предусмотрено.

Если кто-то из них желает судиться, то им стоит помнить : 1) это они сами запустили синхронизацию 2) сами получили данные 3) они могли настроить свои программы так, чтобы не видеть запрещенный контент. 4) если согласно закону они не хотят хранить у себя запрещенный контент - то должны его удалить а т.к. нет технической возможности - то решить, что удалить не получилось и успокоится. Они не должностные лица государства и не обязаны вообще говоря ничего делать с увиденным контентом, кроме того не они его создали (скорее всего) и не имеют права удалять.

Если государство заставит эту техническую возможность удаления реализовать, то это работает в обе стороны : можно будет по закону обратиться во все организации и гос органы и заставить их удалить о себе всю персональную информацию и отговорка "нет технической возможности" не прокатит. Это значит что нужно будет перестать использовать в архитектуре программного обеспечения только базы данных которые подразумевают удаление, а не пометку "удаленные данные", а реальное физическое удаление это очень дорогая техническая операция - стоимость ИТ систем взлетит до небес. затраты на такие системы тоже.

Как гос органы могут помешать распространению запрещенного контента?

Помешать распространению - никак. Они могут создать от своего имени особые пометки, что некоторые сведения они считают "запрещенным контентом".

Могут попробовать внушить гражданам (**или людям? ли лицам физ юр**) поставить на программах фильтр, чтобы граждане не изучали сведения с этой пометкой.

Но граждане (**или люди?**) вправе сами ставить или снимать этот фильтр и если хотят изучать любые доступные им сведения.

.....

"распространение информации" предполагает передачу информации "неопределенному кругу лиц". Если лицо, перед передачей ему информации представляется любым способом идентификации (в том числе анонимным адресом "на деревню к дедушке", которые реально работает), то это уже не "распространение", а "получение" информации неким, пусть и анонимным лицом.

....

Закрепляя право на информацию, в Конституции РФ применена конструкция: "Каждый имеет право свободно... распространять информацию **любым законным способом**". В.В. Лапаева рассматривает данную норму как "дополнительную гарантию против злоупотребления со стороны носителей конституционных прав и свобод" [8, с. 17 - 18].

....

Основные требования закреплены в базовом Законе "Об информации", в частности, запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность [16, ч. 6 ст. 10].

Для этого субъект должен "иметь представление о всех сведениях как о информации т.е. отдавать себе отчёт в том, что он именно распространяет". В общем случае можно считать, что субъект а) никогда не может быть уверен, что данные на его компьютере это информация (т.к. он возможно с ними не знаком и не давал им оценку) б) мы заменили процесс "распространение" на "получение", то рисков для субъекта нет. в) передача данных (а не информации) может происходить по специальной лицензии, которая устраняет остаточные возможные юридические риски.

.....

Исходя из указанного определения, можно выделить следующие сущностные характеристики распространения информации:

- **цель или предвосхищаемый результат**, ради достижения которого осуществляется информационная активность: возможность влияния на сознание человека и манипулирование им, формирование определенных взглядов, системы ценностей, управление эмоционально-чувственной сферой и т.д.;
- **содержание** передаваемой информации напрямую зависит от цели и обуславливает формирование собственно деятельности распространения информации;
- наличие **воли и осознания** субъектом своих действий по доведению информации до сведения;
- получателями информации всегда будет **широкий круг лиц** (или - **многие**);
- распространитель информации не нарушает законные интересы иных лиц - **незлоупотребление правом**;

- распространение информации осуществляется **любым законным способом**.

Для распространения информации прежде всего необходима именно информация. Даже не осмысленные сведения информацией формально не являются. Тем более не являются информацией данные, которые хранятся в форме файлов.

