



Почему важно продвигать культуру защиты персональных данных, что граждане думают по этому поводу, и что с этим делать.

Анна Гусарова
Серик
Джаксылыков
2020

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В КАЗАХСТАНЕ: СТАТУС, РИСКИ И ВОЗМОЖНОСТИ

Содержание

Содержание	2
Глоссарий	3
Терминология	4
1. Культура защиты персональных данных: краткий обзор	6
1.1. Мировая практика	7
1.2. Куда движется мир	10
2. Защита персональных данных в Казахстане	16
2.1. Status Quo	16
2.2. Public Opinion	24
Выводы и рекомендации	48

Глоссарий

АРТ - (advanced persistent threat; «развитая устойчивая угроза»; также целевая кибератака) противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения

Blockchain – выстроенная по определенным правилам непрерывная последовательная цепочка блоков, содержащих информацию

Cookie – небольшие текстовые файлы, в которые браузер записывает данные с посещенных пользователем сайтов. **Файлы cookie** позволяют сайтам «запоминать» своих посетителей, например, чтобы каждый раз не переспрашивать их логин и пароль.

DDoS-атака – хакерская атака на вычислительную систему с целью довести ее до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднен.

DPI – технология глубокой проверки пакетов трафика (Deep Packet Inspection)

DNS – система доменных имен (Domain Name System)

GDPR – Общий регламент по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г.) — General Data Protection Regulation

FaceApp – мобильное приложение, создающее образ пользователя в старости (2017 г.)

IP-адрес – адрес интернет-протокола, уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP.

VPN - Virtual Private Network, виртуальная частная сеть — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети

ЕС – Европейский союз

ИИ – искусственный интеллект

КНБ – Комитет национальной безопасности Республики Казахстан

МВД – Министерство внутренних дел Республики Казахстан

КНР – Китайская Народная Республика

ПО – программное обеспечение

РК – Республика Казахстан

РФ – Российская Федерация

СНГ – Союз независимых государств

США – Соединенные штаты Америки

ФГД – фокус-групповые дискуссии

ЦАРКА – Центр анализа и расследования кибератак

ЦИК – Центральная избирательная комиссия Республики Казахстан

ЦОНЫ – центры обслуживания населения в Республике Казахстан

Терминология¹

Персональные данные — это информация, относящаяся к идентифицированному или идентифицируемому лицу.

Идентифицируемое лицо - это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на такой идентификатор, как имя, идентификационный номер, данные о местоположении, сетевой идентификатор или на один или несколько факторов, характерных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности этого физического лица.

То, что идентифицирует человека, может быть таким же простым, как имя или номер телефона, или может включать другие идентификаторы, такие как IP-адрес или идентификатор cookie, или абсолютно другие факторы². Если возможно идентифицировать человека непосредственно из информации, которую вы обрабатываете, то эта информация может являться персональными данными. Персональные данные могут также включать специальные категории персональных данных – данные о судимости и преступлениях. Поскольку они считаются более чувствительными, их обработка возможна только в более ограниченных обстоятельствах.

Если вы не можете напрямую идентифицировать человека по этой информации, тогда следует подумать, можно ли его идентифицировать. Необходимо принять во внимание информацию, которую вы обрабатываете, вместе со всеми средствами, которые могут быть использованы вами или любым другим лицом для идентификации этого человека. Даже если лицо идентифицируется прямо или косвенно по данным, которые вы обрабатываете, это не персональные данные, если они не «связаны» с данным лицом.

При рассмотрении вопроса о том, относится ли информация к какому-либо лицу, необходимо принять во внимание ряд факторов, включая содержание информации, цель или задачи, для которых ее обрабатывают, и вероятное влияние этой обработки на человека. Возможно, что эта информация является персональными данными для одного субъекта, в то время как для другого она не будет позиционироваться в качестве персональных данных.

¹ Общий регламент по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г.) или GDPR — General Data Protection Regulation.

² What Is Personal Data? The UK's Information Commissioner's Office, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>.

При этом важно отметить, что информация, для которой идентификаторы были удалены или заменены с целью псевдонимов данных, по-прежнему будет являться персональными данными. Если информация, которая относится к конкретному лицу, является неточной (то есть фактически неверной или относится к другому лицу), эта информация по-прежнему является персональной информацией, поскольку она относится к этому лицу.

GDPR (Общий регламент по защите данных, Регламент ЕС 2016/679) устанавливает семь ключевых принципов:

- 1) Законность, справедливость и прозрачность обработки данных,
- 2) Ограничение цели сбора и использования данных,
- 3) Минимизация данных (сбор только необходимых данных),
- 4) Точность (неточные данные должны быть удалены или исправлены),
- 5) Ограничение хранения (срок хранения данных),
- 6) Честность и конфиденциальность (защита от несанкционированной или незаконной обработки, уничтожения или повреждения данных),
- 7) Подотчетность (обязанность соблюдать GDPR и способность продемонстрировать соответствие регламенту)

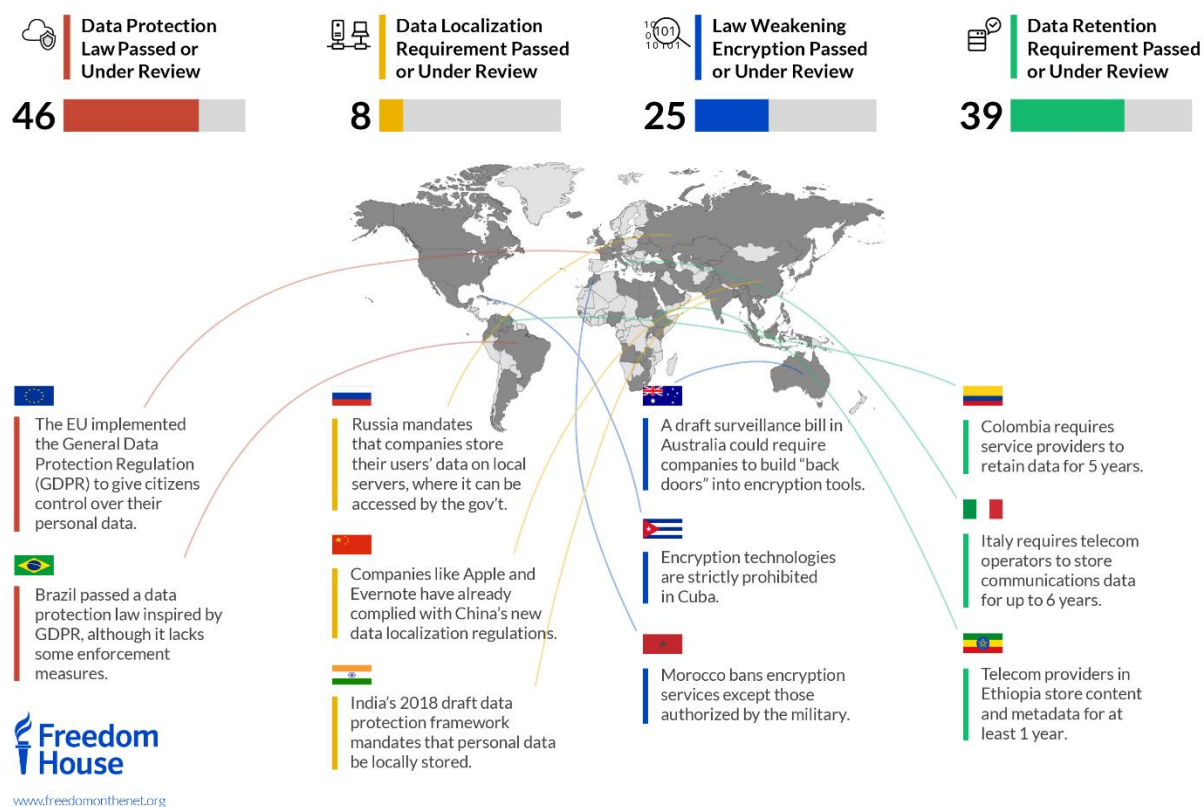
Эти принципы должны лежать в основе любого подхода к обработке персональных данных в Европе, они также обладают экстерриториальным принципом. Это означает, что все организации, собирающие, обрабатывающие и хранящие персональные данные физических лиц, которые сотрудничают с Евросоюзом, должны соответствовать требованиям GDPR.

** В основу данного отчета легли мнения, позиции, выступления и комментарии участников и выпускников Программы по кибербезопасности Европейского центра изучения вопросов безопасности им. Дж. Маршалла в декабре 2019 года, в которой авторка проекта является приглашенным профессором.*

1. Культура защиты персональных данных: краткий обзор

В ответ на опасения по поводу повсеместного сбора и присущей безопасности персональных данных многие страны принимают законодательство, которое предоставляет отдельным лицам право контролировать, как их данные собираются, обрабатываются и передаются государственными и частными организациями. Согласно отчету Freedom House 2018³, по крайней мере, 15 стран рассмотрели законы о защите данных, и в 35 странах уже есть такой закон. Законы о защите персональных данных, которые были предложены или приняты в Аргентине, Бразилии и Индонезии, очень напоминают европейский GDPR, вступивший в силу в мае 2018 года.

Where your Privacy Is (and Isn't) Protected



Во всем мире правительства и корпорации все больше жаждут получения больших объемов личной информации, чтобы использовать ее либо для политических репрессий, либо разработки алгоритмов искусственного интеллекта (ИИ). К сожалению, у обычных граждан на вооружении имеется не

³ Adrian Shahbaz, "Freedom on the Net 2018. The Rise of Digital Authoritarianism," *Freedom House*, 2018, <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism>.

так много вариантов противостоять такому положению дел. Было бы логично, если правительства и компании стремились повысить прозрачность в отношении использования личных данных, обеспечивая переносимость данных между платформами и позволяя людям просматривать и удалять все данные, собранные о них - ниши, которые некоторые из крупнейших компаний уже заняли.

Одним из способов реакции на такое положение дел, согласно докладу Freedom House⁴, могло бы стать включение гарантии прав человека в национальные стратегии по искусственному интеллекту. Поскольку директивные органы рассматривают, как ИИ может продвигать национальные приоритеты и улучшать жизнь и безопасность граждан, им следует обеспечить, чтобы все предлагаемые планы исследований и разработок включали тщательную оценку любых возможных последствий для прав человека, включая права на неприкосновенность частной жизни и свободу выражения. При этом оценки прав человека для рассматриваемых технологий должны быть доступны для широкой общественности.

1.1 Мировая практика

С принятием GDPR Европейский союз сделал еще один шаг на пути к тому, чтобы каждый человек вносил вклад в культуру, обеспечивающую конфиденциальность данных, и одновременно выступал ее движущей силой с целью дальнейшего укрепления права отдельных лиц в отношении их личных данных.

Современные масс медиа уже не раз демонстрировали, как нарушения, связанные со сбором, обработкой и хранением персональных данных, могут оказать негативное влияние на репутацию компаний и доверие потребителей. Это, по сути, может оказаться куда более разрушительным, чем самые огромные штрафы, предусмотренные GDPR. Поэтому защита персональных данных, согласно новому регламенту, стала не просто очередной задачей или проблемой европейской бюрократии, а новым способом мышления и создания культуры⁵ внутри каждой организации, где люди думают о том, как бы они хотели, чтобы обрабатывалась их личная информация. GDPR требует, чтобы владельцы персональных данных получали более осмысленное согласие, повышали прозрачность того, какие данные собираются и почему, и

⁴ Ibid.

⁵ Sarah Thompson, "How to gear up for GDPR and create a data privacy culture," *Personnel Today*, June 21, 2017, <https://www.personneltoday.com/hr/gear-gdpr-create-data-privacy-culture/>.

предоставляли пользователям возможность загружать, передавать или удалять свою информацию.

Очевидно, что европейский регламент не распространяется на вопросы национальной безопасности и обороны, и, таким образом, не может ограничить безудержный и, по сути, бесконтрольный сбор данных правительствами. При этом сохраняется неопределенность в отношении того, как несколько статей GDPR будут реализованы на практике, например, положение, которое может позволить «законным интересам» компании заменить право человека на неприкосновенность частной жизни, или противоречивое «право на забвение», согласно которому общественные деятели пытаются удалить статьи или данные о себе, которые они считают нелестными.

Почему мы говорим о GDPR и необходимости ему соответствовать? Во-первых, этот регламент направлен на фундаментальное изменение способа обработки персональных данных во всех секторах Европы. Во-вторых, это положение повысило осведомленность специалистов и отдельных лиц о проблемах защиты данных. В-третьих, регламент предоставил новые широкие полномочия людям в том, как они могут контролировать свои данные. И наконец, в-четвертых, речь идет об осведомленности и обучении граждан о правах на защиту персональных данных.

Согласно замеру Eurobarometer 2019 года⁶, увеличение количества запросов и жалоб подтверждает рост осведомленности о правах на защиту данных среди отдельных лиц. Действительно, 67% опрошенных граждан ЕС указали, что они слышали о GDPR, 36% из них указали, что они хорошо знают, что влечет за собой регламент. Кроме того, 57% из них указали, что им известно о существовании профильного государственного органа в их стране, ответственного за защиту прав на защиту персональных данных. По данным Европейской комиссии, этот результат на 20% превышает аналогичные замеры 2015 года.

