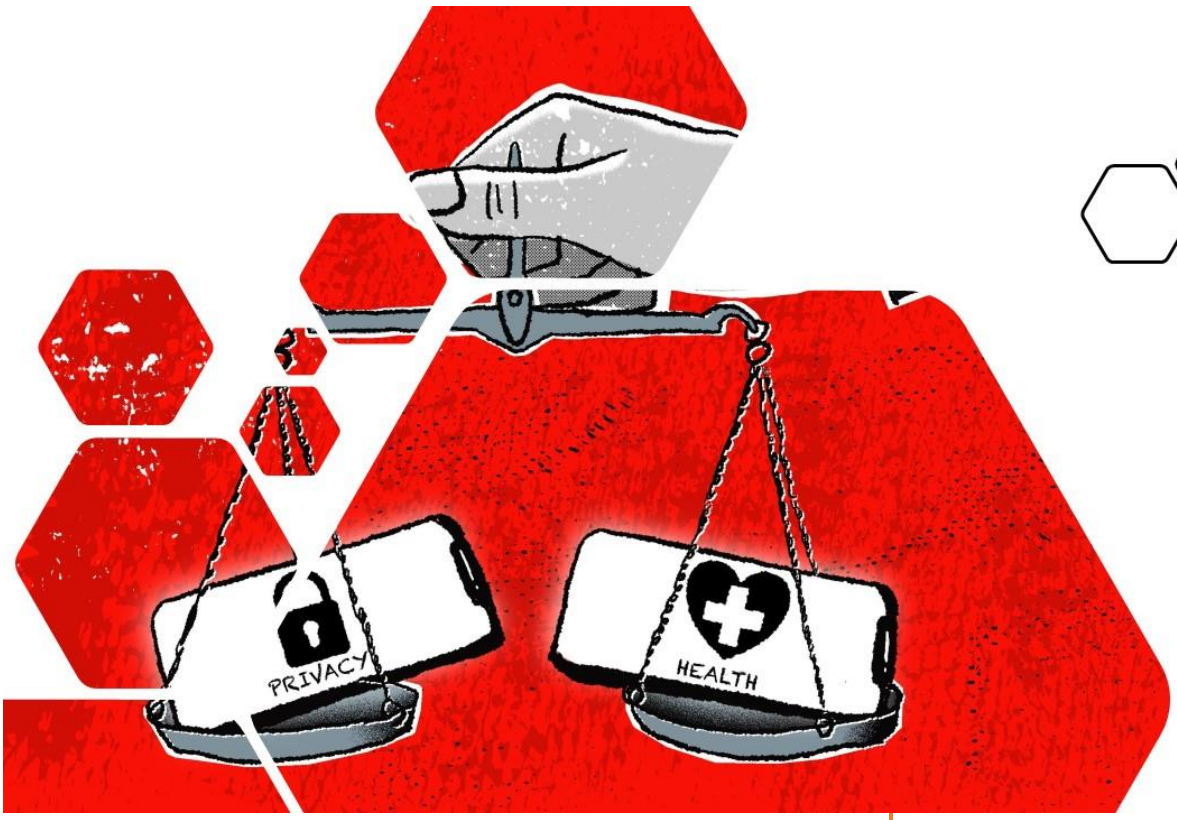
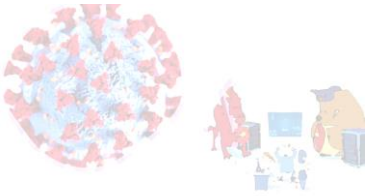


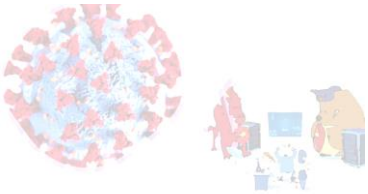
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В КАЗАХСТАНЕ 2.0: ЦИФРОВОЙ СЛЕД COVID-19

Анна Гусарова
Серик Джаксылыков
2021

Проект реализован при финансовой поддержке Фонда Сорос-Казахстан. Точка зрения авторов, отраженная в данном исследовании, может не совпадать с точкой зрения Фонда Сорос-Казахстан. Ответственность за факты, сведения, суждения и выводы, содержащиеся в публикации, несут авторы.



Содержание



Глоссарий

AT&T – американская многонациональная холдинговая компания, крупнейшая в мире телекоммуникационная компания, крупнейший поставщик услуг мобильной связи и крупнейший провайдер услуг фиксированной телефонной связи в Соединенных Штатах через AT&T Communications.

CATI (Computer Assisted Telephone Interview) - компьютерная система для проведения телефонных опросов, позволяющая организовать «безбумажную» технологию опроса (тексты вопросов появляются на экране оператора).

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.

COVID-19 – коронавирусная инфекция, заболевание, вызванное тяжелым острым респираторным синдромом коронавирусом 2 (SARS-CoV-2).

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

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

NHS (National Health Service) – Национальная служба здравоохранения Великобритании

QR-код (Quick Response Code) – код быстрого реагирования

SARS (Severe Acute Respiratory Syndrome) – тяжелый острый респираторный синдром, атипичная пневмония (2002-2004 годы)

SPSS (Statistical Package for the Social Sciences*)* — компьютерная программа для статистической обработки данных, предназначена для проведения прикладных исследований в общественных науках.

Биометрические данные - персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность.

ВОЗ – Всемирная организация здравоохранения

ИКТ – информационно-коммуникационные технологии

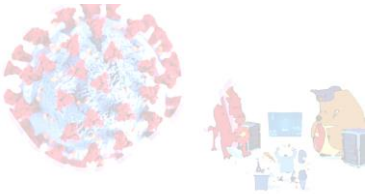
ИИ – искусственный интеллект

КНБ – Комитет национальной безопасности Республики Казахстан

ПИ – персональная информация

ПЦР - полимеразная цепная реакция (метод теста на COVID-19)

США – Соединенные Штаты Америки



Терминология[1]

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 факторы[2]. 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.

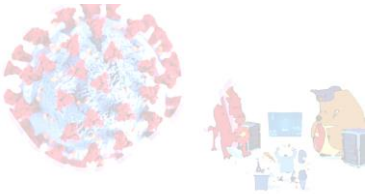
Если вы не можете напрямую идентифицировать человека по этой информации, тогда следует подумать, можно ли его идентифицировать. Необходимо принять во внимание информацию, которую вы обрабатываете, вместе со всеми средствами, которые могут быть использованы вами или любым другим лицом для идентификации 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.

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.

[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/.



Введение

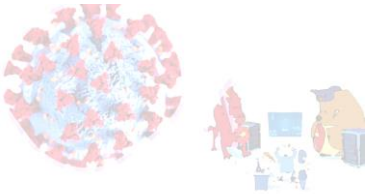
В Казахстане вопросы и проблемы, связанные с защитой персональных данных, обретают все большую актуальность особенно в условиях противодействия пандемии COVID-19. С одной стороны, несмотря на наличие Закона о персональных данных, многие его элементы на практике пробуксовывают, а также отсутствует стратегическое видение движения в сторону принятия ключевых принципов европейского Общего регламента по защите данных GDPR.

С другой недавние кейсы о масштабных утечках персональных данных казахстанцев 2019 года из государственных баз данных ставят под сомнение возможность и обязательство государства защищать персональные данные в соответствии с Законом о персональных данных, ст.20 п.1[3]. Вместе с тем результаты проведенного в 2019 году исследования о персональных данных в Казахстане свидетельствуют о ***критической необходимости повышения осведомленности и понимания важности продвижения культуры защиты персональных данных среди казахстанцев для выстраивания общенациональной системы кибербезопасности и киберустойчивости***.

Сегодня в условиях масштабного внедрения технологий по распознаванию лиц, алгоритмов искусственного интеллекта и сбора отпечатков пальцев казахстанцев в предстоящие годы, с одной стороны, и реализацию амбициозных задач в рамках государственной программы «Цифровой Казахстан» с целью обеспечения национальной безопасности и создания информационного общества, с другой, важно обеспечивать безопасный сбор, обработку и хранение персональных данных в соответствии с принципами GDPR.

Более того, важность и необходимость масштабной цифровизации должна сопровождаться соблюдением основных прав и свобод в онлайн и офлайн среде, избегая манипуляций с технологиями с целью цифровой слежки за гражданами (особенно активистами) и чрезмерного сбора персональных данных в момент чрезвычайной ситуации и карантина в связи с COVID-2019. В этой связи представляется важным понимать, как казахстанцы относятся к подобным непропорциональным мерам борьбы с пандемией со стороны государства, как они сказываются на ценности персональных данных и их защите, а также каким образом текущая и ожидаемая государственная политика может быть улучшена с точки зрения продвижения культуры защиты персональных данных в Казахстане.

[3] Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 03.07.2020 г.), Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 03.07.2020 г.) - ПАРАГРАФ-WWW (zakon.kz).



1. Защита персональных данных: цифровые последствия COVID-19

Пандемия COVID-19 превратилась в глобальную чрезвычайную ситуацию с разрушительными последствиями в виде человеческих жертв и экономического спада. D В Казахстане и Центральной Азии быстрое распространение COVID-19 в 2020 году спровоцировало политических лидеров объявить о чрезвычайных ситуациях в национальном масштабе, быстро перейдя к политике сдерживания и смягчения последствий. Были приняты жесткие меры: введение карантина, комендантского часа и других ограничений (медицинских, транспортных, физических, правовых и иных) как в масштабах страны, так и на местах, хотя поначалу реакция правительства была неохотной[4].

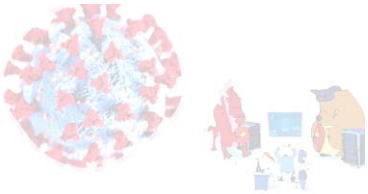
Важной задачей остается остановить распространение болезни и сдерживать ситуацию, чтобы не повторить весенне-летнего «пожарного» распространения коронавируса в огромных масштабах. Нынешняя ситуация в государствах Центральной Азии во многих отношениях аналогична ситуации во многих других странах мира - их будущее неясно. Однако в некоторых других отношениях проблемы, стоящие перед государствами Центральной Азии, уникальны и требуют мер, направленных на устранение долгосрочных последствий COVID-19 с учетом конкретной ситуации в регионе.

Однако помимо этих, казалось бы, очевидных и ожидаемых последствий COVID-19 мир увидел новые масштабы применения цифровых технологий для обеспечения безопасности посредством контроля медицинской ситуации с одной стороны, а с другой – нарушения прав и свобод человека. Хотя приверженность соблюдению стандартов в области прав человека на протяжении нескольких лет все больше ослабевает во всем мире, пандемия COVID-19 ускорила эрозию демократического и свободного общества, от которого в итоге зависит защита прав человека. Пандемия перевернула нашу жизнь так же, как 11 сентября 2001 года и финансовый кризис 2008 года, а скорее всего, даже больше. Коронавирус предоставил многим правительствам идеальный предлог для использования страхов и подавления инакомыслия, ограничения прав людей и принятия законодательства в условиях чрезвычайно ситуации, который может иметь долгосрочные последствия, помимо кризиса в области здравоохранения[5].

Растущее количество кейсов демонстрирует, что сбор, использование и дальнейшая обработка данных может помочь ограничить распространение вируса и ускорить восстановление, особенно с помощью цифрового отслеживания контактов. Данные о мобильности, полученные в результате использования людьми мобильных телефонов, электронной почты, банковских операций, социальных сетей, почтовых служб, например, могут помочь в отслеживании распространения вируса и поддерживать осуществление

[4] Gregory Gleason, Anna Gussarova, "COVID-19'S LONG-TERM IMPLICATIONS FOR CENTRAL EURASIA," *Diplomatic Courier*, May 6, 2020, COVID-19's Long-Term Implications for Central Eurasia (diplomaticourier.com).

[5] "*The impact of COVID-19 on human rights and how to move forward*," Council of Europe, December 10, 2020, The impact of COVID-19 on human rights and how to move forward - View (coe.int).



деятельности институтов власти, финансовых учреждений, международных организаций[6]. Такой сбор и обработка данных, в том числе для цифрового отслеживания контактов и общего наблюдения за состоянием здоровья, может включать сбор огромных объемов личных и неличных конфиденциальных данных. Это может иметь значительные последствия за пределами начальной фазы реагирования на кризис, в том числе, если такие меры будут применяться в целях, прямо или абстрактно не связанных с реагированием на COVID-19, что может привести к нарушению основных прав и свобод человека[7]. Это беспокойство особенно актуально, если некоторые чрезвычайные меры, принятые для борьбы с пандемией, такие как цифровое отслеживание контактов, со временем превращаются в стандартную практику.

1.1. Основные тенденции

Наиболее серьезные нарушения приватности происходят на макроуровне, поскольку правительства и бизнес объединяют свои усилия с целью отслеживания и остановки распространения вируса. ***Китай***, например, заблокировал более 500 миллионов в основном здоровых людей, чтобы держать под контролем COVID-19; в стране используются беспилотные летательные аппараты для сканирования массового скопления людей и обнаружения заболевших. Китайское государственное телевидение также отмечало, что людям на изоляции в Шанхае прикрепляли цифровые устройства наблюдения к дверям их домов[8].

Другой пример - поисковая компания Baidu, которая разработала для полиции Пекинского метро алгоритм, позволяющий быстро выявлять пассажиров без масок. Платформа онлайн-консультаций для врачей Baidu обработала более 15 миллионов запросов и собрала более 100 000 врачей, ответивших на вопросы. Китайский закон, похоже, не ограничивает то, что Baidu может делать с этой медицинской информацией о своих пользователях[9]. Крупнейшая в мире компания электронной коммерции, Alibaba, запустила службу доставки лекарств для лечения людей с хроническими заболеваниями, чтобы облегчить больницы, загруженные пациентами с COVID-19. Получается, что Alibaba переносит информацию о здоровье пациентов из больницы в обширную базу данных, которая также отслеживает их покупки в интернете. Другая компания Tencent, оператор WeChat, запустила чат-бот людям, которым нужен базовый диагноз, и бесплатные онлайн-консультации по вопросам здоровья (неизвестно, какие персональные данные собираются и обрабатываются в ходе этого)[10].

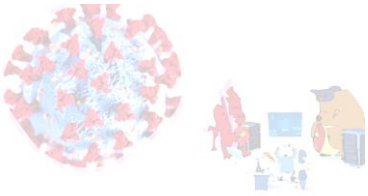
[6] WHO issued "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing." More information can be found at https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1.

[7] Joint Statement on Data Protection and Privacy in the COVID-19 Response, World Health Organisation, November 19, 2020, Joint Statement on Data Protection and Privacy in the COVID-19 Response (who.int).

[8] Theodore Claypoole, "COVID-19 and Data Privacy: Health vs. Privacy," *Business Law Today*, March 26, 2020, COVID-19 and Data Privacy: Health vs. Privacy | Business Law Today from ABA.

[9] Ibid.

[10] Arjun Kharpal, "China's giants from Alibaba to Tencent ramp up health tech efforts to battle coronavirus, *CNBC*, March 3, 2020, Coronavirus: China's Alibaba, Tencent, Baidu boost health tech efforts (cnbc.com).



Считается, что ***Южная Корея*** лучше многих государств справляется со сдерживанием вируса: правительство использовало беспилотные летательные аппараты для распыления дезинфицирующих средств и тепловые очки, которые считывали температуру людей на расстоянии. Южная Корея также «развернула приложение для отслеживания «Self-Quarantine Safety Protection[11], чтобы следить за цифровыми технологиями порядка 30 тысяч человек, находящимся дома на карантине в течение двух недель». Если человек выносит свой телефон за пределы разрешенной зоны, ему и сотруднику государственного отдела передается мобильное оповещение. Страна также работала с промышленностью над внедрением системы распознавания лиц на основе мобильных приложений, которая позволяет медицинским работникам и другим лицам быстро определять имена пациентов[12]. Кроме того, секретность, религиозные обычаи и требования к сканированию отпечатков пальцев[13] южнокорейской секты попали под пристальное международное внимание[14], когда большое количество ее членов заполнили статистику страны по COVID-19.

Израиль отдал приказ оставаться дома всем гражданам и использовало инструмент отслеживания за мобильными телефонами[15], который ранее применялся правительством исключительно для борьбы с терроризмом[16]. Этот инструмент регистрирует движение мобильных телефонов, чтобы правительство могло определить, игнорируются ли его приказы, и отслеживать действия граждан. Оппозиционные политики раскритиковали мониторинг мобильных телефонов как посягательство на частную жизнь израильтян. Известная компания SuperCom со штаб-квартирой в Израиле рассматривает пандемию COVID-19 как способ продать свою биометрическую систему мониторинга инфицированного населения. Это решение включает в себя водонепроницаемый гипоаллергенный браслет на щиколотку с Bluetooth, смартфон и программное обеспечение SAAS в облаке, но также может быть настроен, например, для мониторинга только со смартфона. SuperCom также заявляла, что уже ведет переговоры с рядом государственных организаций о глобальном развертывании этой технологии[17].

[11] Timothy W.Martin, "Fever-Detecting Goggles and Disinfectant Drones: Countries Turn to Tech to Fight Coronavirus," *The Wall Street Journal*, March 10, 2020, Fever-Detecting Goggles and Disinfectant Drones: Countries Turn to Tech to Fight Coronavirus - WSJ.

[12] Sohn Ji-young, "New mobile facial identification system unveiled in Korea," *The Korea Herald*, November 23, 2016, New mobile facial identification system unveiled in Korea (koreaherald.com).

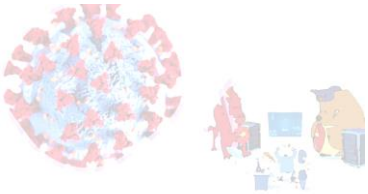
[13] Andrew Salmon, "Korean cases soar, fingerprint scanners face suspicion," *Asia Times*, February 29, 2020, Korean cases soar, fingerprint scanners face suspicion – Asia Times.

[14] Coronavirus: Opaque South Korean sect draws scrutiny with spike in infections," *The Straits Times*, February 21, 2020, Coronavirus: Opaque South Korean sect draws scrutiny with spike in infections, East Asia News & Top Stories - The Straits Times.

[15] "Israel To Track Cellphones For Coronavirus Contact Tracing," *CNN*, March 19, 2020, Israel set to track cellphones for coronavirus contact tracing (cnn.com).

[16] Israel to use 'anti-terror' technology to counter coronavirus," *Aljazeera*, March 15, 2020, Israel to use 'anti-terror' technology to counter coronavirus | Coronavirus pandemic News | Al Jazeera.

[17] Theodore Claypoole, "COVID-19 and Data Privacy: Health vs. Privacy," *Business Law Today*, March 26, 2020, COVID-19 and Data Privacy: Health vs. Privacy | Business Law Today from ABA.



Другие страны также не остались в стороне от поиска и внедрения технологических решений для сдерживания вируса. К примеру, ***Япония*** использовала сканеры температуры для всех прибывающих пассажиров. ***Сингапур*** работал с местными технологическими компаниями, используя QR-коды для отслеживания граждан.

В ***США*** также фиксировались некоторые подобные примеры правительственного надзора для борьбы с новым коронавирусом. Компания по сбору данных Palantir работает с Центрами по контролю заболеваний, чтобы смоделировать распространение вируса, и «другие компании, которые собирают данные из общедоступных социальных сетей, имеют контракты с агентством и Национальными институтами здравоохранения»[18]. Другая компания Crimson Hexagon, часть Brandwatch, имеет контракт на 30 тысяч долларов с Центром по контролю заболеваний с осени 2019 года. Crimson предоставляет компаниям и правительствам инструменты «социального прослушивания» посредствам очищения общедоступных постов в Facebook, Instagram и Twitter для оценки настроений[19]. Базы данных социальных сетей можно использовать для поиска симптомов, которые люди обсуждают, например, одышки, лихорадки или кашля.

Спонсируемый Google веб-сайт Project Baseline связывает информацию о людях, желающих пройти тестирование, с другими данными, которые Google собирает о них. Правительство США работает с Facebook, чтобы отслеживать передвижения людей, и с Google, чтобы находить полезные сведения с помощью личного использования картографических приложений[20]. Федеральные правоохранительные органы приобрели крупные базы данных о местоположении сотовых телефонов у Verizon и AT&T, что, вероятно, частично является реакцией на решение Верховного суда США (решение Carpenter[21]), ограничивающее доступ правительства к подобной информации без судебных повесток. При этом не отмечается, какие правительственные базы данных останутся в руках администрации после окончания кризиса.

Еще один пример - гигант базы данных по распознаванию лиц Clearview A.I., нарушающий конфиденциальность, «ведет переговоры с государственными агентствами об использовании своей технологии для отслеживания пациентов, инфицированных коронавирусом»[22]. Это повлечет за собой отслеживание государством людей с помощью распознавания лиц и сопоставления с общественными или бизнес-камерами. Вполне

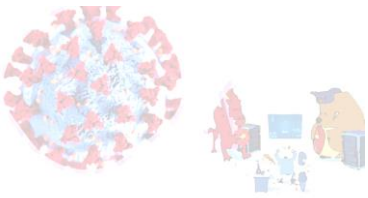
[18] Kirsten Grind, Robert McMillan, and Anna Wilde Mathews, "To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits," *The Wall Street Journal*, March 17, 2020, To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits - WSJ.

[19] Ibid.

[20] Tony Romm, Elizabeth Dwoskin, and Craig Timberg, "U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus," *The Washington Post*, Match 18, 2020, Location data gathered by Facebook, Google, other tech companies could be used to battle coronavirus spread - The Washington Post.

[21] 16-402 Carpenter v. United States (06/22/2018) (supremecourt.gov).

[22] Kirsten Grind, Robert McMillan, and Anna Wilde Mathews, "To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits," *The Wall Street Journal*, March 17, 2020, To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits - WSJ.



вероятно, что распознавание автомобильных номеров, которым пользуются почти все правоохранительные органы, также будут задействованы для этой задачи[23].

В ***Великобритании*** разработали приложение NHS Covid-19[24] (разработчики Apple и Google), в основе которого лежат принципы приватности и конфиденциальности. Летом от первой версии приложения NHS, которая собирала больше данных централизованно, отказались, отчасти потому, что она не могла идентифицировать контакты между некоторыми iPhone. Вторая версия, запущенная в Англии и Уэльсе в конце сентября 2020 года, была построена на децентрализованной модели Apple и Google[25]. Это связано со строгими ограничениями на объем данных, которые могут быть извлечены - например, запрещается приложению отслеживать местоположение пользователя. Вдобавок, пользователи не предоставляют номер телефона, а просто видят предупреждение и могут решить, подчиняться ли ему.

Ирландское приложение для отслеживания контактов, которое также использует набор инструментов Apple и Google, действительно спрашивает пользователей, готовы ли они предоставить свой номер телефона. Затем, если они получают предупреждение о контакте, им также звонят из службы отслеживания контактов с дальнейшими советами. Более 80% пользователей согласились предоставить свой номер, который хранится на их телефоне, а не централизованно и предоставляется только после запуска уведомления о контакте. Разработчики приложения говорят, что это означает, что они лучше понимают, насколько оно эффективно[26].

Несмотря на все позитивные моменты и успешность многих технологических решений, все эти новые биометрические технологии идут вразрез с тенденцией в законе о приватности и конфиденциальности. Общий регламент ЕС по защите данных, а также законы таких штатов США, как Иллинойс, Вашингтон и Техас, ограничили использование биометрических идентификаторов компаниями. Конфликт между очевидной пользой биометрических данных как практического инструмента безопасности и здравоохранения и фиксирования наших физических характеристик продолжится и, скорее всего, усилится из-за использования нами биометрических инструментов для борьбы с COVID-19, угрожающих приватности и конфиденциальности.

Сдерживание вспышки COVID-19 жизненно важно, и в таких кризисах здоровье многих перевешивает конфиденциальность одного. Но подтолкнет ли нас этот инцидент на три шага дальше к полноценному обществу слежки[27]? Это позволило Китаю опробовать

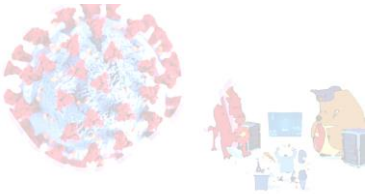
[23] Theodore Claypoole, "COVID-19 and Data Privacy: Health vs. Privacy," *Business Law Today*, March 26, 2020, COVID-19 and Data Privacy: Health vs. Privacy | Business Law Today from ABA.

[24] NHS Covid-19 app: Privacy Notice. Guidance. Department of Health and Social Care. NHS COVID-19 app: privacy notice - GOV.UK (www.gov.uk).

[25] Rory Cellan-Jones, "Is the UK's NHS Covid-19 app too private?" *BBC News*, October 30, 2020, Is the UK's NHS Covid-19 app too private? - BBC News.

[26] Ibid.

[27] Ram, Natalie, and David Gray. "Mass Surveillance in the Age of COVID-19." *Journal of Law and the Biosciences* 7, no. 1 (2020): Lsaa023.; Amit, Moran, Heli Kimhi, Tarif Bader, Jacob Chen, Elon Glassberg, and Avi Benov. "Mass-



технологические методы социального контроля, и вероятно, эти инструменты никуда не исчезнут в пост-ковидное время. Все правительства создают множество новых типов баз данных и аналитики для изучения населения, включая отдельных людей и небольшие сообщества. Будут ли эти инструменты сохранены или отменены? Государственная и местная полиция также использует все больше технологий наблюдения за людьми. Они скорее всего продолжат использовать полученную информацию даже после того, как вирусная угроза будет смягчаться и вовсе исчезнет.