Если же гос-во по своей глупости огульно обязует фильтровать по содержанию и данные тоже (это кстати противоречит определению т.к. данные не могут иметь информационного содержания - там обратная логическая зависимость. это понятие содержания базируется на понятии данных, а не наоборот) то это заработает и в обратную сторону = можно будет заставить анализировать данные при передаче и гос корпорации и все учреждения это делать и это застопорит всё. это застопорит все коммуникации и сети. застопорит весь интернет, который потеряет смысл.

Система корни имеет две части

1. первая часть, редакторы и просмотрщики - вообще не взаимодействуют с другими лицами никаким образом (даже в теории не могут ничего передавать и принимать). Эта часть системы сохраняет результаты в файлах, у каждого приложения своя структура файлов, есть лишь общие рекомендации.
2. транспортная система синхронизации ДАННЫХ, которая не анализирует содержание файлов и данных т.к. имеет целью только синхронизацию самих файлов - чтобы обеспечить всем участникам равный набор. данная подсистема не работает с информацией - только с данными, обмен идет в форме команд, а данные являются параметрами команд. т.е. передаются команды. Получатель забирает данные, а не информацию, сообщая свой анонимный адрес (т.е. "это индивидуальная передача" каждый раз, а не распространение многим), агенты не злоупотребляют правом "свободы информации" т.е. не навязывают ~~информацию~~ данные, система работает для одного пользователя (своего), транспортная система не знает как пользователь воспользовался данными, понял ли он их, видел ли их итд. транспортная система не касается контента, никак его не анализирует - работает только с непонятными ей файлами.

Можно ли найти автора какого - то контента

это вопрос анонимности авторов. Я бы хотел использовать полностью анонимные технологии общения, т.е. техническими средствами нельзя будет сказать где именно располагается и какому человеку соответствует тот или иной автор контента и его правок. Для ряда приложений нужна публичность, для справедливого общества, например.

Лицо может раскрыть себя своими неаккуратными действиями, например где-то написать что он Иван Иванов и приложить свой паспорт. Или раскрыть себя как - то иначе.

Однако это поле для провокаций и подстав. кто-то , не Иван Иванов, может представится Иваном Ивановым без его ведома, выложить как бы свои фото или украденный паспорт в доказательство того что он якобы Иван Иванов.

Надо четко понимать, что "невозможно достоверно установить" именно это и значит и не верить пустым словам.

Для решения задачи доверия в условиях когда нет авторитетов доверия существует другая технология - БЛОКЧЕЙН.

....

так как "контент - это информационное содержание интернет ресурса" , а у нас в системе нет понятия "интернет ресурса", то и термин "контент" не имеет отношения к этой системе.

Однако, допустим, что вместо "интернет ресурса" можно поставить "информационное содержание информационного ресурса"... это "масло масляное", но, допустим...

В этом случае единственный информационный ресурс который можно тут подразумевать это "приложение в котором пользователь видит информацию (на самом деле он увидит "сведения", т.к. "информацией" они для пользователя являются после его оценки, которую он может никуда не распространять т.е. доказать, что данный пользователь видел в приложении "информацию" может быть в нашем случае затруднительно, разве, что в суде он скажет , что он её видел. И еще надо будет убедиться понял ли он её мысл?)"

Таким образом выходит, что пользователь на своем компьютере с помощью некоторого приложения увидел какие то сведения, которые он сам получил откуда-то (не известно откуда т.к. логи система принципиально не ведет и пользователь на был это согласен, запуская синхронизацию).

Во-первых, приложение не имеющее сетевых функций, всё таки, нельзя назвать информационным ресурсом, как например, нельзя назвать программу блокнот или калькулятор информационным ресурсом.

Во-вторых, это его личная программа и данные он сам получал другой программой и к кому предъявлять претензии не ясно.

В третьих, пользователь сам при синхронизации данных соглашается, что сеть анонимна и что логов не ведётся и что программа не анализирует данные, которые получает для пользователя и что "каждый пользователь, отдающий данные" не может считаться "распространителем данных" т.к. отдаёт свои данные лично ему.

....