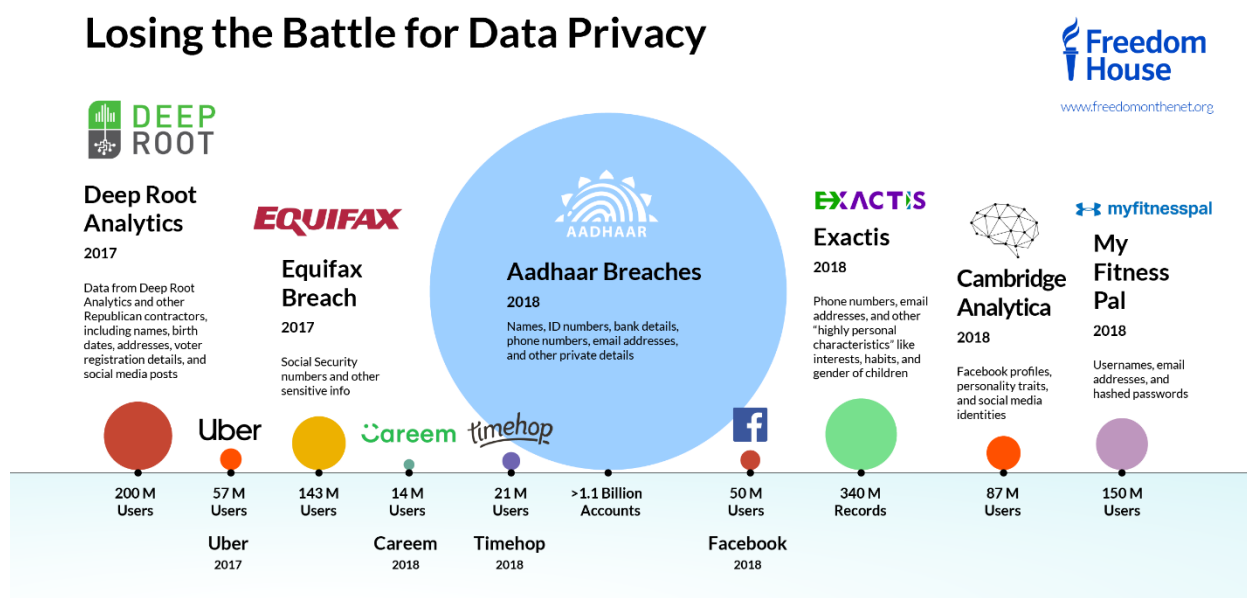
Если говорить о практических изменениях, то можно обратиться к статистике за один год с момента принятия GDPR. Так, общее количество дел, о которых сообщили органы защиты данных из 31 страны ЕС, составило 206,326, из которых 94,266 жалоб, и 64,684 из этих дел были возбуждены на основании уведомления контроллеров о нарушении данных. 52% вышеупомянутых дел завершены, а 1% оспаривается в национальных судах. Также органы защиты данных из 11 стран

⁶ Malia Thuret-Benoist, "One year of GDPR: GDPR enforcement and awareness," *Tech GDPR*, May 25, 2019, <https://techgdpr.com/blog/one-year-gdpr/>.

ЕС сообщили о наложении административных штрафов в рамках GDPR на общую сумму 55,955,871 евро.⁷

Очевидно, что создать культуру защиты персональных данных невозможно за один день, месяц или даже год. Европейскому союзу потребовалось несколько лет, чтобы значительно повысить уровень осведомленности среди своих граждан, а также объяснить, почему это важно, и что для этого необходимо делать. Более того, масштабное поощрение и продвижение этой правовой культуры позволило повысить уровень доверия и коммуникаций между государственными органами, бизнес организациями и гражданами.

GDPR и европейский правовой подход не является единственным вариантом решения проблем по обеспечению защиты персональных данных. Страны предпринимают различные усилия, разрабатывают и принимают законы, создают профильные органы, чтобы заниматься вопросами защиты информации в условиях массового развития кибертехнологий и пытаться бороться с еще более изысканными цифровыми преступлениями, зачастую объясняя принимаемые меры необходимостью обеспечения национальной безопасности и противодействия терроризму, при этом заметно ограничивая права и свободы как оффлайн, так и онлайн пространстве.



К примеру, в Эстонии, показавшей лучший показатель интернет свободы в 2018 году, разработали уникальную национальную модель по защите персональных данных. Это платформа X-Road для безопасного обмена данными работает на

⁷ Ibid.

основе эстонской технологии *blockchain* под названием KSI⁸, посредством которой все входящие и исходящие транзакции проходят проверку подлинности и шифруются.

Среди других преимуществ платформы важно отметить тот факт, что граждане получают уведомление, когда к их файлам данных обращаются государственные органы (за исключением случаев продолжающихся расследований). Учитывая сильную правовую базу Эстонии в отношении прав на неприкосновенность частной жизни и признанную на международном уровне репутацию передового игрока в обеспечении кибербезопасности для цифрового общества, система обеспечивает более надежную защиту, чем в странах, где данные граждан хранятся в незашифрованном виде на разрозненных серверах, и при этом отсутствует механизм информирования их о том, кто владеет информацией или как она используется.

В США некоторые штаты приняли свои собственные законы о конфиденциальности личных данных⁹:

- В Колорадо в 2018 году был принят закон, который заставляет предприятия принимать разумные меры безопасности, когда речь заходит о личной информации.
- Массачусетс требует от каждой бизнес организации, которая владеет или лицензирует личную информацию, реализовывать письменные программы информационной безопасности.
- Вермонт недавно принял закон, нацеленный на компании, которые собирают и продают личную информацию.
- В Калифорнии в 2020 г. планируется введение закона, аналогичного европейскому GDPR, который предоставит потребителям право запрашивать записи о том, какие типы данных о них хранятся в компании и как они используются.
- Нью-Йорк разработал аналогичное законодательство, которое требует от компании предоставлять потребителям копию информации, хранящейся в архиве.

1.2 Куда движется мир

Защита персональных данных в разных частях планеты обретает другие оттенки, поскольку в большей степени связана с управлением и контролем над интернетом, и, как следствие, масштабным ростом авторитаризма. По сути,

⁸ E-Estonia. Security and safety, <https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/>.

⁹ Patchwork legislation makes data privacy difficult, Best VPN, <https://bestvpn.org/privacy-index/#tab-con-7>.

интернет превратился в современную публичную сферу, а социальные сети и поисковые системы обладают огромной силой и весомой ответственностью за обеспечение того, чтобы их платформы служили общественному благу. Неограниченный сбор личных данных ограничивает право человека на одиночество, без которого мир, процветание и свобода личности - плоды демократического мира – невозможно сохранить или использовать¹⁰.

Пока некоторые страны добиваются реального прогресса в сфере свободы интернета, как например страны ЕС, другие же, наоборот, ужесточают и ограничивают свободу интернета. Достаточно вспомнить, когда граждане Малайзии проголосовали за премьер-министра, который пообещал отменить недавно принятый закон о фейковых новостях, который активно использовался его предшественником.

Однако наиболее интересными с точки зрения формирования трендов развития киберпространства и, как следствие, влияния на защиту персональных данных и цифровых прав, безусловно, являются **Россия** и **Китай**, представляющие альтернативу европейскому GDPR.

Когда Марк Цукерберг давал показания перед Конгрессом в начале 2018 года в отношении практики передачи данных Facebook, он предупреждал, что регулирование использования персональных данных платформой приведет к тому, что США отстанут от китайских компаний, когда речь заходит об инновациях с интенсивным использованием данных, таких как искусственный интеллект. Его аргумент отразил общепринятое мнение, что китайская интернет-индустрия обладает огромным количеством пользовательских данных, собранных для исследования ИИ благодаря слабому регулированию сбора данных в Китае.

¹⁰ Adrian Shahbaz, "Freedom on the Net 2018. The Rise of Digital Authoritarianism," *Freedom House*, 2018, <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism>.

За последние два десятилетия великий китайский firewall превратился в пугающе эффективный (при этом весьма привлекательный) аппарат цензуры и цифровой слежки. Более того, **Kumai** предпринимает шаги по популяризации и распространению своей модели за рубежом¹¹, проводя широкомасштабные



тренинги для иностранных чиновников, предоставляя технологии авторитарным правительствам и требуя, чтобы международные компании соблюдали китайские правила, даже работая за пределами Китая. Эти тенденции представляют собой существенную угрозу будущему открытого интернета, перспективам демократического мира и ценностям открытого общества.

Однако для самого Китая защита персональных данных тоже оказалась в приоритете, несмотря на, казалось бы, всю парадоксальность ситуации. Несколько громких кейсов и публичная реакция на них позволили по-новому взглянуть на цифровые права в Китае. В 2016 году 18-летняя китайская школьница умерла в результате телефонного мошенничества¹². Этот случай стал катализатором бурной дискуссии о защите личной информации в интернете. Тогда же и началась разработка законодательства по защите персональных данных в Китае, когда Постоянный комитет высшего законодательного органа КНР - Национального народного конгресса принял Закон о кибербезопасности. Закон, вступивший в силу 1 июня 2017 года¹³:

- запрещает поставщикам онлайн-услуг собирать и продавать личную информацию пользователей без согласия пользователя;
- устанавливает основные требования конфиденциальности;
- запрещает сетевым операторам собирать данные, не относящиеся к их услугам;
- запрещает обмениваться идентифицируемыми данными без согласия;

¹¹ В 2017 году в Китае состоялся двухнедельный «Семинар по управлению киберпространством для должностных лиц стран в рамках инициативы «Пояс и путь». Иностранные должностные лица осмотрели штаб-квартиру компании, занимающейся «системами управления общественным мнением с использованием big data», включая инструменты для мониторинга негативного общественного мнения в режиме реального времени и «систему управления общественным мнением с позитивной энергией».

¹² Wei Sheng, "One year after GDPR, China strengthens personal data regulations, welcoming dedicated law," *Technode*, June 19, 2019, <https://technode.com/2019/06/19/china-data-protections-law/>.

¹³ Ibid.

- требует от компаний защищать личные данные.

В законе не прописано, что компании должны делать, чтобы соответствовать ключевым требованиям, касающимся согласия, анонимности и защиты личной информации. Но эти вопросы рассматриваются в документе, опубликованном *Национальным техническим комитетом по стандартизации информационной безопасности Китая (TC260)*, который выпустил национальный стандарт - *Спецификацию безопасности личной информации*, которая охватывает сбор, хранение, использование, обмен, передачу и раскрытие личной информации¹⁴.

Среди недавних кейсов по персональным данным в Китае можно вспомнить, как остро китайское онлайн сообщество отреагировало на комментарий Робина Ли, основателя Baidu, в начале 2018 года о «торговле конфиденциальностью для удобства», когда его замечание вызвало бурю негодования среди интернет-пользователей. По счастливой случайности, в том же году Baidu подала в суд на группу по защите прав потребителей в провинции Цзянсу за сбор данных о пользователях без согласия (судебный процесс был впоследствии отозван, после того как компания удалила функцию по мониторингу контактов и действию пользователей).

Кроме того, в сентябре 2019 года в Китае была разработана собственная версия шторма конфиденциальности FaceApp. Используя методы искусственного интеллекта и машинного обучения, приложение Zao позволяло пользователям обмениваться лицами со знаменитостями в фильмах или телешоу¹⁵. Он стал вирусным инструментом для создания глубоких подделок (deep fakes), но вскоре возникли опасения, когда люди заметили, что пользовательское соглашение Zao предоставило приложению глобальные права на бесплатное использование любого изображения или видео, созданных на платформе.

После публичного протеста по поводу этих противоречивых условий конфиденциальности пользователей и вопросов, касающихся безопасности данных, компания пояснила, что приложение не будет хранить личную информацию пользователей. Под давлением компания также заявила, что, как только пользователь удалит Zao или свою учетную запись, приложение удалит соответствующую информацию, как того требуют правила, и «обеспечит сохранность личной информации и данных всеми возможными способами».

¹⁴ Ibid.

¹⁵ Zack Doffman, "Chinese Deepfake App ZAO Goes Viral, Privacy Of Millions 'At Risk'," *Forbes*, September 2, 2019, <https://www.forbes.com/sites/zakdoffman/2019/09/02/chinese-best-ever-deepfake-app-zao-sparks-huge-faceapp-like-privacy-storm/#118865ce8470>.

И, наконец, третий пример, относящийся к конфиденциальности личных данных китайских интернет-пользователей, связан с Ant Financial, финансовым подразделением Alibaba. Компания запустила Zhima (Sesame) Credit, онлайн-сервис для кредитного скоринга, который предлагает кредиты на основе цифровой активности пользователей, записей транзакций и присутствия в социальных сетях. Пользователи обнаружили, что они были зачислены в систему кредитного скоринга по умолчанию и без согласия. Под давлением общественности Alibaba извинилась.

Что касается *России*, то помимо обвинений в подрыве честности и легитимности американских президентских выборов в 2016 году, а также разработке массовых фейк-кампаний и пропаганды в странах СНГ, ЕС и США, Москва пытается пролоббировать концепцию «суверенного интернета» на площадке ООН и пространстве ЕАЭС, а также разработать Евразийский аналог GDPR.

