РОДИТЕЛЬСКИЙОТПОР.РФ
За семью! За Родину! За традиции!

Президенту Российской Федерации
Владимиру Владимировичу Путину,
103132, Российская Федерация, г. Москва, ул. Ильинка, д.23
http://letters.kremlin.ru/letters/send

От _____

Адрес для ответа, телефон: _____

ОБРАЩЕНИЕ К ОТВЕТСТВЕННОМУ РУКОВОДИТЕЛЮ ГОСУДАРСТВА

с требованием наложить вето, отменить, антиконституционный законопроект № 211535-8 «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», как пролоббированный с вопиющими нарушениями процедуры и сроков рассмотрения, изменения концепции, без общественных слушаний.

Уважаемый Владимир Владимирович! Обращаемся к вам, как к Гаранту Конституции России!

Просим вам защитить будущее нашей страны! **Отклоните, наложите вето на законопроект «О единой и тотальной биометрической системе», который продавлен цифролоббистами** с грубейшими нарушения регламента, процедуры, сроков голосования, отсутствием обязательных к 3 чтению нормативно-правовых актов, разработанных Правительством во исполнение бланкетных норм. Данный ПФЗ прямым образом угрожает суверенитету и национальной безопасности

Попытка в 8ой раз навязать гражданам электронное биометрическое удостоверение и подтверждение личности такими антиконституционным законопроектом означает намерение поставить под удар репутацию гаранта Конституции в такое непростое время, связанное как с внешней, так и с внутренней политической и экономической обстановкой.

В начале декабря 2022г. официальные СМИ нашей страны со ссылкой на «The Times» пестрили одной из главных, на наш взгляд, политических новостей последнего времени: США больше не настаивают на том, чтобы ВСУ не наносили удары по российской территории, так как меньше опасаются эскалации со стороны Москвы. Означает ли подобное заявление то, что возможны удары со стороны «коллективного запада» по критической и энергетической инфраструктуре на нашей территории? Нас не может не тревожить вопрос сохранности нашей жизни и жизни наших детей. Ведь обновленная стратегия национальной безопасности США именно об этом и говорит: «США берут курс на сдерживание России». Против нашей страны идет мощнейшая кибер, информационная и ментальная война. И цель наших врагов не столько захват территорий и присвоение ресурсов. Главная цель - захват будущего, которое сосредоточено в судьбах наших детей. А в дополнение ко всем информационным атакам на нашу страну, на каждого ее жителя, даже детей, в условиях затяжной СВО, мы видим, как министры—цифровые гастарбайтеры, на задумываясь о последствиях, желают втянуть всю страну в цифровой апокалипсис, любой ценой раздеть и раскрыть всю Россию, сделать доступными для врагов все тайны от лица их носителей.

Выступая в Совете Федерации, советник министра обороны РФ Андрей Ильницкий отметил:*«…принятие такого рода НПА влечет за собой увеличение количества мошеннических действий в связи с утечкой ПД, а объединение в единую систему баз данных, имеющих разные цели, содержащих медицинскую, генетическую информацию и другие идентификаторы, может угрожать жизни и здоровью граждан, нести в себе подрыв национальной и государственной безопасности, поскольку утечка данных в этой системе позволит оказывать влияние на любого гражданина также и извне государства <…>. Национальная безопасность должна быть приоритетом. Если вы (обращаясь к законотворцам) усматриваете в каком-то законопроекте хоть минимальный ущерб национальной безопасности, то его надо снимать с рассмотрения и возвращать на доработку».* Андрей Михайлович также в одном из своих интервью отмечает, что «Россия – это главный барьер на пути глобального Запада. Без ликвидации России развитие западного мира в его сегодняшнем изводе просто невозможно». Конфликт на Украине Ильницкий называет первой цифровой войной.

Руководитель Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Андрей Липов считает, что утечки персональных данных являются незаконной агрегацией информации о гражданах России, кроме того, для западных спецслужб такие утечки становятся основным источником ценной информации о россиянах: их социальном статусе и предпочтениях. «Незаконная агрегация информации о гражданах России впоследствии используется для мошеннических действий против людей, буллинга, диффамации, вовлечения в противоправные мероприятия, в том числе экстремистской и террористической направленности».