т.к. контент хранится на "интернет ресурсах", а интернет ресурс : "Каждый интернет-ресурс должен иметь уникальный адрес, который позволяет найти его в Сети."

то, поскольку в этой сети нет понятия "интернет ресурса" и "адреса", а адресация происходит "по контенту", то получается, что для этой технической архитектуры нужно переделать юридическое определение контента. и пока это не произошло нельзя говорить и о "запрещенном контенте".

Но когда определение будет переделано, то т.к. адресация в системе идет по хеш функциям для контента, которых существует множество то , придется сопоставить запрещенный контент его хешам т.е. запретить некоторые хеши... а поскольку хеш это математическая криптографическая функция, то я не представляю как это может быть реализовано технически.

Как ваша система защищает "персональные данные"

т.к. пользователи системы изначально полностью анонимны, а система не просит их предоставлять о себе любые данные, то в системе помимо действий самого пользователя "персональные данные" появиться не могут.

Сам пользователь вправе представится кем угодно и представить любые и даже выдуманные сведения о себе.

Верить любым сведениям в системе никто не обязан даже в инструкции ясно сказано, что "кто угодно тут может выдавать себя за кого угодно" и система не рашает эту проблему. т.е. даже если лицо опубликует о себе или другом лице все возможные так называемые "персональные сведения" это не будет являться ими т.к. нет этому никакого доверия и не предполагается что такое доверие должно ког-либо возникнуть.

Для решения проблемы доверия существуют другие системы "блокчейн", "цифровая подпись".

Если лицо хочет чтобы документ вызывал доверие и считался юридически значимым и достоверным - лицо должно ссылаться на подписанные документы и записи в блокчейнах.

"Персональные данные" устаревшее юридическое понятие, а не техническое. Но сейчас уже существуют технические способы распознать лицо по косвенным признакам, нарушая повсеместно юридический запрет на это. Это более важная проблема которая требует решения перед тем, как начинать обсуждать защиту персональных данных на анонимных системах, которые изначально рпроектируются так, чтобы там такие данные даже не появлялись.

Авторское право как защитить в системе "корни"?

Авторское право - юридическая абстракция и до сих пор в мире "защитить авторское право" ни одна правовая система не способна потому, что существуют уже серьезные сложности с этим как технические так и юридические.

1. вопрос технический : что именно защищает автор? как определить объект защиты?
2. с какой стати автор считает что имеет право на своё произведение?
3. есть прецеденты: объекты защиты авторского права ходят по интернету и запретить это невозможно. эта невозможность полностью лишает всякого смысла сам термин "защита авторского права", этот процесс попусту тратит ресурсы и не приводит к результату.

короткий ответ , система корни может предложить:

- если сведения начали ходить по пользователям , то нужно считать , что произошла "утечка информации" и остановить это уже не удастся. это не удаётся технически сейчас и это тем более не удастся уже юридически т.к. пользователь который получил и раздаёт данные приобрел их на каких-то уже изменившихся но законных условиях и распространяет уже своё, а не ваше. (аналогично происходит с

украденной собственностью, при многократной перепродаже и смене собственника - вернуть её уже практически невозможно)

- обычно предпринимаются попытки прервать распространение такого контента. в системе корни это невозможно. данные принимают миллионы людей сами по своей воле и нет в этом никакого центра и эти люди делают это без умысла (т.к. это данные и они лишены смысла) и делают это не преднамеренно (т.к. не могут при получении заранее знать, что именно они получают от других людей). Люди, принимая данные, по общедоступной лицензии становятся владельцами этих данных, люди не обязаны анализировать все свои данные т.к. не являются все без исключения должностными лицами государства.
- поэтому авторы контента которые в этой системе хотят заработать на своих трудах должны заранее однократно собрать средства и уже потом открыть доступ к данным всем или группе лиц, но если произойдет "утечка данных", то она произойдет и никто не исключает эту вероятность. в следующий раз авторы контента будут думать кому давать доступ и как организовать узкую группу лиц и как пометить раздаваемый контент, чтобы отследить источник утечки.