По сути, борьба с COVID-19 привела к внедрению обширных новых электронных и ориентированных на данные технологий, которые, несомненно, помогут спасти жизни многих людей. По мере внедрения этих технологий мы также должны быть осторожны с тем, что мы теряем[28]. Благодаря вниманию, уделяемому изменениям в европейских и калифорнийских законах о приватности и конфиденциальности, компании выстраивают внутренние методы защиты конфиденциальности людей. Борьба с вирусом подвергает некоторую часть этой личной информации риску. Пока COVID-19 угрожает здоровью, а борьба с ним угрожает экономике, важно не потерять ценность приватности и конфиденциальности в пост-ковидное время.

1.2. Ограничения и возможности

Чтобы тщательно проанализировать последствия пандемии COVID-19 для приватности и конфиденциальности, необходимо рассмотреть право на неприкосновенность частной жизни и защиту персональных данных. Приватность и право на защиту данных являются основными правами, но не абсолютными. Согласно философской традиции, право является абсолютным, когда оно перевешивает все остальные элементы, включая другие права и свободы, включая моральный императив спасения человеческих жизней и защиты эффективности экономической системы[29].

Чрезвычайное положение, национальные интересы, и исключительные обстоятельства в прошлом допускали временные ограничения основных прав, таких как право на неприкосновенность частной жизни. Пандемия COVID-19, определенная Всемирной организации здравоохранения как «угроза для любой страны»[30], является исключительным обстоятельством, которое заставило страны во всем мире объявить чрезвычайное положение. Согласно ст.52(1) Хартии основных прав Европейского Союза[31], ограничения на осуществление прав и свобод, признанных Хартией, могут быть наложены

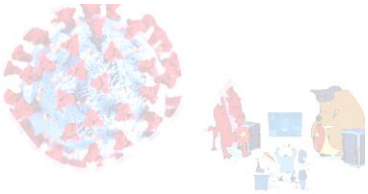
surveillance Technologies to Fight Coronavirus Spread: The Case of Israel." *Nature Medicine* 26, no. 8 (2020): 1167-1169.

[28] Theodore Claypoole, "COVID-19 and Data Privacy: Health vs. Privacy," *Business Law Today*, March 26, 2020, COVID-19 and Data Privacy: Health vs. Privacy | Business Law Today from ABA.

[29] Leif Wenar, Rights. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy (2020). https://plato.stanford.edu/archives/spr2020/entries/rights/.

[30] WHO Director-General's opening remarks at the media briefing on COVID-19, 5 March 2020, https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19—5-march-2020.

[31] Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.



только в том случае, если они действительно отвечают целям, представляющим общий интерес, признанным Союзом.

В отношении приватности Европейская конвенция о правах человека перечисляет законные цели, которые могут оправдать нарушение права на уважение частной и семейной жизни:

> «[...] в интересах национальной, общественной безопасности или экономического благополучия страны, для предотвращения беспорядков или преступлений, для защиты здоровья и нравственности или для защиты прав и свобод других лиц»[32].

Общий регламент по защите данных Европейского союза (GDPR)[33] добавляет некоторые подробности по этим вопросам: защита данных всегда должна рассматриваться в связи с ее функцией в обществе и уравновешиваться другими основными правами. Кроме того, ст.23(1) GDPR позволяет государствам-членам ограничивать права субъектов данных, а также принципы защиты данных, изложенные в ст.5 GDPR, если это делается в законодательном порядке и уважает сущность тех же основных прав и свобод. Эти ограничения, при условии, что они воплощены в необходимых и соразмерных мерах демократического общества, должны быть направлены на защиту, среди прочего, «важных целей, представляющих общественный интерес [...], включая денежные, бюджетные и налоговые вопросы, общественное здравоохранение и социальное обеспечение»[34].

В особых обстоятельствах пандемии обработка персональных данных необходима для принятия соответствующих мер по сдерживанию распространения вируса и последующему смягчению его последствий[35]. Во-первых, обработка определенных типов персональных данных (имя, домашний адрес), рабочее место, информация о путешествии) могут быть полезны, чтобы понять, посещал ли человек районы или встречался с людьми, подверженными воздействию вируса. Во-вторых, обработка особых категорий персональных данных (таких как данные о здоровье, включая результаты диагностических тестов) имеет решающее значение для понимания того, проявляются ли у человека симптомы, связанные с инфекцией.

Контролеры данных, будь то государственные или частные организации, продолжают подчиняться стандартным правилам защиты данных даже в чрезвычайных обстоятельствах. Во-первых, их обязанность полагаться на правовую основу остается существенной для гарантии законности операций по обработке данных.

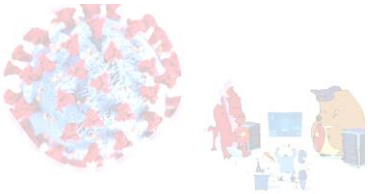
---

[32] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

[33] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[34] Art. 23(1)(e) GDPR.

[35] Marcello Ienca, Effy Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic." *Nat. Med.* 26, 463–464 (2020). https://doi.org/10.1038/s41591-020-0832-5.



Соответствующие персональные данные, отличные от данных специальной категории, могут обрабатываться для целей, изложенных выше, в соответствии со ст.6(1)(d) и (e) GDPR. В то время как первое правовое основание позволяет обрабатывать персональные данные, необходимые для защиты жизненно важных интересов людей (для спасения жизней), на второе можно полагаться для защиты общественных интересов или при осуществлении официальных полномочий, возложенных на контролера. Принимая во внимание тот факт, что общественный интерес может быть определен только законодательством Европейского союза или государства-члена, GDPR прямо упоминает мониторинг эпидемий как обстоятельства, при которых обработка может служить как важным основанием общественного интереса, так и жизненно важным интересам субъектов данных.[36]

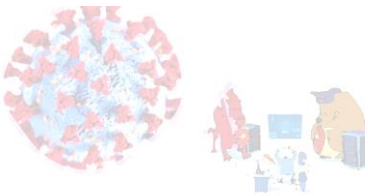
Что касается данных о состоянии здоровья, правовую основу для обработки можно найти в ст. 9(2)(i) GDPR, а дальнейшие инструкции приведены в разделах 52 и 54. Согласно Регламенту, обработка особых категорий персональных данных разрешается, когда это необходимо по причинам общественного интереса в области общественного здравоохранения, «например, для защиты от серьезных трансграничных угроз здоровью»[37]. Чтобы сделать эту правовую основу применимой, на основе практических действий со стороны органов здравоохранения и других соответствующих органов власти должны быть предоставлены не только рекомендации и инструкции, но и приняты соответствующие конкретные меры предосторожности из-за чувствительности этих категорий данных.

Хотя может показаться, что у контролеров есть достаточно места для маневра при выборе подходящей правовой основы для обработки персональных данных с целью сдерживания распространения вируса, оценка соразмерности остается краеугольным камнем в применении мер, которые не должны быть чрезмерными или дискриминационными. Соображения соразмерности должны способствовать установлению приоритетов и защите человеческого достоинства людей. Например, разглашение личности уязвимого человека (например, человека с положительным результатом теста на COVID-19) возникает редко, и в большинстве случаев альтернативные меры, позволяющие избежать идентификации людей, могут быть столь же эффективными для предупреждения других о потенциальном контакте.[38]

[36] Recital 46 indeed clarifies that '[s]ome types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in situation of natural and man-made disasters.'

[37] Art. 9(2)(i) GDPR. Additionally, Recital 54 specifies that 'public health should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the cause of mortality'.

[38] Emanuele Ventrella, "Privacy in emergency circumstances: data protection and the COVID-19 pandemic," ERA Forum 21, 379–393 (2020). https://doi.org/10.1007/s12027-020-00629-3.



Если говорить о трекинге, использовании данных о местоположении и цифрового отслеживания контактов, еще в 2003 году во время вспышки атипичной пневмонии SARS были развернуты инструменты ИКТ[39] для быстрого обнаружения источников инфекции, случаев и путей передачи. Безусловно, пандемия COVID-19 способствовала массовому распространению этих методов и инструментов, в частности за счет использования данных о местонахождении для поддержки ответных мер и отслеживания контактов пострадавших людей для ограничения распространения вируса.

Во-первых, данные о местонахождении были собраны с целью получения статистических данных о совокупном перемещении людей, независимо от их состояния здоровья[40]. Такие данные позволяют правительствам отслеживать и оценивать общую эффективность собственных мер сдерживания вируса (например, локдаун). Использование данных о местоположении подразумевает, что поставщики услуг электронной связи или приложения поставщиков услуг информационного общества будут обмениваться агрегированными и анонимными наборами данных, указывающими географическое положение смартфона, с государственными должностными лицами, что позволяет им отслеживать перемещения населения[41]. Хотя использование таких методов потребует усилий по устранению возможности связывания данных с идентифицированными или идентифицируемыми лицами, исследования показали, что анонимности данных о местоположении труднее добиться, чем ожидалось, поскольку следы мобильности людей по своей сути уникальны и сильно коррелируют[42].

Во-вторых, отслеживание контактов — это процесс мониторинга, используемый для предотвращения дальнейшей передачи вирусов и направленный на отслеживание людей, которые были в тесном контакте с инфицированным. Его можно представить в три ступени, согласно руководству ВОЗ[43]:

i. *идентификация контактов*: практика выявления контактов путем выяснения действий инфицированного человека, а также ролей и действий окружающих его людей.
ii. *список контактов*: практика составления списка контактов инфицированного человека, информирование его о значении их статуса, а также необходимости принятия соответствующих мер (карантин или добровольная самоизоляция).

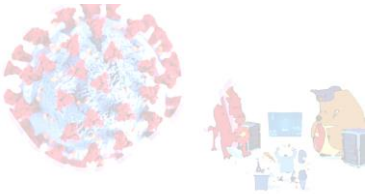
[39] Ting, D.S.W., Carin, L., Dzau, V., et al.: Digital technology and COVID-19. Nat. Med. 26, 459–461 (2020). https://doi.org/10.1038/s41591-020-0824-5. 2020

[40] COVID-19: отчеты о передвижении жителей (google.com).

[41] Emanuele Ventrella, "Privacy in emergency circumstances: data protection and the COVID-19 pandemic," ERA Forum 21, 379–393 (2020). https://doi.org/10.1007/s12027-020-00629-3.

[42] Stuart A. Thompson, Charlie Warzel, "Twelve million phones, one dataset, zero privacy," *The New York Times*, December 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html; Hoffman-Andrews, J., Crocker, A.: How to protect privacy when aggregating location data to fight COVID-19. (2020). Electronic Frontier Foundation, April 6, 2020, https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19.

[43] World Health Organization: Contact tracing in the context of COVID-19. Interim guidance, May 10, 2020, Contact tracing in the context of COVID-19: interim guidance, 10 May 2020 (who.int).



iii. *контактное наблюдение*: практика регулярного наблюдения за всеми контактами для отслеживания симптомов и проверки на наличие признаков инфекции.

В условиях пандемии COVID-19 использование инструментов ИКТ стало все более распространенным явлением, и страны во всем мире стали доверять цифровым технологиям и приложениям для отслеживания контактов, чтобы смягчить последствия чрезвычайной ситуации. Пожалуй, за исключением Китая и некоторых других стран, такие инструменты не включали обработку данных о местоположении и пытались избежать сбора больших объемов данных на централизованном сервере[44]. Например, наиболее часто применяемые системы отслеживания цифровых контрактов требовали установки приложения на смартфоны как можно большего числа людей[45] (это необходимо для совпадения карт активности большинства населения с инфицированными людьми).

При первой криптографической генерации временных идентификаторов каждые несколько минут эти виды приложений будут использовать технологию Bluetooth с низким энергопотреблением, чтобы определять, оказались ли два смартфона, а следовательно, и два человека, в непосредственной близости друг от друга[46]. Как только эта близость достигнута и сохранится достаточно долго, два приложения будут использовать идентификаторы друг для друга. Зашифрованный список зарегистрированных идентификаторов будет храниться локально на телефоне.

В случае, если у пользователя приложения диагностирован COVID-19, метод проверки с участием медицинских работников подтвердит состояние здоровья пострадавшего без сохранения его или ее личности. После этого список контактов будет передан в защищенном виде в государственные органы. Когда чей-то телефон включен в список идентификаторов, хранящихся у человека с диагнозом COVID-19, этот человек получит уведомление от государственных органов вместе с последующей информацией о том, находится ли он на карантине или в самоизоляции. Затем этому потенциально затронутому человеку потребуется связаться с местными органами здравоохранения, чтобы отслеживать симптомы и пройти тест на коронавирус[47]. Чем раньше будет

[44] Paul Mozur, Raymond Zhong, Aaron Krolik, “In coronavirus fight, China gives citizens a color code, with red flags,” *The New York Times*, March 1, 2020, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

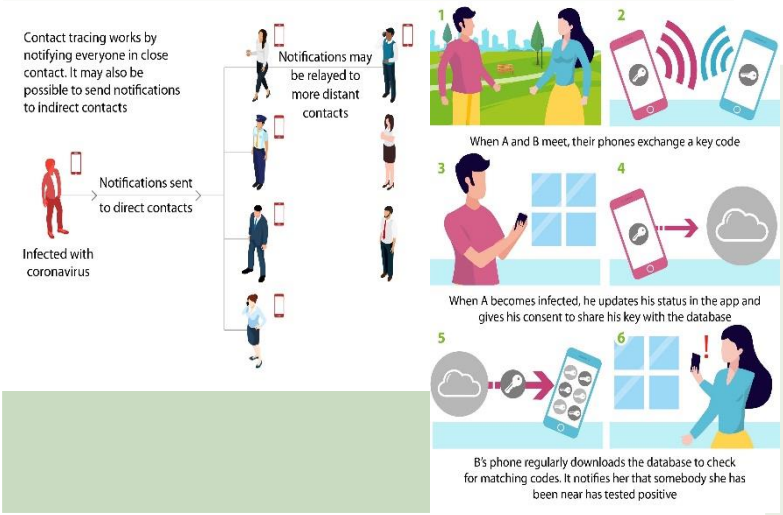
[45] Эпидемиологи и исследователи из Оксфордского университета обнаружили, что для радикального сокращения числа инфекций приложение должно использовать около 56% населения или около 80% пользователей смартфонов. См. подробнее Kelly Servick, “COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?” May 21, 2020, https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how.

[46] Ferretti, Luca, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing." *Science (New York, N.Y.)* 368, no. 6491 (2020): 619-.

[47] https://youtu.be/jkcgrkJnyqU.

проведено это тестирование, тем быстрее государственные органы смогут отследить дополнительные контакты, связанные с этим человеком.

Рисунок 1. Схема работы отслеживающего приложения в Европе[48]



Общеевропейский протокол отслеживания близости с сохранением конфиденциальности (PEPP-PT) DP-3T.

Когда пользователь объявляется зараженным, приложения отслеживания контактов могут отправлять на сервер либо историю близких контактов, полученную в результате сканирования, либо список их собственных идентификаторов, которые были переданы в широковещательном режиме. Это способствует разнице между централизованным и децентрализованным подходами к отслеживанию цифровых контактов. При централизованном подходе идентификаторы зараженного пользователя и его контакты хранятся в центральной базе данных, что позволяет правительствам и службам здравоохранения повысить видимость данных. Примеры такого подхода были реализованы во Франции и Великобритании. При децентрализованном подходе идентификаторы генерируются телефоном пользователя, и только идентификаторы, переданные зараженным пользователем, передаются внутреннему серверу. Примерами этого подхода являются страны, принимающие общеевропейский протокол отслеживания близости с сохранением конфиденциальности (PEPP-PT) DP-3T. 10 апреля 10 2020 года Apple и Google объявили о разработке интерфейсов прикладного программирования (API) для поддержки децентрализованного подхода.

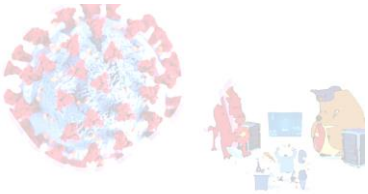
Европейский подход по защите данных не предназначен для того, чтобы препятствовать мерам, которые необходимо реализовать в борьбе с пандемией COVID-19[49]. Напротив, защиту данных следует рассматривать как важный инструмент в создании необходимого социального доверия, которое гарантирует эффективность этих мер. Что касается использования данных о местоположении, то национальное законодательство, реализующее Директиву о приватности и электронной связи[50], устанавливает условия для законной обработки данных о трафике и местоположении. Что касается приложений для отслеживания цифровых контактов, Европейский совет по защите данных определил широкомасштабный мониторинг контактов между людьми как «серьезное вторжение в частную жизнь»[51].

[48] TechDispatch #1/2020: Contact Tracing with Mobile Applications | European Data Protection Supervisor (europa.eu).

[49] Statement on the processing of personal data in the context of the COVID-19 outbreak, European Data Protection Board, March 20, 2020, Statement on the processing of personal data in the context of the COVID-19 outbreak | European Data Protection Board (europa.eu).

[50] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in electronic communications sector.

[51] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, European Data Protection Board, April 21, 2020, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak | European Data Protection Board (europa.eu).



1.3. Что дальше? Искусственный интеллект…

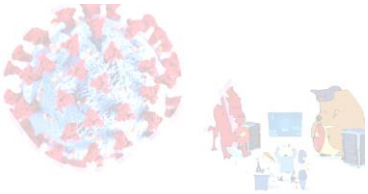
Искусственный интеллект и COVID-19

По мере того, как 2020 год подошел к концу и начался 2021 год, одно можно сказать наверняка: пандемия COVID-19 оказала необратимое влияние на мир и цифровое «здоровье». Более того, пандемия вынудила поставщиков медицинских услуг и правительства всего мира ускорить разработку инструментов искусственного интеллекта (ИИ) и расширить их использование в медицине еще до того, как будет доказана их эффективность[52]. Непроверенный алгоритм искусственного интеллекта даже получил разрешение Управления по санитарному надзору за качеством пищевых продуктов и медикаментов США[53]. Но поможет ли использование непроверенных систем ИИ пациентам с COVID-19 или помешает, и главное, чего ждать в будущем с точки зрения приватности, медицинской тайны и прав человека?

Слабое регулирование алгоритмов искусственного интеллекта для COVID-19 вызвало серьезную обеспокоенность среди медицинских исследователей. Так подчеркивается, что «модели искусственного интеллекта COVID-19 плохо сообщаются и обучаются на небольших или низкокачественных наборах данных с высоким риском систематической ошибки»[54]. Гэри Коллинз, профессор медицинской статистики Оксфордского университета отмечал, что «полная и прозрачная отчетность по всем ключевым деталям разработки и оценки моделей прогнозирования COVID-19 имеет жизненно важное значение… Неспособность сообщить важные детали не только приводит к потере результатов исследований, но, что более важно, может привести к использованию плохо разработанной и оцененной модели, которая может принести больше вреда, чем пользы при принятии клинических решений»[55]. Поэтому для поддержки прозрачной и воспроизводимой отчетности исходный код и деидентифицированные наборы данных пациентов для алгоритмов ИИ COVID-19 должны быть открытыми и доступными в первую очередь для исследовательского и медицинского сообществ.

Одно из таких исследований сообщает о новом скрининговом тесте ИИ COVID-19 под названием CURIAL AI[56], в котором используются регулярно собираемые клинические данные пациентов, поступающих в больницу. В надежде, что ИИ может помочь обеспечить безопасность пациентов и медицинских работников, исследователи заявляют, что тест ИИ может позволить исключить пациентов, не болеющих COVID-19, и

[52] Casey Ross, "Hospitals are using AI to predict the decline of Covid-19 patients — before knowing it works," *Statnews*, April 24, 2020, AI used to predict Covid-19 patients' decline before proven to work - STAT (statnews.com).
[53] Rebecca Robins, "FDA issues rare emergency authorization for an algorithm used to inform Covid-19 care," *Statnews*, October 5, 2020, FDA issues rare emergency authorization for AI tool for Covid-19 care (statnews.com).
[54] "Prediction models for diagnosis and prognosis of covid-19: systematic review and critical appraisal," BMJ, April 7, 2020,Prediction models for diagnosis and prognosis of covid-19: systematic review and critical appraisal | The BMJ.
[55] "Artificial Intelligence for COVID-19: Saviour or Saboteur?" Ed., *The Lancet Digital Group*, 3:1, January 1, 2021, Artificial intelligence for COVID-19: saviour or saboteur? - The Lancet Digital Health.
[56] Curia.ai | Practical AI for a Value-Based World.



обеспечить быстрое лечение пациентов с COVID-19[57]. Это одно из крупнейших на сегодняшний день исследований искусственного интеллекта с клиническими данными по более чем ста тысячам случаев в Великобритании. Предполагаемая валидация скринингового теста ИИ показала точные и более быстрые результаты по сравнению с «золотым» стандартом ПЦР.

Однако, как и другие модели искусственного интеллекта COVID-19, CURIAL AI требует проверки среди географически и этнически разнообразных групп населения, чтобы оценить его реальную эффективность. Даже если предварительные модели, такие как CURIAL AI, доказали, что они позволяют точно диагностировать заболевания в широком диапазоне групп населения, добавляют ли они клиническую ценность системам здравоохранения? Разработчики ИИ не всегда хорошо понимают, как эти инструменты диагностики состояний здоровья могут улучшить медицинское обслуживание. Поэтому модели искусственного интеллекта COVID-19 должны разрабатываться в тесном сотрудничестве с медицинскими работниками, чтобы понять, как результаты этих моделей могут быть применены в уходе за пациентами.

В начале сезона гриппа перед инструментами искусственного интеллекта встает все более сложная задача - помочь различать две респираторные инфекции с похожими симптомами. Если невозможно доказать, что инструменты ИИ позволяют отличить одну пневмонию от другой, преждевременное использование этих технологий может привести к ошибочному диагнозу и подорвать клиническую помощь пациентам. Подобные ошибки, если их допустить, замедлят будущее использование потенциально спасающих жизнь технологий и подорвут доверие врачей и пациентов к ИИ. Чтобы оценить истинную точность инструментов ИИ для COVID-19, необходимы клинические испытания для установления того, как они могут поддерживать пациентов с COVID-19 в реальном мире[58]. Безусловно, ИИ может стать спасителем от нынешней пандемии, просто нужно это доказать с медицинской точки зрения, на это нужно время, разработанные политики и исследования.

Искусственный интеллект и персональные данные

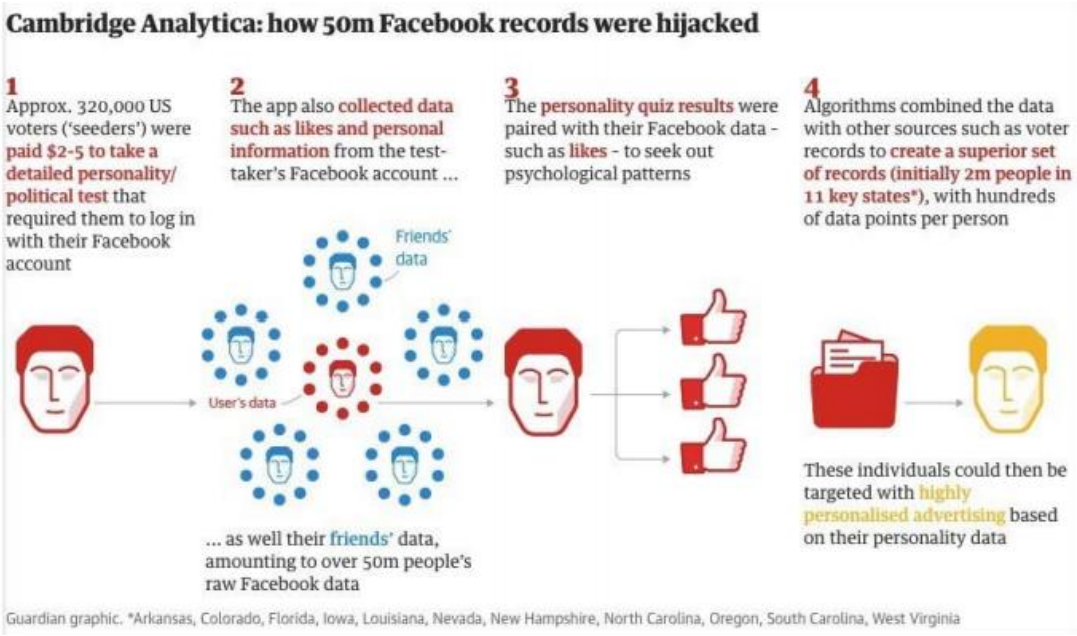
Многие приложения с ИИ обрабатывают личные данные. С одной стороны, персональные данные могут вносить вклад в наборы данных, используемых для обучения систем машинного обучения, в частности для построения их алгоритмических моделей. С другой стороны, такие модели могут применяться к персональным данным, чтобы делать выводы относительно конкретных людей. Благодаря ИИ все виды персональных данных могут использоваться для анализа, прогнозирования и влияния на поведение людей, что дает возможность преобразовывать такие данные и результаты их обработки в ценные товары

[57] Andrew A S Solan et al. “Rapid triage for COVID-19 using routine clinical data for patients attending hospital: development and prospective validation of an artificial intelligence screening test,” The Lancet Digital Health, December 11, 2020, Rapid triage for COVID-19 using routine clinical data for patients attending hospital: development and prospective validation of an artificial intelligence screening test - The Lancet Digital Health.

[58] The Lancet Digital Health. "Artificial Intelligence for COVID-19: Saviour or Saboteur?" *The Lancet. Digital Health* 3, no. 1 (2021): E1.

(теперь цифровые следы превратились в ценные дорогостоящие ресурсы). Например, сервисные платформы Uber или Lyft в разделе совместного использования пассажиров регистрируют производительность сотрудников, а также взаимные обзоры сотрудников и клиентов и связывают различные аспекты эффективности работы с вознаграждениями или штрафами. Этот новый способ управления человеческим поведением может привести к эффективным результатам, но он влияет на психическое благополучие и автономность людей[59].