Глава британской военной разведки генерал Джим Хокенхалл на недавнем вебинаре, посвященном событиям на Украине, говорил о том, что ведение военных действий строится сегодня не на традиционных военных возможностях и было бы невозможно без информации из открытых источников Интернет– ресурсов, в том числе коммерчески доступных услуг. По его мнению, это оказало значительное влияние на события на Украине. Была реализована возможность свободно обмениваться с украинцами информацией о действиях русских, будь то развертывание, полное развёртывание и подготовка к вторжению или сам процесс вторжения. В контексте войны за национальное выживание украинская общественность оказалась привержена тому, чтобы сыграть существенную роль в предоставлении своим военным информации, обеспечивающей преимущество. Техническим базисом стали коммерческие сети, обеспечившие высокую доступность и охват, плюс они оказались невероятно надежны: гарантированно обеспечили альтернативные пути передачи ценной информации. Группировка коммерческих спутников (по сути натовских аппаратов), позволила украинским военным расширить возможности ситуационной осведомленности и их возможности вести наблюдение и разведку. Работа американской компании Starlink на Украине – показательный пример. Резюмируя сказанное, генерал Хокенхалл сообщил: сочетание информации из открытых и секретных источников стало на Украине бесценным, обеспечив возможность отслеживать информационные и военные операции (особенно российские), оценивать их влияние на ход боевых действий. **Если мы не хотим нанесения большего ущерба нашей стране, необходимо остановить безумные подрывные проекты цифроизменников нашей Родины, иначе начнется жуткий реванш Запада на взломанную и раздетую цифровиками Россию.**

Давайте спросим у инициаторов ПФЗ «О единой и тотальной биометрической системе», а также у всех тех, кто поддержал данный проект, даже не читая его, с какой целью собираются огромные массивы данных россиян, в интересах кого работают «народные» избранники? Наша страна занимает первую строчку в списке самых уязвимых стран мира! С начала специальной военной операции произошло более 140 утечек персональных данных, сообщают в Роскомнадзоре. В сеть попало более 600 млн записей о гражданах России. В пресс-службе ведомства уточнили, что была нарушена конфиденциальность медицинских персональных данных, подлежащих особой защите. Также в данных содержится информация об актуальных социальных связях россиян. Основными крупными источниками персональных данных россиян, появляющихся в незаконном открытом доступе в сети, являются региональные органы исполнительной власти, банковские структуры и мобильные операторы (то есть по сути все те структуры, которых немногим ранее под

страхом административной ответственности просто законодательно принудили к сбору биометрических данных россиян). Практически все государственные и муниципальные ресурсы (особенно медицинские, образоательные) были атакованы или взломаны. Мы не верим, что цифроминистры этого не знают! Еще не утих недавний скандал с утечкой баз данных из Московской электронной школы, когда в «слитой» информации были обнаружены данные о семьях российской элиты: сыне Артура Очеретного, дочери Сергея Суровикина, дочери Сергея Шойгу, родственнике Германа Грефа. Естественно, ДИТ Москвы поторопился опровергнуть эту информацию. Но это далеко не первая утечка с mos.ru. В конце 2018 года с сайта утекли сотни квитанций с ФИО, ИНН и телефонами плательщиков, в июне 2020-го в даркнете пытались продать базу данных с 9 млн записей о жителях Москвы (в т.ч. детей), а в декабре 2020-го были обнародованы документы с полной информацией о 300 тыс. переболевших COVID-19. И буквально в дни принятия данного антинародного ПФЗ была обнародована еще одна история, связанная с крупной утечкой данных, предположительно из сегмента ЕСИА (т.е. непосредственно связанного через Госуслуги с системой ЕБС). Специалисты Ростелекома в своем анализе утечки пытались убедить, что она произошла из базы «Почты России», в этом же людей пытался уверить министр Максут Шадаев, но результаты независимого анализа показали, что вероятнее всего вскрыта была именно система ЕСИА.

Ведущий специалист в области кибербезопасности Наталья Касперская, президент InfoWatch, неоднократно заявляла, что она сами лично очень отрицательно относится к биометрии. Ведь если «логин- пароль можно поменять при их потере либо взломе системы, то чувствительные биометрические данные изменить невозможно, невозможно так просто взять и изменить лицо». Если биометрические данные будут украдены или скомпрометированы, то у человека возникнет много сложностей с доказательством своей невиновности или реализацией определенных прав. Она уверена, что никакой 100% защиты биометрических персональных данных быть не может, за последний год произошло 19 масштабных утечек из государственных информационных систем, за которые никто не понес ответственности. Готовы ли Вы, как ответственный руководитель страны, рискнуть персональными и биометрическими данными всех граждан России, как будто для удобства геополитических противников, собранных в единую базу, ведь в случае взлома этой единой системы хватит и одного случая, чтобы создать риски для личной и национальной безопасности?

Отвечая на вопрос сенатора М. Павловой о том, на каком оборудовании будет работать ЕБС, замминистра цифрового развития О. Пак заверил, что все оборудование сертифицировано и соответствует требованиям ФТЭК и ФСБ. Вот только он умышленно умолчал о том, какие страны производят оборудование и «начинку» для выстраивания системы цифрового концлагеря в нашей стране. Сам ПФЗ предполагает дополнительную возможность сдачи и управления своей биометрии при помощи мобильных приложений на смартфоне. Но в нашей стране еще не производятся и не покупаются массово качественные мобильные телефоны, а значит, биометрия будет хранится на устройствах иностранного производства!

