МРНТИ 11.15.89 https://doi.org/10.26577/jpcp.2022.v80.i2.013

М. Асанбаев, Т. Килыбаев, Ж. Симтиков*

Казахский Национальный педагогический университет им. Абая, Казахстан, г. Алматы
*e-mail: zhomart-67@mail.ru

КАЗАХСТАН В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ: МЕЖДУ ЦИФРОВИЗАЦИЕЙ СФЕРЫ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ И КОНТРОЛЕМ ЛИЧНЫХ ДАННЫХ

Политика ряда стран, вступивших на путь узаконенного отслеживания мобильной телефонной связи для обеспечения соблюдения карантинных ограничений в отношении людей, подвергшихся заражению COVID-19, породила острые дискуссии в научной среде по поводу угроз, исходящих от современных цифровых технологий. Чрезмерное использование цифровых технологий привело не только к усилению полномочий государства в общественной жизни, но и подвергло угрозе неприкосновенность частной жизни и конфиденциальность личных данных. Однако начало этим чрезвычайным полномочиям государства было положено еще в 2001 году, когда развернулась глобальная война с терроризмом. Именно с этого момента следует датировать начало процесса упадка верховенства закона, приведшего к ограничению личного пространства граждан. Сегодня правительства ряда стран замечены в склонности к использованию антитеррористических мер для визуализации виртуальной угрозы как внутренней угрозы, что нередко служит оправданием для усиления системы контроля над собственными гражданами. Если в США, государствах-членах Европейского Союза, России и ряде других стран эта политика в основном используется ныне для оправдания нарушения конфиденциальности личных данных, то в Китае эта политика усилилась настолько, что фактически привела к слежке и преследованию политического инакомыслия и дискриминации мусульманских этнических меньшинств. В Китае, по сути, запущена инвазивная система внутреннего надзора за собственными гражданами, что вызывает серьезную обеспокоенность мировой общественности и правозащитных организаций, справедливо опасающихся нарушения баланса интересов между государственным контролем граждан и безопасностью личных данных.

Усиление контроля государства над гражданами в последнее время все отчетливее наблюдается и в Казахстане. Общественность страны обеспокоена фактами нарушения конфиденциальности личных сведений и неприкосновенности частной жизни.

Ключевые слова: Казахстан, Россия, Китай, цифровые технологии, интернет-пространство, телекоммуникационная отрасль, контроль над гражданами, неприкосновенность частной жизни, конфиденциальность личных данных.

M. Assanbayev, T. Kilybayev, Zh. Simtikov

Abay Kazakh National Pedagogical University, Kazakhstan, Almaty
*e-mail: zhomart-67@mail.ru

Kazakhstan in the digital age: between the digitalization of public security and the control of personal data

The policy of a number of countries that have embarked on the path of legalized mobile phone tracking to ensure compliance with quarantine restrictions on people infected with COVID-19 has generated heated discussions in the scientific community about the threats posed by modern digital technologies. The excessive use of digital technologies has led not only to the strengthening of the powers of the State in public life, but also threatened the privacy and confidentiality of personal data. However, the beginning of these extraordinary powers of the State was laid back in 2001, when the global war on terrorism unfolded. It is from this moment that the beginning of the process of the decline of the rule of law, which led to the restriction of the personal space of citizens, should be dated. Today, the governments of a number of countries are seen to be inclined to use anti-terrorist measures to visualize a virtual threat as an internal threat, which often serves as an excuse to strengthen the system of control over their own citizens. While in the United States, the member states of the European Union, Russia and a number of other countries, this policy is now mainly used to justify the violation of the confidentiality of personal data, in China this policy has intensified so much that it has actually led to the surveillance and persecution of political dissent and discrimination against Muslim ethnic minorities. In fact, China has

launched an invasive system of internal surveillance of its own citizens, which causes serious concern to the world community and human rights organizations, who rightly fear a violation of the balance of interests between state control of citizens and the security of personal data.

The strengthening of state control over citizens has recently been more and more clearly observed in Kazakhstan. The public of the country is concerned about the facts of violation of the confidentiality of personal information and privacy.

Key words: Kazakhstan, Russia, China, digital technologies, Internet space, telecommunications industry, control over citizens, privacy, confidentiality of personal data.