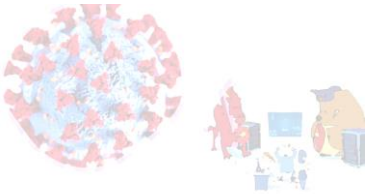
Рисунок 2. Кейс Кэмбридж аналитика.



Наконец, ИИ позволяет автоматизировать принятие решений даже в тех областях, где требуется сложный выбор, основанный на множестве факторов и критериях. Во многих случаях автоматизированные прогнозы и решения не только дешевле, но также более точны и беспристрастны по сравнению с человеческими, поскольку системы искусственного интеллекта могут избежать типичных ошибок человеческой психологии и подвергаться строгому контролю.

Однако алгоритмические решения также могут быть ошибочными или дискриминационными, воспроизводить человеческие предубеждения или генерировать новые. Даже когда автоматизированные оценки людей являются справедливыми и точными, они могут негативно повлиять на заинтересованных лиц, которые подвергаются всеобъемлющему наблюдению, постоянной оценке, влиянию или возможным манипуляциям. Обработка на основе искусственного интеллекта огромных массивов данных об отдельных лицах и их взаимодействиях имеет социальное значение: она

[59] Ibid.



предоставляет возможности для социальных знаний и лучшего управления, но рискует привести к крайностям ***«шпионящего капитализма»*** или ***«государства слежки»***[60].

Шошана Зубофф, американская писательница, профессорка Гарвардского университета и социальный психолог, отмечает, что еще не разработаны адекватные правовые, политические или социальные меры, с помощью которых можно было бы сдерживать потенциально разрушительные последствия «шпионящего капитализма» и удерживать их в равновесии[61].

На правительственном уровне «шпионящий капитализм» находит свою параллель с так называемым «государством слежки», которое характеризуется следующими характеристиками: в «государстве слежки» правительство использует наблюдение, сбор данных, сопоставление и анализ для выявления проблем для защиты от потенциальных угроз, чтобы управлять населением и предоставлять социальные услуги[62]. ***«Государство слежки»*** — это особый случай информационного государства, когда оно пытается выявлять и решать проблемы управления посредством сбора, сопоставления, анализа и производства информации[63]. И в правительстве искусственный интеллект и big data могут принести огромные преимущества, поддерживая эффективность управления общественной деятельностью, координируя поведение граждан и предотвращая социальный ущерб. Однако они могут вводить новые виды влияния и контроля, основанные на целях и ценностях, которые вступают в противоречие с требованиями демократического общества.

Искусственный интеллект и приватность

Масштабы массового цифрового наблюдения (surveillance) подняли вопросы о том, в какой степени международные правовые стандарты и национальные механизмы в достаточной мере защищают людей от нарушений неприкосновенности частной жизни и приватности. И здесь высказывание Элизабет Денхэм, комиссара по информации Великобритании, как нельзя лучше описывает проблемы, которые появились в результате четвертой промышленной революции и расширения внедрения технологий искусственного интеллекта: ***«Ценой инноваций не обязательно должно быть нарушение основных прав на неприкосновенность частной жизни»***.

Наиболее часто упоминаемые проблемы[64] приватности, связанные с ИИ и другими аналогичными технологиями, включают отсутствие понимания фундаментальных концепций, таких как присутствие в сети и персональные данные, полученные от всего

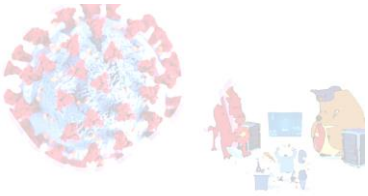
[60] The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliament, EPRS, June 2020, EPRS_STU(2020)641530_EN.pdf (europa.eu). 25-26

[61] Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. First ed. 2019.507

[62] Шошана Зубофф, «Шпионящий капитализм», *Project Syndicate*, January 3, 2020, Шпионящий капитализм by Shoshana Zuboff - Project Syndicate (project-syndicate.org).

[63] Jack M. Balkin. "The Constitution in the National Surveillance State." *Minnesota Law Review* 93 (2008): 1-2274.

[64] Sara W. Denton, Eleonore Pauwels, “There’s Nowhere To Hide,” Policy Report, March 2018, ai_and_privacy.pdf (iapp.org).



онлайн-населения; неявное или неохотное согласие на сбор и обработку данных; отсутствие контроля над личными данными и приватностью; обманчивое использование условий соглашений; и торговля приватностью для бесплатных услуг, в частности развлекательного характера.

Вместе с тем, согласно отчету Privacy International[65], различные приложения и программы на базе ИИ могут по-разному влиять на право на неприкосновенность частной жизни: каждое из этих новых вмешательств в частную жизнь является значительным: приватность и конфиденциальность необходимы для осуществления ряда прав человека, таких как свобода выражения мнений, свобода объединений. Более того, приватность является основополагающим фактором для осуществления личной автономии и свободы выбора[66], а также более широких социальных норм[67]. Защита персональных данных играет решающую роль в обеспечении права на неприкосновенность частной жизни[68], но не может устранить все риски, связанные с конфиденциальностью, которые возникают из-за различных приложений и использования ИИ.

***

Наконец, помимо массового внедрения программ с использованием алгоритмов искусственного интеллекта защита персональных данных с помощью технических и организационных мер получит особый приоритет в работе по обеспечению кибербезопасности. В большинстве случаев киберугрозы и их стремительный рост в период пандемии COVID-19 безусловно влияют на конфиденциальность, целостность или доступность персональных данных. В этой связи ожидается рост числа кейсов, связанных с утечкой личных данных, что в результате вынудит контролеров данных действовать в соответствии с рядом международных обязательств, стандартов и требований, которые вытекают непосредственно из режима защиты данных[69].

Главной задачей по минимизации рисков как для государственных, так и бизнес-организаций станет внедрение процедур, направленных на защиту персональных данных, и принятие мер кибербезопасности на всех уровнях. С одной стороны, для обеспечения быстрого реагирования должны быть реализованы превентивные организационные меры, демонстрирующие учет уровня риска и ценности обрабатываемых данных (речь идет о реестрах рисков защиты данных, процедурах уведомления о несанкционированном доступе к персональным данным, графиках и

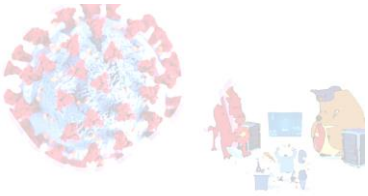
[65] “Privacy and Freedom of Expression In the Age of Artificial Intelligence.” Privacy International, Article 19, April 2018, Privacy-and-Freedom-of-Expression-In-the-Age-of-AI.pdf (iapp.org)

[66] “Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family.” *Choice Reviews Online* 52, no. 02 (2014): 52-0887.

[67] Post, Robert C. “The Social Foundations of Privacy: Community and Self in the Common Law Tort.” 77, no. 5 (1989): 957-1010.

[68] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. U.N. Doc. A/HRC/17/27, 58. May 16, 2011, 17/27 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue / RightDocs - Where human rights resolutions count (right-docs.org)

[69] В разделе 2 GDPR представлены обязательства.

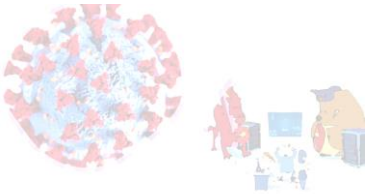


политике хранения данных, а также планах обеспечения непрерывности работы организации). С другой стороны, технические меры с учетом современного уровня технологий, а также связанные с этим затраты должны быть реализованы как на этапе проектирования, так и во время обработки и хранения данных (security by design, security by default). Эти меры могут включать системы двухфакторной аутентификации, надежные политики паролей и средства контроля доступа, надежное антивирусное программное обеспечение, защиту конечных точек и процедуры управления уязвимостями. Кроме того, в свете целостного подхода к защите и безопасности данных организациям следует включить обучение всех сотрудников в свою более широкую стратегию киберустойчивости.

Филипп Аманн, руководитель стратегического отдела Европейского центра по борьбе с киберпреступностью Европола, в своем интервью сказал[70]:

> «Кибербезопасность — это общая ответственность, и, хотя технологии могут обеспечить базовую защиту, особое внимание следует уделять человеческому фактору. Это означает, что постоянное и целевое обучение, образование и повышение осведомленности крайне важны и дополняют технологические меры для поддержки высокого уровня кибербезопасности и киберустойчивости. [...] Организациям необходимо управлять внутренними рисками и рисками в среде, в которой они работают. Это потребует наличия как технических, так и организационных мер для обеспечения безопасности систем и информации. Сюда входят ресурсы, возможности, процессы и инструменты для обнаружения, защиты и эффективного и действенного реагирования на кибератаки. Безопасность, включая основные принципы, такие как безопасность и конфиденциальность по своему замыслу, должна быть ключевым элементом всех бизнес-процессов и деятельности организации».

[70] Cyber Threats and Pandemics: Tackling Risk Through Shared Responsibility. Trilateral Research. Cyber Threats and Pandemics: Tackling Risk Through Shared Responsibility - Trilateral Research.



2. Статус и положение персональных данных в Казахстане: цифровая повестка и пост-ковидное будущее

Появление электронного правительства в Казахстане способствовало существенному изменению взаимоотношений между обществом и государством в целях содействия демократизации и эффективному государственному управлению. Другая сторона этого процесса – широкое внедрение технологических решений, массовый сбор данных и цифровое наблюдение (surveillance). В условиях перехода Казахстана к цифровому обществу возникло немало возможностей, трудностей и ограничений.

Министерства здравоохранения и внутренних дел Казахстана частично обратились к технологическим решениям для борьбы со вспышкой COVID-19. Так, около 8000 казахстанцев в Алматы и Нур-Султане, находящихся на обязательном карантине, обязали использовать приложение для отслеживания SmartAstana, которое позволяет гарантировать, что люди остаются в изоляции[71]. Для этого необходимо включить настройки геолокации, Wi-Fi и Bluetooth, чтобы можно было отслеживать и гарантировать, что люди перемещаются не более чем на 30 метров от назначенного расположение. Если телефон человека неактивен в течение четырех часов или если министерство здравоохранения уведомлено о том, что он отошел слишком далеко, то человек получает видеозвонок с уточнением[72]. Помимо трекинга приложение SmartAstana также позволяет пользоваться некоторыми государственными услугами и сервисами.

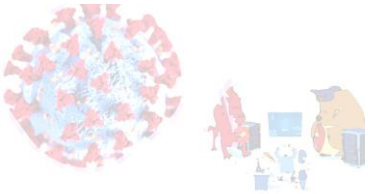
Спустя почти год с начала эпидемии COVID-19 в Казахстане министерство цифрового развития, инноваций и аэрокосмической промышленности совместно с министерством здравоохранения и национальной палатой предпринимателей продолжают разрабатывать технологические решения для контроля эпидемиологической ситуации в отдельных городах. Речь идет о мобильном приложении Ashyq, которое должно обезопасить посещение общественных мест (аэропорты, вокзалы, кафе и рестораны, магазины и торгово-развлекательные центры) и способствовать постепенному восстановлению малого и среднего бизнеса в стране. Согласно разработчикам, людей разделят по цветам и будут пускать в ряд заведений только по QR-коду, при этом цвет будет зависеть от того, болеет ли человек коронавирусом и имеется ли у него ПЦР-тест[73].

---

[71] Дана Жайык, «Вирусный мониторинг: Как коронавирус распространил мировую слежку», The Steppe, April 3, 2020, Вирусный мониторинг: Как коронавирус распространил мировую слежку | Steppe (the-steppe.com).

[72] "Kazakhstan cities use mobile app to enforce quarantine," Privacy International, March 30, 2020, Kazakhstan cities use mobile app to enforce quarantine | Privacy International; Мария Дубовая, « Находящихся на домашнем карантине обяжут установить приложение для контроля их передвижения», *Inform бюро*, March 30, 2020, Находящихся на домашнем карантине обяжут установить приложение для контроля их передвижения | informburo.kz.

[73] Ажар Оразбай, "Казахстанцев разделят на цвета и будут пускать в заведения только по QR-коду," *Tengrinews*, February 1, 2021, Казахстанцев разделят на цвета и будут пускать в заведения только по QR-коду: 01 февраля 2021, 13:10 - новости на Tengrinews.kz.



Министерство внутренних дел использовало технологию видеонаблюдения «Сергек», производимую местной телекоммуникационной компанией «Коркем Телеком», для поиска нарушителей карантинного режима в Алматы[74]. В Уральске местные власти планируются получить доступ к карте перемещения людей для выявления массового скопления людей от операторов сотовой связи[75].

Кроме того, KazUAV, ведущий казахстанский поставщик услуг беспилотных летательных аппаратов и член японской корпорации Terra Drone Corporation, предоставляла прямую поддержку оперативному штабу и Управлению полиции Нур-Султана, созданному для предотвращения распространения коронавируса в Казахстане, посредством патрулирования границ столицы с помощью дронов, обеспечивая бесконтактное наблюдение[76]. Наконец, использование программного обеспечения с алгоритмами ИИ для определения пневмонии и признаков COVID-19 также имело место в Алматы летом 2020 года[77].

Эти примеры являются одними из немногих публичных инициатив, когда местные органы власти использовали новые технологии для борьбы с распространением COVID-19 и соблюдения санитарных норм в различных городах.

Однако на ряду с очевидной пользой этих мер возникают и другие не менее важные вопросы. В частности, кто обрабатывает собранные персональные данные, кто имеет к ним доступ, как обеспечивается обезличивание данных, как долго эти данные будут храниться на серверах, как предотвратить несанкционированный доступ и утечки, какие протоколы разработаны на эти и другие кризисные ситуации, как Агентство по защите данных будет курировать все эти инициативы и мониторить их соответствие закону и соблюдению цифровых прав казахстанцев и многие другие моменты, ответы на которые пока нет.

Кроме того, первичные технологические решения, вызванные необходимостью предотвратить ухудшение эпидемиологической ситуации в отдельных городах и стране, сегодня продолжают видоизменяться и трансформироваться в долгосрочные механизмы сбора, обработки и хранения персональных данных миллионов казахстанцев.

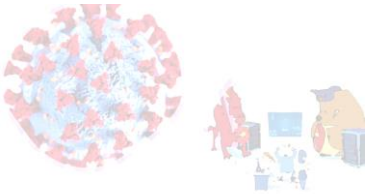
---

[74] «С помощью «Сергек» будут выявлять нарушителей карантина в Алматы», Inform.kz, March 30, 2020, https://www.inform.kz/ru/s-pomosch-yu-sergek-budut-vyyavlyat-narushiteley-karantina-v-almaty_a3631162.

[75] "Отслеживать массовое скопление уральцев власти планируют через сотовую связь", Мой Город, January 20, 2021, https://mgorod.kz/nitem/otslezhivat-massovoe-skoplenie-uralcev-vlasti-planiruyut-cherez-sotovuyu-svyaz/?fbclid=IwAR2-Lkk-ndmGGwBTPK0OLi2M2uLp_xrapc_JfPu67SNDcAARTTaTXKkSCek.

[76] "Kazakhstan uses drones to patrol capital city during COVID-19 lockdown," Terra news, April 9, 2020, Kazakhstan uses drones to patrol capital city during coronavirus lockdown (terra-drone.net).

[77] "Искусственный интеллект помогает казахстанским врачам диагностировать коронавирус", Forbes, May 9, 2020, Искусственный интеллект помогает казахстанским врачам диагностировать коронавирус — Forbes Kazakhstan.



2.1. Персональные данные и цифровизация

Правительство Казахстана рассматривает цифровизацию исключительно как процесс автоматизации максимально возможного числа государственных услуг - 335 по состоянию на июль 2020 года[78]. Более крупные инициативы GovTech, такие как электронное правительство – egov.kz, получили довольно широкое распространение, поскольку правительства стремятся повысить эффективность своих операций за счет оцифровки рабочего процесса и внедрения новых инструментов. Действительно, казахстанский проект электронного правительства помог государству существенно сократить время ожидания, упростить процедуры и принести пользу гражданам.

Тем не менее, наряду с безусловной эффективностью этого технологического решения в стране не хватает стратегического видения и подходов, основанных на принципах security by default и security by design. В результате казахстанские усилия по цифровизации уязвимы вдвойне. С одной стороны, речь идет об уязвимостях, исходящих от государственных и негосударственных игроков (от утечек данных до кибератак)[79]. С другой стороны, как показала первая часть исследования «Защита персональных данных в Казахстане: статус, риски и возможности»[80], отсутствует видение по формированию культуры цифровизации, продвижению кибергигиены и цифровой грамотности среди граждан для продвижения демократических реформ и соблюдения прав человека.

В 2017 году правительство представило программу «Цифровой Казахстан»[81], национальный план цифровизации до 2020 года на основе опыта сингапурской инициативы «Умная нация»[82]. В этой программе есть пять направлений диджитализации (экономика, цифровое государство, интернет и связь, развитие человеческого капитала, создание экосистемы из представителей бизнеса, научного сообщества и государства), и ни в одном из них не говорится о необходимости защиты персональных данных и продвижении цифровой культуры.

Безусловно, любой процесс цифровизации сопряжен с рисками. В Казахстане специфика диджитализации заключается в преобладающей роли государства, чрезмерном внимании к сектору ИКТ и необходимости получения быстрых количественных

---

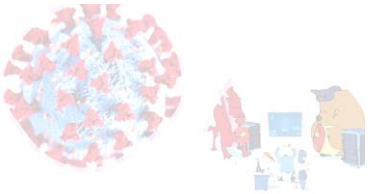
[78] Электронное правительство Казахстана в цифровую эпоху. July 10, 2020. Profit. https://profit.kz/articles/14612/Elektronnoe-pravitelstvo-Kazahstana-v-cifrovuu-epohu/.

[79] Victoria Kelly-Clark, "Central Asia: The Land of CyberCrime?" *Global Risk Insight*, April 29, 2019, https://globalriskinsights.com/2019/04/central-asia-cybercrime-land/.; Catalin Cimpanu, "Extensive Hacking Operation Discovered in Kazakhstan," *ZDNet*, November 23, 2019, https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/.; Almaz Kumenov, "Hackers eyeing Kazakhstan as a safe haven," *Eurasianet*, November 27, 2018, https://eurasianet.org/hackers-eyeing-kazakhstan-as-a-safe-haven.

[80] Гусарова Анна, Джаксылыков Серик, «Защита персональных данных в Казахстане: статус, риски и возможности», 2020, Алматы, ЗащитА персональных данных в казахстане: статус, риски и возможности (soros.kz).; Cyber Security and Cyber Hygiene. Data Protection (caiss.expert).

[81] Государственная программа «Цифровой Казахстан» на 2017-2020 года. https://zerde.gov.kz/images/%D0%93%D0%9F%20%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9%20%D0%9A%D0%B0%D0%B7%D0%B0%D1%85%D1%81%D1%82%D0%B0%D0%BD%20%D0%BD%D0%B0%202017-2020%20%D0%B3%D0%BE%D0%B4%D1%8B.pdf.

[82] Smart Nation Singapore. https://www.smartnation.gov.sg/why-Smart-Nation/pillars-of-smart-nation.



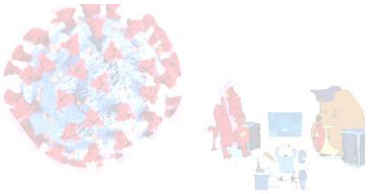
результатов (чаще всего это позиции страны в глобальном индексе развития электронного правительства ООН, в рейтинге «умных» городов и кибербезопасности) посредством создания новых рабочих мест и получения потенциальной финансовой прибыли от внедрения новых технологий.

Кроме того, возможности Казахстана по достижению своих стратегических целей по цифровизации ограничены и зависят от иностранной помощи и поддержки в области технологий, инвестиций и навыков. С одной стороны, чрезмерный упор на ИКТ может привести к более быстрой цифровой трансформации, не раз обозначенной во многих национальных программах и посланиях президента к народу. С другой стороны, упор на более агрессивный, непрозрачный и быстрый подход к оцифровке государственных услуг исключает знания и культуру в понимании долгосрочных выгод и побочных эффектов для людей, их свобод и доверия к правительству.

Далеко идущие последствия нахождения быстрых решений в поиске технологий для реализации программы модернизации привели к выбору российского и китайского программного обеспечения и технологий[83], а также опыту регулирования защиты данных и «цифровой слежки» (инвестиции ЕС и США, их знания и опыт, связанный с приватностью и конфиденциальностью, уступили практикам цифровой секьюритизации). Более того, в стране с очень сильной государственной позицией в экономической и политической системах возможности по выстраиванию партнерства с бизнесом существенно ограничены. В результате общая ответственность и долгосрочные инвестиции в кибербезопасность, благосостояние и устойчивое развитие общества бизнеса, которые являются одним из главных движущих элементов цифровой трансформации, в реальности пока слабы. Новый пилотный проект SmartBridge[84], направленный на интеграцию бизнеса с государственными базами данных, в перспективе позволит усилить партнерство государства с частным сектором. Уже сейчас его партнерами являются 726 юридических лиц, из которых 195 – государственные органы и предприятия, 25 – банки второго уровня, 42 – национальные компании и 464 – представители бизнеса.

Другой особенностью цифровизации является непоследовательность и крайне слабая координации между всеми государственными органами. Хотя внедрение передовых технологий во все аспекты общественной жизни остается важной задачей, разные министерства и ведомства имеют разные уровни цифровизации и технического прогресса (службы безопасности использовали свои возможности для увеличения возможностей наблюдения по причине борьбы с экстремизмом и терроризмом). Президент Токаев лично обратил внимание на эту проблему, предложив создать единую систему мониторинга, которая должна объединить все государственные органы в рамках информационно-

[83] "Kazakhstan to Use Chinese Digitalisation Technology." *BBC Monitoring Central Asia* (London), 2019.
[84] Меруерт Сарсенова, "Асет Турысов: Мы хотим развивать концепцию омниканальности," Kapital, January 8, 2021, Асет Турысов: Мы хотим развивать концепцию омниканальности - Капитал (kapital.kz).



аналитической системы «Smart Data Ukimet»[85], к которой подключены 46 из 127 информационных систем государственных органов[86].

Еще один важный аспект, связанный с цифровой трансформацией Казахстана, — это скорость и время внедрения новых технологий, особенно Big Data, облачных технологий и искусственного интеллекта. С одной стороны, они по-прежнему имеют первостепенное значение для общества, промышленности, бизнеса и правительства в цифровом мире. С другой стороны, большинство новых технологических решений были быстро внедрены в технологически благоприятной среде крупных городов с уже имеющейся инфраструктурой. В результате эта политика значительно увеличила цифровой и социально-экономический разрыв между городскими и сельскими регионами страны и отдаленными сообществами. Кроме того, на деле цифровизация пока не привела к серьезному экономическому прорыву, быстрым выгодам и прибыли, как хотелось: благосостояние казахстанцев остается относительно низким, а государство перегружено последствиями недальновидной экономической политики.

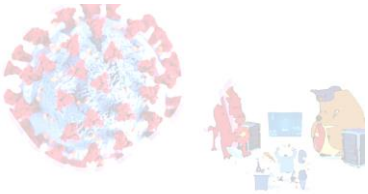
Казахстану, безусловно, необходимо сделать интернет более безопасным, учитывая растущее использование электронной коммерции и растущую оцифровку личной информации граждан через платформу электронного правительства. Однако вопросы регулирования интернета остаются на повестке дня. В частности, речь идет об ограничении интернета и контроле информационного потока, которые уже стали обычной практикой (Open Democracy, 2018; Targeted News Service, 2019). Казахстан остается одной из наименее свободных в Мировой индексе свободы прессы (RSF, 2020, 158-е место), и большое количество граждан, подвергшихся наказанию за политическую деятельность и активизм, свидетельствует о приоритете обеспечения безопасности над индивидуальными свободами.

Если говорить о защите персональных данных, то 25 июня 2020 года Президент Токаев подписал закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий»[87]. Одним из пунктом этого пакета реформ стало создание уполномоченного органа в сфере защиты персональных данных (по аналогии с Data Protection Agency). Им стал Комитет информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности РК.

[85] Глава государства провел совещание по реализации Государственной программы «Цифровой Казахстан», Ak Orda, March 4, 2020, https://www.akorda.kz/ru/events/akorda_news/meetings_and_sittings/glava-gosudarstva-provel-soveshchanie-po-realizacii-gosudarstvennoi-programmy-cifrovoi-kazahstan.; Искусственный интеллект и Большие данные | Электронное правительство Республики Казахстан (egov.kz).

[86] Меруерт Сарсенова, “Асет Турысов: Мы хотим развивать концепцию омниканальности,” Kapital, January 8, 2021, Асет Турысов: Мы хотим развивать концепцию омниканальности - Капитал (kapital.kz).

[87] ЗАКОН РЕСПУБЛИКИ КАЗАХСТАН О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий (29 апреля 2020 года), Досье на проект Закона Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» (29 апреля 2020 года) (принят) - ПАРАГРАФ-WWW (zakon.kz).



За нарушение законодательства о персональных данных и их защите предусмотрена ответственность в рамках административного и уголовного кодексов РК:

> *(ст.147 и 211 Уголовного Кодекса «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите» и «Неправомерное распространение электронных информационных ресурсов ограниченного доступа», ст. 205 «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций», ст. 208 «Неправомерное завладение информацией», ст.79, 641 Кодекса об административных правонарушениях «Нарушение законодательства Республики Казахстан о персональных данных и их защите») с наказанием от штрафов до лишения свободы*[88].