Управление интернетом с сильным государственным суверенитетом – отличительная черта российского подхода. Достаточно вспомнить закон Яровой 2016 г., который обязал телекоммуникационные компании хранить контент текстовых сообщений, телефонных разговоров, изображений и видео в течение шести месяцев, а также их метаданные в течение трех лет на территории России, предоставляя эту информацию службам безопасности по запросу.

Так называемый *закон о «суверенном интернете»*¹⁶, принятый Госдумой в ноябре 2019 г., предоставляет чиновникам широкие полномочия по ограничению трафика в российской сети. Вместе с тем существуют опасения, что Кремль пытается создать firewall, аналогичный тому, который используется в Китае. Кроме того, введение нового контроля над интернетом усугубляется необходимостью поддержания безопасности режима и, как следствие, связано с подавлением любого рода политических оппонентов. В результате этот закон позволит:

- Роскомнадзору более эффективно блокировать сайты (DPI),
- Внедрить российскую национальную систему доменных имен (DNS);
- интернет-провайдерам идентифицировать источник трафика и фильтровать контент (цензура), а также
- отключить интернет в случае чрезвычайной ситуации.

Многие эксперты отмечают, что полная реализация суверенного интернета в России будет чрезмерно трудной, но эта модель, безусловно, приведет к

¹⁶ “Russia internet: Law introducing new controls comes into force,” *BBC News*, November 1, 2019, <https://www.bbc.co.uk/news/world-europe-50259597>.

ужесточению государственного контроля над обществом и дополнительным трудностям как для российских, так и иностранных компаний. Ожидается, что это ускорит фрагментацию глобального интернета и существенно увеличит зависимость России от китайских технологий¹⁷. Вместе с тем, параллельно Россия продвигает альтернативную модель управления интернетом с сильным государственным суверенитетом в рамках Международного союза электросвязи ООН.

Подводя итог важно отметить, что на данном этапе существует несколько альтернативных способов создания правового режима по защите персональных данных. Важно понимать, что разработка и принятие профильного закона, делегирование полномочий или же создание профильного органа, продвижение вверх в индексах интернет свободы или кибербезопасности – это всего лишь первый шаг многолетних усилий по созданию устойчивой цифровой экосистемы.

Для Казахстана, который проходит процесс массовой цифровизации с целью интеграции в глобальные информационные и экономические процессы, помимо законодательных и других инициатив, необходимых для регулирования этой сферы, важно сконцентрировать усилия на повышении осведомленности о важности защиты персональных данных и продвижении культуры цифровых прав посредством цифровой грамотности и кибергигиены. Очевидно, что Казахстану будет крайне сложно балансировать между тремя основными игроками – ЕС, РФ и КНР – в поиске и разработке собственного подхода к защите персональных данных на практике.

¹⁷ Alena Epifanova, "Deciphering Russia's "Sovereign Internet Law," *DCAP Analysis*, January 16, 2020, <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>.

2. Защита персональных данных в Казахстане

Казахстан, будучи страной серьезным образом интегрированной в мировое политическое и экономическое реальное пространство, демонстрирует впечатляющие темпы интеграции в мировое информационное пространство, как на уровне государственных структур, так и на уровне общества. Недостаточное внимание к новым возможностям, а также рискам и угрозам способно спровоцировать выпадение страны из общего тренда мирового развития и вытеснение на периферию международных процессов.

Появление системы электронного правительства способствовало, с одной стороны, изменению взаимоотношений между обществами и их правительствами в пользу демократизации, а с другой стороны, в значительной степени способствовало снижению бюджетных трат на администрирование.

В то же время сетевизация (как в ее кибернетическом, так и в социальном измерениях) повлекла за собой утерю монополии на осуществление власти. В данном случае под властью подразумевается возможность воздействовать на деятельность и поведение других людей и задавать тренды общественного движения. Очевидно, что тот, кто имеет возможность, в первую очередь техническую, влиять на контент информационных потоков в информационном пространстве, способен манипулировать массовым сознанием. Осознание значимости данного вызова и бесперспективность попыток реагирования на него только лишь в административном порядке путем использования технических средств (к примеру, создание firewall или сертификатов безопасности) подвигло национальные правительства к изменению стратегий информационной политики. Параллельно с положительными изменениями в информационно-коммуникационной составляющей Казахстана, наблюдается тенденция увеличения реальных угроз в сфере информационной и кибербезопасности страны.

2.1 Status Quo

21 мая 2013 г. в Казахстане был принят Закон «О персональных данных и их защите». Как и в любом другом законе, в нем содержится терминологический аппарат и основные направления работы по защите персональных данных.

Согласно закону, «персональные данные - сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином

материальном носителе».¹⁸ Главной целью этого закона является «обеспечение защиты прав и свобод человека и гражданина при сборе и обработке его персональных данных» (ст.2), при этом о хранении речи пока не идет.

Компетенции уполномоченного органа (Прокуратура РК) в сфере защиты персональных данных представлены в ст.27-1 проекта Закона РК О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам регулирования цифровых технологий.

Если сравнивать этот документ с аналогичными законами в других странах мира, следует обратить внимание, что с одной стороны он достаточно прямолинейный и комплексный, при этом некоторые аспекты защиты персональных данных на практике провисают. Так, к примеру, ст.20 закона говорит о том, что персональные данные подлежат защите и ее гарантом выступает государство.

Принимая во внимание крупнейшие утечки личных казахстанцев в 2019 году¹⁹ из баз данных ЦИК и Генпрокуратуры, возникает вопрос, каким образом государство может гарантировать защиту личной информации, если, согласно данным ЦАРКА, утечка происходила из базы данных Генеральной прокуратуры РК, т.е. уполномоченного органа в сфере защиты персональных данных, а МВД РК приостановило дело об утечке данных за отсутствием состава преступления, потому что «указанные сведения с данными граждан РК в сети интернет не были обнаружены»²⁰?

«...На направленную нами информацию орган упорно не реагирует. Возможно, руководству докладывают об исправлениях, но в реальности ничего не меняется. Более того, имеются факты активного сбора данных злоумышленниками с целью коммерциализации и иной передачи третьим лицам (надеемся на возбуждение уголовного дела)», - ЦАРКА²¹.

¹⁸ Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 28.12.2017 г.), https://online.zakon.kz/document/?doc_id=31396226#pos=3;-157.

¹⁹ Catalin Cimpanu, "Extensive Hacking Operation Discovered in Kazakhstan," *ZDNet*, November 23, 2019, <https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/>.

²⁰ Официальный аккаунт ЦАРКА в Facebook, https://m.facebook.com/story.php?story_fbid=2636221533272242&id=1674347306126341.

²¹ "Утечка данных из базы Генпрокуратуры РК: счёт идёт на месяцы," *Ratel*, February 14, 2020, http://www.ratel.kz/kaz/utechka_dannyh_iz_bazy_genprokuratury_rk_schet_idet_na_mesjatsy?fbclid=IwAR2Rvr0DA GyJGUIGLBCDuic-sGpyWH9IBICn2tUoP34XfREbMXOWjol-t5s.

Напомним, что в конце 2019 года стало известно о том, что известная китайская компания по кибербезопасности Qihoo 360 заявила, что обнаружила данные, полученные от зараженных компьютеров казахстанцев из 13 городов страны.

Исследователи говорят, что «продвинутая хакерская группа использует специально разработанные хакерские инструменты, дорогие комплекты для слежки, мобильные вредоносные программы и оборудование для перехвата радиосвязи, чтобы шпионить за казахстанскими целями» (См. карту ниже). Собранные данные касались в основном офисных документов, взятых со взломанных компьютеров. Вся украденная информация была размещена в папках каждого города, каждая папка города содержала данные на каждом зараженном хосте.

Интересным представляется тот факт, что мнение аналитиков по этому громкому кейсу разделилось, однако наиболее распространенные теории в основном касались:

- (1) российской APT (advanced persistent threat, Golden Falcon),
- (2) казахстанской разведки, шпионящей за своими гражданами,
- (3) российской наемной группы, которая шпионит по просьбе правительства Казахстана.



Другим кейсом по нарушению защиты персональных данных казахстанцев стало громкое дело о появлении архивных документов Qazkom банка (сейчас Halyk Bank) на мусорной свалке в Астане в 2017 г.

«...Я в шоке! Сегодня увидел, как в отделении «Казкомбанка» по ул. Куйши Дина, 31 в Астане уничтожают архивы документов своих клиентов за 2016 год. Где сохранность личных данных?! Ведь такие документы должны храниться в архивах банка либо уничтожаться через шредер»²², — писал пользователь Facebook Тимур Асылханов.

Казалось бы, парадоксальная ситуация, поскольку для уничтожения архивных документов существуют специальные правила хранения и утилизации документов. Пресс-служба банка принесла извинения своим клиентам, пообещав разобраться в ситуации и «наказать виновных». Это наиболее распространенная практика привлечения к ответственности в РК, причем необязательно уголовной или административной, чаще всего проявляется в

²² «Документы клиентов "Казкома" оказались возле мусорной свалки в Астане,» *Caravan*, September 25, 2019, <https://www.caravan.kz/news/dokumenty-klientov-kazkoma-okazalis-vozhle-musornojj-svalki-v-astane-401834/>.

виде увольнения. В результате руководитель отделения банка в Астане был уволен.

Очередная утечка персональных данных была зафиксирована компанией Центр информационных технологий «ДАМУ», когда в июле 2019 года произошел инцидент передачи третьим лицам информации, содержащей конфиденциальные данные от лица, имеющего легальный авторизованный пользовательский доступ в Медицинскую информационную систему DamuMed²³.

Ожидалось, что компания займется разбором полетов в соответствии действующим законодательством, а именно Кодексом Республики Казахстан «Об административных правонарушениях» ст. 79 «Нарушение законодательства о персональных данных и их защите» и Уголовным Кодексом РК ст. 205 «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций», ст. 208 «Неправомерное завладение информацией», однако информация по разрешению этого дела в публичном пространстве отсутствует. Остается только догадываться, понес ли кто-то ответственность за этот инцидент.

«... На данный момент мы готовим материалы для передачи их в правоохранительные органы для проведения тщательного разбирательства... По факту публикации в ФБ скриншотов, сообщаем, что беспокоиться не о чем, медицинские данные доступны только авторизованным пользователям, лицо которое получило их в свое распоряжение, получило их незаконным способом и его действия могут квалифицироваться перечисленными выше нормами Уголовного законодательства. Никакого слива в общедоступные ресурсы не было!»²⁴, - говорит DamuMed в своем официальном аккаунте в Facebook.

Эти и другие примеры утечки персональных данных казахстанцев, согласно Министерству цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан, свидетельствуют о наличии целого ряда проблем. Во-первых, «каждый государственный орган-владелец баз данных самостоятельно отвечает за сохранность своих баз и соблюдение норм

²³ “В Казахстане вновь произошла утечка персональных данных,” *Kursiv*, July 9, 2019, <https://kursiv.kz/news/obschestvo/2019-07/v-kazakhstane-vnov-proizoshla-utechka-personalnykh-dannykh>.

²⁴ Официальный аккаунт DamuMed в Facebook, <https://www.facebook.com/damumed/posts/435054947079785>.

и правил по использованию и конфиденциальности хранящейся там информации»²⁵.

Во-вторых, ни у одного государственного органа нет компетенций и полномочий заниматься мониторингом интернета в части нарушения законодательства в сфере персональных данных и их защиты.

В-третьих, в стране отсутствует профильный орган по защите персональных данных (по аналогии с европейским Data Protection Agency).

Однако помимо этих очевидных проблем и анализа вышеприведенных кейсов утечки личной информации, ставших публичными, важно обратить внимание как минимум на еще три момента:

- Привлечение к ответственности за нарушение законодательства. Здесь речь идет об увольнении руководителя отделения, на примере кейса Qazkom, и штрафе для должностных лиц²⁶, как ожидалось в случае с утечкой данных 11 млн казахстанцев. Однако по факту никакой правовой статистики по защите персональных данных нет, правовой механизм необходимо развивать открыто и прозрачно. Важно развивать культуру защиты персональных данных, в том числе путем сообщения об утечках информации субъектам персональных данных²⁷, что позволит выстроить доверительные отношения и воспринимать всерьез ответственность по сбору, обработке и хранению персональных данных.

- Защита данных vs конфиденциальность данных. Если защита данных — это защита от несанкционированного доступа, то конфиденциальность данных — это авторизованный доступ - кто имеет, и кто его определяет. Иными словами, защита данных — это, по сути, техническая проблема, тогда как конфиденциальность данных является правовой (юридической). Дело в том, что только технологии не смогут обеспечить конфиденциальность личных данных. Большинство протоколов защиты конфиденциальности по-прежнему уязвимы для уполномоченных лиц, которые могут получить доступ к данным. Бремя этих уполномоченных лиц, прежде всего, связано с законом о конфиденциальности, а не с технологиями²⁸.

²⁵ “Насколько казахстанцы защищены от утечки персональных данных,” *Profit*, July 11, 2019, <https://profit.kz/news/53478/Naskolko-kazahstanci-zaschischeni-ot-utechki-personalnih-dannih/>.