М. Асанбаев, Т. Килыбаев, Ж. Симтиков*

Абай атындағы Қазақ Ұлттық педагогикалық университеті, Қазақстан, Алматы қ.
*e-mail: zhomart-67@mail.ru

Қазақстан цифрлық технологиялар дәуірінде: қоғамдық қауіпсіздік саласын цифрландыру мен жеке деректерді бақылау арасында

Covid-19 жұқтырған адамдарға қатысты карантиндік шектеулердің сақталуын қамтамасыз ету үшін ұялы телефон байланысын заңдастырылған бақылау жолына түскен бірқатар елдердің саясаты қазіргі цифрлық технологиялардың қауіптері туралы ғылыми ортада қызу пікірталастар туғызды. Сандық технологияларды шамадан тыс пайдалану мемлекеттің қоғамдық өмірдегі өкілеттіктерін күшейтіп қана қоймай, жеке өмірге және жеке деректердің құпиялылығына қауіп төндірді. Алайда, мемлекеттің осы төтенше өкілеттіктерінің басталуы 2001 жылы жаһандық терроризмге қарсы соғыс басталған кезде басталды. Дәл осы сәттен бастап азаматтардың жеке кеңістігін шектеуге әкелетін заң үстемдігінің құлдырау процесі басталды деп айтса болады. Бүгінгі таңда бірқатар елдердің үкіметтері виртуалды қатерді ішкі қауіп ретінде көрсету үшін терроризмге қарсы шараларды қолдануға кіріскен, яғни бұл көбінесе өз азаматтарын бақылау жүйесін күшейтуге негіз болады. Егер АҚШ-та, Еуропалық Одаққа мүше мемлекеттерде, Ресейде және басқа да бірқатар елдерде бұл саясат негізінен жеке деректердің құпиялылығын бұзуды негіздеу үшін пайдаланылса, Қытайда бұл саясат соншалықты күшейе түсті. Бұл іс жүзінде мұсылман этникалық қауымдастардың саяси көзқарастары мен дискриминациясын бақылауға және оларды қудалауға әкелді. Қытайда, шын мәнінде, өз азаматтарын ішкі қадағалаудың инвазивті жүйесі іске қосылып, бұл азаматтардың мемлекеттік бақылауы мен жеке деректердің қауіпсіздігі арасындағы тепе-теңдікті бұзады деген қауіппен әлемдік қоғамдастық пен адам құқықтары жөніндегі ұйымдар қарап отыр.

Мемлекет азаматтарын бақылаудың күшеюі соңғы уақытта Қазақстанда да айқын байқалады. Ел жұртшылығы жеке ақпараттың құпиялылығы мен жеке өмірге қол сұғылмаушылықты бұзу фактілеріне алаңдап отыр.

Түйін сөздер: Қазақстан, Ресей, Қытай, цифрлық технологиялар, интернет-кеңістік, телекоммуникация саласы, азаматтарды бақылау, жеке өмірге қол сұқпаушылық, жеке деректердің құпиялылығы.

Введение

Спор о балансе интересов между полномочиями государства в сфере общественной безопасности, развитием цифровых технологий, неприкосновенностью частной жизни и конфиденциальностью личных данных становится все более поляризованным. Каким бы ни был компромисс в этом вопросе, спор должен основываться на верховенстве закона, общественной безопасности и праве граждан на неприкосновенность частной жизни. Однако используемые для мониторинга граждан новые цифровые технологии, особенно перспектива их быстрого и неконтролируемого развития в мире, будут иметь непредсказуемые последствия для современного общества. Они приведут, прежде всего, к нарушению принципов верховенства закона и как следствие этого сужению всеобщих прав на неприкосновенность частной жизни и конфиденциальности информации.

Так, например, последствия развития цифровых технологий в ближайшее время станут неоспоримыми фактами нашего бытия. Искусственный интеллект, «большие данные», биоинформатика, биоинженерия и другие области технического прогресса уже стали тесно взаимосвязанными процессами. В скором времени их поистине революционный эффект непременно даст о себе знать. Если сделать сравнительную градацию, то по важности сохранения личного пространства граждан на первом месте

среди всех этих инноваций стоит развитие искусственного интеллекта и его способность думать и принимать решение за человека. Следом идет развитие «больших данных» для управления большим объемом сведений, конечная цель которого заключается в выведении полезной информации. Замыкает цепочку биотехнология, которая включает в себя биоинформатику и биоинженерию, это использование или модификация живых существ, чтобы их можно было использовать в качестве полезных продуктов или инструментов для использования в полезных процессах.

Большинство из этих новых технологий основаны на алгоритмах, некоторые обходятся без них. В любом случае, создается впечатление, что человечество пытается построить машины, которые могут думать и принимать решение за нас. Такие машины способны значительно облегчить нам жизнь. Но также верно, что «технологические революции будут набирать силу в следующие несколько десятилетий и поставят человечество перед самыми тяжелыми испытаниями, с которыми мы когда-либо сталкивались»(1).