2.2. Программы и задачи: биометрия, искусственный интеллект, система распознавания лиц

Темы цифрового наблюдения, защиты данных и конфиденциальности в казахстанском обществе стояли на повестке дня задолго до вспышки коронавируса. Их продвигали и поддерживали правозащитники в ответ на расширение «цифрового» сотрудничества с Китаем с 2018 года, когда правительство Казахстана запустило национальную стратегию «Цифровой Казахстан» и проекты «Умный город» по изменению формы городских территорий с помощью информационно-коммуникационных технологий[89].

Более того, в октябре 2019 года после государственного визита в Китай Президент Токаев поручил перенять китайский опыт массовой цифровизации в Казахстане[90]. С тех пор технологии распознавания лиц, биометрии, искусственного интеллекта и видеонаблюдения стали быстро развиваться внутри страны в тесном сотрудничестве с российскими, белорусские и несколькими китайскими компаниями, такими как Hikvision и Dahua Technology[91] (против которых США ввели санкции за их содействие нарушениям прав человека мусульманских меньшинств в Китае). Dahua Technology является ключевым партнером местной компании «Коркем Телеком» в создании потенциала видеонаблюдения в Казахстане для снижения дорожно-транспортных происшествий и преступной деятельности в крупных городах Казахстана (широко известных как Сергек).

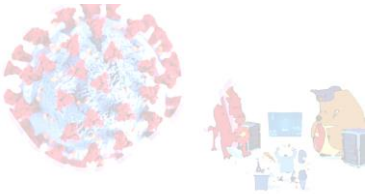
---

[88] Гусарова Анна, "Цифровая приватность. Защита персональных данных," drfl.kz, October 10, 2020, Защита персональных данных (drfl.kz).

[89] Gussarova, Anna. "Kazakhstan Experiments With Surveillance Technology to Battle Coronavirus Pandemic." *Jamestown*, April 08, 2020, Accessed September 1, 2020, https://jamestown.org/program/kazakhstan-experiments-with-surveillance-technology-to-battle-coronavirus-pandemic/.

[90] "Токаев поручил перенять у Китая опыт цифровизации граждан," *Kursiv.kz*, October 9, 2019, https://kursiv.kz/news/obschestvo/2019-10/tokaev-poruchil-perenyat-u-kitaya-opyt-cifrovizacii-grazhdan.

[91] Распознавание лиц (dh-security.kz).



Экстраполяция этих решений в масштабах страны приведет к появлению сотен тысяч камер, которые должны быть установлены до 2022 года в соответствии с планом[92] Министерства внутренних дел по предупреждению преступности, с одной стороны, и введением общенациональной биометрической идентификации и сбора отпечатков пальцев в 2023 году[93], с другой. Это приведет к самой крупной оцифровке личных данных казахстанцев, которые должны собираться, обрабатываться и безопасно храниться на локальных серверах с адекватной защитой от вторжений и утечек.

Когда речь идет о защите персональных данных, неясно, кто имеет доступ и контролирует безопасность сбора, обработки и хранения личной информации казахстанцев. ***Остается непонятным, как и будут ли государственные органы, особенно службы безопасности, уважать права граждан на защиту личных данных***. В контексте внедрения Национальной системы видеонаблюдения вопрос заключается в том, как правительство будет балансировать между правом на неприкосновенность частной жизни и вмешательством в нее для поддержания общественного порядка и обеспечения национальной безопасности.[94]

Созданное профильное агентство (хоть и не независимое, как того хотелось в рекомендациях 2019-2020 годов[95]) активно включилось в работу по соблюдению законодательства в сфере защиты персональных данных. Так, за вторую половину 2020 года Министерством рассмотрено 40 жалоб[96] по нарушению законодательства о персональных данных и их защите.

Рисунок 3. Жалобы по нарушению законодательства о персональных данных в Казахстане за июнь-декабрь 2020 года[97]

Регион	***Количество жалоб***
Юридические лица	
Нур-Султан	**4**
Алматы	**1**
Актобе	**1**
Караганда	**1**
Физические лица	

[92] "Во дворах многоэтажек хотят установить камеры видеонаблюдения к 2022 году." *Profit.kz*, September 25, 2019, https://profit.kz/news/56690/Vo-dvorah-mnogoetazhek-hotyat-ustanovit-kameri-videonabludeniya-k-2022-godu/.

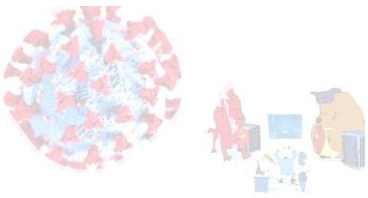
[93] "Сдачу отпечатков пальцев казахстанцами перенесли на 2023 год," Tengrinews.kz, January 03, 2021, Сдачу отпечатков пальцев казахстанцами перенесли на 2023 год: 03 января 2021, 14:43 - новости на Tengrinews.kz.

[94] "Большой брат: как будет работать национальная система видеомониторинга в Казахстане," *Forbes*, February 20, 2020, https://forbes.kz/process/technologies/bolshoy_brat_po-kazahski_1582187734.

[95] Гусарова Анна, Джаксылыков Серик, «Защита персональных данных в Казахстане: статус, риски и возможности», 2020, Алматы, ЗащитА персональных данных в казахстане: статус, риски и возможности (soros.kz).

[96] Ответ Министерства цифрового развития, инноваций и аэрокосмической промышленности РК на обращение № ЗТ-А-653 от 6 декабря 2020 года через портал egov.kz.

[97] Составлено автором на основе данных Министерства цифрового развития, инноваций и аэрокосмической промышленности РК на обращение № ЗТ-А-653 от 6 декабря 2020 года.



Нур-Султан	9
Алматы	12
Караганда	2
Шымкент	1
Актобе	1
Актау	1
Акмолинская область	3
Североказахстанская область	2
Восточноказахстанская область	1
Атырауская область	1

Чаще всего, жалобы касались сбора данных без согласия, бездействия операторов при отзыве согласия на сбор и обработку персональных данных, использования интернет-ресурсами данных, опубликованных в общедоступных ресурсах государственных органов:

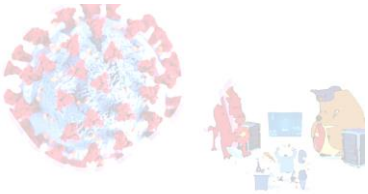
- *за ненадлежащее осуществление мер по защите персональных данных, содержащихся на электронных информационных ресурсах (пп. 1) ч. 1 ст. 641 КоАП РК), к административной ответственности привлечены два оператора связи, 1 страховая компания, 1 должностное лицо;*
- *за незаконный сбор и обработку персональных данных (ч. 1 ст. 79 КоАП РК) к административной ответственности привлечены 1 физическое лицо (владелец интернет-ресурса) и 1 туристическая компания.*

Согласно информации, полученной от Министерства цифрового развития, инноваций и аэрокосмической промышленности, за этот же период следующие нарушения были зафиксированы:

- бездействие операторов баз, содержащих персональные данные, при отзыве согласия физических лиц на сбор и обработку персональных данных;
- сбор и обработка избыточных персональных данных;
- отсутствие перечня персональных данных, необходимых и достаточных для выполнения осуществляемых оператором задач, а также лицо, ответственное за организацию обработки персональных данных;
- несоблюдение требования по своевременному обнаружению фактов несанкционированного доступа к персональным данным;
- отсутствие средств криптографической защиты информации с параметрами, соответствующими требованиям СТ РК1073-2007[98], при хранении и передаче персональных данных.

Сейчас существуют некоторые проблемы с тем, что персональные данные (ФИО, ИИН, данные удостоверения личности, штрафы, административные дела, судебные решения и пр.) доступны в различных поисковых системах. При этом, согласно ответу Министерства цифрового развития, инноваций и аэрокосмической промышленности, «за публикацию вышеуказанных сведений и персональных данных не представляется возможным

[98] СТ РК 1073-2007, СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования» (с поправками) - ПАРАГРАФ-WWW (zakon.kz).



привлечь к административной ответственности…можно только заниматься поступающими жалобами»[99].

Логично ожидать, что в 2021 году национальное агентство по защите персональных данных продолжит свою работу по продвижению культуры защиты персональных данных среди государственных органов, представителей бизнеса и гражданского общества, в частности речь идет о соблюдении принципов открытости и гласности, получении согласия на удаление персональных данных, обезличивание данных и сроки их хранения.

Искусственный интеллект и технологии распознавания лиц

В современном цифровом мире искусственный интеллект, безусловно, создает новые риски для прав человека, в частности недискриминации, приватности и конфиденциальности, безопасности, свободы выражения мнений, свободы объединений, права на работу и доступ к общественным услугам. По прогнозу Huawei[100], к 2025 году 86% транснациональных компаний внедрят искусственный интеллект в свои производственные процессы. ***Можно ли и главное каким образом разработать подход к искусственному интеллекту, краеугольным камнем которого будут права человека и исключение возможностей их нарушения при использовании алгоритмов ИИ в мире и в Казахстане в частности?***

В Казахстане об искусственном интеллекте говорят последние несколько лет[101]. В начале 2020 года премьер-министр Аскар Мамин рассказал[102] о планах создать национальный кластер искусственного интеллекта и институт смарт-систем и ИИ на базе Назарбаев Университета, а также Центр четвертой промышленной революции на базе МФЦА. Экономическая польза от внедрения ИИ насчитывает миллиарды - только в Казахстане по разным данным общий экономический эффект от применения ИИ может составить около 25 млрд долларов США в год, наибольший эффект ожидается в сфере услуг – до 15 млрд и в добывающем секторе – до 9 млрд[103].

Во всем мире активное применение новых технологий приводит к появлению новых вызовов наравне с очевидными экономическими выгодами. ***Принимая во внимание недавние крупные случаи утечки персональных данных, крайне важно начать работу над выработкой национальной стратегии по использованию и внедрению алгоритмов искусственного интеллекта в различных сферах общественной жизни с***

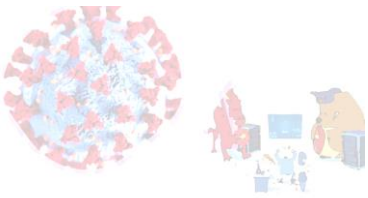
[99] Ответ Министерства цифрового развития, инноваций и аэрокосмической промышленности РК на обращение № ЗТ-А-653 от 6 декабря 2020 года через портал egov.kz.

[100] Искусственный интеллект изменит людей и экономику, Huawei, Искусственный интеллект изменит людей и экономику - Huawei в Республике Казахстан.

[101] Искусственный интеллект и большие данные, Искусственный интеллект и Большие данные | Электронное правительство Республики Казахстан (egov.kz).

[102] Готов ли Казахстан к технологической гонке? Forbes, May 10, 2020, Готов ли Казахстан к технологической гонке? — Forbes Kazakhstan.

[103] “Аскар Мамин: У искусственного интеллекта в Казахстане есть потенциал,” Forbes, January 31, 2020, Аскар Мамин: У искусственного интеллекта в Казахстане есть потенциал — Forbes Kazakhstan.



учетом этических норм и прав человека, а также законодательства, которых на данным этапе все еще нет.

Поэтому первым шагом на этом пути должна стать разработка двух стратегических документов. Первый - стратегия по искусственному интеллекту, долгосрочное видение по разработке и применению ИИ во всех сферах жизни, ориентированного, прежде всего, на человека. Инклюзивный подход, поддержка научных исследований и многостороннего сотрудничества со всеми задействованными стейкхолдерами для улучшения благосостояния – это всего лишь некоторые столпы подобного критически важного решения. Второй – руководящие принципы этики применения искусственного интеллекта и ценности, которые лежат в основе этого процесса. В частности, речь идет о соблюдении прав человека, таких как конфиденциальность и приватность, защита персональных данных, человеческое достоинство, недискриминация и защита прав потребителей.

Безусловно, ИИ должен разрабатываться, использоваться и основываться на этических и социальных ценностях ради общего блага, поэтому изучение и обмен опыта с европейскими и британскими партнерами станет более полезным и важным, чем быстрое внедрение и копирование китайского опыта по внедрению технологии ИИ и распознавания лиц. Потому что помимо технологий, удобства сбора, анализа и обработки больших данных, важно обеспечивать их безопасность и не допускать утечек, взломов и несанкционированных доступов к персональным данных граждан, соблюдая при этом их права и свободы.

Тем не менее, уже сейчас речь идет о предложениях законодательно закрепить использование ИИ в секторе здравоохранения, где на данном этапе используются алгоритмы искусственного интеллекта для выработки схем лечения, «одного из сложных вариантов использования ИИ, требующего совершенно иного уровня медицинских стандартов, инфраструктуры и данных»[104]. Об опасностях быстрого внедрения ИИ в медицине проведено и опубликовано не мало исследований, а обзор некоторых из них представлен в Разделе 1. При этом в Казахстане помимо медицины технологии ИИ уже используются в сфере образования, бизнесе, обеспечения безопасности, включая борьбу с пандемией COVID-19[105].

Однако наряду с экономическим и финансовым потенциалом внедрения технологии искусственного интеллекта важно также использовать его для повышения качества жизни казахстанцев. В докладе[106] McKinsey отмечался высокий потенциал использования ИИ для навигации и трудоустройства слабовидящих, управления городской транспортной системы в Алматы с точки зрения пробок. Кроме того, для получения максимального

[104] "В Казахстане предлагают законодательно закрепить использование искусственного интеллекта в медицине," Informburo, October 16, 2020, В Казахстане предлагают законодательно закрепить использование искусственного интеллекта в медицине | informburo.kz.

[105] "В Казахстане для борьбы с коронавирусом будут использовать искусственный интеллект,"Liter, April 28, 2020, В Казахстане для борьбы с коронавирусом будут использовать искусственный интеллект (liter.kz).

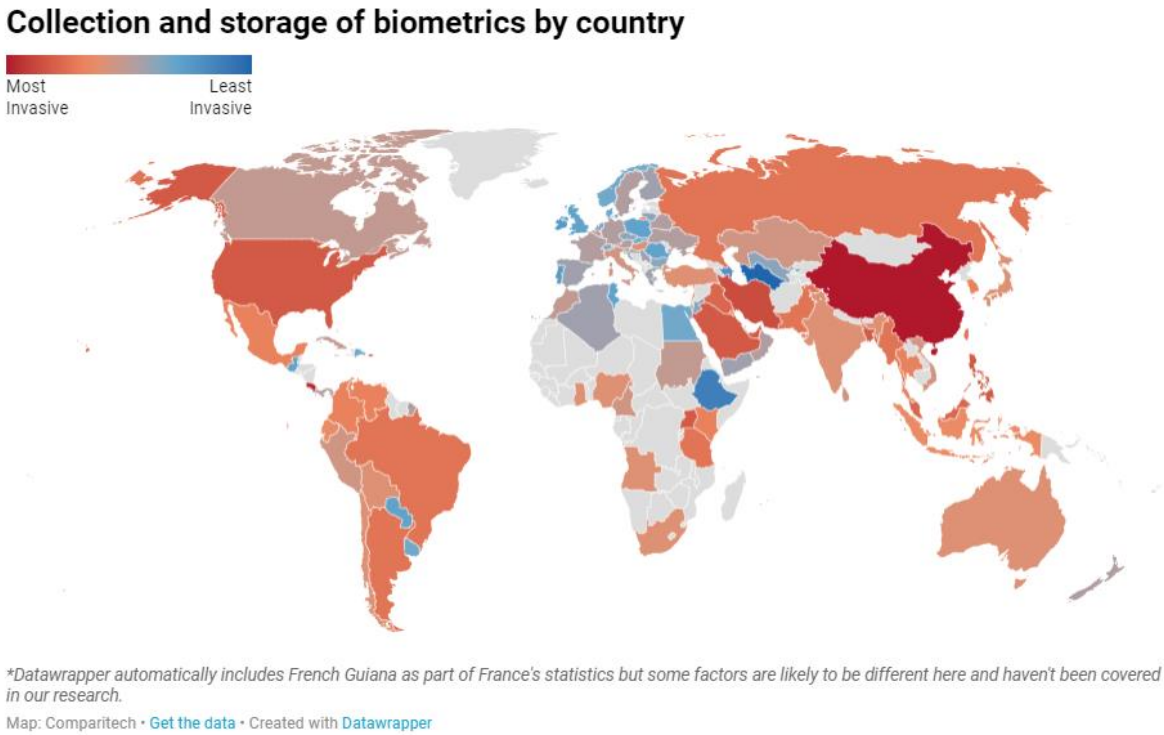
[106] Что даст искусственный интеллект Казахстану? Kursiv, June 12, 2019, https://kursiv.kz/news/hi-tech/2019-06/chto-dast-iskusstvennyy-intellekt-kazakhstanu.

эффекта от внедрения новых технологий в Казахстане на рынке труда к 2030 году должны появиться 5–10 тысяч аналитиков данных, 20–25 тысяч разработчиков систем данных, 2–5 тысяч исследователей данных[107], что представляется крайне маловероятным учитывая негативные последствия[108] и влияние COVID-19 на систему образования в среднесрочной перспективе.

Технологии распознавания лиц

Результаты исследования британской компании Comparitech[109], анализирующего использование биометрических данных в 96 странах, неутешительны. В каждой стране биометрика внедрена в сфере банковских услуг (отпечатки пальцев). Во многих странах отпечатки пальцев собирают у иностранных граждан, а также используют либо тестируют камеры видеонаблюдения с технологией распознаванием лиц.

Рисунок 4. Рейтинг стран по биометрическим данных[110]



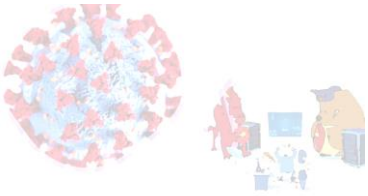
TOP 5 стран, эффективно регулирующих распознавание лиц и биометрию	TOP 5 стран, агрессивно собирающих и хранящих данные граждан
Ирландия	Китай

[107] Ibid.

[108] Жан-Франса Марто, “Пандемия и образование в Казахстане: Серьезные потери и увеличение неравенства,” World bank, November 16, 2020, Пандемия и образование в Казахстане: Серьезные потери и увеличение неравенства (worldbank.org).

[109] Paul Bischoff, “Biometric data: 96 countries ranked by how they’re collecting it and what they’re doing with it,” Comparitech, January 27, 2021, Biometric data collection by country: What's collected, how is it used? (comparitech.com).

[110] Составлено автором по данным Comparitech.



Португалия	Пакистан
Великобритания	Малайзия
Кипр	США
Румыния	Индия

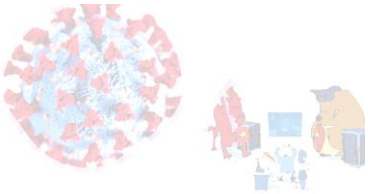
Считается, что биометрические данные лучше защищены в европейских странах, на которые распространяется действие GDPR. Вместе с тем Европейская комиссия с 2020 года пересматривает использование технологий распознавания лиц в общественных местах: правозащитные организации и вовсе настаивают на их полном запрете. Ожидается, что Евросоюз предоставит новые предложения[111] по искусственному интеллекту, которые охватят секторы с высоким уровнем риска – здравоохранение, энергетика, транспорт – уже к середине 2021 года. Тем временем, в Сан-Диего, Калифорния, вступил в силу мораторий на использование системы тактической идентификации TACIDS до 2023 года[112].

В то время как дебаты об использовании технологий распознавания лиц в ЕС и США сосредоточены на угрозе приватности и конфиденциальности правительств или компаний, выявляющих и отслеживающих людей, в Китае обсуждения часто строятся вокруг угрозы утечки информации третьим сторонам, а не злоупотреблений со стороны власти и самих операторов[113].

В Китае система распознавания лиц регистрирует почти каждого гражданина страны с обширной сетью камер по всей стране. Утечка[114] базы данных в 2019 году показала, насколько широко распространены инструменты наблюдения в Китае - более 6,8 миллионов записей за один день, снятых с камер, расположенных вокруг отелей, парков, туристических мест и мечетей, с сохранением подробностей о людях в возрасте от 9 лет и старше.[115] При этом генетические и биометрические данные исключены из закона о персональных данных Китая[116].

Китайские компании давно расширяют свои горизонты и рынки в Африке, Азии, Европе. Один из примеров подобного сотрудничества - Huawei помогала правительствам Уганды

[111] "EU civil rights groups want ban on biometric surveillance ahead of new laws," *Reuters*, February 17, 2021, EU civil rights groups want ban on biometric surveillance ahead of new laws | Reuters.
[112] "San Diego to suspend facial recognition tech program used by police, ICE access blocked," ZDNet, December 12, 2019, San Diego to suspend facial recognition tech program used by police, ICE access blocked | ZDNet.
[113] Yuan Yang, Madhumita Murgia, "Facial Recognition: How China Cornered the Surveillance Market," *Financial Times*, December 7, 2019, Facial recognition: how China cornered the surveillance market | Financial Times (ft.com)
[114] Alfred Ng, "Chinese facial recognition company left database of people's locations exposed," *C|Net*, February 13, 2019, Chinese facial recognition company left database of people's locations exposed - CNET.
[115] Alfred Ng, "How China uses facial recognition to control human behavior," *C|Net*, August 11, 2020, How China uses facial recognition to control human behavior - CNET.
[116] Paul Bischoff, "Biometric data: 96 countries ranked by how they're collecting it and what they're doing with it," Comparitech, January 27, 2021, Biometric data collection by country: What's collected, how is it used? (comparitech.com).



и Замбии «следить за оппозицией»[117]. Другой - соглашения между Министерством образования Узбекистана и компаниями ZTE и Huawei о внедрении технологий видеонаблюдения в систему образования: оборудование для распознавания лиц будет использоваться для контроля посещаемости студентов и оценки работы учителей[118].

Безусловно, постоянное цифровое наблюдение стало особенностью повседневной жизни, людям часто трудно сформулировать, осмыслить или признать его последствия. Но даже когда практики «цифровой слежки» воспринимаются как должное, они не обязательно принимаются гражданами полностью[119]: именно здесь иногда могут возникать зарождающиеся аффективные реакции – люди говорят о «жутких» методах цифрового наблюдения и боятся, что другие слишком много о них знают, не зная на самом деле, кто эти другие.

В Казахстане все большее использование китайских технологий может поставить под угрозу системы государственной безопасности и персональные данные граждан. Реализация проекта «Умный город» и внедрение цифровых технологий в масштабах страны, в том числе распознавание лиц для оплаты транспорта[120], будет способствовать снижению уровня преступности и профилактике правонарушений с одной стороны. С другой, все эти тенденции и реализация национальных планов по цифровизации страны способствуют непропорциональному сокращению прав и свобод граждан (см. Раздел 3 ниже), а главное еще более серьезным рискам и угрозам кибербезопасности в перспективе.

2.3. Медицинские фейлы и возможности

С начала пандемии COVID-19 в Казахстане ситуация с защитой персональных данных ухудшилась, несмотря на создание специализированного агентства. Во-первых, вся обычная рутинная жизнь большинства людей автоматически перешла на цифровые рельсы: граждане стали чаще пользоваться онлайн услугами – торговля, банкинг и пр.

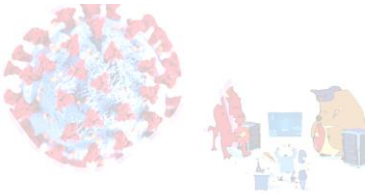
В-вторых, несмотря на очевидный цифровой и технологический сдвиг, который шоковым методом катализировал масштабную диджитализацию различных секторов, персональные данные первых заболевших не были защищены должным образом,

[117] Joe Parkinson, Nicholas Bariyo and Josh Chin, “Huawei Technicians Helped African Governments Spy on Political Opponents,” *The Wall Street Journal*, August 15, 2019, Huawei Technicians Helped African Governments Spy on Political Opponents - WSJ.

[118] Информация с сайта МОН РУз не доступна, однако упоминание о данном соглашении доступно здесь: Bradley Jardine, “China’s Surveillance State Has Eyes on Central Asia,” Foreign Policy, November 15, 2019, China's Surveillance State Spreads Into Central Asia (foreignpolicy.com).

[119] Lupton, D, Michael, M. Big data seductions and ambivalences. Discover Society, 2015, http://discoversociety.org/2015/07/30/big-data-seductions-and-ambivalences/.

[120] “Будущее уже здесь? В Нур-Султане тестируют оплату проезда в автобусах по фото”, Esquire, October 15, 2019, Будущее уже здесь? В Нур-Султане тестируют оплату проезда в автобусах по фото (esquire.kz).



впрочем, как и базовые права и свободы человека, такие как право на частную жизнь, свобода передвижения, право на доступ к информации и т. д.

Достаточно вспомнить абсурдные публикации о том, как заваривали двери и закрывали подъезды[121] в домах, когда становилось известно о заболевшем человеке, или как в чатах информация о том или ином человеке распространялась с целью дальнейших издевательств, унижения и дискриминации, использование врачебной тайны для неразглашения информации по заболевшим представителям Парламента и других органов власти, препятствия в силу COVID-19 для наблюдателей на выборах и активистов для проведения мирных собраний.

В-третьих, утечки персональных данных продолжаю фиксировать специалисты. Так, 15 июля 2020 года ЦАРКА снова заявила об утечке персональных и медицинских данных в Telegram:

> *«…только за 2020 год в системе уже накопилось порядка 24,5 тысячи аудиозаписей телефонных разговоров и десятки гигабайтов персональных данных из интегрированной Государственной базы данных физических лиц… Эта информация доступна в сети любому неавторизованному пользователю уже больше полугода»[122].*

Интересно, что министерство здравоохранения отрицало факт утечки данных и какое-то дальнейшее разрешение ситуации, впрочем, как и информация по ней, в публичном поле отсутствует. Примерно аналогичный исход прослеживается по делу Damumed, утечкам данных и припискам несуществующих членов семьи или посещений врачей.