²⁶ “Должностных лиц, виновных в утечке данных 11 млн казахстанцев, накажут штрафом,” *Informburo*, July 9, 2019, <https://informburo.kz/novosti/dolznostnyh-lic-vinovnyh-v-utechke-dannyh-11-mln-kazahstancsev-nakazhut-shtrafom-92602.html>.

²⁷ Защита персональных данных в Казахстане: неработающий закон и осторожное движение к GDPR, *Soros Foundation Kazakhstan*, June 4, 2019, <https://www.soros.kz/ru/personal-data-protection-in-kz/>.

²⁸ Rick Robinson, “Data Privacy vs Data Protection,” *IPS Watch Blog*, January 20, 2020, <https://blog.ipswitch.com/data-privacy-vs-data-protection>.

○ Технологические возможности и партнеры для сотрудничества. В первую очередь с точки зрения защиты персональных данных возникают вопросы о том, кто имеет доступ и контролирует безопасность сбора, обработки и хранения личной информации, полученной с помощью, к примеру, камер «Сергек». Этот вопрос обретает особую актуальность в связи с тем, что два технических партнера, поставляющих продукцию на казахстанский рынок, являются китайская фирма Dahua Technology (партнер «Коркем Телеком» по Сергеку) и Hikvision (работает в РК с 2015 года)²⁹, в отношении которых США ввели санкции за содействие нарушению прав человека в отношении мусульманских меньшинств КНР³⁰.

Этот компонент усугубляется и тем, насколько государственные органы будут соблюдать права граждан на защиту персональных данных, и здесь, прежде всего, речь идет о функциях и возможностях силовых структур РК, в частности Комитета национальной безопасности (КНБ). В условиях внедрения Национальной системы видеомониторинга возникает главный вопрос, каким образом будет достигаться баланс между правом на частную жизнь и вмешательством в нее во благо соблюдения общественного порядка и обеспечения национальной безопасности³¹.

В целом система стейкхолдеров, так или иначе участвующих в процессах, связанных с защитой персональных данных, является очень большой. Несмотря на наличие профильных ведомств, курирующих надзорные органы и других задействованных участников информационного процесса – сбор, обработка, хранение, уничтожение личных данных, важно понимать, что, по сути, рисуя схему следует отразить все существующие государственные органы и их комитеты, департаменты и отделы, поскольку у каждого института власти есть как минимум одна база данных, с которой они работают. Это означает, что культура защиты персональных данных должна превратиться в то самое связующее звено, которое позволит гармонично взаимодействовать государственным органам друг с другом и с обществом, повысить уровень доверия и коммуникаций, что является неотъемлемой частью цифрового

²⁹ Канат Алтынбаев, «Китайская техника в городах Казахстана вызвала опасения из-за возможной шпионской слежки», *Karavan Sarai*, December 11, 2019, https://central.asia-news.com/ru/articles/cnmi_ca/features/2019/12/11/feature-01.

³⁰ Канат Алтынбаев, «Спасаясь от преследования, этнические казахи из Китая ищут убежища в Казахстане», *Karavan Sarai*, November 8, 2019, https://central.asia-news.com/ru/articles/cnmi_ca/features/2019/11/08/feature-01.

³¹ «Большой брат: как будет работать национальная система видеомониторинга в Казахстане», *Forbes*, February 20, 2020, https://forbes.kz/process/technologies/bolshoy_brat_po-kazahski_1582187734.

общества, создание которого предусмотрено Законом РК о персональных данных и их защите.

Согласно данным, приведенным на сайте Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан, *«вопросы защиты оставлены на усмотрение собственников и операторов персональных данных (владельцы интернет-ресурсов, интернет-магазины, кредитные бюро, микрофинансовые, организации и др.)»*³² При этом технические требования по защите информации в информационных системах, содержащих персональные данные, установлены только для государственного сектора.

ТЕКУЩИЙ СТАТУС

- ⊖ рост неконтролируемого со стороны граждан и государства обращения персональных данных в незаявленных и коммерческих целях (в т.ч. «большие пользовательские данные»)
- ⊖ отсутствие регулируемого рынка персональных данных в обороте цифровой экономики
- ⊖ (BigData, фин-тех, электронная коммерция и др.)
- ⊖ технические требования по защите информации в информационных системах, содержащих персональные данные, установлены только для государственного сектора

ПУТИ РЕШЕНИЯ

- ✓ **внести изменения в законодательство в части:**
 - совершенствования принципов сбора и обработки персональных данных, соответствующих gdpr;
 - ведения реестра операторов персональных данных;
 - усиления контроля за использованием персональных данных
- ✓ выработать технические требования к обработке персональных данных для операторов персональных данных
- ✓ автоматизировать процессы уведомления и получения согласия граждан на доступ и передачу персональных данных третьим лицам (подана бюджетная заявка на 2020 г. на 220 млн.тенге)
- ✓ определить комитет по информационной безопасности микроаппаратным органом в сфере защиты прав субъектов персональных данных (т.н. «Data protection agency»)

Следуя этой логике, складывается парадоксальная ситуация, когда государственные органы пытаются обезопасить себя от потенциальной утечки личной информации (т.е. апгрэйднуть свои возможности), однако недавние кейсы, рассмотренные выше, свидетельствуют об обратном. Утечка данных произошла из баз данных Центральной избирательной комиссии и Генеральной прокуратуры. Очевидно, что дьявол кроется в деталях, и проблема заключается не столько в техническом, сколько в человеческом факторе, и, как следствие, тесно связана с построением правовой культуры вокруг ценности персональных данных.

Однако среди новых функций Комитета по информационной безопасности нет никакого упоминания об этом. Вернее, из целого пакета законопроекта «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам регулирования цифровых технологий» по защите персональных данных ожидается «появление ответственного органа и введение сервиса по

³² Защита персональных данных (Data Protection Agency), <http://isdpm.dai.gov.kz/ru/page/zaschita-personalnykh-dannykh-data-protection-agency>.

защите персональных данных, который намерен уведомлять граждан о действиях с его данными»³³.

Сервис позволит уведомить граждан о совершаемых действиях с его данными и контроле за соблюдением требований по защите персональных данных. И как бы не стремились государственные ведомства априори обеспечить собственную безопасность, чтобы быть менее уязвимыми перед лицом новых угроз, очень часто они забывают о своих гражданах, которых также необходимо обучать и повышать их осведомленность в этих вопросах.

2.2 Public Opinion

В рамках данного исследования был проведен опрос³⁴ общественного мнения посредством сервиса SurveyMonkey с общим числом респондентов 500 человек. Результаты этого опроса позволяют восполнить пробелы причинно-следственных связей, выявленных в ходе проведения фокус групповых дискуссий (См. далее по тексту), а также понять, что думают активные пользователи социальных сетей и различных мобильных приложений в Казахстане по поводу важности защиты персональных данных.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ЗАМЕР ОБЩЕСТВЕННОГО МНЕНИЯ (I)

Во-первых, в опроснике отсутствовал базовый вопрос «Что такое персональные данные?», поскольку в ходе ФГД большинство людей так или иначе перечисляли определенные категории информации, которые представляют собой персональные данные.

Во-вторых, опрос носил общий характер, поскольку в рамках исследования ставилась задача понять, как обстоят дела с защитой персональных данных, и почему казахстанцы не видят важности и необходимости в этом вопросе.

В-третьих, полученные предварительные данные в ходе ФГД подтвердили первоначальные гипотезы о том, что граждане не мотивированы защищать персональные данные в силу убеждений о том, что «государство и так ведет цифровую слежку и все знает, а скрывать нечего».

В-четвертых, несмотря на недоверие к государственным органам – полиции, КНБ, ЦОНам и пр. – и проводимой политике, у опрошенных респондентов

³³ Гаухар Кадыргалиева, “Для защиты персональных данных граждан определяют уполномоченный орган,” *Liter*, March 12, 2020, <https://liter.kz/dlya-zashhityi-personalnyh-dannyh-grazhd/>.

³⁴ С опросником можно ознакомиться в приложении.

сохраняются патерналистские взгляды на то, кто должен заниматься продвижением культуры защиты персональных данных в Казахстане. При этом люди крайне заинтересованы в повышении уровня осведомленности в этих вопросах.

В-пятых, несмотря на, казалось бы, достаточно узкое направление в области прав человека и безопасности, защита персональных данных в Казахстане крайне тесно связана с общей политикой по сохранению безопасности режима, борьбе с терроризмом и религиозным экстремизмом и регулированию локального сегмента киберпространства, включая интернет.



И, в-шестых, для наиболее эффективной имплементации необходимых мер по повышению уровня кибербезопасности и, как следствие, росту позиций Казахстана в глобальном рейтинге кибербезопасности, крайне важно проводить системную работу по повышению уровня осведомленности о проблемах, связанных с утечкой персональных данных, важности кибергигиены и элементарных способах,

как граждане с меньшей долей вероятности хищения каких-либо данных могут находиться в интернете.

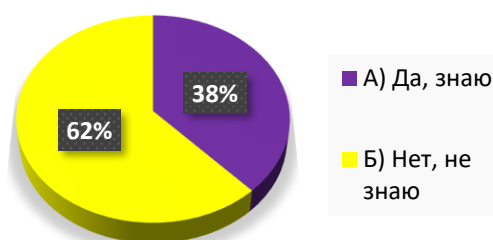
Наиболее ожидаемым результатов опроса стал тот факт, что почти две трети опрошенных респондентов не верят в то, что их персональные данные защищены. В принципе с этим тесно связана достаточно низкая осведомленность о концепции кибергигиены. Практически прямая корреляция по этим двум вопросам отражает отсутствие компетенций и знаний по максимально безопасной навигации в сети интернет, что также подтверждается на примерах, приводимых в рамках фокус групповых обсуждений.

Киберпреступники слишком хорошо понимают, что 95% нарушений кибербезопасности происходят вследствие человеческой ошибки. Вот почему они, как правило, концентрируют свои усилия на возможностях проникновения с помощью электронной почты. Из-за повсеместного использования электронной почты в современном мире это остается самым простым способом распространения вредоносных программ среди ничего не подозревающих пользователей. Если в Казахстане раньше эти письма приходили на английском и русском языках, то сейчас уже на казахском. Хакеры, которые используют эту среду для своего вектора атаки, в значительной степени полагаются на то, что

они заставляют получателей нажимать на вредоносные ссылки и вложения, часто выдавая себя за другого сотрудника или знакомого. Некоторые из самых популярных мошеннических писем счастья — это фишинговые мошенничества, которые содержат ссылки на сайты, которые выглядят законными³⁵. Когда человек переходит на веб-сайт, ссылка крадет его учетные данные или заражает его устройство вредоносным программным обеспечением.

Кибергигиена — это действия и шаги, которые пользователи компьютеров и других устройств предпринимают для поддержания работоспособности системы и повышения онлайн-безопасности. Эти практики часто являются частью повседневной деятельности по обеспечению безопасности личности и других компонентов, которые могут быть украдены или испорчены. Как и физическая гигиена, кибергигиена проводится регулярно, чтобы предотвратить естественное ухудшение состояния и общие угрозы.

Знаете ли Вы, что такое кибергигиена?



По данным Лаборатории Касперского, многие пользователи и предприятия в Казахстане (как и в других странах Центральной Азии) продолжают использовать пиратское программное обеспечение, такое как незащищенные копии старых операционных систем Windows³⁶ для своей онлайн-деятельности, подвергая риску все действия в интернете из-за отсутствия опыта и образования в области информационных технологий и кибербезопасности в открытом доступе. Отсутствие опыта означает, что Казахстан и Центральная Азия в целом чрезвычайно привлекательны для киберпреступников, которые эксплуатируют эти слабости и зарабатывают на них. При этом в Казахстане только 3% онлайн-преступлений преследуются по закону³⁷.

Компьютеры с доступом к интернету подвергаются взлому каждые 39 секунд только в США³⁸, и нет сомнений в том, что организациям, бизнесу и гражданам

³⁵ Chris Brook, "What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More," *Digital Guardian*, December 5, 2018, <https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more>.

³⁶ Anna Gussarova, "Kazakhstan Adapts to the Cyber Age," *Per Concordiam*, European George C. Marshall Center for Security Studies, Garmisch-Partenkirchen, Vol. 7 Issue 2, 2016: *Unipath CENTCOM*, April 7, 2017, <https://unipath-magazine.com/kazakhstan-adapts-to-the-cyber-age/>.

³⁷ Almaz Kumenov, "Hackers eyeing Kazakhstan as a safe haven," *Eurasianet*, November 27, 2018, <https://eurasianet.org/hackers-eyeing-kazakhstan-as-a-safe-haven>.

³⁸ "Hackers Attack Every 39 Seconds," *Security Magazine*, February 10, 2017, <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>.