Что значит нельзя определить "как определить объект защиты?" авторского права?

Объясню на примере: некто "автор" создал "фильм", записал его в файл и это по его мнению объект защиты авторского права.

Значит если где то "органы защиты авторского права" детектируют этот файл, то там этот файл должен быть удален.

Но при этом они должны доказать что детектирован именно этот фильм. как они это докажут владельцу файла? проверить диски чужого компьютера они права не имеют - они пытаются поймать факт передачи файла от "распространяющего к получателю", для этого они могут, например, прикинутся получателем.

Pear-to-pear (читает пир ту пир) технологии обходят эту юридическую несуразность например таким способом как торренты:

допустим объект авторского права защищает весь файл фильма - тогда нужно получить целиком файл, чтобы доказать факт распространения этого объекта.

сеть торрент делает так : а) половину файла раздаёт пете (или 99%), б) половину файла раздаёт Васе в) петя отдаёт органам почти весь файл, но не весь, а от васи берет недоающее. ни никто из "потетенциальных нарушителей закона" не отдал файл целком - факта нарушения закона нет.

допустим каждая любая часть этого "ценнейшего произведения" защищена авторским правом, значит нужно доказать что передаются эти части. в таком случае очевидно что это просто последовательности байт не факт, что они принадлежат к этому произведению, это нарушение здравого смысла.

Но все же пробуем смоделировать ситуацию. торрент сеть решает задачу следующим способом: файл бьётся на блоки (чанки), система раздаёт идентифицирует каждый блок и раздаёт их. "органы" пытаются доказать факт раздачи блока принадлежащего якобы к фильму (не факт что это часть фильма а не случайный набор байт т.к. весь фильм они еще из них не собрали).

"Правильный" торрент клиент при получении каждого файла говорит какие блоки ему нужны и какие есть, если есть , то раздающий клиент просит отдать один имеющийся блок; если нет ни одного блока, то первый блок раздающий отдаёт не целиком, а отдав половину, просит отдать обратно то, что получил, и только в этом случае отдаёт остальную часть блока.

В этом случае сторона получающая блоки, которая хочет доказать факт нарушения путем раздачи блоков байтов, якобы защищенных авторским правом, сама становится соучастником такого нарушения, и их, так называемая, "улика"-блок получена с нарушением закона и таким образом не является доказательством.

Безусловно можно придумать массу обходных вариантов передачи данных так, чтобы это невозможно было проверить и доказать. Авторское право не может быть реализовано в принципе. И методы контроля авторского права даже в теории не могут законным путем решить свою задачу. Считаю, говорить об авторском праве нет никакого смысла, ввиду отсутствия основы для разговора.

Тема "пиратского контента", как система регулирует это?

Система корни - система для решения задач ~~приватных~~ группы лиц. Групп лиц может существовать множество, они могут частично пересекаться по набору пользователей.

Отдельная группа лиц может включать всех жителей страны или нескольких стран (как интернет).

Бизнес "Пиратов контента" во все времена расцветал когда в государстве все было "плохо устроено" - пираты как санитары леса , они восполняют пробел в спросе, который откуда - то искусственно возник. Я бы даже сказал что пираты - это нормальный элемент рыночной системы. Когда цены адекватны и человеку выгодно платить официально - он не пойдет к пиратам, если цены не адекватны - только тогда человек пойдет искать пиратский контент. Расцвет пиратов это признак "руки рынка".

В системе корни пираты могут чувствовать себя "безнаказанно" т.к. аккаунты в группах анонимны и к пиратам никак не придраться по другим причинам. однако ряд приложений может потребовать верифицированных человеческих аккаунтов - имеют право, и это может быть в их интересах.

Авторы контента выкладывая свой контент НЕ в системе корни рискуют - если цены авторов не адекватны, то в системе корни контент будет распространяться дешевле и совершенно безнаказанно.