Почему так много разговоров об аппаратном и программном обеспечении, но мало кто вспоминает о, пожалуй, самом важном: человеческом факторе?! Кто получит доступ к централизованным базам данных всех граждан нашей страны? Насколько они ответственны и не поддадутся ли соблазну продать базы? Насколько можно быть уверенным, что их не завербуют или они сами не захотят сбежать к геополитическому противнику? Ведь можно вспомнить яркий пример, связанный с компанией NtechLab (видеонаблюдение с распознаванием лиц в Москве и некоторых других городах), когда один из акционеров компании, имея в своем распоряжении огромные базы биометрических данных москвичей, стал информатором наших врагов, осуществив, по сути, госизмену. Через какое время сотрудники «Ростелекома» или АО «Центр биометрических решений», не устояв от хорошего вознаграждения или под влиянием других факторов, побегут к нашим западным «партнерам» с базами данных на россиян? Помимо этого, ПФЗ «О единой и тотальной биометрической системе» предусматривает возможность при прохождении аккредитации передавать биометрию трансгранично. Так как ПФЗ предполагает передачу всех данных по интернету, вся информация в котором перехватывается американцами, то можно ожидать, что все методы шифрования биометрии будут также взломаны квантовыми суперкомпьютерами противников. Мы видим в этом коррупционную составляющую, а также задаем вопрос: с какой целью потребовалось вносить в закон такую возможность передавать чувствительные биометрические данные за границу, прямо в руки наших врагов?

В условиях, когда у нас нет никакой защиты от электронного мошенничества, а с начала военной спецоперации мы наблюдаем постоянные хакерские атаки на ресурсы органов самоуправления, исполнительной власти, электронные ресурсы образовательных организаций, учреждений здравоохранения, федеральные цифровые платформы, персональные данные граждан страны утекают в сеть, продаются в «даркнете», абсолютно прозрачны для киберпреступников, разведывательных управлений иностранных государств, у людей возникают обоснованные опасения, что в любой момент киберпреступники, захватившие электронную подпись или электронный идентификатор, а тем более биометрию, смогут ограбить, переписать права людей, имущество, детей на кого угодно, лишить всего этого человека простым нажатием кнопки, по сети Интернет.

В текущих геополитических условиях постоянной охоты врагов страны на чувствительные персональные данные, прежде всего, военных, представителей силовых структур, а также детей и отдельно каждого человека, против которого геополитические противники решат развязать информационную, финансовую войну, недопустимо рассматривать проект закона, в которых в том числе говорится, что своими правами смогут воспользоваться только те граждане, которые согласятся на сдачу биометрии, накопление информации, тотальную слежку за собой. Пока наши мужчины защищают Родину, будущее своих детей на фронте, в тылу пытаются лишить этого самого светлого будущего и страну, и подрастающее поколение, заточив их в электронный концлагерь, опосредовав реализацию их естественных прав и свобод цифровыми идентификаторами, поставив под угрозу личные и биометрические данные каждого взрослого и ребенка. Разве подобный проект имеет право быть принятым?

Мы верим, что в отличие от депутатов партии большинства и многих сенаторов, которым было написано около 100.000 тысяч обращений, писем, телеграмм, комментариев в социальных сетях, Вы услышите народ! Мы просим вас защитить право на неприкосновенность каждого из нас, защитить будущее наших детей от оцифровки и само существование нашей страны!

Вы - гарант Конституции Российской Федерации! **Наложите вето на антинародный, антиконституционный ПФЗ № 211535-8, несущий прямую угрозу национальной безопасности нашей Родине бесшовным захватом персональных данных граждан страны в ЕБС (биометрическую систему).**

Во избежание потери самой сути нашей традиционной цивилизации и смысла государственности, разрушения суверенитета страны наднациональным цифровым контролем, Мы, граждане РФ, настоятельно просим ветировать, отклонить данный законопроект, сохранить и закрепить во всем законодательстве использование самых надежных от взлома традиционных систем учёта и получения конституционных обязательств от государства без цифровых посредников и паразитов, пытающихся оцифровать всю РФ по западным планам, а Руководителя России - остаться Гарантом Конституции и естественных прав Человека!

Людям нужна полная уверенность в том, что западные человекохищнические технологии не смогут подступить к следующим поколениям. Нам нужна уверенность в будущем, уверенность в защищенности наших детей со стороны государства!

Нам не нужны иные поздравления в 2023 году! Мы просим избавить нас от западных траекторий человекохищнической цифровизации и не принимать данный закон «О единой и тотальной биометрической системе», взламывающий конституционный каркас базовых прав человека и угрожающий суверенитету и безопасности страны!

С уважением _____/ ПОДПИСИ В КОЛИЧЕСТВЕ_____