необходимо принимать во внимание растущие проблемы кибербезопасности. К примеру, в финансовом секторе Казахстана киберпреступники взламывали не только аккаунты, но и банкоматы и платежные терминалы. Львиная доля атак состояла из вирусов и фишинговых атак³⁹. Эти компрометирующие устройства генерируют спам или участвуют в атаках распределенного отказа в обслуживании (DDoS-атаки). Киберпреступники также использовали взломанные машины для запуска DDoS-атак. Обычно они требуют, чтобы жертва заплатила выкуп за прекращение атаки. Ярким примером является кейс с Альфа-Банком, произошедший в 2017 году. По словам IT-специалиста Альфа-Банка Евгения Нозикова⁴⁰, хакеры искали вознаграждение в виде выкупа, и банку пришлось заплатить определенную сумму в обмен на то, чтобы злоумышленники разблокировали IT-системы банка.

Логично ожидать, что подобные инциденты происходят не только в финансовом секторе и более того не только в Казахстане, поэтому для обычных граждан, которые либо никогда не задумывались о такого рода мошенничестве, либо, сталкиваясь с ним, предпочитают решить проблему самостоятельно и не обращаться в органы правопорядка, однако очевидно, что в этих и других вопросах крайне важно обучать людей и объяснять, в чем заключается опасность киберпреступлений и связанных с ними кража или утеря персональных данных.

Общеизвестно, что первым шагом на пути к обеспечению безопасности в сети интернет и контролю конфиденциальности являются адекватные пароли и их хранение. Как видно по результатам опроса на примере достаточно малого



³⁹ Victoria Kelly-Clark, "Central Asia: The Land of CyberCrime?" *Global Risk Insight*, April 29, 2019, <https://globalriskinsights.com/2019/04/central-asia-cybercrime-land/>.

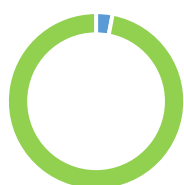
⁴⁰ Almaz Kumenov, "Hackers eyeing Kazakhstan as a safe haven," *Eurasianet*, November 27, 2018, <https://eurasianet.org/hackers-eyeing-kazakhstan-as-a-safe-haven>.

числа респондентов, люди не уделяют должного внимания генерации и регулярной смене паролей от различных онлайн-сервисов.

Почти четверть опрошенных не намерены тратить свое время на регулярную смену паролей от социальных сетей и услуг онлайн банкинга из-за навязчивой идеи о том, что «наше государство и так следит за нами». Поразительно, что чуть более трети респондентов ни раз не меняли свои пароли с момента регистрации, а 37% поменяли только после взлома аккаунта. Только 2% регулярно обновляют свои пароли раз в полгода и 3% опрошенных – один раз в месяц.

Если не учитывать достаточно сильный характер веры казахстанцев в теории заговоров, что также подтверждается в фокус-групповых обсуждениях, то

Вас когда-либо шантажировал
другой человек или организация
наличием информации личного
характера о вас?



■ А) да ■ Б) нет

картина представляется не совсем тревожной. Однако на самом деле это не так: согласно этому графику, более трети опрошенных уже столкнулись со взломом аккаунтов, а значит с утерей и/или кражей их персональных данных. При этом следует отметить, что 97% опрошенных ни разу не оказывались в ситуации, когда их шантажировали наличием информации личного характера.

И очевидно, эта проблема не так сильно волнует казахстанцев, в сравнении с теми проблемами, которые несут прямую угрозу материального характера (т.е. физическая кража денег) или другие ежедневные проблемы.

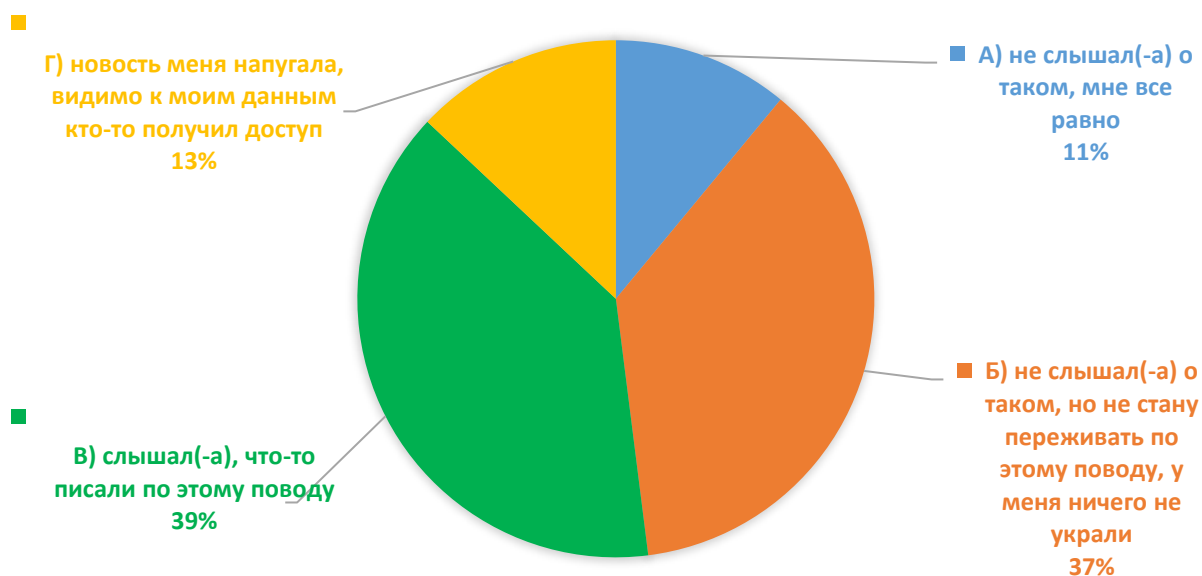
37 % опрошенных считают, что в реальной жизни и так хватает проблем, поэтому думать о безопасности в интернете нет смысла и необходимости. Интересно, что те же 37% респондентов не слышали о самой крупной утечке данных казахстанцев⁴¹, случившейся в июле 2019 года, и, как следствие, не переживали по этому поводу, потому что наивно полагали, что у них ничего не украли. Более того, согласно Центру анализа и расследования кибератак (ЦАРКА)⁴², утечка данных происходила из информационной системы Прокуратуры Республики

⁴¹ Catalin Cimpanu, "Extensive Hacking Operation Discovered in Kazakhstan," *ZDNet*, November 23, 2019, <https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/>.

⁴² "Утечка данных из базы Генпрокуратуры РК: счёт идёт на месяцы," *Ratel*, February 14, 2020, http://www.ratel.kz/kaz/utechka_dannyh_iz_bazy_genprokuratury_rk_schet_idet_na_mesjatsy?fbclid=IwAR2Rvr0DAGyJGUIGLBCDuic-sGpyWH9IBICn2tUoP34XfREbMXOWjol-t5s.

Казахстан и «раскрыла данные о всех гражданах Казахстана и иностранцах, в отношении которых когда-либо велось административное делопроизводство».

ЧТО ВЫ ДУМАЕТЕ ОБ УТЕЧКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ 11 МЛН КАЗАХСТАНЦЕВ В СЕТЬ ИНТЕРНЕТ В ИЮЛЕ 2019 ГОДА?



Четверть респондентов продолжают объяснять свое нежелание обеспечивать свою безопасность в интернете теорией заговора – «за нами и так следит наше государство», что также коррелирует с полученными результатами в фокус группах в разных частях страны.

Вместе с тем, каждый пятый опрошенный имеет один и тот же пароль и считает это наиболее эффективным способом его не забыть, хотя на самом деле представляет наиболее уязвимую часть населения с

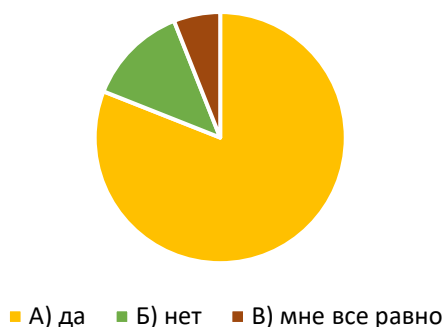
Почему Вы используете один пароль в разных аккаунтах в социальных сетях, образовательных, туристических, развлекательных и финансовых платформах?



точки зрения информационной и кибербезопасности. При этом важно отметить, что 16% используют три и более паролей для входа в различные онлайн сервисы

и платформы, что уже свидетельствует о наличии оптимизма в выработке культуры защиты персональных данных и важности ответственного использования интернета.

Готовы ли Вы повысить уровень осведомленности по теме защиты ваших персональных данных?



Несмотря на достаточно пессимистичные результаты опроса, 81% опрошенных респондентов хотели бы повысить свой уровень осведомленности и знаний по теме защиты персональных данных. Это не может не радовать, более того это крайне необходимо в условиях понимания и применения национального законодательства о защите данных и законодательства,

регулирующего доступ к публичной информации с учетом европейских тенденций в области прав человека, а также адекватного балансирования между конфиденциальностью и свободой информации. Доступ к цифровой среде и ее использование, безусловно, важны для реализации основных прав и свобод человека. Отсутствие доступа к цифровой среде или если этот доступ ограничен из-за плохой связи означает ограничение способности в полной мере осуществлять свои права⁴³.

Регулярные отключения связи («глушение» интернета), связанные с протестами в основных городах страны, полномасштабная реализация национальной программы кибербезопасности «Киберщит Казахстана» и, как следствие, усиление управления и контроля над интернетом (разработка и имплементация «электронного суверенитета»), а также разработка локального ПО для обеспечения безопасности в интернете только подтверждают важность продвижения культуры защиты персональных данных как правозащитную и информационную концепцию. Казахстан, безусловно, нуждается в том, чтобы сделать интернет более безопасным, особенно учитывая растущее использование сектора e-commerce и повышение уровня цифровизации личной информации граждан через платформу электронного правительства (e-gov)⁴⁴. Однако используемые методы и большое количество граждан, которые

⁴³ "Guidelines to respect, protect and fulfil the rights of the child in the digital environment," Recommendation CM/Rec(2018)7 of the Committee of Ministers Council of Europe, September 2018, p.13, <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>.

⁴⁴ Anna Gussarova, "Kazakhstan Adapts to the Cyber Age," *Per Concordiam*, European George C. Marshall Center for Security Studies, Garmisch-Partenkirchen, Vol. 7 Issue 2, 2016: *Unipath* CENTCOM, April 7, 2017, <https://unipath-magazine.com/kazakhstan-adapts-to-the-cyber-age/>.

невольно совершали интернет-преступления или были наказаны за свою политическую активность, сигнализируют о приоритете обеспечения безопасности в отношении индивидуальных свобод.

Нужно ли в Казахстане продвигать культуру защиты персональных данных?

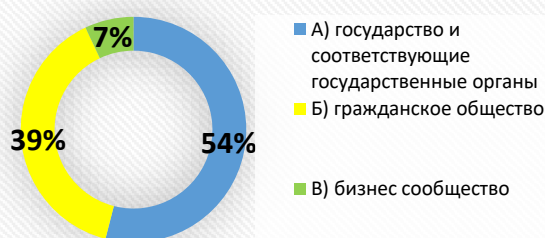


Согласно результатам опроса, в совокупности только 28% опрошенных (практически каждый третий) согласен с идеей о том, что необходимо продвигать культуру защиты персональных данных в Казахстане, при этом 63% не считают это необходимым. Из этого числа 26% не считают защиту персональных

данных серьезной проблемой, поэтому не нужно на это тратить время и ресурсы, а 37% опрошенных казахстанцев уверены, что в реалиях страны принято, что «все обо всем узнают так или иначе». Практически каждого десятого опрошенного казахстанца не волнует проблема безопасности персональных данных.

При этом важно обратить внимание, что чуть более половины респондентов (54%) считают, что государство и соответствующие государственные органы должны нести ответственность и заниматься вопросами защиты персональных данных, в то время как 39% уверены, что гражданское общество вполне может взять ответственность на себя и активно работать в этом поле. Только 7% опрошенных считают, что представители бизнес сферы должны заниматься защитой персональных данных, хотя на самом деле именно для бизнес сообщества (впрочем, как и для государства) вопросы конфиденциальности, безопасности и защиты данных являются основополагающими. К примеру, большинство потребителей в США не имеют права владеть или управлять собственными данными, поскольку компании, чьи продукты или услуги жители используют ежедневно, используют персональные данные (т.е. полное имя, адрес, история поиска в Google и т.д.) и

Кто должен заниматься вопросами защиты персональных данных?



продают их рекламодателям (таргетированная реклама)⁴⁵. За последние 25 лет персональные данные превратились в золотой рудник для корпораций. И пока они должны выбирать между защитой пользовательских данных и максимизацией прибыли, они будут выбирать прибыль каждый раз (поскольку это их прямая обязанность перед акционерами).

Поэтому крайне важно предпринимать проактивный подход к конфиденциальности данных, поскольку отказаться от мейнстрима в цифровом потреблении не представляется возможным. В этой связи особую актуальность обретает финансовый сектор страны и недавние резонансные кейсы об утечке персональных данных (документы Qazkom - удостоверения личности, контракты) на мусорной свалке в Астане в 2017 году. Этот пример лишь подтверждает идею о том, что граждане страны не осведомлены о важности защиты персональных данных и связанными с этим вопросом рисками утечки данных. В этом конкретном случае сотрудник финансовой организации, вероятно, не подумал о том, что нарушает конфиденциальность данных, права и законодательство. Вместе с тем, ответом на эти действия стало увольнение сотрудника банка⁴⁶.