Возгласы авторов не принимаются - НЕ публикуйте пока еще свой контент в других системах, сами первые публикуйте контент в системе "корни" первыми , чтобы исключить посредников по адекватным ценам , таким, чтобы пиратам было лень возиться с перевыкладыванием.

Возможен ли новый "Джулиан Асанж"?

Ошибка Ассанджа была в том, что он все разместил на своём ресурсе и когда его просили выключи - он не подчинился.

Сам ресурс викиликс бесподобен и является нужным всему миру источником гласности. Если кадры выбраны правильно - они не станут "стучать". но если кто то замыслил плохое - мир об этом может и услышать, идея хорошая.

Давление на Асанджа имело смысл т.к. он мог вырубить ресурс. если бы это был "джин выпущенный из бутылки" и он как идея начал бы ходить по миру то возникло бы более разумное решение, такое в котором не существовало бы никаких действий которые бы блокировали этот процесс.

Система корни в том числе способна 1) создать такой викиликс который не выключить, 2) создать такой набор фотографий о например котиках который не выключить итд. "не выключаемость" - базовое требование, которым люди защищаются от произвола современных облачных сервисов.

Определения

- Файл - данные, представленные в виде последовательности байт.
- Байт - комбинаторная позиционная числовая бинарная форма цифрового кодирования данных из 8-и бит (были байты из другого числа бит, в истории байта было и 6 бит и 4...) .
- бит - минимальный квант информации о том, что абстрактный сигнал изменился. на практике используется только для комбинаторной записи "данных".
- Детектирование (факта) - процесс определения наличия того или иного факта в виде да/нет
- Распознавание - детектирование, в котором определяются признаки и характеристики детектируемого факта, его индивидуальные атрибуты или детали.
- Сырые данные - неклассифицируемый и не распознанный никаким образом последовательность байтов.
 - Википедия: **Данные** — поддающееся многократной интерпретации представление **информации** в формализованном виде, пригодном для **передачи, связи**, или обработки (ISO/IEC 2382-1:1993)[1].
- Сведения - данные , которое прошли классификацию и детектирование (но не распознавание), или "просто-народно": "сведения это данные, разложенные в картотеку".
- Информация - сведения, которым придан смысл неким лицом - или "сведения со смыслом". Смысл детектирован и распознан. информация не обязана подвергаться оценке, чтобы считаться информацией. Информация которой придана оценка - засорена субъективной оценкой. Но информация обязана иметь смысл, иначе это сведения.

- **ИНФОРМАЦИЯ** - один из объектов гражданских прав, предусмотренных ст. 128 ГК РФ. В самом ГК РФ не определено понятие И. ; защита предусмотрена для более узкого объекта данного вида - служебной и коммерческой тайны. В соответствии с ФЗ Об информации, информатизации и защите информации от 25 января 1995 г. **И. представляет собой сведения** о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.
- Википедия: сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов **материального** или **духовного мира** в процессе коммуникации (ГОСТ 7.0-99)[9].
- **источник...**Одним из важнейших выводов, сделанных Винером, является определение информации как обозначения **содержания**, полученного из внешнего мира в процессе нашего приспособления к нему [2, с. 27]. Получаемая при этом информация "**координируется** мозгом и нервной системой; после процесса накопления, сличения и отбора она присоединяется к уже накопленному запасу информации, оказывая влияние на будущее действие" [2, с. 27]
- Знания - информация , которая прошла закрепление у конкретного индивидуума через практику (практические действия). Или иначе : знания это информация проверенная и подтвержденная практикой. т.е. знания позволяют индивидууму приспособляемость к среде т.к. точно соответствуют объективной реальности. Если они не соответствуют объективной реальности, то практика их опровергнет - это заблуждения, а не знания.
 - Википедия: **Знание** — это осведомленность или понимание кого и чего угодно, которое можно логически или фактически обосновать и **эмпирически** или практически проверить[1]. Согласно распространённой трактовке современной **эпистемологии**, **знание** — это реальное положение дел, обоснованное **фактами** и **рациональными** аргументами убеждение человека[2]. Говоря о знании, чаще всего подразумевают отражение действительности в сознании человека[3].
- Умысел -- ??? я понимаю как осознанные планы дееспособного человека на нарушение закона, но не действия. **уточнить** умысел требуется доказывать т.к. существует презумпция невиновности.... что то там есть про косвенный умысел
- Цель - осознанные планы дееспособного человека в виде образа результата. как умысел, но безотносительно закона.