Исходя из вышесказанного, мы должны рассмотреть все возможные последствия этой новой реальности, как на национальном, так и на глобальном уровне. Позиция «золотой середины» предполагает, что достижения технологических революций открывают человечеству не только новые возможности, но и множество новых возможных проблем. Это не означает, что успехи, которые мы получаем в области искусственного интеллекта или больших данных, обязательно уничтожат нас, но такие опасения имеют право присутствовать в наших разговорах о будущем развитии. Разница между общественной безопасностью и конфиденциальностью личных данных, которую необходимо обсуждать уже сегодня, все еще слишком сложна, чтобы ее разрешить. Тем не менее, наше ближайшее будущее может характеризоваться появлением новых типов угроз, связанных с утечкой конфиденциальности личных данных и нарушением закона о неприкосновенности частной жизни.

В связи с этим важно понять, какие угрозы таит в себе неконтролируемое использование цифровых технологий. При этом характер государственной политики напрямую зависит не столько от уровня развития цифровых технологий или даже всей системы внутреннего надзора или слежки, сколько от того, как эти вопросы интерпретируются и отражены в законодательстве и практике того или иного государства, а также приверженностью государства к вышеуказанным универсальным ценностям современного общества.

Между общественной безопасностью и сохранением приватности частной жизни

Когда мы принимаем условия использования глобальной сети или различных мессенджеров, мы обычно не осознаем содержащихся в них рисков. Отправив семейное фото в социальные сети или личное сообщение с помощью мессенджеров, мы фактически стираем грань между личным пространством и глобальной сетью. Мы даже не рассматриваем возможность того, что любая информация, которую мы ищем через поисковые системы или при посещении различных веб-сайтов, будет сохранена в глобальной сети. «Как только эти сообщения будут отправлены, их метаданные (с кем мы общаемся, где мы были, когда это произошло и как долго мы разговаривали) и содержание сообщений потенциально могут быть прочитаны государственными органами при наличии ордера»(2). Аналогичным образом происходит утечка конфиденциальных сведений, когда мы подключаемся к Интернету и доверяем свои данные национальному провайдеру. Это означает, что мы больше не можем рассчитывать на конфиденциальность информации. Неслучайно во многих (если не во всех) странах существует закон, согласно которому государственные учреждения могут при определенных обстоятельствах получать доступ к истории пользователей вашего компьютера в реальном времени или в любом удобном формате. Это может произойти практически в любой стране. Другое дело как это происходит. С вашего ведома или без вашего ведома. Но даже возражения по поводу последнего не имеют смысла, поскольку любая местная телекоммуникационная компания обязана передавать информацию о вашей истории в Интернете в соответствующие государственные органы, отвечающие за информационную безопасность страны. Во многих странах эта реальность уже стала неотъемлемой частью национального законодательства. Власти уверены, что эти меры необходимы для предотвращения потенциальных террористических угроз.

Как свидетельствуют сравнительно недавние случаи террористических атак в различных частях мира, терроризм остается угрозой для всех

стран, независимо от их мощи и возможностей. Этот простой факт логически подтолкнул национальные правительства к принятию мер по выявлению и предотвращению террористической деятельности и искоренению экстремистских идей в Интернете. Однако каждый регион мира имеет свои локальные особенности. Разница в политической системе и политической культуре – два немаловажных фактора, обусловивших появление различных подходов и мер, предпринимаемых на национальном уровне для борьбы с терроризмом в Интернете. В государствах-членах Европейского Союза серия террористических атак (нападение на издательство Шарли Эбдо в Париже, атаки в Брюсселе, Берлине, Барселоне и Лондоне), организованная их собственными гражданами в 2011-2012 годах, побудила европейские правительства к принятию мер против подстрекательства к совершению террористических актов и распространения экстремистской идеологии в Интернете. В Китае меры, принятые против терроризма в Интернете, совпали с правительственными мерами по усилению контроля над мусульманскими этническими меньшинствами. Попытки Пекина отслеживать поведение огромного населения породили так называемую систему социального кредитования, количественную оценку ожидаемого поведения жителей страны. Последние политические события, связанные с нарушением неприкосновенности частной жизни и прав человека по другую сторону северной границы Китая, в России, включают в себя использование властями угрозы безопасности, исходящей от ИГИЛ и других внешних источников для усиления контроля правительства над своими гражданами и оправдания преследования политического инакомыслия.

Глобальная война с терроризмом, начавшаяся после событий 11 сентября 2001 года в США, имела серьезные последствия для неприкосновенности частной жизни и конфиденциальности информации во всем мире. Большую обеспокоенность вызывает опыт России и Китая. Если в России власти пошли по пути контроля над политическим инакомыслием и пресечения деятельности диссидентов и оппонентов режима, тогда в Китае речь уже идет о системе внутреннего надзора и слежки, основанной на тотальном контроле практически всех аспектов человеческой жизни. Такое положение дел достигло апогея в 2020 году, когда в Китае была запущена противоречивая система социального кредитования. Эта программа все еще находится на стадии разработки и совершенствования, поскольку она вводится поэтапно, но некоторые китайские граждане уже стали подвергаться дискриминации из-за его реализации. В Китае война с террором уже рассматривается как предлог для оправдания нарушений не только неприкосновенности частной жизни и конфиденциальности информации, но также свободы веры, слова и гражданских прав мусульманских меньшинств.