Поэтому если говорить о том, каким образом граждане предпочитали бы повысить свой уровень знаний и осведомленности о защите персональных данных, мнения опрошенных казахстанцев разошлись:

- 22% респондентов хотели бы принять участие в тренингах и семинарах по этим вопросам;
- 18% уверены, что имея краткое пособие по защите персональных данных, они смогут улучшить свои знания;
- 14% предполагают, что видео (уроки) на YouTube позволят повысить осведомленность в этих вопросах;
- 13% предпочитают иметь мобильные приложения;
- 5% опрошенных готовы пройти курс по защите персональных данных и 4% хотели бы самостоятельно изучать проблематику.

⁴⁵ Om Mahida, "It's 2020 and we still have a data privacy problem," *The Next Web*, February 17, 2020, <https://thenextweb.com/podium/2020/02/17/ive-worked-in-a-virtual-office-for-3-years-heres-what-ive-learned/>.

⁴⁶ Жанна Сагидуллакызы, "Главу отделения Qazkom в Астане уволили после скандала с выброшенными документами клиентов," *Tengrinews*, September 25, 2017, <https://informburo.kz/novosti/glavu-otdeleniya-qazkom-v-astane-uvolili-posle-skandala-s-vybrosheennymi-dokumentami-klientov.html>.

Каким образом Вы бы хотели больше узнать о защите ваших персональных данных?



При этом важно отметить, что 24% опрошенных казахстанцев не верят в то, что персональные данные могут быть защищены, опять-таки обуславливая это верой в теории заговора и слежкой собственного государства за своими гражданами.

В конечном счете мнение казахстанцев по вопросам защиты персональных данных и повышению уровня осведомленности о проблемах, связанных с этими вопросами как в сети интернет, так и в результате проводимой государственной политики, во многом противоречиво.

В результате массовой цифровизации и доминирования онлайн компонента человеческой жизни защита персональных данных обретает особую актуальность в эпоху стремительного роста киберпреступлений и развития кибертехнологий. Защита и конфиденциальность данных должны стать приоритетным направлением развития этой сферы в РК, поскольку оно должно всегда соответствовать имеющимся международным стандартам в области прав человека. Именно подход с точки зрения прав человека должен преобладать в таких важных вопросах, связанных с личной информацией.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ЗАМЕР ОБЩЕСТВЕННОГО МНЕНИЯ (II)

Для понимания степени осведомленности казахстанцев о защите персональных данных и их взглядов в отношении актуальных вопросов в этой сфере были также проведены 12 фокус-групповых дискуссий в 6 крупных городах Казахстана⁴⁷. В результате ожидалось собрать сведения о том, насколько хорошо

⁴⁷ Для сбора данных были отобраны крупнейшие города страны и города, представляющие основные регионы: Алматы, Астана, Шымкент (юг), Актобе (запад), Усть-Каменогорск (восток), Петропавловск (север). Всего было проведено 12 ФГД, по 2 группы в каждом городе. Дискуссии проводились на казахском и русском языках. Все ФГД проводились по одному гайду.

В ФГД принимали участие представители двух возрастных групп: 6 групп в возрасте 25-30 лет и 6 групп в возрасте 40-45 лет. Возрастные ограничения были продиктованы двумя требованиями: во-первых, участники должны

граждане осведомлены в вопросах защиты персональных данных, какие представления о защите персональных данных бытуют в казахстанском обществе, и как обращаются со своими персональными данными в сети казахстанцы.

Одним из главных ограничений данного исследования является то, что как онлайн опрос, так и все фокус группы проводились в крупных городах, соответственно, взгляды и представления жителей сел и малых городов не попали в фокус. Таким образом, следует понимать, что результаты исследования представляют только городской и более молодой сегмент казахстанского общества. Предполагается, что для проецирования сделанных выводов на все общество, следует делать поправку в сторону более низкого уровня осведомленности о защите персональных данных и онлайн правах в данной сфере.

Хранение и использование персональных данных, которые предоставляют пользователи социальных сетей и различных онлайн сервисов, привлекает к себе все больше внимания. В последнее время можно наблюдать споры между правительствами стран и интернет-компаниями, которые собирают, хранят и используют персональные данные своих пользователей. Но если в демократических открытых обществах широко обсуждаются вопросы «справедливого» налогообложения интернет-компаний, гарантий тайны персональных данных, то для Казахстана более актуальными являются вопросы доступа государственных органов к персональным данным, собираемым и хранящимся интернет-компаниями, а также вопросы соблюдения прав граждан (в т.ч. цифровых).

Во-первых, в данном исследовании рассматривается уровень осведомленности казахстанцев о сборе, хранении и использовании персональных данных, которые они предоставляют онлайн, их восприятию возможности контролировать свои персональные данные, хранящиеся в сети.

быть активными пользователями социальных сетей и услуг онлайн (торговых) площадок, которые самостоятельно принимают решения относительно покупок товаров и услуг; во-вторых, среди участников должны быть родители детей школьного возраста, которые могли бы рассказать о своем опыте родительского контроля над поведением детей в сети интернет.

Мужчины и женщины были представлены в группах в равной мере. При отборе участников учитывались и некоторые другие социально-демографические критерии: все участники должны были быть занятыми, иметь постоянный доход, быть активными пользователями интернета, в том числе социальных сетей и онлайн площадок.

Во-вторых, часть дискуссий посвящалась знанию прав в области персональных данных, представлениях о системе правовых взаимоотношений между интернет-компаниями, пользователями их услуг и государством.

В-третьих, ряд вопросов исследования относился к восприятию мониторинга активности граждан в сети интернет со стороны государственных органов, роли государства в обеспечении сохранности персональных данных.

Знают ли о сборе, хранении и использовании персональных данных?

Что знают? Какие представления?

- Почти все участники ФГД знали о том, что интернет компании собирают, хранят и используют персональные данные своих пользователей, хотя подавляющее большинство имели только поверхностные представления о том, какие именно это данные и для чего они используются.
- Почти никто из участников ФГД не читает условия соглашения о сборе, хранении и использовании персональных данных, которое предлагают интернет компании, использующие персональные данные своих пользователей. Такое поведение респонденты объясняли прежде всего отсутствием выбора – условия приходится принимать в обмен на право пользоваться сервисом.
- Недостаток надежной информации заполняется различными мифами, которые иногда по содержанию близки к теории заговора. Одним из подобных мифов является убежденность в том, что казахстанские (и иностранные) спецслужбы имеют доступ не только к персональным данным, но и к содержанию электронных писем и сообщений онлайн мессенджеров.

Чувствуют ли контроль над своими персональными данными?

Насколько беспокоит вопрос контроля?

- Как правило, участники ФГД не верят в возможность полностью контролировать свои персональные данные, которые предоставляют онлайн. В частности, распространена убежденность в том, что даже если пройти процедуру изменения или удаления своих данных, последние все равно остаются на серверах интернет компании.
- Убежденность в отсутствии полного контроля над своими персональными данными не рассматривается респондентами как серьезная проблема.

Участники ФГД принимают это, скорее, как неизбежное условие, которое приходится принимать в обмен на возможность пользоваться сервисом.

- Как правило, людей заботит безопасность персональных данных только в тех случаях, когда есть риск кражи денег или имущества мошенниками-хакерами. Тайна других персональных данных, от которых не зависит сохранность денег, мало заботит участников ФГД. Это можно объяснить тем, что несанкционированный доступ к персональным данным не воспринимаются как нарушение права на неприкосновенность частной жизни.

Знание прав в сфере персональных данных. Как относятся к роли и пределам компетенции государственных органов?

- ФГД обнаружили очень низкий уровень знаний участников о правах субъекта персональных данных – ни один из них не смог сказать, что знает свои права. Никто не знал определенно, какие законы в Казахстане определяют персональные данные и их защиту, регулирует отношения в этой сфере, хотя почти все полагали, что такой закон в стране должен быть.

- Многие участники ФГД склонны не доверять интернет компаниям, не верят в соблюдение ими тайны персональных данных, и самое главное – не верят в соблюдение законности в сети интернет. Отсюда согласие на закрепление за государственным аппаратом широких полномочий.

- Обсуждение тестирования «сертификата безопасности» как примера возможных будущих инициатив властей страны, касающихся персональных данных, продемонстрировал, что в обществе имеют место как критика этой инициативы, так и ее поддержка. Первых возмущает нарушение права неприкосновенности частной жизни, вторые готовы жертвовать этим правом ради вопросов национальной безопасности, которыми власти объясняют необходимость данной инициативы.

ОСВЕДОМЛЕННОСТЬ И ПРЕДСТАВЛЕНИЯ О СБОРЕ, ХРАНЕНИИ И ИСПОЛЬЗОВАНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

ФГД начинались с вопросов, ответы на которые должны были показать уровень общей осведомленности участников по теме. Здесь также было важно узнать какие представления о персональных данных распространены, что вызывает озабоченность у людей, а также некоторые сведения о поведении, установках и привычках пользователей интернета.

Хотя почти все участники ФГД заявляли, что знают о том, что их персональные данные, предоставляемые онлайн, собираются, хранятся и используются интернет компаниями, ответы на более детальные вопросы показали, что эти знания часто поверхностны. К примеру, познания участников о том, какие именно данные собираются, ограничиваются в основном анкетными данными: имя, номер телефона, контакты, пол, возраст, локация. О сборе таких данных, как модель телефона, уровень заряда батареи, активность в сети, запросы поиска и прочее, знают скорее в редких случаях.

Почти никто из участников ФГД, пользующихся услугами интернет компаний, не читает условия соглашения о политике использования персональных данных, условия политики в отношении файлов cookies. Ни один участник не читает эти условия при каждой новой регистрации, лишь единицы заявили, что читали это во время первой регистрации в социальных сетях.

Свое нежелание читать условия соглашения участники ФГД объясняли по-разному: одни считают, что должны принимать все условия, если хотят пользоваться сервисом; другие полагают, что условия являются формальностью, и компании все равно соберут всю нужную информацию и используют по своему желанию; третьи просто не хотят тратить время на чтение условий.

«Я склоняюсь к тому, что там выбора нет. И не охота время тратить, понимаешь, что тебе нужно получить услугу, и какая разница, что ты прочитаешь. И даже если ты будешь не согласен, ты воспользуешься».
(Мужчина, 43 года, Астана)

Еще одним, хотя и косвенным, свидетельством поверхностности представлений о персональных данных является то, что только единицы из числа участников всех групп когда-либо меняли настройки персональных данных в своих браузерах или социальных сетях.

В тех группах, где возраст участников был от 40 до 45 лет, отдельно обсуждалась тема родительского контроля над активностью своих детей в сети интернет. Предполагалось, что через призму родительского контроля можно узнать больше о представлениях и взглядах людей среднего возраста о защите персональных данных.

Большинство родителей детей старшего школьного возраста призналось, что не могут контролировать активность своих детей в интернете в силу того, что у последних знаний в этой области гораздо больше. То есть уровень знаний интернета не позволяет родителям осуществлять надлежащий контроль. В таких случаях родители рассчитывают на доверительные отношения, беседы, но

контролировать средствами, которые предлагают разработчики социальных сетей, браузеров и приложений, они не могут.

В то же время было немало и таких родителей (в особенности отцов), чьи познания позволяют вести родительский контроль. Хотя все-таки родителей больше пугает риск попадания детей под влияние экстремистских организаций радикального ислама, религиозных сект, или организаций, которые подталкивают подростков и молодежь на суицид.

«Он [сын] мальчик с головой, учится на отлично. Вроде не замечал. Единственное, чего боюсь, — это то, что говорили: борода, короткие штаны... Даже секты не так страшны, как это мусульманство — ваххабиты, салафиты». (Мужчина, 45 лет, Шымкент)

Как правило, респонденты имеют общее представление о том, что данные используются в маркетинговых целях, например, для адресной рекламы. Они относятся к этому вполне спокойно, нейтрально, считая, что предоставляют свои персональные данные в обмен на возможность пользоваться услугами интернет компаний, например, социальными сетями. То есть персональные данные, с этой точки зрения, являются оправданной платой за услуги.

В то же время, по мнению респондентов, такая логика применима только в тех, случаях, когда речь идет о всемирно известных сетях или сервисах (Facebook, Instagram, WhatsApp и другие). Такую позицию респонденты объясняли высоким уровнем доверия к таким сервисам, который в свою очередь подтверждается фактом подписки миллионов пользователей по всему миру. И напротив, в отношении малоизвестных ресурсов, названия которых не стали именами нарицательными, респонденты относятся с настороженностью в плане предоставления своих персональных данных. Так, по мнению некоторых участников, безопасность и сохранность персональных данных зависит от самих пользователей — «нельзя раскрывать свои данные на неизвестных («сомнительных») сервисах».

Спокойное или нейтральное отношение к сбору и использованию персональных данных не всегда говорит о доверии интернет компаниям. Так, некоторые участники признавались в том, что указывают ложные данные: например, вымышленные имя, возраст, адрес. Некоторые пользователи интернета, указывают неактивный (или запасной) номер телефона, который приобретался специально для подобных нужд и активируется только в тех случаях, когда нужно получить код или подтвердить какие-то действия. Подобным образом некоторые участники ФГД указывают адреса электронной почты, которые

создают специально для авторизации в социальных сетях или торговых площадках.