Если говорить о законодательном аспекте, непонятно, каким образом могут быть задействованы статьи о нарушении законодательства о персональных данных, если ответ Министерства внутренних дел на запрос о ситуации с DAMUMED говорит о том, что «расследование уголовного дела в г. Шымкент прекращено на основании ст.35 ч.1 п.4 Уголовно- процессуального кодекса (за истечением срока давности)», а Комитет по правовой статистике Генеральной прокуратуры в своем ответе №2-20-20-10159 от 20 декабря 2020 года «сведениями об утечках персональных данных, в том числе в системе Damumed, не располагает».

Так же что не так с Damumed, и почему так важно продвигать защиту персональных данных, включая медицинскую информацию и врачебную тайну? 9 июля 2019 года Центр анализа и расследования кибератак (ЦАРКА) на своей странице в Фейбуке рассказали об утечке персональных данных медицинской системы DAMUMED[123].

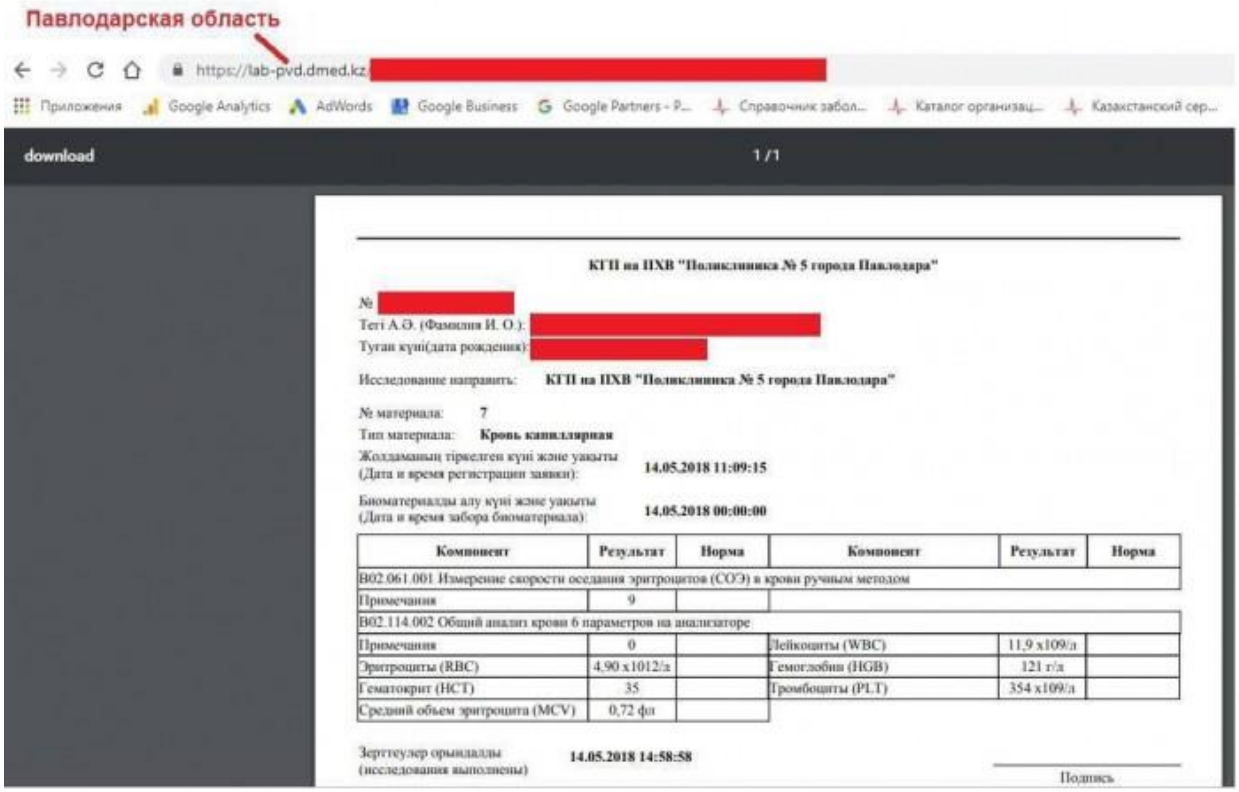
---

[121] "Минздрав не рекомендовал заваривать двери и закрывать целые подъезды на карантин," *Liter*, May 19, 2020, Минздрав не рекомендовал заваривать двери и закрывать целые подъезды на карантин (liter.kz).

[122] Рабига Дюсенкулова "Минюст высказался об утечке данных казахстанцев," *Tengrinews*, July 15, 2020, Минюст высказался об утечке данных казахстанцев: 15 июля 2020, 18:19 - новости на Tengrinews.kz.

[123] Утечка данных тысяч пациентов произошла в Казахстане: 09 июля 2019, 10:39 - новости на Tengrinews.kz

Рисунок 5. Скриншот публикации ЦАРКА по системе Damumed.



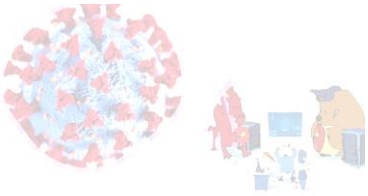
Речь идет о неавторизованном доступе к медицинским документам сотен тысяч пациентов, которые попали в сеть. Позднее Damumed опубликовал официальный пресс-релиз на своей странице Фейсбук, отрицая факт утечки. Вот некоторые самые интересные его выдержки:

> *«... проанализировав некоторые посты и комменты тут в ФБ и прочих СМИ, официально заявляю - не было никакой массовой утечки, а также не было возможности просмотреть данные конкретного пациента! Все могут быть спокойны, никакого ущерба никому нанесено не было! И все что произошло, произошло только благодаря так называемому пользователю-инсайдеру, умысел которого будут расследовать компетентные органы»*[124].
>
> *«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».*[125]

Позднее в августе-сентябре 2020 года стало известно о новом инциденте утечки персональных данных в системе Damumed. Теперь речь шла о том, что «третьи лица могли узнать не только информацию о состоянии здоровья пользователей, но и контактные

[124] Damumed - Posts | Facebook.

[125] Утечка данных тысяч пациентов произошла в Казахстане: 09 июля 2019, 10:39 - новости на Tengrinews.kz.



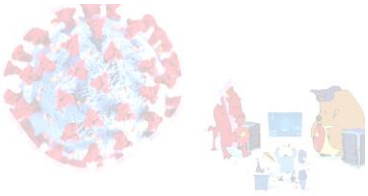
данные, ИИН, род деятельности и размер налогов».[126] Кроме того, стало также известно о том, что приложение приписывало гражданам чужих членов семьи: мужей, жен и детей, а также приписки[127], т. е. «несуществующие записи и посещения врачей» (по некоторым данным в середине 2020 года их сумма превысила 75,5 млн тенге)[128]. И все это на фоне вспышки коронавируса в Казахстане.

Если попытаться разобраться в ситуации, то возникает несколько вопросов: кто все-таки понесет наказание за утечку персональных данных, несмотря на отсутствие виновных в соответствии с полученными ответами государственных органов, когда наконец заработает закон о персональных данных, и главное – что с этим делать и какие уроки вынести из подобной ситуации, которая продолжается по сей день[129] и ничего не изменилось.

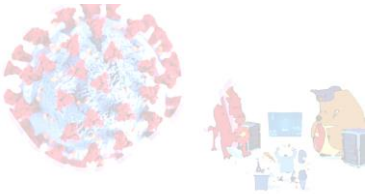
Если говорить о последствиях, ситуация на самом деле является критической по нескольким причинам.

i. Кризис не разрешен, хоть и проблема взята под контроль Министерства здравоохранения: все еще продолжают появляться публикации в социальных сетях о приписках и доступе к персональным данным третьих лиц.
ii. Поскольку в результате утечек персональные данные казахстанцев попали в сеть в открытом доступе, логично говорить об уязвимости системы и потенциальном использовании данных во всевозможных целях, в частности мошенниками.
iii. Об инцидентах утечки данных, неавторизованном доступе к персональным данным должны сообщать организации, в которых подобные кризисные ситуации происходят, а не кто-то другой. Это нормальный стандартный протокол, набор инструментов и практик не только присутствует в европейском GDPR (регламент по защите персональных данных), но и во всех компаниях в мире.
iv. Эта ситуация как нельзя четко демонстрирует ситуацию с культурой безопасности в стране, вернее с ее отсутствием. Закон о персональных данных и их защите не работает, а государство не выполняет свои обязательства по защите персональных данных своих граждан. Штрафы и ответственность за нарушение законодательства должны распространяться на всех, включая государственные органы и их представителей.

[126] Обнаружена утечка персональных данных в Damumed (profit.kz).
[127] Больше всего подобных фактов в Атырауской области. Здесь обнаружили 7 102 случая на 10,6 миллиона тенге. В Мангистауской области нашлось 237 приписок на 2,3 миллиона тенге. В Алматинской области - 970 приписок на 2,2 миллиона тенге. Какие поликлиники чаще делают приписки в Damumed: 16 сентября 2020, 14:39 - новости на Tengrinews.kz.
[128] Приписки на 75,5 миллиона тенге выявили в Damumed: 06 августа 2020, 14:01 - новости на Tengrinews.kz.
[129] В DamuMed снова всплыли приписки | kz.media.



v. Внедрение прозрачных протоколов управления рисками позволит не только усилить компонент по защите систем и персональных данных, но и сократить имеющиеся серые зоны, которые могут использоваться в коррупционных целях. Эти практики должны массово внедряться во все государственные органы, работающие с базами данных, не говоря о частном бизнесе.



3. Что думают казахстанцы о защите персональных данных с начала пандемии COVID-19

Вместе с доступом к безграничным ресурсам информации и контента, к новым товарам и услугам, интернет, занимающий все больше места в жизни людей, открыл доступ и в обратном направлении – к личной жизни самих пользователей. В обмен на доступ ко всем соблазнительным благам всемирной сети пользователь интернета должен позволить собирать и использовать информацию личного характера о себе. И тогда возникает вопрос о возможности контролировать этот самый доступ к личной информации.

Беспрецедентные карантинные меры, принятые в 2020 году в связи с пандемией COVID-19, привели к еще более широкому и интенсивному использованию возможностей сети интернет. Соответственно, вопросы контроля над доступом к личной информации и связанные с этим риски должны, очевидно, стать еще более актуальными.

Власти Казахстана, которые старались не отставать от мировых трендов и потратили немало усилий на обеспечение всеобщего доступа к интернету, с этого времени должны выстраивать свою политику в сфере защиты персональных данных, собираемых через всемирную сеть и посредством технологий. Казахстанское общество в целом и каждый его представитель в отдельности должны в свою очередь быть готовыми к новым рискам, принимать осознанные решения, знать свои права и уметь требовать их соблюдения.

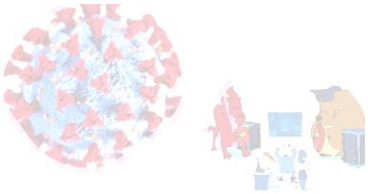
Насколько хорошо осведомлены казахстанцы, активно пользующиеся интернетом, в вопросах защиты персональных данных? Насколько их беспокоит проблема контроля над доступом к своим личным данным? Знают ли они свои права в этой сфере? Каковы их представления о роли государства в этих вопросах? Вот вопросы, которые стали очень актуальны в последние несколько лет.

В 2019 году было проведено исследование, в рамках которого был проведены фокус-групповые дискуссии, позволившие сделать качественный анализ представлений и взглядов казахстанцев, пользующихся интернетом. Тогда было важно понять, что думают казахстанцы о защите персональных данных и на чем основаны их взгляды. То исследование позволило выделить основные точки зрения и понять их логику.

Данное исследование больше нацелено на изучение количественных характеристик распространенных в казахстанском обществе представлений о защите персональных данных[130]. Основными вопросами исследования стали следующие:

- Каков уровень осведомленности о защите персональных данных?
- Каков уровень обеспокоенности проблемой защиты персональной информации?
- Каков уровень осведомленности о правах в этой сфере?

[130] В данном отчете речь будет идти о тех персональных данных, которые предоставляются / собираются онлайн (через сеть Интернет). В некоторых случаях также обсуждаются вопросы, связанные со сбором персональной информации государственными органами: фото и видео материалы, собираемые через камеры наружного наблюдения, а также некоторые биометрические данные, которые государственные органы собирают для регистрации граждан или оказания государственных услуг.



- Каково отношение к государственной политике в этой сфере?

Вопросы (в том числе заданные в форме высказываний), использованные в анкете, были сформулированы на основе результатов исследования 2019 года «Защита персональных данных в Казахстане: статус, риски и возможности».[131]

В исследовании используются первичные данные, собранные методом телефонного опроса. Всего было опрошено 1503 человека. В опросе участвовали только активные пользователи Интернета старше 18 лет. Активными пользователями в данном исследовании считаются те, кто пользуется электронной почтой или мессенджерами, имеет активный аккаунт в социальных сетях, а также совершает какие-либо онлайн транзакции (покупка товаров или услуг, денежные переводы, получение кредита). Для отбора активных пользователей интернета применялись соответствующие вопросы-фильтры. Более подробное с анкетой можно ознакомиться в Приложении 1.

3.1. Методология замера общественного мнения

Данные получены в результате телефонного опроса жителей Республики Казахстан в возрасте 18 лет и старше, отвечающих следующим критериям отбора:

1. Пользование электронной почтой и/или интернет-мессенджерами;
2. Владение активными аккаунтами в социальных сетях;
3. Опыт совершения денежных транзакций в сети интернет, хотя бы один из трех видов:
    a. Покупка товаров или услуг через интернет;
    b. Денежные переводы;
    c. Кредиты онлайн.

Общий объем выборки исследования составил 1503 респондента. Опрос проводился по Казахстану (включая, города и села) с применением метода случайного отбора респондентов.

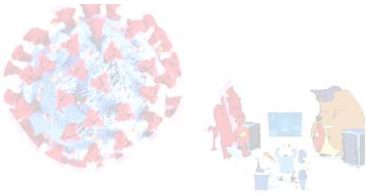
Процедура отбора респондентов состояла из 2 этапов:

- отбор респондентов по случайно сгенерированным телефонным номерам;
- отбор респондентов согласно отборочной анкете.

Отбор респондентов по случайно сгенерированным телефонным номерам

Для проведения полевых работ использовался метод случайной генерации телефонных номеров. В специализированное программное обеспечение для проведения телефонных опросов встроена система автодозвона, которая переводит звонок на оператора только

[131] Гусарова Анна, Джаксылыков Серик, «Защита персональных данных в Казахстане: статус, риски и возможности», 2020, Алматы, ЗащитА персональных данных в казахстане: статус, риски и возможности (soros.kz).



при результативном дозвоне до респондента. На каждого оператора в зависимости от настроек создается несколько звонков.

Отбор респондентов согласно отборочной анкете

Респондентам, согласившимся принять участие в опросе, задавался ряд фильтрационных вопросов, если респондент успешно проходил все отборочные вопросы анкеты, то с ним проводилось основное интервью.

Полевые работы

Метод интервьюирования - телефонный опрос методом CATI. Респондентам, участвовавшим в опросе, гарантировалась строгая конфиденциальность. Полевые работы были проведены в период с 15 по 28 сентября 2020 года.

После проведения необходимого количества интервью все анкеты были проверены и закодированы, обработка данных осуществлялась в программе SPSS.

Количественные характеристики полученного массива данных

Возраст	Количество	%
от 18 до 24 лет	317	21%
от 25 до 30 лет	350	23%
от 31 до 40 лет	489	33%
от 41 до 50 лет	228	15%
от 51 до 60 лет	119	8%
Всего	**1503**	**100%**

Тип поселения	Количество	%
Город республиканского значения	427	28,4
Город-областной центр	482	32,1
Город областного или районного подчинения	234	15,6
Село	360	24,0
Итого	**1503**	**100,0**

Регионы	Количество	%
Астана и Акмолинская область	204	13,6
Актюбинская область	67	4,5
Алматы и Алматинская область	340	22,6
Атырауская область	45	3,0
Восточно-Казахстанская область	122	8,1
Жамбылская область	63	4,2
Западно-Казахстанская область	63	4,2
Карагандинская область	132	8,8

Костанайская область	79	5,3
Кызылординская область	40	2,7
Мангистауская область	48	3,2
Павлодарская область	65	4,3
Северо-Казахстанская область	63	4,2
Шымкент и Туркестанская область	172	11,4
Итого	**1503**	**100,0**

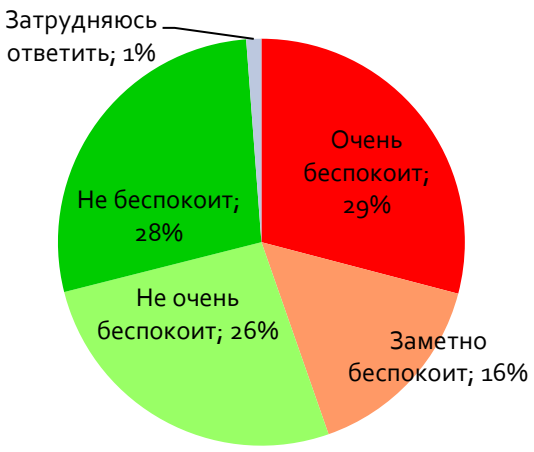
3.2. Обеспокоенность, осведомленность и влияние карантина

Основная часть телефонного интервью начиналась с вопроса о том, насколько комфортно себя чувствуют пользователи интернета относительно предоставления своей персональной информации онлайн. Далее следовали вопросы об осведомленности о защите персональных данных и правах в этой сфере, а также влиянии карантина во время пандемии COVID-19.

Немногим менее половины (45%) опрошенных обеспокоены проблемой безопасности персональной информации, предоставляемой онлайн.

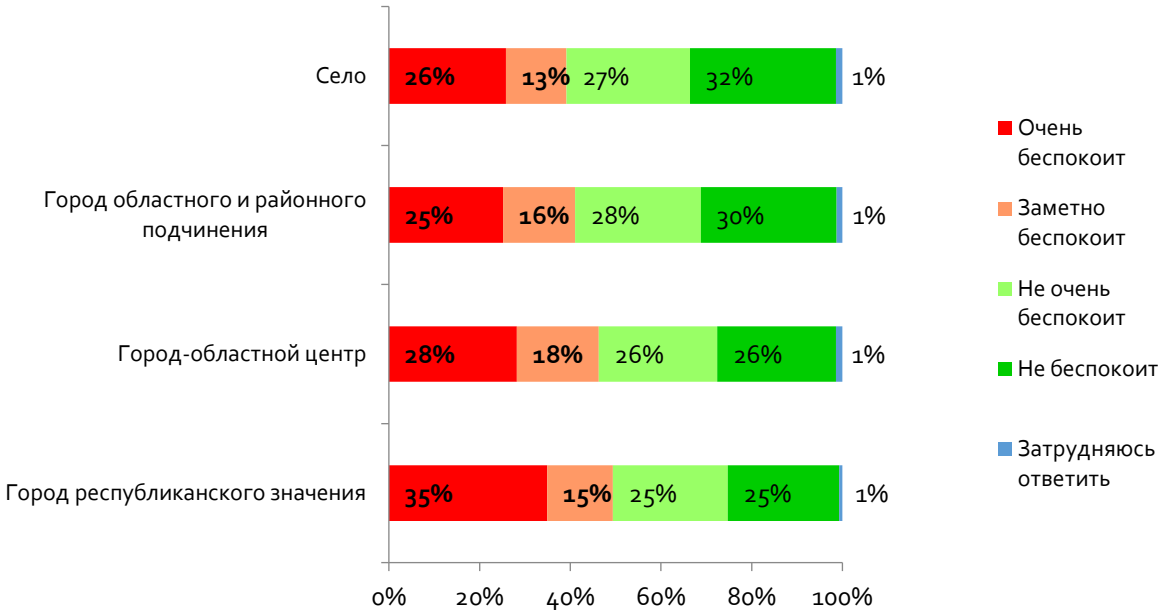
45% активных пользователей Интернета заявили, что их беспокоит проблема безопасности персональных данных, которые они предоставляют онлайн. В том числе 29% выбрали вариант ответа «Очень беспокоит». В то же время более половины (54%) опрошенных не чувствуют беспокойства по этому поводу.

Рисунок 6. Насколько Вас беспокоит безопасность Вашей персональной информации, которую вы предоставляете онлайн? (N=1503, все респонденты)



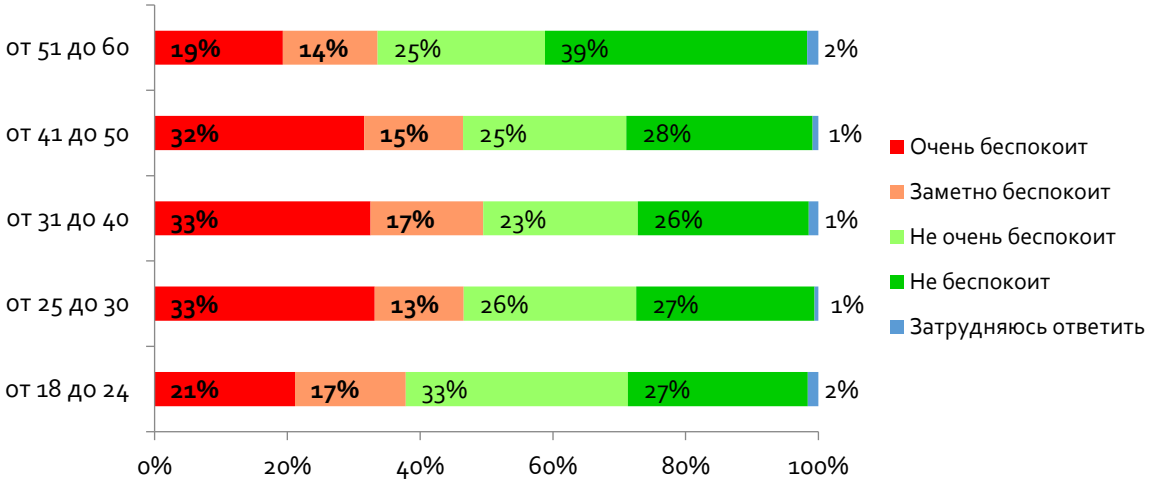
Если рассмотреть распределение ответов на этот вопрос в разных типах поселений (города республиканского значения – 3 самых крупных города страны, областные центры, города областного или районного значения, села), то видно, что уровень обеспокоенности немного выше в самых крупных городах, беспокойство выразили 50% респондентов. Меньше других этой проблемой обеспокоены сельские жители – 39%.

Рисунок 7. Насколько Вас беспокоит безопасность Вашей персональной информации, которую вы предоставляете онлайн? (N=1503, все респонденты)



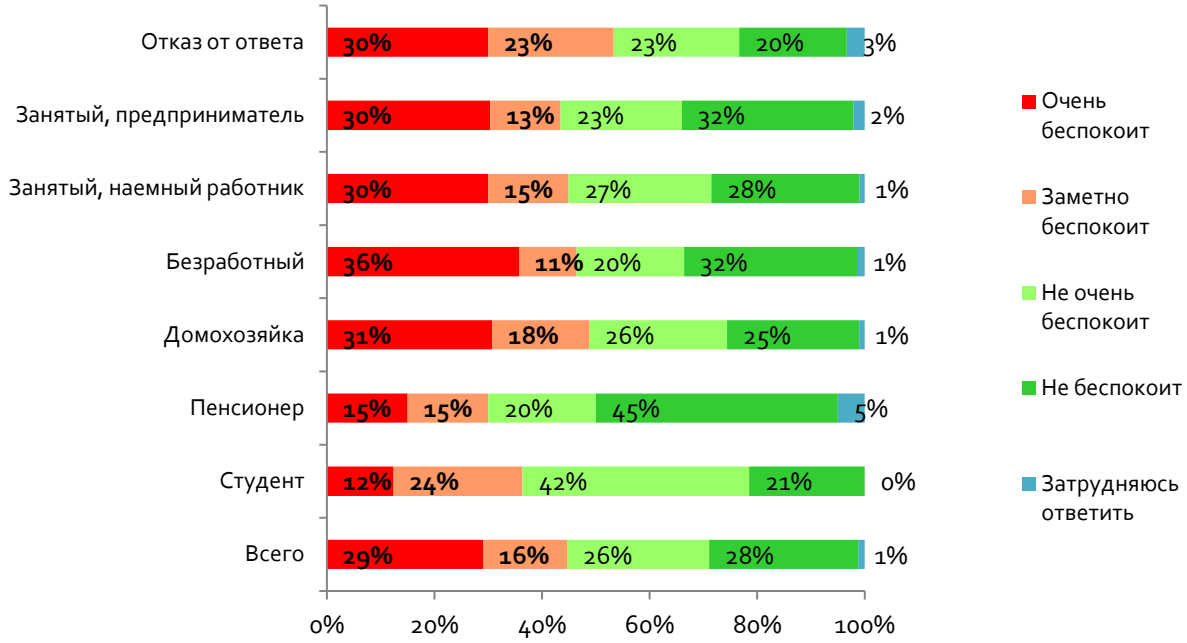
Поскольку принято считать, что активность в пользовании интернетом различается между разными поколениями людей, было интересно сравнить распределение ответов в разных возрастных группах. Оказалось, что разница в уровне обеспокоенности безопасностью персональной информацией заметна между возрастными группами – реже выражали свое беспокойство самая старшая группа (от 51 до 60 лет) и самая младшая (от 18 до 24 лет). В первой обеспокоенности выразило только 33% респондентов этой группы, в последней – 38%. Для сравнения, **в возрастной группе от 31 до 40 лет свою обеспокоенность безопасностью персональных данных выразило 50% респондентов**.