В тоже время Россия и Китай всегда оказывали большое влияние на внутреннюю и внешнюю политику Казахстана, что повлияло на характер государственной политики последнего в отношении глобальной войны с экстремизмом и терроризмом. Не удивительно, что опыт России и Китая в сфере обеспечения общественного порядка и национальной безопасности способствует продвижению аналогичной политики в Казахстане. В особенности следует отметить широкое использование китайских технологий распознавания лица, голоса и других биометрических данных человека в Казахстане, которые задают тон развитию местной телекоммуникационной отрасли.

Развитие цифровых технологий в Казахстане: вслед за Россией и Китаем

Россия и Китай, две страны, с которыми Казахстан тесно сотрудничает в различных сферах политики и экономики, сегодня играют ключевую роль в развитии казахстанской модели регулирования телекоммуникационной сферы и Интернета.

С одной стороны, Казахстан активно заимствует у России технологический стандарт, законодательную базу и опыт законодательных инициатив по регулированию интернет-пространства и телекоммуникационной отрасли, создавая систему тотальной цензуры в средствах массовой коммуникации, в особенности в социальных сетях. Государственные и частные российские компании – желанные партнеры в реализации проектов в Казахстане по развитию и контролю средств коммуникаций – мобильной связи, мобильных приложений, национального сегмента Интернета и т.п.

С другой стороны, Китай все чаще воспринимается в Казахстане как желанный образец государства, где власти могут поддерживать строгий контроль над своими гражданами посредством цифровых технологий. Китай и его огромный технологический прорыв быстро превратил его

в самое передовое полицейское государство в мире, а его цифровые технологии в особенности привлекательны для многих развивающихся стран. Казахстан здесь не исключение. Поэтому большое внимание заслуживает широкое использование китайских технологических стандартов наблюдения, например, система распознавания лиц и анализа больших данных, которые сегодня лидируют на казахстанском рынке и способствуя развитию телекоммуникационной инфраструктуры Казахстана, в то время как такие компании, как Huawei или Xiaomi, становятся все более популярными среди казахстанских пользователей мобильной связи.

Российский опыт законодательного регулирования телекоммуникационной отрасли в Казахстане

Подход России к политике в области телекоммуникаций и Интернета оказывает долгосрочное влияние на многие постсоветские государства. Казахстан – одна из наиболее заметных стран в этом длинном перечне. Так, в 2016 году в России был принят антитеррористический законодательный акт, получивший название «Закона Яровой», по имени разработчика, депутата Госдумы Ирины Яровой. Данный закон обязал провайдеров телекоммуникационной связи и интернет-услуг хранить телефонные разговоры, текстовые сообщения и видео сроком до полугода. Телекоммуникационные компании обязались три года хранить исчерпывающую информацию об о всех звонках и контактах абонентов связи. Аналогичные обязательства были наложены на провайдеров интернет-услуг сроком на один год. По запросу Федеральной службы безопасности России, компании-провайдеры электронной связи и социальных сетей также обязаны всячески содействовать в расшифровке данных пользователей(3). Такие драконовские меры вызвали озабоченность правозащитных организаций, а также действующих в России телекоммуникационных компаний(4), усомнившихся в возможности реализации вышеуказанных положений закона Яровой в силу их экономической нецелесообразности.

В течение первого полугодия 2016 года, когда в России рассматривался и принимался законопроект Яровой, власти Казахстана внимательно следили за этим процессом. Наблюдая за внешней реакцией и критикой в адрес России, вернее за безрезультатной международной критикой со стороны различных правозащитных организаций, власти Казахстана уже тогда видимо решились на принятие аналогичного комплекса мер в рамках борьбы с экстремизмом и терроризмом. Как и в России, власти Казахстана решили придать широкой публичной огласке это намерение. Осенью 2016 года в обсуждении проекта закона «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам противодействия экстремизму и терроризму» приняли участие представители силовых структур, правозащитники и неправительственные организации. Несмотря на критику в СМИ(5) о возможном злоупотреблении властью со стороны государственных органов, данный законопроект был принят 22 декабря 2016 года(6). Принятие данного закона способствовало принятию в 2017 году в недрах Комитета национальной безопасности приказа о внедрении нового технического регламента, направленного на регулирование деятельности телекоммуникационных компаний и провайдеров. Название данного технического регламента говорит само за себя: «Общие требования к телекоммуникационному оборудованию по обеспечению проведения оперативно-розыскных мероприятий, сбора и хранения служебной информации об абонентах».