«У меня вообще только рабочая почта есть, где нет моей фотографии, ни данных моих, только название фирмы. И я с ней захожу, потому что я не хочу, чтобы за моей жизнью кто-то следил. Я не склоняюсь, что у всех должно быть, и у меня должно быть. Лично я не хочу, чтобы кто-то видел, где я был, с кем я ходил. Думаю, это не нужно, лично у меня своя жизнь, и я этим довольствуюсь». (Мужчина, 27 лет, Актобе)

Очевидно, люди прибегают к таким приемам для того, чтобы сохранить анонимность тогда, когда этого нельзя сделать иным способом. И поскольку для компаний, которые преследуют маркетинговые цели, анонимность не является проблемой, и их могут устраивать вымышленные имена, можно предположить, что **люди, скрывающие свои личные данные, остерегаются не интернет компаний, а слежки со стороны государственных служб.**

На вопрос о том, допускают ли пользователи интернета использование их личных данных не в маркетинговых целях, отличающихся от заявленных в соглашении, большинство участников ответило утвердительно. Многие участники считают, что персональные данные попадают третьим лицам или в руки спецслужб Казахстана и стран, где размещены интернет компании.

«Нас даже на работе предупреждают: комментарии не приводить, потому что все прослушивается и записывается, а вы педагоги и вы обязаны ничего лишнего не говорить, о какой-то политике или еще что-то». (Женщина, 42 года, Актобе)

В целом лишь небольшая часть участников ФГД чувствует, что контролирует свои персональные данные, предоставленные онлайн, - могут изменять их или удалять. Подавляющее большинство считает, что введенные однажды данные уже нельзя никогда стереть или изменить, что все введенные данные остаются на серверах навсегда, даже если пользователь прибегает к процедуре корректировки или удаления своих персональных данных.

Следует отметить, что отсутствие ощущения полного контроля над своими персональными данными не порождает чувство беспокойства или тревоги. Участники ФГД воспринимают отсутствие контроля как данность, как правила игры, которые приходится принимать. Респонденты выражали большие сомнения по поводу возможности контролировать интернет компании и гарантировать, что персональные данные действительно удаляются по запросу их субъекта.

«...Я тоже считаю, что есть более интересные люди, чем я. Я не знаю, кому будут нужны мои данные». (Мужчина, 43 года, Астана)

«...Кому мои данные нужны?! В принципе, если даже мои данные продадут, и что толку от этого? Работаю в бюджетной организации, и я не думаю, что там счета у меня какие-то, чем я могу быть интересна для этих людей. И что, если у них мои данные? Что они им дадут?» (Женщина, 40 лет, Астана)

По мнению многих участников, **беспокоиться стоит только в тех случаях, когда речь идет о данных, утечка которых может напрямую привести к потере денег или имущества**. Это, прежде всего, данные банковского счета, кредитной карты, данные документов, удостоверяющих личность.

«...Если честно, я не беспокоюсь. Если где-то будут данные личного характера, то я не переживаю. Я переживаю за данные своих банковских карт, за свои личные данные, ИИН, например, или еще что-нибудь, или какое у меня имущество движимое, недвижимое. А то, что касается данных в социальных сетях моих, мне не важно». (Мужчина, 29 лет, Астана)

Восприятие сложившейся системы сбора, хранения и использования персональных данных, предоставленных онлайн, иногда бывает **связано с верой в идеи теории заговора**. Так, к примеру, некоторые участники считают, что социальные сети были изобретены для того, чтобы легальным путем собирать информацию о гражданах иностранных государств. Некоторые убеждены, что казахстанские спецслужбы имеют доступ к персональным данным, которые казахстанцы предоставляют онлайн, могут просматривать контент электронных писем и сообщений в мессенджерах.

ЗНАНИЕ ПРАВ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Проведенные ФГД продемонстрировали очень низкий уровень знаний участников о правах субъекта персональных данных – ни один из них не смог сказать, что знает свои права. Никто не знал определенно, какие законы в Казахстане определяют персональные данные и их защиту, регулируют отношения в этой сфере, хотя почти все полагали, что такой закон в стране должен быть.

«...Права? У нас есть конституция, там все написано, но ничего у нас не работает. Это мое глубокое убеждение. Не поддаётся объяснению». (Мужчина, 43 года, Астана)

«...Да даже если ты там проходил в школе или в университете [Основы права], толку нет от этого. Человек вышел на митинг, и его просто взяли закрыли на 3-4 суток, и сказали еще раз выйдешь – тебе конец. Хотя говорят, там в конституции свобода слова, мы все свободные, никаких прав нет у нас». (Мужчина, 30 лет, Актобе)

Некоторые респонденты могли только рассуждать на эту тему, и смогли своими словами описать какие права, по их мнению, должны быть закреплены законом. В таких случаях респонденты смогли назвать одно-два права; они описывали их как «право на тайну персональных данных», «право не предоставлять свои персональные данные».

Участники ФГД были также плохо осведомлены о том, в какие государственные органы следует обращаться по вопросам персональных данных и их защиты. Поскольку почти никто не был абсолютно уверен в этом вопросе, люди высказывали свои предположения: полиция (Министерство внутренних дел), Комитет национальной безопасности (КНБ), Прокуратура, суды, Министерство юстиции, Министерство информационных технологий, и даже фискальные органы.

Интересно то, что довольно часто в этом контексте респонденты называли Комитет национальной безопасности. В таких случаях участники приводили разные объяснения своему предположению. Например, одни считали, что полиция не обладает достаточным уровнем компетентности, чтобы раскрывать подобные преступления, а в КНБ есть компетентные специальные подразделения. Другие полагали, что поскольку Комитет национальной безопасности уже занимается мониторингом активности граждан страны в интернете, то, соответственно, этот орган и должен рассматривать подобные обращения. Третьи думали, что вопросы защиты персональных данных относятся к сфере национальной безопасности в целом, поэтому обращаться нужно в КНБ.

«КНБ. Национальная безопасность превыше всего, со стороны КНБ должен быть контроль соцсетей. Ну, почему они запрашивают данные, например? Какое они имеют право? Они, наверно, тоже должны брать какое-то разрешение у правоохранительных органов, чтобы нашу информацию обрабатывали». (Женщина, 30 лет, Астана)

В то же время, важно отметить, многие респонденты выразили большие сомнения в том, что обращение в государственные органы по вопросам защиты персональных данных будет иметь положительный для обратившегося исход.

Такое мнение респонденты объясняли низким уровнем доверия правоохранительным органам, в особенности полиции и суду, и подкрепляли свои слова примерами из своего опыта или опыта близких.

«Мне кажется, если проблема возникнет, никто не возьмет на себя никакую ответственность, будет отнекиваться и скажет просто «твои проблемы, решай сам», и никто не будет тебя защищать».
(Женщина, 25 лет, Актобе)

«Мое мнение, что все-таки не вводить лишнего, ты если не введешь, ничего лишнего с тобой не случится. Не включил геоданные, не показал, где ты, и никто с тобой ничего не сделает». (Женщина, 25 лет, Актобе)

Следующей темой, которую обсуждали в группах, была ответственность сторон – интернет компаний, пользователей их услуг и государственных органов. Данная тема обсуждалась с целью лучше понять представления участников о правах и обязанностях трех названных сторон.

Многие участники обнаруживали склонность не доверять интернет-компаниям, считая, что те ради прибыли могут пойти на любые действия, даже на нарушение соглашений и законов. Другие считают, что в первую очередь ответственность несет сам пользователь, он должен осознавать риски: представив свои персональные данные в интернете, не стоит рассчитывать на соблюдение их тайны и сохранности.

Поэтому, как полагали многие, государство должно строго контролировать деятельность частных компаний. Некоторые участники в своих суждениях доходили до необходимости лицензирования деятельности интернет компаний, а когда понимали, что мировые гиганты не пойдут на это ради небольшого казахстанского рынка, то были готовы отказаться от их услуг и согласиться в качестве альтернативы перейти на местные сервисы, которые можно было создать.

В ходе таких рассуждений некоторые из тех участников одобрительно привели примеры Китая и России, где государство пытается максимально строго регулировать интернет и стимулирует создание своих мессенджеров и социальных сетей как альтернативу Facebook, WhatsApp и Instagram.

В этих разных позициях угадывается одна общая черта – участники ФГД склонны не доверять интернет компаниям, не верят в соблюдение ими тайны персональных данных, и самое главное – не верят в соблюдение законности в сети интернет. Обратной стороной таких представлений является склонность

возлагать широкие полномочия на государственный аппарат – государство должно следить за сетью, оно должно быть гарантом сохранности персональных данных.

ОТНОШЕНИЕ К РОЛИ И КОМПЕТЕНЦИИ ГОСУДАРСТВЕННЫХ ОРГАНОВ

Обсуждение этой темы началось с вопросов о доверии Центрам обслуживания населения (ЦОНЫ). Ожидалось, что данная тема актуальна в обществе после громкого скандала, связанного с историей самовольной выдачи сотрудником ЦОНа города Алматы справки третьему лицу без разрешения со стороны субъекта данных. Хотя услуги ЦОНов безальтернативны, и у граждан нет выбора, тем не менее, было интересно узнать, насколько доверяют этой государственной структуре и каковы суждения граждан на этот счет.

Мнения участников ФГД на этот счет разделялись: многие заявляли о полном доверии ЦОНам, другие придерживались противоположного мнения. Те, кто доверяет, считают, что скандальная история произошла по причине так называемого «человеческого фактора» - недобросовестности одного сотрудника, и винить за это всю систему ЦОНов нельзя. В свою очередь, их оппоненты не доверяют ЦОНам вследствие множества примеров доступности персональных данных третьим лицам без соответствующего согласия субъекта этих данных.

«По секрету скажу, в ЦОНе все продается, мой братишка [там] работает. У него спроси, он на следующий день скажет тебе: вот тот там работает...» (Мужчина, 40 лет, Актобе)

«Давайте начнем с того, что у нас в свободном доступе есть база статистики, база пенсионеров, база недвижимости. В свободном доступе, потому что за небольшие деньги, так скажем за 20,000 – 30,000 тенге, это все можно приобрести у сотрудников, которые работают в государственном учреждении. Ну, нелегально. Как я могу доверять всей системе, если я знаю, если были случаи при мне, что люди торгуют базами [данных] там, где они работают». (Мужчина, 43 года, Усть-Каменогорск)

«Я раньше думал персональные данные никуда не передают, а оказывается, передают. Случай был такой, одна компания в Астане занимается интернет площадкой. Человек там работал, и он говорит, у нас там сейчас появилась база на почти 4 млн человек, и он мне просто сказал, что эту базу купили у «КазПочты». Просто к шефу подошли, и столько денег, и нам нужны контакты, и они просто нам слили 4 млн

анкет. После этого я уже не доверяю ни «КазПочте», ни налоговой».
(Мужчина, 30 лет, Актобе)

Можно сказать, что в обсуждении работы ЦОНов в очередной раз проявилась склонность многих участников всецело доверять государственным органам, даже несмотря на приводимые оппонентами примеры коррупции, халатности или недобросовестности.

Обсуждение ЦОНов переходило к теме **доверия государственным органам, их роли и пределов их компетенции в вопросах персональных данных**. Здесь группы делились на тех, кто полностью доверяет, и тех, кто не доверяет государственным органам.

Первые поддерживают идею наделения силовых структур очень широкими полномочиями. Такую позицию они объясняют страхом перед террористическими организациями, организациями радикальных течений ислама. Они считают, что силовые структуры должны иметь свободный доступ к персональным данным граждан страны, чтобы лучше справляться с подобными угрозами.

«Ну, знают и пусть знают. Ничего страшного, криминального, ничего такого нет». (Женщина, 40 лет, Усть-Каменогорск)

Часто можно было слышать, что ради безопасности своих детей, семьи, люди готовы закрыть глаза на то, что силовые структуры имеют возможность читать личную переписку, слушать разговоры и т. д. Интересно, что во всех группах назывались одни и те же источники угрозы: ваххабиты, террористы, «Синий кит». Последний представляет собой мифическую игру (ее реальное существование не доказано), в которой якобы подростков доводят до суицида.

«Про WhatsApp просто слышала, что будут просматривать, прослушивать. Это в целях того, что налеты эти тогда начались. Может, оно и правильно. Те же дети. Раз и звонок мне поступил: ваш ребенок интересуется... Я потом только спасибо сказала бы». (Женщина, 44 года, Актобе)

Их оппоненты не считают, что борьба с терроризмом оправдывает нарушение права на неприкосновенность частной жизни. Более того, многие участники из этого лагеря были убеждены, что названные угрозы преувеличены именно для того, чтобы оправдать противоправные действия спецслужб.