- Распространение информации - процесс в котором есть 1) субъект действия, который активно распространяет, 2) объект - информация, и 3) другой субъект, который пассивно принимает информацию. Распространение предполагает какой-то канал. Часто в законах фигурирует понятие "средства массовой информации", "средства цифровой связи" итд. **уточнить**
 - статья на сайте "мудрый юрист" <https://wiselawyer.ru/poleznoe/92677-ponyatie-rasprostraneniya-informacii>
 - **источник**.... На законодательном уровне толкование права на распространение информации дается в Федеральном законе "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. N 149-ФЗ (далее - Закон "Об информации") [16]: "распространение информации - действия, направленные на получение информации **неопределенным кругом лиц** или передачу информации **неопределенному кругу лиц**".
 - источник тот жеВ.С. Хижняк отмечает, что "получать информацию - значит стать ее обладателем, добиться ее предоставления на законных основаниях", "правомочие получать информацию предполагает личную заинтересованность и реализацию субъектом намерения" [14, с. 14 - 15]..... Следовательно, получение информации всегда связано с **личной заинтересованностью субъекта в искомых или предлагаемых сведениях, волевым намерением приобрести данные сведения и его реализацией**.
 -
- Поиск информации - процесс, когда субъект совершает активные действия с целью (не обязательно умыслом - умысел требуется доказывать) найти в "картотеке" или просмотрев и распознав все данные то, что удовлетворит его запрос. т.к. поиск это осмысленный процесс то даже данные и сведения на его выходе становятся информацией автоматически, поэтому и не распространен термин "поиск сведений" или "поиск данных". т.о. сервис поиска информации всегда распространяет информацию. Сегодня в поиске используются алгоритмы с ИИ типа "черный ящик". т.е. есть юридический нонсенс, когда ИИ можно распространять информацию безконтрольно, а человеку в ряде случаев запрещено, что ставит ИИ выше человека в области информационного права.
- **Интернет-ресурс** (синонимы «веб-ресурс, **веб-сайт**, веб-сервис, сайт») – это совокупность интегрированных средств технического и программно-аппаратного характера, а также информации, предназначенной для публикации во Всемирной паутине. Интернет-ресурс может содержать информацию в текстовой, графической

и мультимедийной форме. **Каждый интернет-ресурс должен иметь уникальный адрес, который позволяет найти его в Сети.**

- Контент - информация потребляемая человеком с какой - то целью (чаще всего игровой и развлекательной, если не осознаётся иное).
 - Контент представляет собой информационное содержание **интернет ресурса.**
-
- Книги - частный случай контента на бумажном носителе (бумажный информационный ресурс).
- Распространение контента - то же что и распространение информации, через разделение доступа к информационному ресурсу. это пассивный процесс "потребления" контента т.к. контент это именно потребляемая информация. в этом процессе потребитель имеет цель всегда, но распространитель не обязан иметь цель.
- Лицензия контента - существуют де факто общепризнанные в мире правила распространения контента, главное правило : распространение контента обязательно делается в рамках какой-то лицензии. Автор может выбирать: существует великое разнообразие готовых лицензий на "любой вкус" , или написать свою собственную. лицензия - накладывает на участников права и обязанности.
- ~~Ценность контента - неизмеримая величина которая "подразумевается" автором контента и по его мнению должна выражаться в деньгах. это требование автора не обосновано т.к. на самом деле на величину влияет много факторов таких как хайп, степень доступности или не доступности, мода, отзывы, ложь, реклама итд.~~
- Человек - субъект действия, суверен, **обладающий правами** человека. Человек может выполнять различные роли, он выбирает роль когда представляется в обществе. **точно можно уточнить согласно римскому праву и английскому праву.**
- Гражданин - (не обязательно человек), который **обязан** выполнять законы государства, которое выдало ему гражданство на территории государства и на территориях входящих в некоторые международные договоренности этого государства. определяется по имеющимся паспортам. **аналогично**
- Физическое лицо - (не человек) юридическая абстракция, маска. цель - ??
уточнить
- Юридическое лицо - (не человек) юридическая абстракция, маска. цель - ??
уточнить