«В него вошли требования к специальному оборудованию операторов мобильной связи Казахстана. В техническом регламенте описываются возможности перехвата, записи, хранения, прослушивания, просмотра, видимо, и сохранение всей этой информации на внешние носители операторами мобильной связи»(7).

С принятием указанного технического регламента возник резонный вопрос о том, как он соотносится с конституцией и действующим в Казахстане законодательством в сфере защиты личных данных граждан. Так, в Конституции Казахстана, в статье 18 говорится о том, что «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства»(8).

В Законе РК «О персональных данных и их защите» от 2013 года, в статье 2 указано об «обеспечении защиты прав и свобод человека и гражданина при сборе и обработке его персональных данных»(9).

Не случайно информация о новом техническом регламенте породила критику со стороны одной из телекоммуникационных кампаний, работающей на рынке Казахстана. В письме,

ставшем достоянием общественности, компания Telia Company выразило сомнение в необходимости принятия новых правил, заявив, что компания обязалась уважать свободу слова в области телекоммуникаций. «Надзор правительства часто служит законным целям, таким как защита определенных прав человека. Но также может противоречить другим правам человека», – говорилось в письме(10). Власти Казахстана поспешили опровергнуть критику, заявив, что «записи разговоров будут вестись выборочно, только отдельных лиц, и только с санкции прокуратуры»(11).

Тем не менее, в техническом регламенте закреплено противоречащее положение о выборочном характере прослушивания и записи переговоров. Согласно этому положению, «перехвату переговоров или сообщений подлежат не менее 1% от общего количества абонентов, подключенных или зарегистрированных на данном коммутационном оборудовании»(12).

После публикации этого письма отношения между компанией Telia Company и руководством Казахстана значительно осложнились, и его содержание неоднократно обсуждалось в местном журналистском сообществе. Уход компании Telia Company из Казахстана стал предсказуемым итогом, поскольку появление данного письма продемонстрировало наличие «непреодолимых препятствий» для дальнейшей деятельности компании Telia Company в Казахстане и его сотрудничества с правительством Казахстана. Менеджеры компании дали ясно понять, что компания не готова поступиться с конфиденциальностью информации об абонентах связи. «12 декабря 2018 года компания Telia Company и Fintur Holdings BV завершили продажу своей доли в казахстанском телекоммуникационном гиганте АО Kcell оператору связи АО «Казахтелеком», компании, контролируемой правительством Казахстана через суверенный фонд «Самрук-Казына»(13).

Следует отметить, что новые требования к операторам связи не являются новшеством. О существовании и использовании в Казахстане системы технических средств, направленной для обеспечения функций оперативно-розыскных мероприятий (СОРМ) известно, как минимум, с начала 2000-х годов. Однако именно с принятием указанной законодательной базы государственные органы Казахстана могут вполне легально и широким охватом использовать внедренные ранее российские системы наблюдения СОРМ-I, СОРМ-II и СОРМ-III, предназначенные для анализа содержимого телекоммуникационной связи, СМИ и Интернета. Говоря техническим языком, для прослушивания телефонных переговоров, протоколирования обращений к сети Интернет и обеспечения сбора информации со всех видов связи и её долговременного хранения.

Таким образом, принятие в Казахстане вышеуказанного технического регламента можно рассматривать как аналог «Закона Яровой» в России. Разница лишь в том, что данный документ не обсуждался в парламенте Казахстана, так как это всего лишь подведомственный документ, направленный на ужесточение антитеррористических мер в стране.

Следует также отметить, что большинство недавно принятых в Казахстане поправок к законам о СМИ, интернете и телекоммуникации, инициированные Министерством информации и коммуникаций РК и одобренные Парламентом страны, а также подведомственные технические регламенты, взяты из российского законодательства. Казахстанские парламентарии и их российские коллеги оказались поразительно схожи в своих стремлениях контролировать доступ граждан к глобальной сети.

Китайские цифровые технологии и проблемы защиты конфиденциальности личных данных в Казахстане

Опираясь на опыт Китая, власти Казахстана запустили в 2017 году в крупных городах, областных и районных центрах страны систему видеонаблюдения «Сергек», предназначенную для видеоконтроля, анализа и прогнозирования нарушения правил дорожного движения, а также для наблюдения во дворах жилых домов, крупных торговых центров и в целом местах массового скопления людей.

Хотя разработкой и поставкой видеокамер «Сергек» занимается казахстанская компания «Коркем Телеком», ее техническим партнером является китайская компания Dahua Technology. Эта китайская компания – известный производитель технологий массовой слежки(14). В 2019 году Dahua Technology и другую китайскую компанию HikVision (поставляет в Казахстан средства видеонаблюдения и безопасности с 2015 года) власти США внесли в черный список из-за обвинений в содействии нарушению прав человека в отношении мусульманских меньшинств Китая(15).