Рисунок 8. Насколько Вас беспокоит безопасность Вашей персональной информации, которую вы предоставляете онлайн? (N=1503, все респонденты)



Наблюдаемое отличие самой молодой и самой старшей группы от других групп других возрастов, скорее всего, следует искать в их экономической активности. Первую группу составляют в основном студенты, вторую – пенсионеры. Как видно на графике ниже, уровень обеспокоенности безопасностью персональных данных заметно ниже среди студентов и пенсионеров. Среди первых обеспокоенность выразили 36%, среди последних – только 30%.

Рисунок 9. Насколько Вас беспокоит безопасность Вашей персональной информации, которую вы предоставляете онлайн? (N=1503, все респонденты)

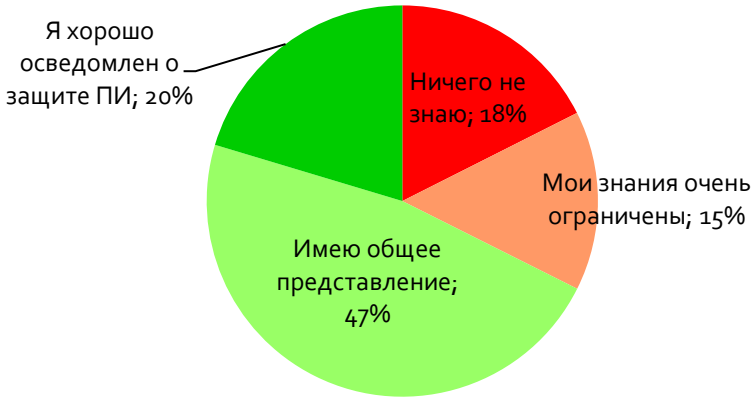


Чтобы объяснить это наблюдение, следует обратиться к результатам прошлогоднего исследования. Тогда фокус-групповые дискуссии показали, что для пользователей интернета безопасность персональных данных воспринимается, прежде всего, с точки зрения безопасности и сохранности банковских счетов, сбережений, имущества. Логично было бы предположить, что студенты и пенсионеры, которых традиционно принято относить к наименее обеспеченным слоям населения, меньше беспокоятся о безопасности персональных данных именно в силу отсутствия больших банковских счетов и сбережений.

Только один из пяти (20%) опрошенных считает, что хорошо осведомлен о защите персональных данных.

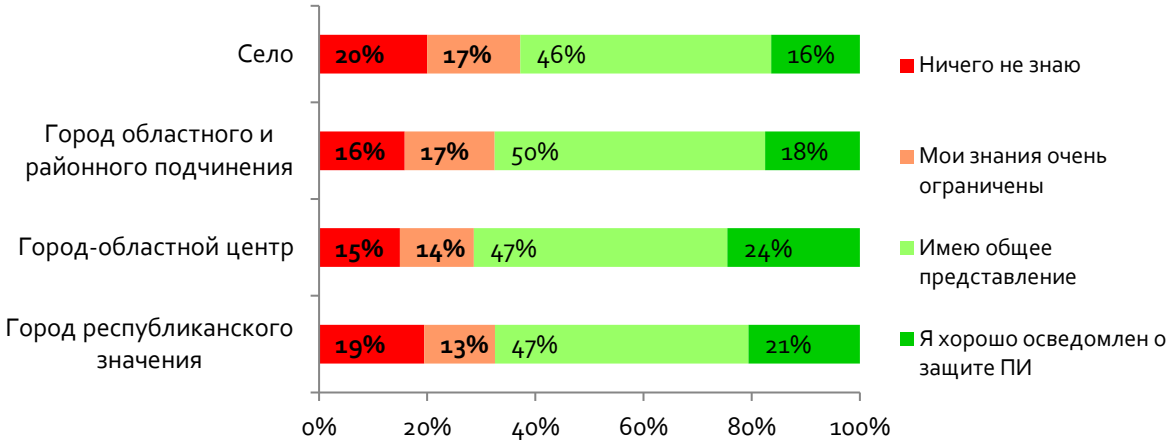
Следующий вопрос касался оценки собственного уровня осведомленности о защите персональной информации. Треть (33%) всех опрошенных заявили, что либо их знания сильно ограничены (15%), либо они ничего не знают (18%). Лишь 20% опрошенных считают, что хорошо осведомлены о защите персональных данных. Основная же масса (47%) респондентов выбрали ответ «имею общее представление». Таким образом, **уровень осведомленности о защите персональной информации среди казахстанцев, активно пользующихся интернетом, следует считать очень низким**.

Рисунок 10. Как бы Вы оценили свои знания о защите персональной информации, которую предоставляете онлайн? (N=1503, все респонденты)



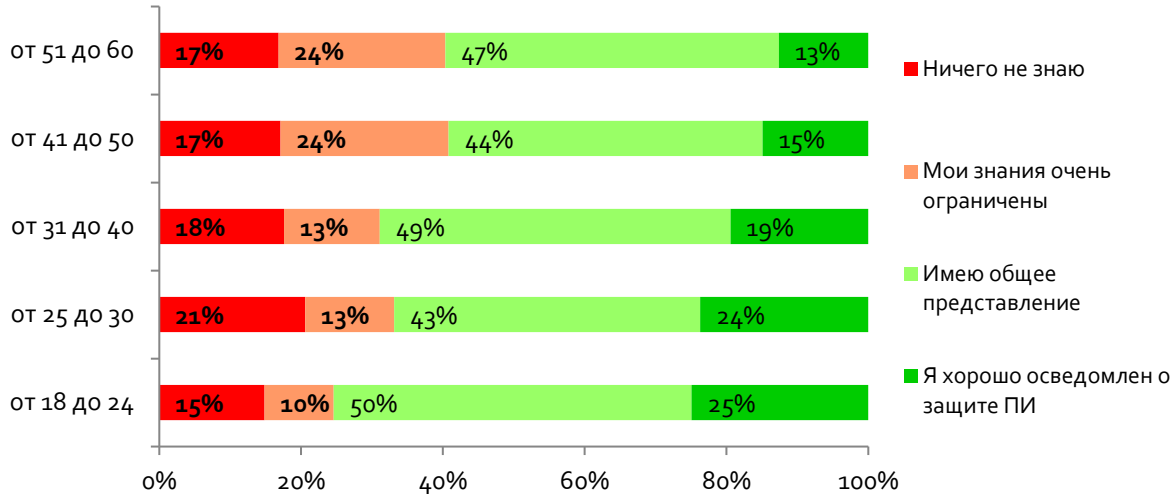
Распределение ответов на данный вопрос в разных типах поселений имеет несущественные и вполне ожидаемые различия, к примеру, **сельские жители обнаружили наименьший уровень осведомленности.**

Рисунок 11. Как бы Вы оценили свои знания о защите персональной информации (ПИ), которую предоставляете онлайн? (N=1503, все респонденты)



Возраст, напротив, как и ожидалось, отражается в уровне осведомленности о защите персональной информации. Как видно на приведенной ниже диаграмме, чем старше возраст респондента, тем меньше вероятность того, что он причислит себя к хорошо осведомленным. Вероятно, старшее поколение просто менее активно пользуется интернетом и не чувствуют потребности в таких знаниях.

Рисунок 12. Как бы Вы оценили свои знания о защите персональной информации (ПИ), которую предоставляете онлайн? (N=1503, все респонденты)

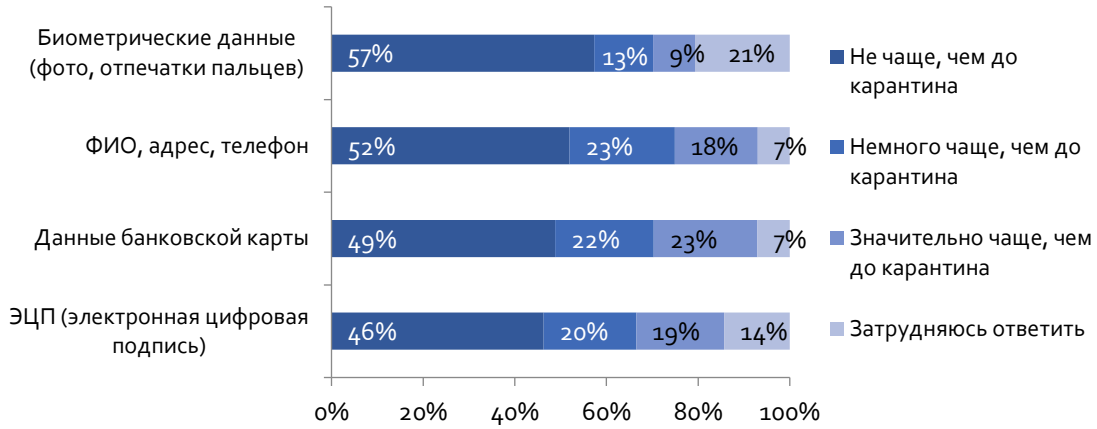


До 44% опрошенных заявило, что стали чаще предоставлять свои персональные данные онлайн за время карантина.

Как известно, во время карантина, введенного во время пандемии COVID-19, люди стали больше пользоваться интернетом, что в свою очередь должно было сказаться на частоте предоставления персональной информации. Для оценки масштаба влияния карантинных мер в анкету был включен соответствующий вопрос.

Согласно полученным данным, за время карантина 44% респондентов стали чаще предоставлять данные своей банковской карты. Почти столько же (41%) респондентов стали чаще предоставлять свои имя, адрес и телефон. **39% опрошенных во время карантина предоставляли электронную цифровую подпись чаще, чем до пандемии**. И наконец, **каждый пятый (22%) респондент во время карантина чаще предоставлял свои биометрические данные.**

Рисунок 13. Можете ли вы сказать про себя, что за время карантина стали чаще предоставлять перечисленные ниже виды персональной информации о себе? (N=1503, все респонденты)

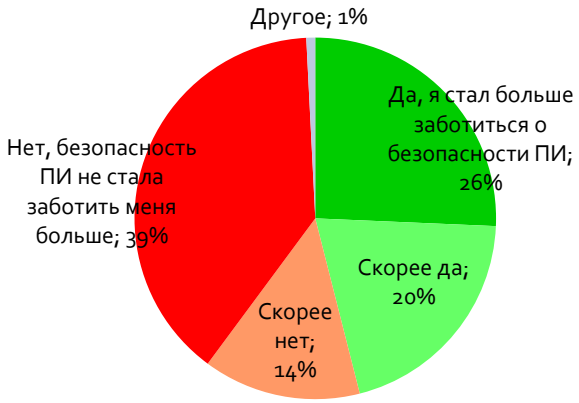


Немногим менее половины (46%) респондентов заявило, что за время карантина стали больше заботиться о безопасности персональной информации.

Если карантинные меры явно отразились на частоте предоставления персональной информации онлайн, то за этим логично следует другой вопрос: как это повлияло на обеспокоенность пользователей интернета вопросами безопасности персональных данных?

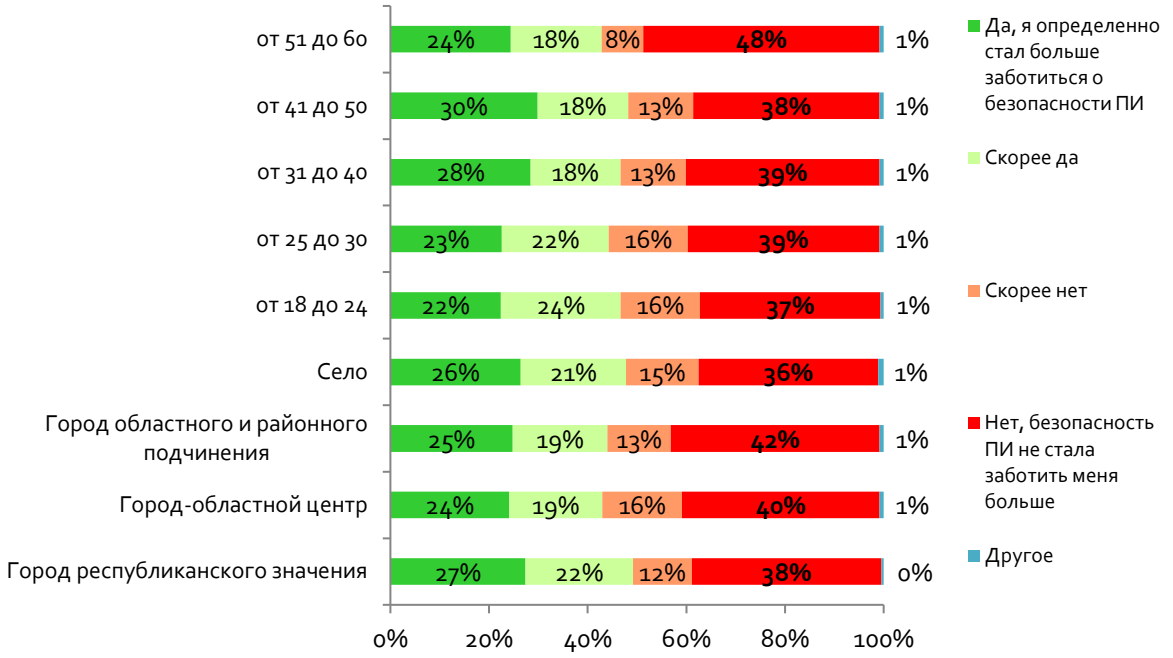
46% опрошенных заявило, что за время карантина стали больше заботиться и думать о безопасности персональной информации, которую предоставляют онлайн. При этом 53% выбрали противоположные варианты ответа: 39% - безопасность персональных данных не стала заботить больше, 14% - скорее нет.

Рисунок 14. Можете ли Вы сказать, что за время карантина Вы стали больше заботиться/думать о безопасности своей персональной информации (ПИ), которую предоставляете онлайн? (N=1503, все респонденты)



Примерно одинаковое распределение ответов на этот вопрос наблюдается во всех типах поселений и возрастных группах, с небольшим преобладанием возрастных групп 31-40 и 41-50 лет (28% и 30% соответственно).

Рисунок 15. Можете ли Вы сказать, что за время карантина Вы стали больше заботиться и думать о безопасности своей персональной информации (ПИ), которую предоставляете онлайн? (N=1503, все респонденты)



Почти половина (48%) из числа тех, кто за время карантина стали больше беспокоиться о безопасности персональной информации, бояться стать жертвой мошенничества.

Тем респондентам, отметившим, что за время карантина стали больше заботиться и думать о безопасности своей персональной информации, которую предоставляют онлайн, был задан вопрос о том, какие именно угрозы их беспокоят. Почти половина (48%) этих респондентов бояться стать жертвой мошенничества. То есть больше всего людей беспокоит сохранность своих банковских счетов, сбережений, имущества.

Далее по частоте упоминания следуют угроза нарушения тайны персональной информации (29%) и нежелательная реклама, спам (16%). **Стремление государственных органов собирать все больше личной информации о гражданах волнует только 7% респондентов**, ответивших на этот вопрос.

Следует также отметить, что большая доля (23%) респондентов затруднилась назвать, какие именно угрозы безопасности персональной информации их беспокоит. Возможно, это связано с ограниченными представлениями о безопасности персональных данных в целом.

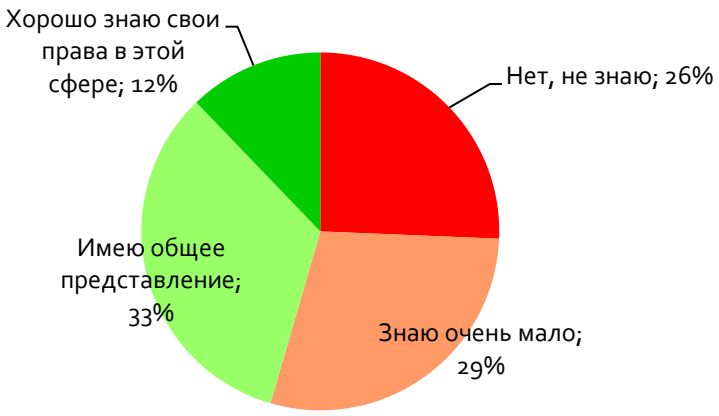
Рисунок 16. Какие именно вопросы, связанные с безопасностью персональной информации (ПИ), стали больше беспокоить Вас за время карантина? (N=703, респонденты, которых безопасность ПИ стала беспокоить больше за время карантина)

Лишь 12% опрошенных смогли сказать, что хорошо знают свои права в сфере защиты персональных данных, предоставляемых онлайн.

Одной из основных характеристик культуры использования интернета в стране является уровень знаний пользователей всемирной сети о своих правах в сфере защиты персональных данных. Фокус-групповые дискуссии, проведенные в 2019 году, с большой уверенностью предполагают, что только небольшая доля казахстанцев, пользующихся интернетом, знают свои права. Результаты данного опроса полностью подтвердили наблюдения, собранные год назад.

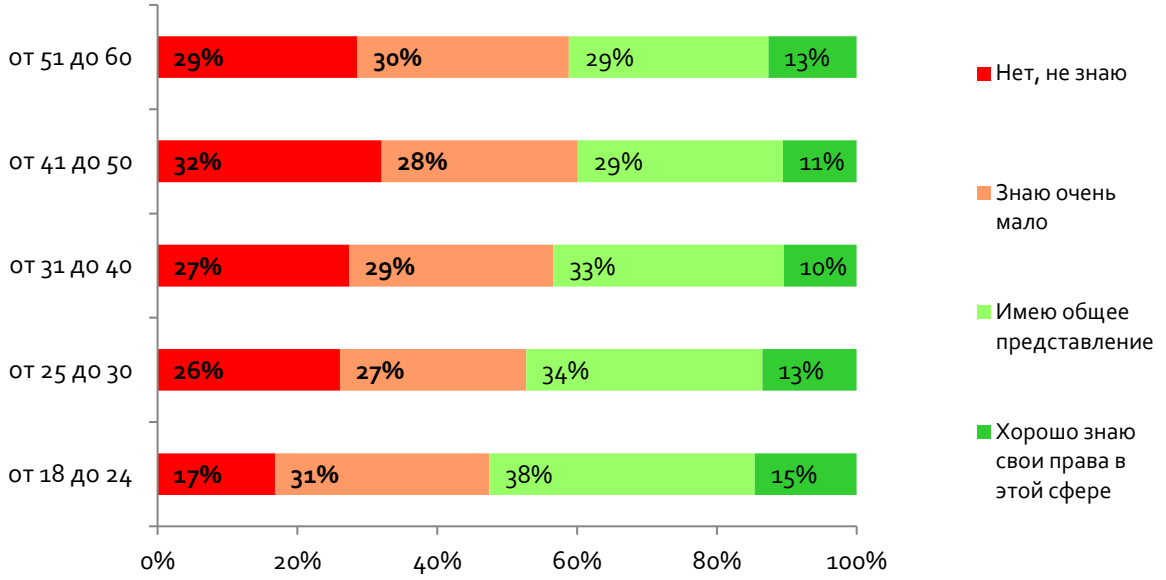
Лишь 12% опрошенных смогли сказать, что хорошо знают свои права в сфере защиты персональных данных, предоставляемых онлайн. Большинство же (54%) респондентов либо не знают свои права (26%), либо знают очень мало (29%).

Рисунок 17. Знаете ли Вы свои права в сфере защиты персональной информации, которую предоставляете онлайн? (N=1503, все респонденты)



Во всех типах поселений наблюдается примерно одинаковое распределение ответов. Среди возрастных групп выделяются самые молодые пользователи интернета, от 18 до 24 лет, где суммарная доля положительных ответов («Хорошо знаю свои права в этой сфере», «Имею общее представление») составила большинство – 52% (15% и 38%, соответственно). Таким образом, **молодое поколение еще раз продемонстрировало признаки более высокой культуры пользования интернетом**.

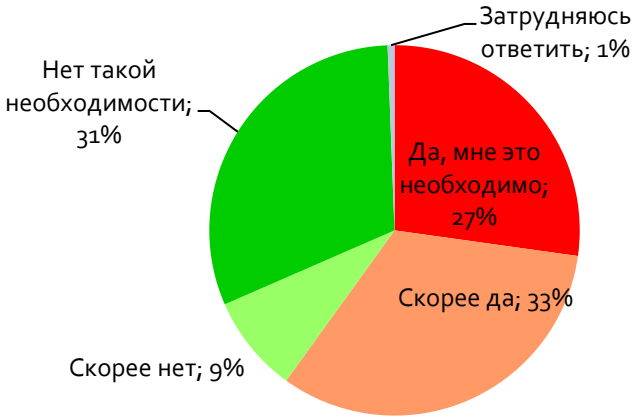
Рисунок 18. Знаете ли Вы свои права в сфере защиты персональной информации, которую предоставляете онлайн? (N=1503, все респонденты)



60% опрошенных чувствуют необходимость в знаниях о своих правах в сфере защиты персональных данных.

С прикладной точки зрения также интересно было узнать, чувствуют ли пользователи интернета необходимость в знаниях о своих правах в сфере защиты персональной информации. Абсолютное большинство (60%) респондентов ответили положительно.

Рисунок 19. Чувствуете ли Вы необходимость узнать больше о защите персональной информации и своих правах в этой сфере? (N=1503, все респонденты)



Таким образом, результаты проведенного опроса во многом подтвердили наблюдения, сделанные в ходе фокус-групповых дискуссий, в том числе о том, что **уровень знаний активно пользующихся интернетом казахстанцев о защите персональной информации очень низок**. Лишь один из десяти (12%) опрошенных смог сказать, что хорошо знает свои права в сфере защиты персональной информации.

3.3. Отношение к государственным инициативам в сфере сбора и использования персональных данных

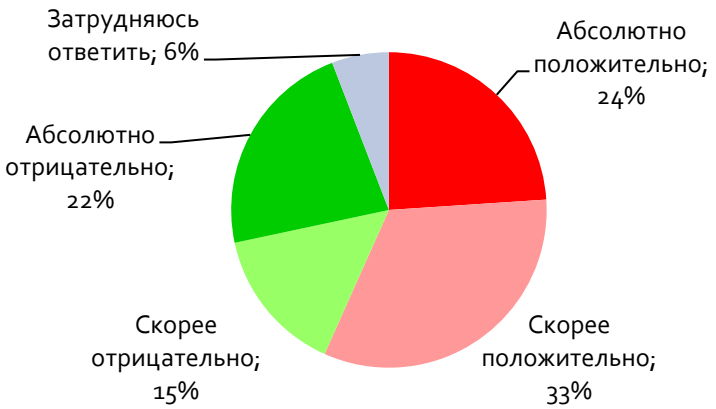
Вторая часть интервью касалась вопросов восприятия государственной политики в сфере сбора и использования персональных данных. Именно этот круг вопросов вызвал наиболее горячие споры в ходе фокус-групповых дискуссий исследования 2019 года, поэтому было особенно интересно узнать, как разделятся мнения в опросе с репрезентативной выборкой.

Первый вопрос этой части интервью касался отношения к инициативе правительства по внедрению так называемой «Национальной системы видеомониторинга», которая позволяла бы посредством камер наружного наблюдения распознавать лица, обрабатывать и хранить данные.

По меньшей мере каждый третий (37%) опрошенный выразил свое отрицательное отношение к планам правительства по внедрению «Национальной системы мониторинга».

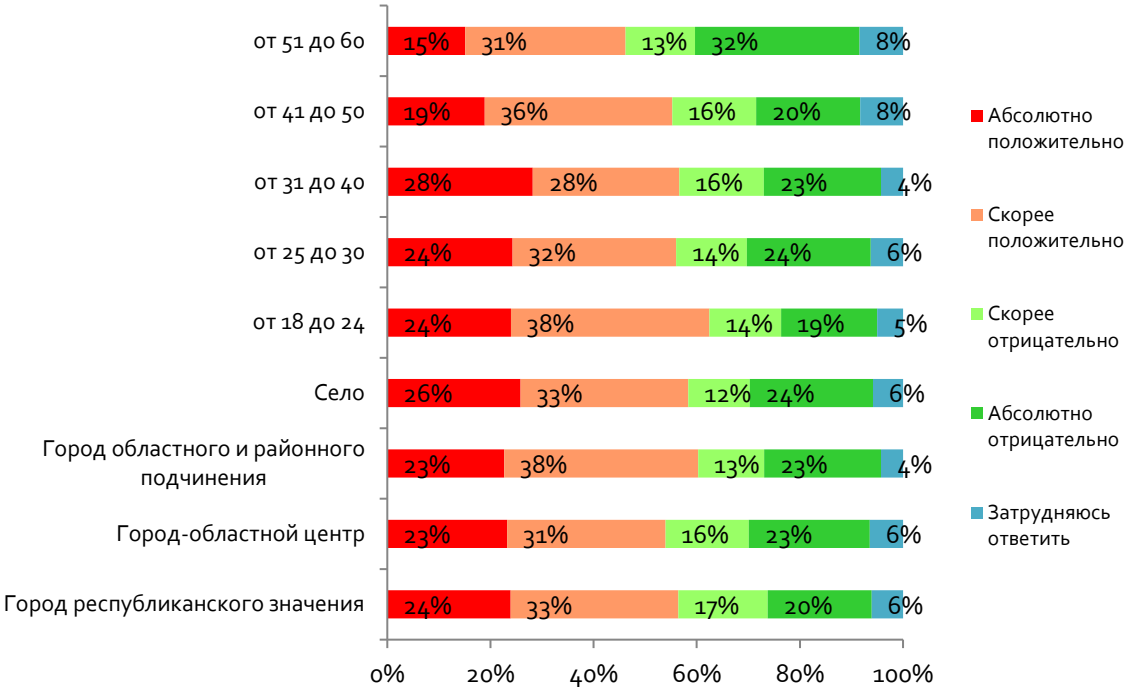
Хотя абсолютное большинство (57%) опрошенных положительно относится к данной инициативе, доля тех, кто выразил отрицательное отношение, значительна – 37%. В том числе каждый пятый респондент (22%) выбрал вариант ответа «абсолютно отрицательно».