- Должностное лицо - (не человек) юридическая абстракция, маска. цель - служба и выполнение государственных функций. гражданам о должностном лице разрешено получать информацию любым доступным образом. должностное лицо выделяется формой, погонами, знаками отличия итд. к должностному лицу понятие персональной информации не применимо, (**уточнить**) но применимо "гос тайна" и другие термины.
- Лицо (в общем смысле) - юридическая абстракция, маска, которая надевается для некоторых целей. Смена лица меняет применимые права и обязанности! у разных лиц разные права и обязанности, которые исходят в том числе из предыстории поведения лиц.
- Аккаунт пользователя - лицо, маска, которую надевает человек (не обязательно человек) для взаимо(р)действия в сети.
- AAA - Authentication, Authorization, and Accounting. Общее название для общего понимания группы трёх процессов. (Важно: AAA это именно набор решений и реализаций, каждое из которых по разному реализует и понимает эти термины и обладает разными плюсами и минусами.)
 - Аутентификация - процесс цифрового представления пользователя, пользователь заявляет свое "лицо" и доказывает, что хочет осуществлять действия от имени этого лица (доказывает, что имеет права на это лицо)
 - Авторизация - цифровой процесс определения состава прав и обязанностей для "лица". Процесс получает права данного лица и удостоверяется, что эти права актуальны.
 - Аккаунтинг - комплексный цифровой процесс, в который входит учет операций и ресурсов: время сессии, утилизация и использования ресурсов, статистика использования информационными ресурсами, время логина и время жизни сессии и время жизни и процесс смены токенов доступа итд. Этот процесс важное звено обеспечения "безопасности" корпорации.
- Персональная информация (в России принято говорить "персональные данные", хотя данные и информация это принципиально разные сущности) - любая информация о человеке и некоторая информация о гражданине и его признаках, которую они по каким-то причинам считают личной, привязанной к своей персоне, индивидуальности и не относящаяся к другим людям и обществу.
 - **Персональные данные** (сокр. ПД) или **личностные данные** — сведения (мнение от Павлова М.А.: "данные" не могут быть "сведениями" т.к. "сведения" определяются через "данные" - получается "рекурсивное определение", это недопустимо), относящиеся к прямо или косвенно определённом или определяемому **физическому лицу (субъекту**

персональных данных), которые могут быть предоставлены другим лицам[1].