Аналогичным образом политика Казахстана в сфере регулирования телекоммуникации стала приобретать черты, схожие с китайской моделью регулирования данной сферы. Как и в Китае, власти Казахстана инициировали обширную регистрации абонентов мобильной связи и заполучили все данные об абонентах мобильной связи. Законодательное обеспечение этой политики началось в 2016 году на фоне масштабных «земельных митингов» в Казахстане, когда принятие вышеуказанного закона «О внесении изменений и дополнений в некоторые законодательные акты РК по вопросам противодействия экстремизму и терроризму» позволило внести соответствующие изменения в Закон РК «О связи». На этот раз, нововведения были разработаны и приняты с подачи министерства информации и коммуникаций РК.

Согласно новому законодательству, действующему в Казахстане с 2016 года, абонент мобильной связи должен пройти у операторов мобильной связи обязательную регистрацию IMEI кода (т.е. 15-значных чисел, которые имеются у каждого персонального телефона) своего смартфона или телефона, произведенного на территории РК или завезенного на территорию Казахстана извне. Требование об обязательной регистрации IMEI-кодов вынудило операторов мобильной связи блокировать телефоны незарегистрированных абонентов(16).

Согласно разработчикам этого закона, данный документ призван ужесточить наказание за террористические и экстремистские преступления. «По заявлению властей страны, обязательная регистрация сотовых телефонов по IMEI-кодам является одной из антитеррористических мер»(17).

В 2018 году были введены дополнительные поправки в правила регистрации абонентских устройств, согласно которым абонент мобильной связи обязан регистрировать не только IMEI код, но и свой индивидуальный идентификационный номер паспорта. Для регистрации создана единая база IMEI-кодов, доступ к которому имеют, как оказывается, не только телекоммуникационные операторы. Как пояснил заместитель председателя Комитета Министерства информации и коммуникаций РК Виталий Ярошенко, «это делается для того, чтобы облегчить работу органам, осуществляющим оперативно-розыскную деятельность, поиск похищенных телефонов, поиск и раскрытие преступлений»(18).

Таким образом, политика Казахстана в сфере цифровых технологий развивается в русле китайской модели цифровизации, при которой используются различные технологии распознавания лица, голоса и других биометрических данных человека. Китайский технический стандарт легко проследить и в телекоммуникационной отрасли, где введено обязательное требование регистрации IMEI кода и индивидуального идентификационного номера паспорта абонентов мобильной связи. При этом до конца не отрегулированными остаются вопросы защиты, хранения и безопасности личных данных абонентов связи. Между тем, казахстанская модель регулирования телекоммуникационной отрасли стремительно развивается, вызывая обеспокоенность общественности и правозащитных организаций. Последние в целом критически относятся к политике властей, полагая, что приватность личного пространства граждан Казахстана завтра будет под большим вопросом. Одним словом, правительство Казахстана сегодня имеет беспрепятственный доступ к личной информации граждан страны, но при этом механизм обеспечения безопасности личных данных остается открытым.

Заключение

Власти Китая и России идут по пути построения жесткого общественного контроля и системы внутреннего надзора, основанных на контроле практически всех аспектов человеческой жизни. Такое положение дел достигло апогея в Китае, где власти, начиная с 2020 года, активно внедряют спорную систему социального кредитования. Эта программа все еще находится в стадии разработки и совершенствования, поскольку она вводится поэтапно, но некоторые китайские граждане уже стали подвергаться дискриминации из-за его реализации. В Китае война с террором уже рассматривается как предлог для оправдания нарушений не только неприкосновенности частной жизни и конфиденциальности информации, но также свободы веры, слова и гражданских прав.

Говоря о заимствовании Казахстаном стратегий Китая и России в сфере цифровых технологий и телекоммуникационной отрасли, можно заметить, что власти страны также имеют намерение обеспечить безопасность граждан способом визуализации возможной виртуальной угрозы как внутреннюю угрозу для усиления

контроля над собственными гражданами. Сегодня эта политика привела к оправданию нарушения конфиденциальности личных данных и беспрецедентному расширению инвазивного внутреннего надзора. Усиление этой политики в Казахстане способно привести к преследованию политического инакомыслия, поскольку оно идет вразрез с всеобщими правами граждан на демократическое управление, свободу и гражданские права.

Литература

Harari Y. 21 Lessons for the 21st Century. New-York: Spiegel and Grau, 2018, 372 p.

Allison P., "Tracking terrorists online might invade your privacy", BBC, 8 September, 2017, available at [https://www.bbc.com/future/story/20170808-tracking-terrorists-online-might-invade-your-privacy], 25 December, 2019.