Рисунок 20. Правительство Казахстана планирует внедрить «Национальную систему видеомониторинга» - систему распознавания лиц, обработки и хранения данных, полученных с камер наружного наблюдения (например, с камер «Сергек»). Как Вы к этому относитесь? (N=1503, все респонденты)



Если сравнить распределение ответов на этот вопрос в разных типах поселений и возрастных группах, то видно, что в первом случае наблюдается одинаковая картина во всех группах, тогда как в последнем – можно увидеть заметные различия. В частности, среди респондентов самой старшей группы доля отрицательных ответов достигает 45%, то есть почти половина опрошенных из этой возрастной группы не поддерживает инициативу внедрения «Национальной системы видеомониторинга». Более того, каждый третий (32%) в этой группе выразил крайне отрицательное отношение. В самой молодой группе, напротив, сильнее преобладает положительное отношение – 62% высказались в поддержку инициативы.

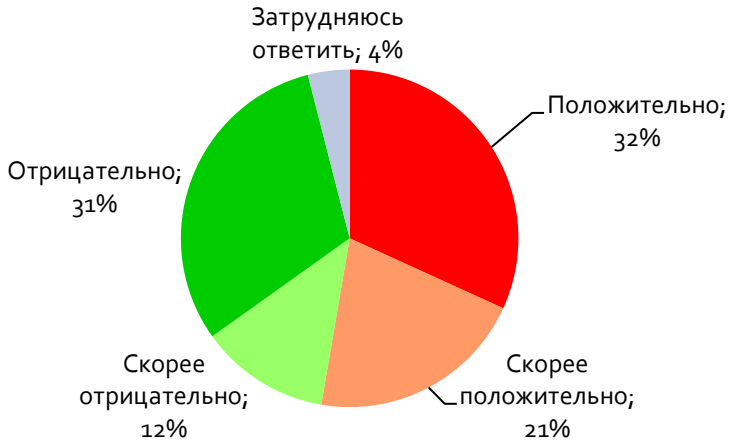
Рисунок 21. Правительство Казахстана планирует внедрить «Национальную систему видеомониторинга» - систему распознавания лиц, обработки и хранения данных, полученных с камер наружного наблюдения (например, с камер «Сергек»). Как Вы к этому относитесь? (N=1503, все респонденты)



Хотя доля тех, кто высказался в поддержку намерений правительства собирать все больше биометрических данных, составила абсолютное большинство (53%), их перевес нельзя назвать большим - 43% респондентов высказали свое отрицательное отношение.

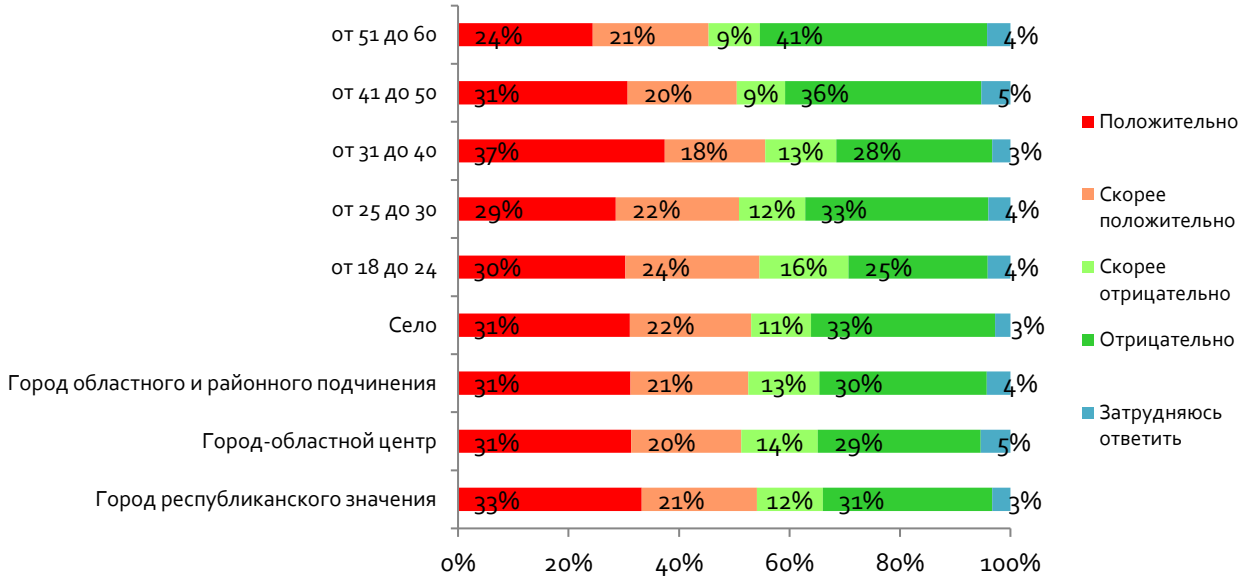
Далее задавался вопрос о намерении правительства собирать больше биометрических данных граждан. Здесь также преобладает положительное отношение – 53% выбрали положительный ответ, но в то же время доля респондентов, относящихся отрицательно, больше, чем в предыдущем вопросе, – 43%. Иными словами, ответы на этот вопрос распределились более равномерно.

Рисунок 22. Также в рамках программы «Цифровой Казахстан» правительство страны намерено начать собирать биометрические данные граждан, например отпечатки пальцев. Как вы относитесь к данной инициативе? (N=1503, все респонденты)



Так же, как и в предыдущем вопросе между типами поселений не наблюдается большой разницы, а в возрастных группах можно увидеть отличие самых взрослых респондентов от всех остальных возрастных групп. Так, в группе от 51 до 60 лет доля тех, кто выразил отрицательное отношение к названной инициативе правительства, составила половину всех опрошенных – 50%. В том числе 41% респондентов выбрал однозначно отрицательный ответ.

Рисунок 23. Также в рамках программы «Цифровой Казахстан» правительство страны намерено начать собирать биометрические данные граждан, например отпечатки пальцев. Как вы относитесь к данной инициативе? (N=1503, все респонденты)



Фокус-групповые дискуссии, проведенные осенью 2019 года, позволили выделить и сформулировать несколько основных точек зрения в отношении государственной политики в сфере сбора и использования персональных данных граждан. Тогда с участниками фокус-групп обсуждалась тема тестирования так называемого «сертификата

безопасности» как примера возможных будущих правительственных инициатив по сбору и использованию персональных данных.

Приведем цитату из отчета о результатах фокус-групповых дискуссий: «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».

Для количественной оценки уровня поддержки каждой из этих точек зрения в рамках данного опроса респондентам было предложено выразить свое отношение к каждому из трех высказываний:

a) «Если такие системы повысят безопасность в стране, то я не против сбора и хранения моей персональной информации, в том числе через камеры наружного видеонаблюдения».

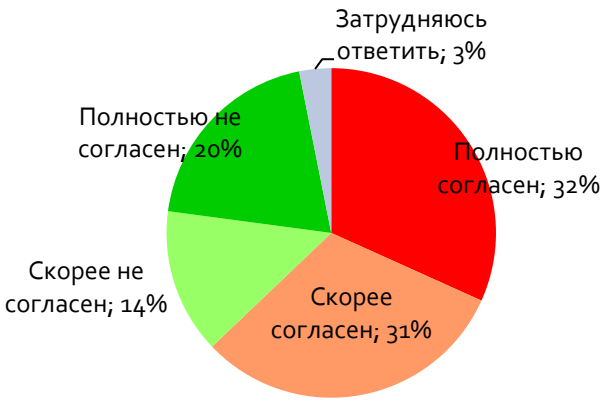
b) «Меня настораживает стремление власти собирать все больше и больше личных данных граждан, это похоже на тотальную слежку».

c) «У людей нет выбора, власти все равно сделают то, что хотят».

63% респондентов не против сбора и использования их персональной информации, в том числе через камеры наружного видеонаблюдения, ради повышения безопасности в стране.

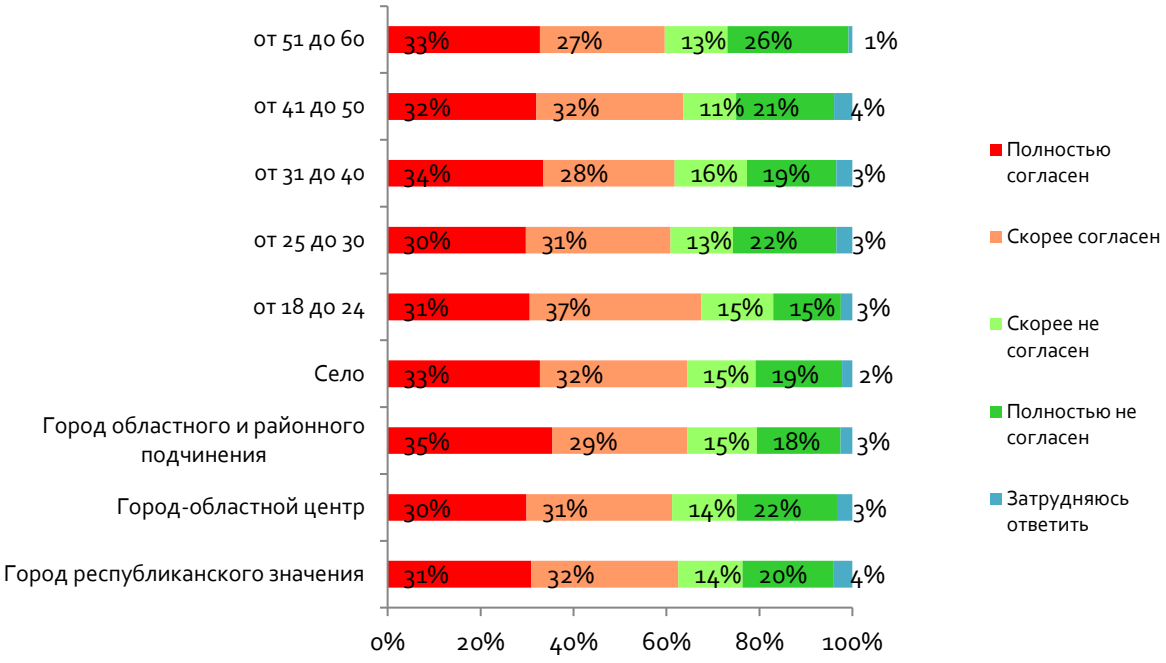
Судя по результатам опроса, среди активных пользователей интернета с большим перевесом преобладают те, кто не возражает против сбора и использования персональной информации государственными органами через камеры наружного наблюдения ради повышения безопасности в стране. Такой точки зрения придерживается 63% опрошенных. Противоположной точки зрения придерживается 34% респондентов.

Рисунок 24. Насколько вы согласны: «Если такие системы повысят безопасность в стране, то я не против сбора и хранения моей персональной информации, в том числе через камеры наружного видеонаблюдения»? (N=1503, все респонденты)



Сравнение распределения ответов на этот вопрос в разных типах поселений и возрастных группах не обнаружило серьезных различий. Во всех группах наблюдаются схожие доли согласных и несогласных.

Рисунок 25. Насколько вы согласны: «Если такие системы повысят безопасность в стране, то я не против сбора и хранения моей персональной информации, в том числе через камеры наружного видеонаблюдения? (N=1503, все респонденты)

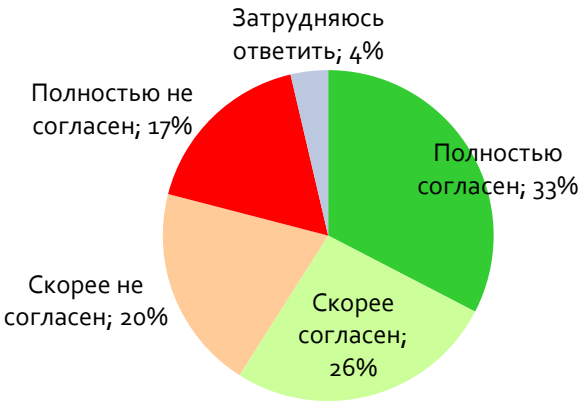


В то же время 59% опрошенных выразили свою настороженность по поводу стремления власти собирать все больше личных данных граждан.

Распределение ответов на второе высказывание может показаться противоречащим ответам на первое. Стремление власти собирать все больше личных данных настораживает 59% респондентов. Несогласие с таким высказыванием выразили 37% опрошенных.

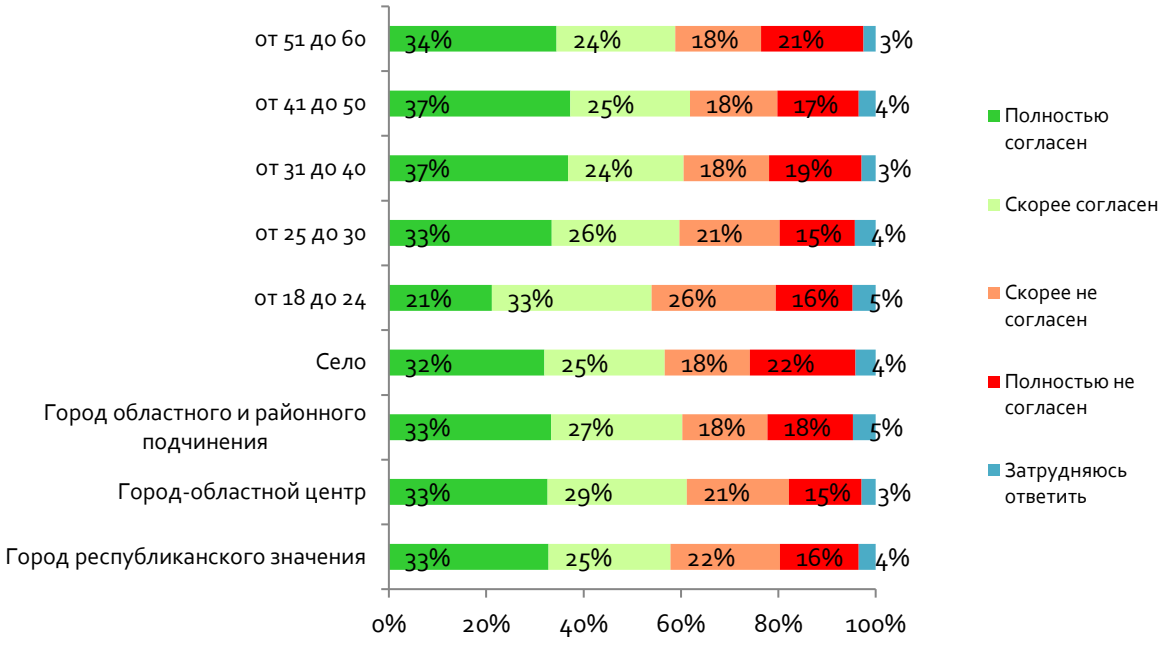
Возможно, объяснение противоречия между восприятием первого высказывания и второго следует искать в представлениях людей о тайне личной жизни, а также компетенциях и полномочиях государственных органов. Восприятие предложенных высказываний еще раз подтверждает наблюдения, собранные в фокус-групповых дискуссиях: в казахстанском обществе представления о том, где пролегает черта между тайной личной жизни и интересами государства пусть даже во имя общественной или национальной безопасности могут сильно различаться.

Рисунок 26. Насколько вы согласны: «Меня настораживает стремление власти собирать все больше и больше личных данных граждан, это похоже на тотальную слежку»? (N=1503, все респонденты)



Интересно, что в этом вопросе так же, как и в предыдущем, выделяется самая молодая группа респондентов – здесь доля согласных с предложенным утверждением заметно меньше, чем в других группах (53%). Иными словами, самых молодых респондентов стремление власти собирать все больше личных данных граждан настораживает в меньшей степени.

Рисунок 27. Насколько вы согласны: «Меня настораживает стремление власти собирать все больше и больше личных данных граждан, это похоже на тотальную слежку»? (N=1503, все респонденты)



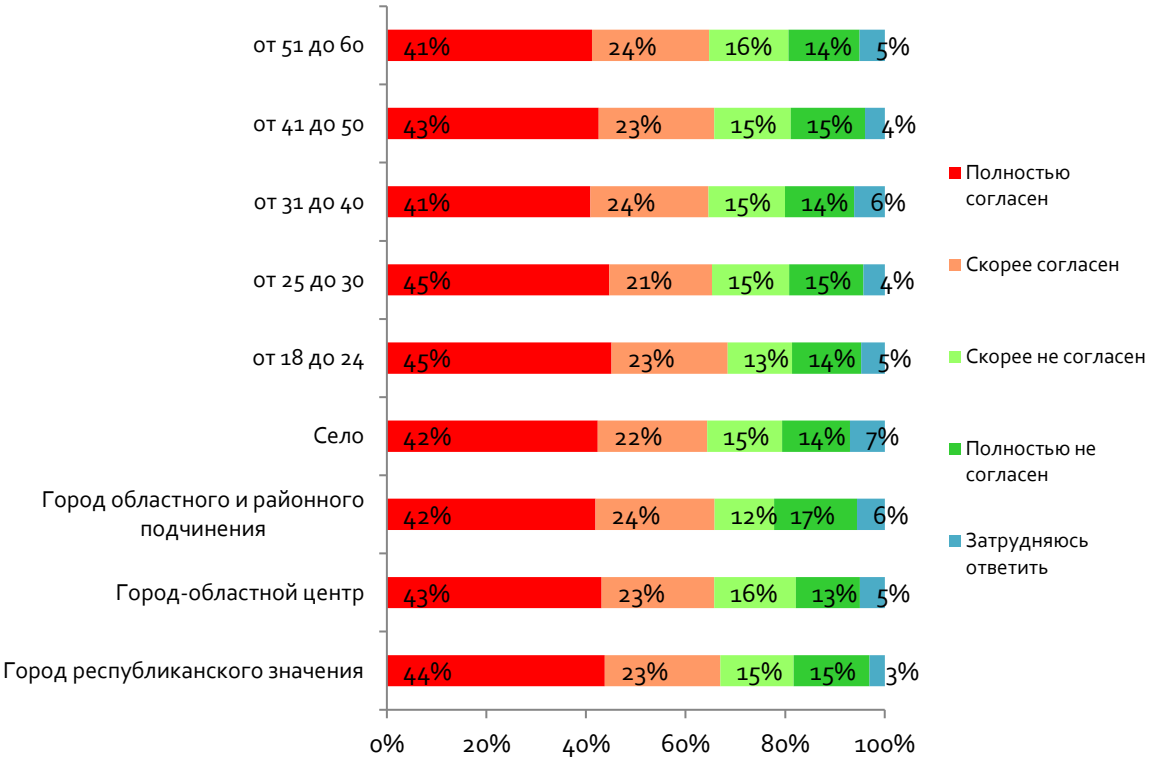
Двое из троих (66%) опрошенных считают, что «у людей нет выбора, власти все равно сделают то, что хотят».

В отношении третьего из предложенных высказываний мнения распределились примерно в той же пропорции. 66% опрошенных высказали свое согласие с тем, что «у людей нет выбора, и власти все равно сделают то, что хотят». Противоположной точки зрения придерживаются 29% опрошенных.

Рисунок 28. Насколько Вы согласны: «У людей нет выбора, власти все равно сделают то, что хотят»? (N=1503, все респонденты)

Как видно из приведенной ниже диаграммы, во всех типах поселений и возрастных группах наблюдается одинаковое распределение ответов на данный вопрос.

Рисунок 1. Насколько Вы согласны: «У людей нет выбора, власти все равно сделают то, что хотят»? (N=1503, все респонденты)



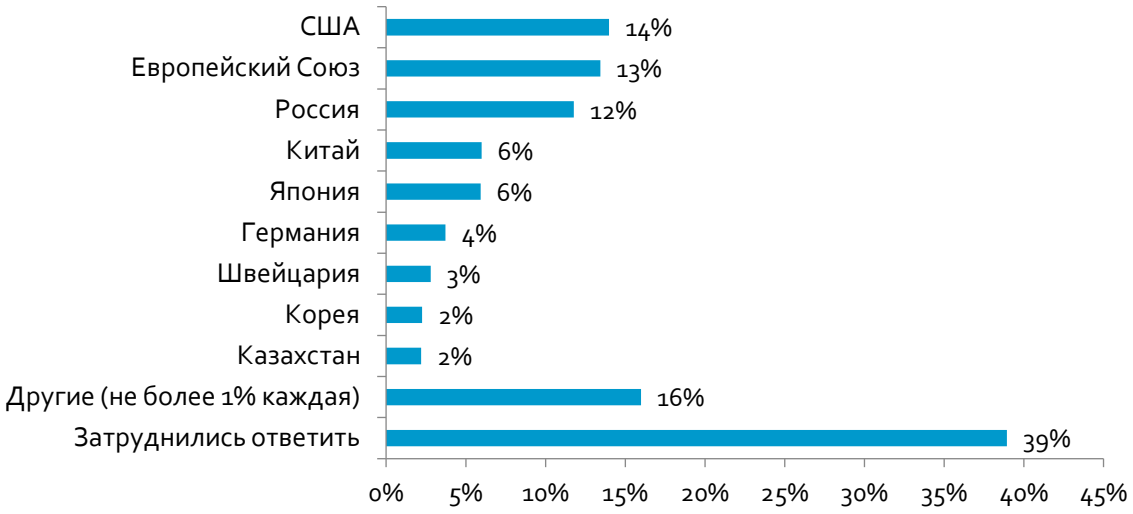
Наконец, интервью завершались вопросами о том, на какие страны следовало и не следовало бы ориентироваться Казахстану в политике защиты персональных данных. Ориентир на определенные страны с их сложившимся имиджем и декларируемыми ценностями является в каком-то смысле проекцией взглядов и представлений людей о том, какой должна быть политика правительства в данной сфере.

Наиболее привлекательным примером, на который следовало бы ориентироваться в выборе политики в сфере защиты персональных данных, по мнению респондентов, является Европейский Союз, который собрал 13% положительных оценок и только 1% - негативных. Лидером отрицательного рейтинга стал Китай – его отметил почти каждый пятый опрошенный.

В этих вопросах фиксировались спонтанные ответы респондентов, то есть варианты ответов не зачитывались. Распределение ответов на первый вопрос (на какие страны СЛЕДУЕТ ориентироваться) не позволяет выделить какую-либо одну страны в качестве безоговорочного лидера. Близкими по количеству полученных голосов стали США (отметило 14% респондентов), Европейский Союз (13%), Россия (12%). За ними следуют с равным количеством голосов Китай и Япония – обе страны получили 6% ответов респондентов.

Здесь также следует отметить, что чаще всего респонденты затруднялись ответить на этот вопрос (39%), что напрямую связано с продемонстрированными выше скудными знаниями и ограниченными представлениями по теме защиты персональных данных.

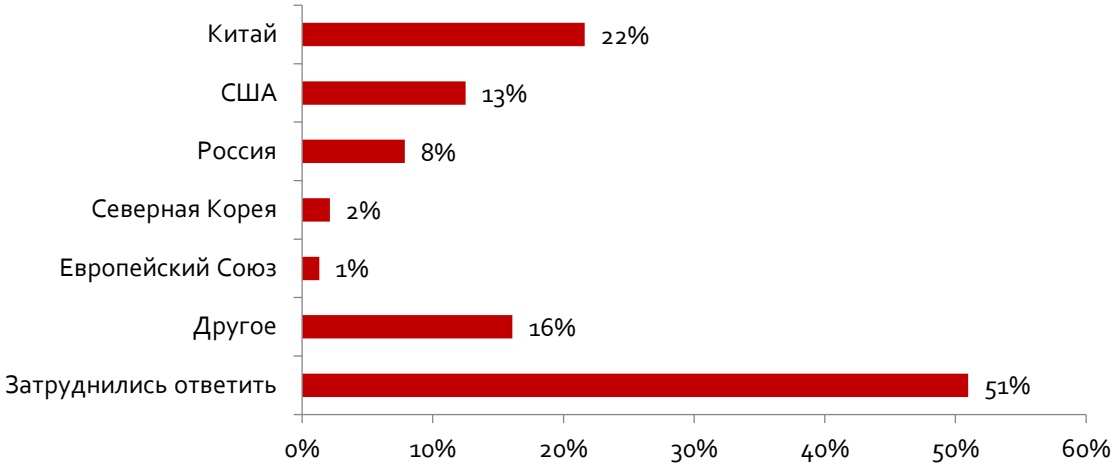
Рисунок 30. Как Вы считаете, на какие страны следует ориентироваться Казахстану в сфере защиты персональных данных граждан? (N=1503, все респонденты)



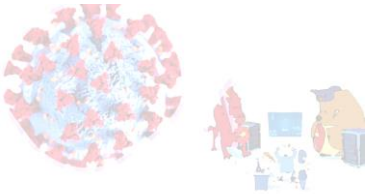
Во втором вопросе (на какие страны НЕ СЛЕДУЕТ ориентироваться) распределение ответов не было таким равномерным, как в первом вопросе. **Лидером отрицательного**

рейтинга стал Китай – его отметило 22% опрошенных. Далее следуют США (13%) и Россия (8%). Европейский Союз в этом вопросе назвали только 1% респондентов.

