Социальные эффекты цифровых городских политик: московский опыт в контексте мирового

Владимир Картавцев,
Артем Космарский

Картавцев Владимир Владимирович, к.ф.н., директор Центра прикладных и полевых исследований Института исследований культуры, Национальный исследовательский университет «Высшая школа экономики»; Российская Федерация, 101000, г. Москва, ул. Старая Басманная, 21/4, стр. 1, каб. А209.
E-mail: vkartavcev@hse.ru
Космарский Артем Анатольевич, к.с.н., старший научный сотрудник Центра прикладных и полевых исследований Института исследований культуры, Национальный исследовательский университет «Высшая школа экономики»; Российская Федерация, 101000, г. Москва, ул. Старая Басманная, 21/4, стр. 1, каб. 210.
E-mail: akosmarskii@hse.ru

В данной обзорной статье рассматривается проблематика приватности как ключевой проблемы, возникающей при столкновении городских политик в сфере цифровых технологий с жизненным миром горожан. Авторы описывают различные аффекты приватности, характерные для цифрового поведения людей и их отношения к новым технологиям — парадокс приватности, цифровой эскапизм, апатия, цинизм в отношении приватности. Затем проводится сравнительный анализ международного опыта и российского (прежде всего на примере г. Москвы) в использовании таких актуальных технологий, как QR-коды, распознавание лиц с помощью видеокамер и цифровые партисипативные платформы (подобные «Активному гражданину»). Авторы делают вывод о том, что противоречие между технократическими цифровыми практиками управления городской средой, являющимися по своей сути организованными вертикально, и горизонтальными практиками самоорганизации горожан в настоящий момент сведено до минимума.

Ключевые слова: Москва; надзор; приватность; цифровые политики; QR-коды

Цитирование: Картавцев В.В., Космарский А.А. (2023) Социальные эффекты цифровых городских политик: московский опыт в контексте мирового // Городские исследования и практики. Т. 8. № 1. С. 61–73. DOI: https://doi.org/10.17323/usp81202361-73

Введение: приватность и цифровые технологии

Большинство культур мира так или иначе разделяют общественное и частное, а также формируют представления о градациях открытости для внешнего мира сферы личной (семейной) жизни, скрытой от публичного обсуждения, — как, например, право в тех или иных ситуациях закрывать или держать открытыми двери своего дома. Однако то, что называется privacy (сфера приватности, сфера частной жизни), как философский, социологический и юридический концепт зародилось и получило распространение по историческим меркам относительно недавно — внутри британского и североамериканского обществ Нового времени, опираясь на традицию юридического оформления неприкосновенности жизни и имущества индивида (habeas corpus и тому подобные юридические концепции). Примечательно, что разделение на публичное и приватное характерно именно для обществ модерна, и стимулом к первому юридическому определению privacy стали новые технологии публичности — массовая пресса и фотография. В 1890 году судьи Верховного суда США Сэмюэль Уоррен и Льюис Брандейс определили его как «право быть оставленным в покое» (The right to be left alone), то есть право человека скрывать свою домашнюю (частную) жизнь от наблюдения и внимания со стороны других.

В XX веке осмысление приватности — ее этическое и юридическое оформление — шло различными путями, с упором, например, на права

субъекта — на физическое уединение, автономию, личное достоинство [Flaherty, 1989] или же на оценку уровня доступа общества к жизни человека (через информацию, наблюдение или физическую близость [Gavison, 1980]). Однако прогресс информационных технологий в последние 30 лет, нарастающая цифровизация повседневной жизни, экономики и общества выдвинули на передний план именно информационную приватность, обычно определяемую как «желание индивидов, групп и институций определять, когда, как и до какой степени информация о них передается другим» [Westin, 1967: 7], и, далее, «как эта информация добывается, каким образом другие [акторы] будут ее использовать». Ниже мы рассмотрим основные концептуальные подходы к изучению privacy в цифровой среде, картографируя ландшафт наиболее влиятельных и актуальных исследований по этой теме.

Парадокс приватности

Начиная с 2000-х годов исследователи начали обращать внимание на несовпадение между декларируемыми установками людей относительно раскрытия сведений об их приватной жизни (страхами и опасениями относительно незащищенности персональных данных) и их реальным поведением — равнодушным отношением к раскрытию информации о себе в сети (и даже активной публикацией сведений о потенциально рискованном поведении, размещении личных фотографий в социальных сетях и т. д.). То есть люди заявляют о важности приватности, однако на практике ведут себя так, будто она вообще не имеет для них значения. Это расхождение между установками и реальным поведением получило в литературе название «парадокс приватности», privacy paradox [Norberg et al., 2007].

Ключевые направления осмысления приватности в современных исследованиях выстраиваются вокруг критики и коррекции чрезмерно упрощенных представлений и моделей, плохо объясняющих поведение людей в эпоху больших данных, платформенного капитализма, поведенческого маркетинга и цифровизации повседневной жизни. Так, юрист Д. Солав в знаменитой работе [Solove, 2013] отмечает, что зафиксированные законами и регуляторной практикой права людей на управление информацией о себе исходят из предпосылки об автономном рациональном индивиде, который принимает решение о плюсах и минусах раскрытия информации о себе и дает свое согласие (consent). Однако то, что происходит с этими данными после получения согласия, кто и как их собирает, использует, раскрывает, — все это оказывается за пределами единичных решений субъектов, за пределами их рациональности (и дело тут не только в том, что люди далеко не всегда внимательно изучают текст пользовательских соглашений, а в невозможности, например, следить за активностью смартфона в реальном времени).