Ermoshina K., Musiani F., "Migrating servers, elusive users: reconfigurations of the Russian Internet in the Post-Snowden Era", Media and Communication, Vol. 5, Issue 1, 2017, pp. 42–53.

Muratov A., "Russia's 'Big Brother' law enters into force", The Moscow Times, 1 July, 2018, available at [https://www.themoscowtimes.com/2018/07/01/russias-big-brother-law-enters-into-force-a62066], 7 January, 2020.

Бекмамбетов М. Законопроект о противодействии терроризму называют жестким // RFE/RL, 9 сентября 2016 [https://rus.azattyq.org/a/zakonoproekt-o-protivodeystvii-terrorizmu/27976657.html], 8 января 2021.

Алматбаева Ж. «Борьба с терроризмом» за счет населения: о новой регистрации в Казахстане // Regnum, 11 января 2017 [https://regnum.ru/news/2225724.html], 8 января 2021.

Ким С. «Пакет Яровой» по-нашему: идет ли Казахстан к блокировке Telegram? // Sputnik Kazakhstan, 14 июня 2018 [https://ru.sputniknews.kz/society/20180614/6024776/kazakhstan-telegram-blokirovka.html], 7 мая 2020.

Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года, с изменениями и дополнениями по состоянию на 23.03.2019) // Zakon.kz, 23 марта 2019 [https://online.zakon.kz/Document/?doc_id=1005029#pos=3;-88], 15 января 2020.

Закон Республики Казахстан от 21 мая 2013 года за № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 28.12.2017) // Zakon.kz, 28 декабря 2017 [https://online.zakon.kz/document/?doc_id=31396226#pos=3;-157], 17 января 2020.

Говоркова В. В Казахстане могут вырасти тарифы на сотовую связь //Капитал, 18 мая 2017, № 16 (572). С. 1.

Половинко В. Говорите, вас слушают // Новая газета, 18 мая 2017 [novgaz.com/index.php/2-news/1843-говорите,-вас-слушают], 14 января 2021.

Ким С. «Пакет Яровой» по-нашему: идет ли Казахстан к блокировке Telegram? // Sputnik Kazakhstan, 14 июня 2018 [https://ru.sputniknews.kz/society/20180614/6024776/kazakhstan-telegram-blokirovka.html], 7 мая 2020.

Telia company, "Divestment of KCELL completed", Newsroom, 21 December, 2018, available at [https://www.teliacompany.com/en/news/news-articles/2018/kcell-closing/], 15 January, 2021.

Денисенко А. Права человека и COVID-19: что ждет Казахстан после пандемии? //CAAN, 8 июня 2020 [https://caa-network.org/archives/19921], 15 января 2021.

Алтынбаев К. Китайская техника в городах Казахстана вызвала опасения из-за возможной шпионской слежки // Каравансарай, 11 декабря 2019 [https://central.asia-news.com/ru/articles/cnmi_ca/features/2019/12/11/feature-01], 19 января 2021.

Мостовой З. Незарегистрированные телефоны будут блокировать в Казахстане // 365 INFO.KZ, 25 января 2017 [https://365info.kz/2017/01/nezaregistrirovannye-telefony-budut-blokirovat-v-kazahstane], 7 октября 2019.

Чернов И. Кому и зачем нужна регистрация мобильников // КТК, 26 января 2017 [https://www.ktk.kz/ru/blog/article/2017/01/26/75563/], 3 ноября 2019.

Ярошенко В. Жителям РК необходимо зарегистрировать свои мобильные телефоны до конца года // Kursiv.kz, 31 марта 2018 [https://kursiv.kz/news/obschestvo/2018-03/zhitelyam-rk-neobkhodimo-zaregistrirovat-svoi-mobilnye-telefony-do-konca?page=46], 7 января 2020.

References

Y. Harari. 21 Lessons for the 21st Century. New-York: Spiegel and Grau, 2018, 372 p.

P. Allison, "Tracking terrorists online might invade your privacy", BBC, 8 September, 2017, available at [https://www.bbc.com/future/story/20170808-tracking-terrorists-online-might-invade-your-privacy], 25 December, 2019.

K. Ermoshina, F. Musiani, "Migrating servers, elusive users: reconfigurations of the Russian Internet in the Post-Snowden Era", Media and Communication, Vol. 5, Issue 1, 2017, pp. 42–53.

A. Muratov, "Russia's 'Big Brother' law enters into force", The Moscow Times, 1 July, 2018, available at [https://www.themoscowtimes.com/2018/07/01/russias-big-brother-law-enters-into-force-a62066], 7 January, 2020.