Рисунок 31. Как Вы считаете, опыт каких стран НЕ СЛЕДУЕТ перенимать и внедрять в Казахстане в сфере защиты персональных данных? (N=1503, все респонденты)



Если соотнести ответы на оба вопрос, то можно заключить, что наиболее привлекательным примером для казахстанцев является Европейский Союз, который собрал 13% положительных оценок и только 1% - негативных. Наименее привлекательным примером опрошенные считают Китай – 6% положительных оценок и 22% - отрицательных.



Выводы и рекомендации

После проведенных в 2019 году фокус-групповых дискуссий по оценке ситуации с персональными данными и их статусом результаты опроса в масштабах страны в период пандемии не стали неожиданными. К примеру, подтвердилось предположение о том, что совсем небольшая доля активных пользователей интернета хорошо осведомлена о защите персональных данных: только каждый пятый опрошенный был уверен в своих знаниях в этой области.

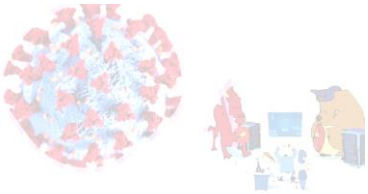
Почти половину респондентов в той или иной мере беспокоит безопасность персональных данных, предоставляемых онлайн, но при этом опрос зафиксировал крайне низкий уровень осведомленности о правах в сфере защиты персональных данных – только один из десяти опрошенных смог сказать, что хорошо знает свои права. Наиболее низкий уровень знаний о защите персональных данных наблюдается среди самых старших пользователей интернета, а также среди сельских жителей.

Карантинные меры, принятые во время пандемии COVID-19, сыграли очень большую роль в развитии культуры обращения с персональной информацией, поскольку в это время люди стали значительно больше пользоваться интернетом и, как следствие, чаще предоставлять свои персональные данные онлайн. Почти половина опрошенных заявила, что за время карантина стали больше думать о безопасности персональных данных, которые предоставляют онлайн: они боятся стать жертвами мошенников.

Хотя вопросы об оценке правительственных инициатив в сфере сбора и использования персональных данных продемонстрировали преобладание поддержки, есть основания полагать, что мнения в обществе разделились так, что ни одна из сторон не имеет подавляющего преимущества. И даже несмотря на низкий уровень знаний настороженное отношение к инициативам правительства распространено достаточно широко.

Так же, как и фокус-групповые дискуссии в 2019 году, в 2020 году культура защиты персональных данных, предоставляемых в сети интернет, еще только начинает входить в жизнь казахстанцев. Развитие этой сферы жизни общества находится на своей ранней стадии, а пандемия COVID-19 и карантинные меры послужили сильным катализатором этого процесса. И, как все новое, этот процесс требует внимательного, глубокого и систематического изучения.

На момент проведения исследования и написания отчета трудно было предвидеть, когда и, если все вернется к привычному «нормальному» состоянию. Когда влияние COVID-19 на приватность, конфиденциальность и защиту личных данных впервые стало проявляться, эксперты по приватности в Европе негласно осудили неизбежность внедрения «Большого брата», который является результатом некоего компромисса между приватностью, конфиденциальностью и здоровьем. Эти опасения не переоценили потенциальные последствия этого катастрофического события, однако недооценили силу и эффективность европейского режима защиты данных. GDPR, его принципы и



обязательства прошли первое серьезное испытание за свое недолгое существование, продемонстрировав миру, как высокие стандарты приватности и конфиденциальности могут поддерживаться даже в чрезвычайных обстоятельствах.

С одной стороны, надзорные органы предоставили полезные рекомендации относительно разработки и внедрения инвазивных мер, используемых для смягчения последствий пандемии. С другой стороны, предприятия и организации фиксировали, что соблюдение требований GDPR, связанных с безопасностью, уже обеспечило необходимые технические и организационные меры для борьбы с ростом киберпреступности во время пандемии.

***

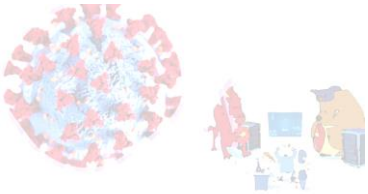
Для Казахстана разработка собственного регламента по защите персональных данных в условиях COVID-19 обретает еще большую актуальность и важность. Безусловно, пандемия внесла свои корректировки в реализацию намеченных планов по массовой цифровизации страны и продвижению идей по защите персональных данных. Создание уполномоченного органа стало первым шагом на пути к тому, чтобы мониторить ситуацию и положение дел, а также способствовать тому, чтобы законодательство в сфере защиты персональных данных соблюдалось всеми неукоснительно – как чиновниками, так и активными гражданами – в каждом конкретном случае без исключения.

Одним из главных итогов цифрового следа COVID-19 стало безусловное следование глобальным трендам на ограничение прав и свобод граждан в ответ на вызовы пандемии и, как следствие, рост киберпреступлений и мошенничества. Вынужденный массовый выход казахстанцев в онлайн пространство в 2020 году привел к увеличению в два раза числа случаев интернет-мошенничества (с 7,700 до 14,100), мошенничества с использованием платежных карт (с 66 до 468) и мошенничества в сфере кредитования (с 6 до 9)[132]. Поэтому киберграмотность и кибергигиена должны стать неотъемлемой частью кампании по продвижению культуры защиты персональных данных в Казахстане.

Другим интересным наблюдением стало усиление социального разрыва между городской и сельской средой и, как следствие, разные возможности и бенефиты от реализуемых программ и инициатив по цифровизации страны. Всемирный банк уже писал о том, что сейчас «в стране сосуществуют четыре Казахстана» - разные уровни доходов, показатели рождаемости и продолжительности жизни: «…по уровню доходов существует четырехкратная разница между регионами с высокими и низкими показателями, по рождаемости север страны можно сравнить с Европой, в то время как юг отражает тенденции стран с низкими доходами, а северо-запад Казахстана по продолжительности жизни схож со странами Африки»[133]. Очевидно, что достаточно противоречивое

[132] https://kursiv.kz/news/finansy/2021-01/v-kazakhstane-vyroslo-chislo-sluchaev-internet-moshennichestva.

[133] Жан-Франса Марто, “Пандемия и образование в Казахстане: Серьезные потери и увеличение неравенства,” World bank, November 16, 2020, Пандемия и образование в Казахстане: Серьезные потери и увеличение неравенства (worldbank.org).



отношение к цифровым инициативам правительства и неоднозначным оценкам важности продвижения культуры защиты персональных данных обусловлено крайне сильной фрагментацией казахстанского общества. Вместе с тем *опрос общественного мнения четко показал, что Казахстану следует двигаться в направлении европейской модели защиты персональных данных, а не китайской.*

i. Комитет информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан может вполне в перспективе усилить взаимодействие с зарубежными аналогичными ведомствами и специализированными органами по многим направлениям, чтобы стать кузницей национальных «кибердипломатов» во всех государственных органах страны. Кроме того, важно, чтобы профильный орган обладал необходимыми координирующими функциями, чтобы собирать все государственные органы для решения различных вопросов, в том числе на регулярной основе, и формировать цифровую повестку в стране с учетом рисков для архитектуры приватности и персональных данных.

ii. Рекомендация по закону о персональных данных и их защите, обозначенная в докладе 2019 года[134], не просто сохраняет свою актуальность, но и получает особое положение в создании работающего регламента по защите персональных данных. Ожидаемая карательная практика пока еще не нашла своего применения. Наоборот, у профильного Агентства функции контроля за применением законов о защите персональных данных и соблюдением требований по защите персональных данных существенно ограничены – никто не понес ответственность за утечки данных в системе Damumed и из других государственных баз данных. Все это не позволяет решать системные проблемы, откладывая решение наиболее важных проблем на более поздний срок - обучение кадров, создание правовой и информационной культуры, прежде всего, у себя дома (т.е. во всем государственном аппарате). Увольнение не может оставаться способом наказания за нарушение законодательства, потому что оно определяет четкие механизмы привлечения к ответственности. Поскольку персональные данные подлежат защите и ее гарантом выступает государство, это означает, что все без исключения должны соответствовать выработанным техническим и юридическим параметрам.

iii. Разработанный SWOT-анализ защиты персональных данных в Казахстане в 2019 году заметно не изменился и остается актуальным по сей день.

	Helpful	Harmful

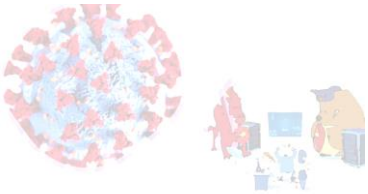
[134] Гусарова Анна, Джаксылыков Серик, «Защита персональных данных в Казахстане: статус, риски и возможности», 2020, Алматы, ЗащитА персональных данных в казахстане: статус, риски и возможности (soros.kz).; Cyber Security and Cyber Hygiene. Data Protection (caiss.expert).

	to Achieving the Objective	*to Achieving the Objective*
Internal Origin *(attributes of the organization)*	**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 *(attributes to the environment)*	**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 внедрение опыта с Китаем и Россией

Одним из интересным наблюдений в ходе сравнения результатов фокус-групповых дискуссий 2019 года и национального опроса 2020 года стало отношение к роли государства. Если в 2019 году мы отмечали глубокую веру в теории заговоров и объяснение происходящего слежкой и прослушкой силовых структур, то в 2020 году опрос общественного мнения зафиксировал некую безнадежность с точки зрения того, что «власти все равно сделают то, что захотят», несмотря на достаточно противоречивую поддержку национальных цифровых инициатив, и усилившуюся настороженность и опасность стать жертвой мошенничества.

iv. Инициативы по внедрению технологии искусственного интеллекта, системы распознавания лиц и других технологический решений должны учитывать риски, связанные с предоставлением, сбором, анализом и хранением персональных данных. Прозрачность таких процессов позволит заметно минимизировать потенциальные уязвимости, адекватно реагировать на кризисные ситуации и усиливать киберустойчивость казахстанской системы.

v. Профильному агентству необходимо разработать регламент по инцидентах утечки данных и неавторизованном доступе к персональным данным. Об этих случаях должны сообщать организации, в которых подобные кризисные ситуации происходят, а не кто-то другой. Это нормальный стандартный протокол, набор инструментов и практик не только присутствует в европейском GDPR (регламент по защите персональных данных), но и во всех компаниях в мире. Внедрение прозрачных протоколов управления рисками позволит не только усилить компонент по защите систем и персональных данных, но и сократить имеющиеся серые зоны, которые могут использоваться в коррупционных целях и ради шпионажа. Эти практики должны массово внедряться во все государственные органы, работающие с базами данных, не говоря о частном бизнесе.



Приложение 1. Анкета и распределение ответов

S1. Сколько Вам лет? *УКАЖИТЕ И ОТМЕТЬТЕ НУЖНЫЙ ВАРИАНТ ОТВЕТА*

Возраст _____ лет

Меньше 18	1	*ЗАВЕРШИТЕ ИНТЕРВЬЮ*
18 – 24	2	*ПРОДОЛЖАЙТЕ*
25 – 30	3	
31 – 40	4	
41 – 50	5	
51 – 60	6	
61 и старше	7	

S2. Пользуетесь ли Вы электронной почтой или интернет-мессенджерами?

Да	1	*ПРОДОЛЖАЙТЕ*
Нет	2	*ЗАВЕРШИТЕ ИНТЕРВЬЮ*

S3. Есть ли у Вас активный аккаунт в социальных сетях (например, в Facebook, Instagram, VK и т. д.)?

Да	1	*ПРОДОЛЖАЙТЕ*
Нет	2	*ЗАВЕРШИТЕ ИНТЕРВЬЮ*

S4. Совершали ли Вы когда-либо следующие перечисленные действия через Интернет? ЗАЧИТАТЬ ВОЗМОЖНО НЕСКОЛЬКО ОТВЕТОВ

Совершаю заказы или покупки через Интернет (товаров, услуг, билетов, такси и т.д.)	1	*ПРОДОЛЖАЙТЕ*
Совершаю денежные переводы через Интернет	2	*ПРОДОЛЖАЙТЕ*
Получал онлайн-кредиты	3	*ПРОДОЛЖАЙТЕ*
Нет, не совершаю ничего из перечисленного	4	*ЗАВЕРШИТЕ ИНТЕРВЬЮ*

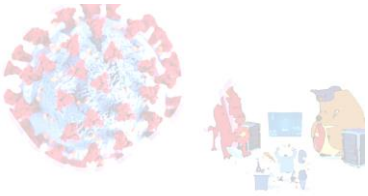
Q1. Насколько Вас беспокоит безопасность Вашей персональной информации, которую вы предоставляете онлайн? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

Очень беспокоит	1
Заметно беспокоит	2
Не очень беспокоит	3
Не беспокоит	4
Затрудняюсь ответить НЕ ЗАЧИТЫВАТЬ	5

Q2. Как бы Вы оценили свои знания о защите персональной информации, которую предоставляете онлайн? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

Ничего не знаю	1
Мои знания очень ограничены	2
Имею общее представление	3
Я хорошо осведомлен о защите персональной информации	4
Другое _____	5

Q3. Во время карантина, введенного во время эпидемии коронавируса, люди стали больше пользоваться Интернетом. Можете ли вы сказать про себя, что за время карантина стали



чаще предоставлять перечисленные ниже виды персональной информации о себе? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА В КАЖДОЙ СТРОКЕ.

	Не чаще, чем до карантина	Немного чаще, чем до карантина	Значительно чаще, чем до карантина	Затрудняюсь ответить НЕ ЗАЧИТЫВАТЬ
Q3-1. ЭЦП (электронная цифровая подпись)	1	2	3	9
Q3-2. Данные банковской карты	1	2	3	9
Q3-3. ФИО, адрес, телефон	1	2	3	9
Q3-4. Биометрические данные (фото, отпечатки пальцев)	1	2	3	9
Другое _____	1	2	3	9

Q4. Можете ли Вы сказать, что за время карантина Вы стали больше заботиться/думать о безопасности своей персональной информации, которую предоставляете онлайн? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

Да, я определенно стал больше заботиться о безопасности своей персональной информации, предоставляемой онлайн.	1	
Скорее да.	2	
Скорее нет.	3	Переход к вопросу Q6
Нет, безопасность моей персональной информации не стала заботить меня больше, чем до карантина.	4	
Другое _____	5	

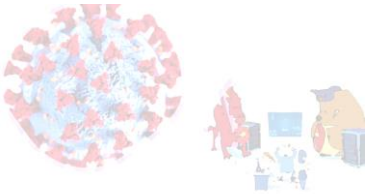
Q5. Какие именно вопросы, связанные с безопасностью персональной информации, стали больше беспокоить Вас за время карантина? ВОЗМОЖНО НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТА

Нежелательная реклама, спам	1
Тайна вашей персональной информации	2
Угроза стать жертвой мошенничества	3
Недобросовестность компаний, которые продают товары или оказывают услуги онлайн	4
Стремление государственных органов собирать все больше личной информации о гражданах	5
Другое _____	6

Q6. Знаете ли Вы свои права в сфере защиты персональной информации, которую предоставляете онлайн? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

Нет, не знаю	1
Знаю очень мало	2
Имею общее представление	3
Хорошо знаю свои права в этой сфере	4
Другое _____	5

Q7. Чувствуете ли Вы необходимость узнать больше о защите персональной информации и своих правах в этой сфере? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.



Да, мне это необходимо	1
Скорее да	2
Скорее нет	3
Нет такой необходимости	4
Затрудняюсь ответить НЕ ЗАЧИТЫВАТЬ	8

Q8. Правительство Казахстана планирует внедрить «Национальную систему видеомониторинга» - систему распознавания лиц, обработки и хранения данных, полученных с камер наружного наблюдения (например, с камер «Сергек»)? Как Вы к этому относитесь? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

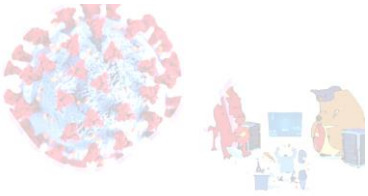
Абсолютно положительно	1
Скорее положительно	2
Скорее отрицательно	3
Абсолютно отрицательно	4
Затрудняюсь ответить НЕ ЗАЧИТЫВАТЬ	9

Q9. Также в рамках программы «Цифровой Казахстан» правительство страны намерено начать собирать биометрические данные граждан, например отпечатки пальцев. Как вы относитесь к данной инициативе? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

Положительно	1
Скорее положительно	2
Скорее отрицательно	4
Отрицательно	5
Затрудняюсь ответить НЕ ЗАЧИТЫВАТЬ	9

Q10. Комитет национальной безопасности заявляет, что системы распознавания лиц, обработки и хранения данных, собранных с камер наружного видеонаблюдения, будут внедряться с целью обеспечения национальной и общественной безопасности.
Оцените, насколько Вы согласны с приведенными ниже высказываниями по этому поводу, выбрав один из вариантов: полностью согласен, скорее согласен, скорее не согласен, полностью не согласен? ОДИН ВАРИАНТ ОТВЕТА В КАЖДОЙ СТРОКЕ.

		1. Полностью согласен	2. Скорее согласен	3. скорее не согласен	4. Полностью не согласен	9. Затрудняюсь ответить НЕ ЗАЧИТЫВАТЬ
Q10-1.	Если такие системы повысят безопасность в стране, то я не против сбора и хранения моей персональной информации, в том числе через камеры наружного видеонаблюдения.	1	2	3	4	9
Q10-2.	Меня настораживает стремление власти собирать все больше и больше личных данных граждан, это похоже на тотальную слежку.	1	2	3	4	9



Q10-3.	У людей нет выбора, власти все равно сделают то, что хотят.	1	2	3	4	9

Q11. Как Вы считаете, на какие страны следует ориентироваться Казахстану в сфере защиты персональной информации граждан? НЕ ЗАЧИТЫВАТЬ. ВОЗМОЖНО НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТА

Европейский Союз	1
Китай	2
Россия	3
США	4
Другое _____	5

Q12. Как Вы считаете, опыт каких стран НЕ СЛЕДУЕТ перенимать и внедрять в Казахстане в сфере защиты персональной информации? НЕ ЗАЧИТЫВАТЬ. ВОЗМОЖНО НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТА

Европейский Союз	1
Китай	2
Россия	3
США	4
Другое _____	5

ТАБЛИЦЫ РАСПРЕДЕЛЕНИЯ ОТВЕТОВ

Q1. Насколько Вас беспокоит безопасность Вашей персональной информации, которую вы предоставляете онлайн? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

	Частота	Процент
Очень беспокоит	437	29%
Заметно беспокоит	234	16%
Не очень беспокоит	397	26%
Не беспокоит	417	28%
Затрудняюсь ответить	18	1%
Итого	1503	100%

Q2. Как бы Вы оценили свои знания о защите персональной информации, которую предоставляете онлайн? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

	Частота	Процент
Ничего не знаю	264	18%
Мои знания очень ограничены	223	15%
Имею общее представление	710	47%
Я хорошо осведомлен о защите персональной информации	306	20%
Итого	1503	100%

Q3. Во время карантина, введенного во время эпидемии коронавируса, люди стали больше пользоваться Интернетом. Можете ли вы сказать про себя, что за время карантина стали чаще предоставлять перечисленные ниже виды персональной информации о себе? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА В КАЖДОЙ СТРОКЕ.

ЭЦП (электронная цифровая подпись)

	Частота	Процент
Не чаще, чем до карантина	695	46%
Немного чаще, чем до карантина	304	20%
Значительно чаще, чем до карантина	288	19%
Затрудняюсь ответить	216	14%
Всего	1503	100%

Данные банковской карты

	Частота	Процент
Не чаще, чем до карантина	733	49%
Немного чаще, чем до карантина	324	22%
Значительно чаще, чем до карантина	340	23%
Затрудняюсь ответить	106	7%
Всего	1503	100%

ФИО, адрес, телефон

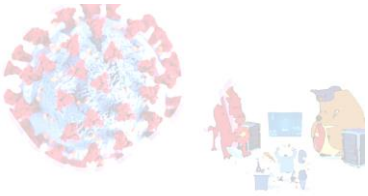
	Частота	Процент
Не чаще, чем до карантина	781	52%
Немного чаще, чем до карантина	345	23%
Значительно чаще, чем до карантина	272	18%
Затрудняюсь ответить	105	7%
Всего	1503	100%

Биометрические данные (фото, отпечатки пальцев)

	Частота	Процент
Не чаще, чем до карантина	861	57%
Немного чаще, чем до карантина	194	13%
Значительно чаще, чем до карантина	137	9%
Затрудняюсь ответить	311	21%
Всего	1503	100%

Q4. Можете ли Вы сказать, что за время карантина Вы стали больше заботиться/думать о безопасности своей персональной информации, которую предоставляете онлайн? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

	Частота	Процент
Да, я определенно стал больше заботиться о безопасности своей предоставляемой онлайн	386	26%
Скорее да	306	20%
Скорее нет	212	14%
Нет, безопасность моей персональной информации не стала заботить больше	587	39%
Другое	12	1%
Всего	1503	100%



Q5. Какие именно вопросы, связанные с безопасностью персональной информации, стали больше беспокоить Вас за время карантина? ВОЗМОЖНО НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТА

	Частота	Процент
Нежелательная реклама, спам	102	15%
Тайна вашей персональной информации	185	26%
Недобросовестность компаний, которые продают товары или оказывают услуги онлайн	302	43%
Стремление государственных органов собирать все больше личной информации о гражданах	40	6%
Стремление государственных органов собирать все больше личной информации о гражданах	42	6%
Другое	239	34%

Q6. Знаете ли Вы свои права в сфере защиты персональной информации, которую предоставляете онлайн? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

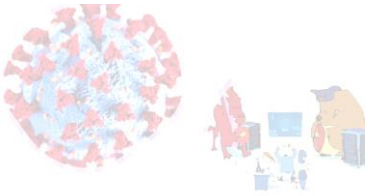
	Частота	Процент
Нет, не знаю	385	26%
Знаю очень мало	433	29%
Имею общее представление	500	33%
Хорошо знаю свои права в этой сфере	183	12%
Другое	2	0%
Всего	1503	100%

Q7. Чувствуете ли Вы необходимость узнать больше о защите персональной информации и своих правах в этой сфере? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

	Частота	Процент
Да, мне это необходимо	409	27%
Скорее да	492	33%
Скорее нет	128	9%
Нет такой необходимости	465	31%
Затрудняюсь ответить	9	1%
Всего	1503	100%

Q8. Правительство Казахстана планирует внедрить «Национальную систему видеомониторинга» - систему распознавания лиц, обработки и хранения данных, полученных с камер наружного наблюдения (например, с камер «Сергек»)? Как Вы к этому относитесь? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

	Частота	Процент
Абсолютно положительно	360	24%
Скорее положительно	492	33%
Скорее отрицательно	225	15%
Абсолютно отрицательно	338	22%
Затрудняюсь ответить	88	6%
Всего	1503	100%



Q9. Также в рамках программы «Цифровой Казахстан» правительство страны намерено начать собирать биометрические данные граждан, например отпечатки пальцев. Как вы относитесь к данной инициативе? ЗАЧИТАТЬ. ОДИН ВАРИАНТ ОТВЕТА.

	Частота	Процент
Положительно	478	32%
Скорее положительно	314	21%
Скорее отрицательно	187	12%
Отрицательно	464	31%
Затрудняюсь ответить	60	4%
Всего	1503	100%

Q10. Комитет национальной безопасности заявляет, что системы распознавания лиц, обработки и хранения данных, собранных с камер наружного видеонаблюдения, будут внедряться с целью обеспечения национальной и общественной безопасности.
Оцените, насколько Вы согласны с приведенными ниже высказываниями по этому поводу, выбрав один из вариантов: полностью согласен, скорее согласен, скорее не согласен, полностью не согласен? ОДИН ВАРИАНТ ОТВЕТА В КАЖДОЙ СТРОКЕ.

«Если такие системы повысят безопасность в стране, то я не против сбора и хранения моей персональной информации, в том числе через камеры наружного видеонаблюдения».

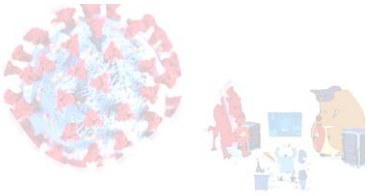
	Частота	Процент
Полностью согласен	477	32%
Скорее согласен	468	31%
Скорее не согласен	214	14%
Полностью не согласен	297	20%
Затрудняюсь ответить	47	3%
Всего	1503	100%

«Меня настораживает стремление власти собирать все больше и больше личных данных граждан, это похоже на тотальную слежку».

	Частота	Процент
Полностью согласен	490	33%
Скорее согласен	397	26%
Скорее не согласен	301	20%
Полностью не согласен	260	17%
Затрудняюсь ответить	55	4%
Всего	1503	100%

«У людей нет выбора, власти все равно сделают то, что хотят».

	Частота	Процент
Полностью согласен	645	43%
Скорее согласен	344	23%
Скорее не согласен	224	15%
Полностью не согласен	215	14%
Затрудняюсь ответить	75	5%
Всего	1503	100%



Q11. Как Вы считаете, на какие страны следует ориентироваться Казахстану в сфере защиты персональной информации граждан? НЕ ЗАЧИТЫВАТЬ. ВОЗМОЖНО НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТА

	Частота	Процент
Европейский Союз	202	13%
Китай	91	6%
Россия	177	12%
США	211	14%
Другое	975	65%
Затрудняюсь ответить	1	0%

Q12. Как Вы считаете, опыт каких стран НЕ СЛЕДУЕТ перенимать и внедрять в Казахстане в сфере защиты персональной информации? НЕ ЗАЧИТЫВАТЬ. ВОЗМОЖНО НЕСКОЛЬКО ВАРИАНТОВ ОТВЕТА

	Частота	Процент
Европейский Союз	20	1%
Китай	325	22%
Россия	118	8%
США	188	13%
Другое	986	66%