«...Не совсем доверяю. Можно сказать, не доверяю. У нас есть одноклассник, который работает в Астане в КНБ, и вот он один раз

написал нам, что он обо всех все знает. Он с одной девушкой дружил и про нее все знает. Знает, что она выезжает за рубеж в год 3-4 раза в Эмираты и Турцию. И обо мне писал, было кое-что в моей жизни, и он знает про это. Как он знает? Получается, он КНБ-шник, и ему интересно стало, кто есть кто, кто где живет, и сколько квартир, открыл и посмотрел. Так получается?» (Женщина, 41 год, Усть-Каменогорск)

Для того, чтобы дискуссия была предметной участникам предлагалось выразить свое мнение по поводу инициативы правительства внедрения **«сертификата безопасности»**, который тестировался летом 2019 года в Астане. Хотя многие не были осведомлены об этой инициативе, краткого ее описания было достаточно, чтобы люди могли высказать свои общие суждения.

Отношение к этой инициативе было таким же, как и в других вопросах, касающихся пределов компетенции государственных органов, группы делились на два лагеря: сторонников и противников. Первые склонны доверять государству, даже жертвуя правом на неприкосновенность частной жизни. И аргументы первых можно свести к двум основным суждениям:

- **ради безопасности перед угрозой терроризма можно жертвовать своим правом на неприкосновенность частной жизни,**
- **законопослушным гражданам нечего скрывать, они не представляют интереса для спецслужб.**

«Я боюсь за своего ребенка. Так что, может, я и согласилась бы ради безопасности ребенка. Я боюсь этих ваххабитов». (Женщина, 44 года, Актобе)

«Это было на государственном уровне, что именно по WhatsApp и в Telegram будет все просматриваться и прослушиваться в связи с терроризмом, именно для пресечения терроризма. Государство объясняет тем, что у нас были теракты в Актюбинской области, и, в связи с этим наша вся переписка будет контролироваться органом КНБ. Это было официально. Я к этому отношусь положительно, потому что я считаю, что чем потом лечить, лучше предупредить». (Женщина, 43 года, Астана)

«А наши государственные органы пусть читают. И кто чист, чего им бояться? А те, кто бандиты... Ну, если они [данные] не разглашаются, и чисто для безопасности, пусть читают». (Женщина, 30 лет, Астана)

Отдельно следует отметить тех, кто считает, что от мнения граждан ничего не зависит, и если власти твердо решат внедрить «сертификат безопасности», то тем или иным способом вынудят граждан установить его.

«Нас заставят все равно. Будут без конца говорить, сделайте, сделайте, зарегистрируйтесь, скачайте себе это. Нас заставят, и поэтому здесь мы как все, если все пошли туда, и нам нужно идти. А от того, что я буду упираться, говорить нет, мне скажут надо. Значит я буду скачивать».
(Женщина, 40 лет, Астана)

Другие не согласны устанавливать «сертификат безопасности», расценивая это как вторжение в частную жизнь граждан, на которое государство идет в политических целях – предупреждать угрозы политическому режиму, наказывать за инакомыслие. Также были и те, кто просто не верит, что государственные органы смогут гарантировать сохранность персональных данных.

«Если они [спецслужбы, КНБ] хотели бы задавить этих ваххабитов, это было бы сделано за неделю. Вот здесь пацанов [имеет в виду вооруженное нападение на магазины и войсковую часть в Актобе летом 2016 года, которое власти страны классифицировали как террористический акт] послали грабить преднамеренно. А ты говоришь ваххабиты! Их настроили, вырастили, выпустили для того, чтобы тебе сказать: сертификат [безопасности] нужен. Ты же раньше без него существовала». (Мужчина, 45 лет, Актобе)

«Нет, никогда бы не установил, и вообще считаю, что это полное беззаконие со стороны государства. То есть ты даешь им право доступа. Получается государство будет посредником между мной и провайдерам, т. е. они будут хранить все мои персональные данные. У меня в телефоне стоит два интернет банкинга, и они в любой момент будут знать мои пароли, и могут слить. Если я буду использовать этот сертификат, я не буду уверен, и интернет банкингом пользоваться нельзя, все. Не то, что переписка или прослушка, мне нечего бояться прослушки, но я боюсь доступа к своим карточкам и своим счетам». (Мужчина, 41 год, Астана)

«Сертификат ставить незаконно, это, во-первых. А во-вторых, у нас бы по умолчанию поставили и дальше бы пользовались, ничего страшного на самом деле бы не произошло. Единственное - теперь КГБ читали бы нашу переписку в WhatsApp и все. Честно, у меня стойкое впечатление, что лет через 5 мы все будем иметь чипы, по которым все будут знать, где

мы находимся, что в данный момент мы делаем». (Мужчина, 41 год, Усть-Каменогорск)

«Если нам каждому, извиняюсь за выражение, по чипу воткнут, 90% промолчат». (Мужчина, 41 год, Усть-Каменогорск)

«Я не слышал, но скорее всего слежка». (Мужчина, 30 лет, Актобе)

«Чтобы им облегчить работу, нас найти легче. То же самое, как была недавно привязка телефонов к SIM карте. Аккаунты все покажите! Они хотят ничего не делать и владеть информацией, чтобы мы сами им все скидывали». (Мужчина, 28 лет, Актобе)

Следует отметить, что многие участники не были готовы выносить суждения в этом вопросе, отвечали уклончиво или быстро меняли мнение. Так, в начале обсуждения темы пределов компетенции государственных органов по численности преобладали те, кто был за наделение государственных органов и спецслужб, в частности, самыми широкими полномочиями. Но после дискуссии о «сертификате безопасности», сильные аргументы противников этой инициативы, приводили к тому, что некоторые меняли свое мнение и соглашались с мнением последних.

Данное наблюдение говорит о том, что сейчас мнение общества по таким специфическим вопросам, как «сертификат безопасности» и пределы компетенции государственных органов в доступе к цифровым персональным данным еще далеко не сформировано. То есть **в обществе есть потребность в информировании, образовании в этих вопросах.**

Выводы и рекомендации

На протяжении последних шести лет Казахстан достиг заметного прогресса в понимании, выявлении и решении проблем, связанных с использованием кибертехнологий в киберпространстве. Это во многом нашло свое отражение в позиции РК в глобальном индексе кибербезопасности (см. таблицу ниже).

	Индекс свободы человека	Индекс свободы интернета	Индекс свободы прессы	Индекс кибербезопасности	Индекс конфиденциальности в интернете
Казахстан	6.74	32/100	158	40	95/106

Вместе с тем, помимо важных инициатив и реализованных мер перед правительством и обществом Казахстана стоит много задач, чтобы быть готовыми максимально быстро восстанавливаться после кибератак, поскольку предотвратить их не представляется возможным, а значит развивать культуру защиты персональных данных и не нарушать основные права и свободы человека в онлайн и оффлайн мирах. Как говорится, предупрежден значит вооружен.

Если сформулировать **основные проблемные моменты, связанные с защитой персональных данных в Казахстане** на основе проведенного анализа, то их кратко можно представить следующим образом (см. таблицу SWOT-анализа ниже по тексту):

(1) **Инициатива проявлена, пора брать ответственность и делать системные вещи.** Отрадно, что Комитет информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан предложил свою кандидатуру в качестве Data Protection Agency (опыт ЕС и европейских стран). В разных странах мира этими вопросами занимаются различные ведомства – в Бангладеш эти вопросы курирует национальный CERT, в Чехии было создано специализированное министерство, которое впоследствии стало кузницей нынешних кибердипломатов⁴⁸. Учитывая срочность поставленных задач и важность быстрых результатов, цели, обозначенные Комитетом на своем сайте, не отражают в должной мере работу главного ведомства страны по защите персональных данных, потому что в основном зациклены на технологических решениях. Было бы интересно посмотреть, как и кому профильный комитет будет предоставлять разъяснения по вопросам защиты данных, насколько открытым будет этот орган.

⁴⁸ Эксперт по кибербезопасности является частью дипломатической миссии за рубежом.

(2) **Закон принят, нужно чтобы он заработал.** Опять же, согласно данным Комитета по информационной безопасности, осуществление контроля за применением законов о защите персональных данных и контроль за соблюдением требований по защите персональных данных станут главными звеньями работы по защите персональных данных.

Однако, карательная практика не позволит решить системные проблемы, а только будет откладывать решение наиболее важных проблем на более поздний срок, в т. ч. обучение кадров, создание правовой и информационной культуры, прежде всего, у себя дома (т.е. во всем государственном аппарате). Впрочем, как и увольнение не может оставаться способом наказания за нарушение законодательства, потому что оно определяет четкие механизмы привлечения к ответственности. При этом поскольку персональные данные подлежат защите и ее гарантом выступает государство, это означает, что все стейкхолдеры без исключения должны соответствовать выработанным техническим и юридическим параметрам.

SWOT-анализ защиты персональных данных Казахстана

	Helpful <i>to Achieving the Objective</i>	Harmful <i>to Achieving the Objective</i>
Internal Origin <i>(attributes of the organization)</i>	S Законодательство Профильное ведомство (ответственность)	W Отсутствие доверия со стороны общества Вера в теорию заговора Авторитарная коррупционная элита Отсутствие правовой культуры и кибергигиены
External Origin <i>(attributes to the environment)</i>	O Технологии Сотрудничество и обмен опытом с Евросоюзом Усиление демократических сил и продвижение ценностей открытого цифрового общества	T Использование технологий для усиления авторитаризм, цензуры и тотальной слежки Сотрудничество и обмен опытом с Китаем и Россией

(3) **Крайне важно понимать концептуальное различие между информационной и кибербезопасностью.** Разведение понятий «информационная безопасность, как защита массового и индивидуального сознания от деструктивного контента» и «кибербезопасность» не позволяет

адекватно оценивать слабые и сильные стороны нетехнологических решений. Эта же логика работает в отношении защиты персональных данных и их конфиденциальности. С технологической точки зрения достижение первого потребует меньшего времени и ресурсов, потому как по второму важно поощрение и продвижение культуры цифровых прав как своего рода вакцинация всего общества и выработка иммунитета к киберпреступлениям. Именно этот компонент существенно провисает на данный момент, и остается не до конца понятным, будет ли Комитет по информационной безопасности заниматься этими вопросами или же это будет кто-то другой. Сейчас эту функцию частично выполняют платные сервисы VPN.

Очевидно, активное участие КНБ РК в выстраивании эффективной системы обеспечения кибербезопасности страны во многом объясняется угрозами национальной безопасности. Однако если мы говорим о приватности и конфиденциальности данных, т. е. правовой компонент цифровой культуры, то хотелось бы действительно использовать опыт передовых стран в этом вопросе. В идеальном варианте функционирование такой системы обеспечивается не только структурами, созданными в рамках силовых ведомств, но и предполагает включенность элементов государственно-частного партнерства, бизнес среды и гражданского общества. Успешное сотрудничество ЦАРКА с различными государственными ведомствами только способствует повышению киберустойчивости экосистемы. Важно привлекать и развивать альтернативные, свежие идеи и видение.

(4) ***На двух стульях не усидишь, а полумером быть не получится.*** С одной стороны, ожидается, что система защиты персональных данных в Казахстане будет дополнена в соответствии с европейским GDPR, а с другой, сочетает в себе элементы российской и китайской концепций - «суверенный интернет», «великий файрволл», цензура и пр.

В условиях, когда общество достаточно глубоко верит в теории заговоров и объясняет происходящее слежкой и прослушкой силовых структур, что подтверждается результатами онлайн опроса и фокус групп, сложно говорить о цифровых правах и защите личных данных. Граждане используют VPN-сервисы, чтобы обеспечить конфиденциальность своих данных не ради защиты персональных данных от кибермошенников, а по сути, от государства.

В этой связи особую актуальность обретает усиление сотрудничества и взаимодействия с европейскими партнерами в рамках Соглашения о расширенном партнерстве и Новой стратегии ЕС в Центральной Азии. Усиление сотрудничества с Польшей и Эстонией, в частности, позволит адекватным

образом усилить уже имеющийся потенциал. С другой стороны, прозрачность и подотчетность в работе с китайскими технологиями требует особого внимания.

(5) ***Награды и наказания создают основу для контроля за состоянием войск, но необходимо прилагать все усилия для поощрения желания сражаться и самоотдачи***⁴⁹. Как показали результаты опроса общественного мнения, казахстанцы практически ничего не знают о защите персональных данных, почему это важно и что для это нужно делать, цифровых правах, а также о роли и функциях государственных органов в этих вопросах.

Невозможно обеспечить информационную и кибербезопасность, если львиная доля граждан не знает о важности защиты персональных данных и кибергигиене. Для создания устойчивой экосистемы правительству крайне важно уделять внимание повышению уровня осведомленности и знаний граждан в сфере цифровых прав и защиты персональных данных.

Если у государства не хватает ресурсов или по любым другим причинам оно не выступает в качестве авторитетного игрока или честного брокера, то в решении подобных задач призваны помочь институты гражданского общества, в частности НПО и исследовательские группы/центры. К примеру, в Бразилии вопросами защиты персональных данных, адвокацией и продвижением цифровой повестки активно занимается исследовательский центр университета Сан Паулу, труды которого активно используются государственными органами.

В этом направлении важно наращивать потенциал казахстанских правозащитных организаций и исследователей, а также их сотрудничество с партнерскими институтами, в частности белорусской организацией Human Constanta, имеющий огромный опыт работы в этом направлении. Киберграмотность и кибергигиена должны стать неотъемлемой частью кампании по продвижению культуры защиты персональных данных в Казахстане.

⁴⁹ Сунь Цзы «Искусство войны».