Bekmambetov M. Zakonoproekt o protivodeistvii terrorizmu nazivayut jestkim [The anti-terrorism bill is called harsh] // RFE/RL_ 9 sentyabrya 2016 [https_//rus.azattyq.org/a/zakonoproekt_o_protivodeystvii_terrorizmu/27976657.html]_ 8 yanvarya 2021.

Almatbaeva J. «Borba s terrorizmom» za schet naseleniya_ o novoi registracii v Kazahstane [Fight against terrorism "for the population: about the new registration in Kazakhstan] // Regnum_ 11 yanvarya 2017 [https_//regnum.ru/news/2225724.html]_ 8 yanvarya 2021.

Kim S. «Paket Yarovoi» po_nashemu_ idet li Kazahstan k blokirovke Telegram [Spring Package ”in our opinion: will Kazakhstan go to block Telegram?] // Sputnik Kazakhstan_ 14 iyunya 2018 [https_//ru.sputniknews.kz/society/20180614/6024776/kazakhstan_telegram_blokirovka.html]_ 7 maya 2020.

Konstituciya Respubliki Kazahstan _prinyata na respublikanskom referendume 30 avgusta 1995 goda_ s izmeneniyami i dopolneniyami po sostoyaniyu na 23.03.2019,[Constitution of the Republic of Kazakhstan (adopted by the republican referendum on August 30, 1995, as amended and supplemented as of March 23, 2019)] // Zakon.kz_ 23 marta 2019.

Zakon Respubliki Kazahstan ot 21 maya 2013 goda za № 94_V «O personalnih dannih i ih zaschite» _s izmeneniyami i dopolneniyami po sostoyaniyu na 28.12.2017,[Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V “On personal data and their protection” (as amended and supplemented as of December 28, 2017)] // Zakon.kz_ 28 dekabrya 2017 [https_//online.zakon.kz/document/doc_id=31396226#pos=3;_157]_ 17 yanvarya 2020.

Govorkova V. V Kazahstane mogut virasti tarifi na sotovuyu svyaz [Tariffs for cellular communication may increase in Kazakhstan] //Kapital_ 18 maya 2017_ № 16 _572,. S. 1.

Polovinko V. Govorite_ vas slushayut [Speak, you are being heard] // Novaya gazeta_ 18 maya 2017 [novgaz.com/index.php/2_news/1843_govorite__vas_slushayut]_ 14 yanvarya 2021.

Kim S. «Paket Yarovoi» po_nashemu_ idet li Kazahstan k blokirovke Telegram? [Spring package in our opinion: is Kazakhstan moving towards blocking Telegram?] // Sputnik Kazakhstan_ 14 iyunya 2018 [https_//ru.sputniknews.kz/society/20180614/6024776/kazakhstan_telegram_blokirovka.html]_ 7 maya 2020.

Telia company, “Divestment of KCELL completed”, Newsroom, 21 December, 2018, available at [https://www.teliacompany.com/en/news/news-articles/2018/kcell-closing/], 15 January, 2021.

Denisenko A. Prava cheloveka i COVID_19_ chto jdet Kazahstan posle pandemii? [Human rights and COVID-19: what awaits Kazakhstan after the pandemic?] //CAAN_ 8 iyunya 2020 [https_//caa_network.org/archives/19921]_ 15 yanvarya 2021.

Altinbaev K. Kitaiskaya tehnika v gorodah Kazahstana vizvala opaseniya iz_za vozmojnoi shpionskoi slejki [Chinese equipment in the cities of Kazakhstan raised concerns due to possible spying] // Karavansarai_ 11 dekabrya 2019 [https_//central.asia_news.com/ru/articles/cnmi_ca/features/2019/12/11/feature_01]_ 19 yanvarya 2021.

Mostovoi Z. Nezaregistrirovannie telefoni budut blokirovat v Kazahstane [Unregistered phones will be blocked in Kazakhstan] // 365 INFO.KZ_ 25 yanvarya 2017 [https_//365info.kz/2017/01/nezaregistrirovannye_telefony_budut_blokirovat_v_kazahstane]_ 7 oktyabrya 2019.

Chernov I. Komu i zachem nujna registraciya mobilnikov [Who needs to register mobile phones and why] // KTK_ 26 yanvarya 2017 [https_//www.ktk.kz/ru/blog/article/2017/01/26/75563/]_ 3 noyabrya 2019.

Yaroshenko V. Jitelyam RK neobhodimo zaregistrirovat svoi mobilnie telefoni do konca goda [Residents of the Republic of Kazakhstan need to register their mobile phones before the end of the year] // Kursiv.kz_ 31 marta 2018 [https_//kursiv.kz/news/obschestvo/2018_03/zhitelyam_rk_neobkhodimo_zaregistrirovat_svoi_mobilnye_telefony_do_koncapage=46]_ 7 yanvarya 2020.