- Хотя концепция персональных данных довольно стара, развитие **сетей связи** и автоматизированного **анализа данных** позволило **централизованно** собирать и массово продавать данные о человеке. В некоторых случаях, даже **воровать**. **Эти данные помогают выследить человека, спланировать преступление против него или постороннему выдать себя за другого**; более мирное применение таким персональным данным — **реклама**.
- Персональные данные — это **юридическое**, а не техническое понятие, тем не менее современные технологии анализа данных позволяют отличить одного человека от другого по косвенным признакам.
- **СОРМ - ???**
 - "Пакет Яровой" - множество поправок в множество законов, принятые в 2016 году в России - касаются узаконенной слежки за гражданами в целях , так называемой "безопасности".
 - Пользователь сервиса - человек или гражданин технического решения (у которого может не, строго говоря, владельца или управляющего лица. например: редактор Atom - техническое решение с микросервисной программной архитектурой, которое пользователь запускает самостоятельно, осуществляет помощь в целях помощи программисту).
 - Облака и облачные сервисы - корпоративные центры, которые самопроизвольно взяли на себя функции хабов распространения информации. следят за поведением пользователей и часто отчуждают поведение пользователей (персональная информация). часто вступают в сговор в государством и/или преступностью. действуют в собственных интересах. Часто считают свой сервис - своей частной собственностью, и считают, что имеют право отключать пользователей за неуплату.
 - На самом деле контент который создают пользователи в облаках - принадлежит пользователям и идея отключения пользователя незаконна. сервис Ютуб, например , при отключении доступа говорит "ваш контент - всё еще ваш, просто мы отключили вам доступ к нему" (неприятно, мягко говоря)
 - Часто облака заключают при создании аккаунта пользователя соглашение, его мало кто читает, но там происходит передача прав на создаваемый контент владельцу облака (юридическому лицу), чтобы иметь больше свободы в отчуждении прав и свобод и заключать договоренности с государством и преступностью от своего имени , не привлекая каждый раз

пользователей ("своих пользователей" так они обычно выражаются про пользователей - как к рабской собственности)

- Технический адрес сервера - адрес сервера в сети в техническом виде , состоит и труднозапоминающихся цифр. может не быть стабильным и меняться в ходе переконфигурации сети.
- Домен - "красивое имя" для технического адреса сервера. имя сдаётся владельцу в аренду на срок за деньги регистратором имен (гос служба). Имя домена часто фигурирует в рекламе и легко запоминается человеком.
- Протокол - специальный диалоговый язык общения технических средств в сети. их существует очень много.
- Адрес в интернете - обычно подразумевают url - универсальный локатор ресурса, но это справедливо только для части протоколов в сети, например http. Часть протоколов не работают с url и понятие адрес (в смысле url) к ним не применимо.

Решение через проект "корни"

Назначение проекта корни

- вернуть свою суверенность каждому человеку, Это проект про цифровой личный суверенитет (это обеспечивает и б2б суверенитет)
- обеспечить цифровую безопасность не за счёт усилий государства, а за счёт изменения способа работы с контентом.
- вечный доступ к данным, которые уже твои
- вечный доступ к возможностям
- невозможность ограничений
- человек сам формирует "свой мир", на это никто не может повлиять.

Человек хочет осуществлять свои планы и достигать цели, его не волнуют проблемы должностных лиц и их функции.

Человек заинтересован защитить свою персональную информацию любыми способами, как с помощью государства так и без неё.

Гражданин имеет право пользоваться доступным ему контентом в своих целях в любое время.

Запретить пользоваться доступным контентом человеку и гражданину никто не в праве (не доступ к контенту а пользоваться доступным). Это правило сродни "я имею право читать свои книги" - чтение личных книг - личный процесс, в которое не имеет право никто вмешаться.

- хранить контент у самих пользователей а не на облаках и сервисах. или на таких сервисах, которые не могут шантажировать пользователей: "отключу за неуплату" или "сменю адрес" или "сотру контент". Контент доступный пользователю находится под его полным контролем.
 - конкретный пользователь может не понимать "что это за контент" - он может быть чужим т.к. никто не обязан вникать в чужие цели и смыслы. таким образом для пользователя картинка выглядит так : "я на своем компьютере храню свой контент и чужие данные"
- разделить программы на две группы
 - "для просмотра и редактирования своего контента", который находится уже под контролем пользователя
 - "для синхронизации данных" с другими людьми огромным множеством способов, так, чтобы это было технически невозможно запретить, ограничить, нарушить. Даже отключение полное интернета не прекратит работу системы (есть и такие методы)
 - Эти программы должны работать по принципу "скачивания" а не по принципу "передачи".