Солав описывает эту ситуацию, прибегая к образам Кафки: «Люди (1) не читают правила хранения персональных данных; (2) если даже читают, то не понимают их; (3) если даже читают и понимают, у них не хватает знаний, чтобы сделать осознанный выбор; (4) даже если они делают осознанный выбор, он искажается множеством факторов. Ситуация напоминает путь героя притчи Франца Кафки “У врат закона”, где ворота охраняются бесконечным множеством стражников, каждый из которых сильнее предыдущего» [Solove, 2013: 1888]. Выход из этой ситуации, по мнению ученого, может заключаться прежде всего во внимании к конкретным (особенно потенциально неприятным для человека) способам использования данных, а не просто к формальному факту согласия (substance over consent); в создании специальных приложений и специализированных центров, которые возьмут за себя защиту данных (вместо того чтобы делегировать эту функцию самим индивидам).

Описанная ситуация может быть проиллюстрирована при помощи данных, собранных в рамках проекта «Трансформация социальных отношений в новой технологической реальности: риски и перспективы»[1]. В ходе проведенных в рамках проекта фокус-групп обсуждались разнообразные повседневные цифровые практики. Респонденты заявляли, что озабочены сохранностью персональных данных в интернете, однако признавались, что каких-либо значительных усилий для того, чтобы разобраться с механикой их сбора и дальнейшего использования, предпринимать не готовы и действуют скорее реактивно:

> *«Я вот только на нашем звонке поняла, созвоне, что номера телефонов, которые — ну, связала количество спам-звонков с тем, что я оставляю где-то телефон. Мне казалось почему-то, что это работает как-то довольно рандомно, и они там подбирают*

1. Поддержан грантом РФФИ и ЭИСИ 21-011-31549 опн, реализовался в 2021–2022 годах.

цифры каким-то, не знаю, искусственным интеллектом, и мне звонят. Так что… Но, по-моему, только в новом обновлении еще iPhone стало появляться «Согласны ли вы, чтобы вашу геопозицию отслеживали, чтобы мы потом предлагали вам рекламу?» И то есть мне сразу связывают это всё. Я нажимаю «нет». А раньше я нажимала, если у меня просто спрашивали: «Можно мы будем отслеживать вашу геопозицию?», я нажимала «Ну ладно, окей». Соглашалась» (ФГ, женщина, 21 год, Москва).

Такой подход к управлению своим присутствием в цифровой среде – прямое следствие развития соответствующих продуктов и сервисов. Сама эволюция информационных технологий и рынка в сторону больших данных, умных городов, постоянного отслеживания в фоновом режиме (данные как товар и источник власти) заставляет переосмыслять исходно индивидуалистическое понятие privacy, с его коннотациями самоконтроля и личной автономии.

«Мое» в «мои данные» – вовсе не то же самое, что «моя» в «моя машина», отмечает философ Лучиано Флориди [Floridi, 2016]. Логика работы корпораций и приложений с данными – это не наблюдение (слежка) за отдельными людьми, а обобщение и агломерация данных о статистических индивидах и их профилях. «Моби Диков очень мало. Большинство из нас – сардины. Отдельная сардинка может считать, что рыболовная сеть хочет поймать именно ее. Это не так. Она пытается поймать весь косяк. Итак, чтобы спасти сардинку, нужно защитить косяк» [Floridi, 2014: 3]. Так работает реклама, опирающаяся на поведенческие факторы, или реклама, опирающаяся на данные умных городов, где, например, эмоции людей, потоками движущихся по транспортным системам, распознаются без согласия с их стороны, и на этой основе настраивается реклама [McStay, 2020].

К сходным с Солавом (философом и юристом) выводам об устаревании и обессмысливании consent'a (акта личного рационального согласия на доступ к своим данным) приходят и исследователи, работавшие на эмпирическом материале. Интернет вещей и социальные сети предполагают обыденность сбора огромного числа данных без любого информированного согласия [Taylor, Floridi, van der Sloot, 2016], а также риски утечек. Можно, конечно, повесить информационные таблички о том, что вас снимают камеры, а поведение фиксируется разнообразными датчиками, однако ни в одном из уже разворачивающихся умных городов невозможно добиться согласия граждан на сбор этого многообразия данных, а также на их последующую рециклизацию (использование для других целей в других приложениях и программных средах) [Löfgren, Webster, 2020]. Это не удается сделать, даже если эта новая реальность входит в противоречие с базовыми юридическими установками, например, Евросоюза (GDPR).

Аффекты цифровой приватности: побег, апатия, цинизм

Распространение и проникновение различных форм цифрового слежения и контроля, конечно же, вызывает противодействие. Более того: исследователи призывают описывать происходящее не как огромную «плиту» цифровой слежки, которая давит всё остальное, но скорее как множество форм «зора» (veillance), взаимодействующих, противоборствующих и пересекающихся. Над-зор (surveillance), с его неравенством надзирающего и надзираемых, перебивается «под-зором» (sousveillance) – например, распространением видеорегистраторов, обязательным ношением нательных видеокамер полицейскими и тому подобными усилиями выровнять дисбаланс [Mann, 2005]

Не менее важен и противо-зор (counterveillance) – стратегия, направленная, с одной стороны, на политический и правовой активизм с целью ограничения возможностей для слежки и контроля законодательными средствами. С другой стороны, эта стратегия предполагает искусство обходить блокировки, устанавливать программное обеспечение для сохранения приватности, переход к защищенным браузерам вроде Tor, серверам вроде Protonmail, криптографическим инструментам работы в сети (вроде Signal) и тому подобным средствам продвинутой цифровой грамотности. Можно сказать, что эти две стратегии (над-зор и противо-зор) разделяются по принципу коллективное versus индивидуальное действие, желание действовать ради общественного блага versus ради личного [Prainsack, 2019]

Наконец, социально важной реакцией на различные формы подавления приватности сейчас оказываются разнообразные формы ухода из цифрового мира (digital disengagement), вызванные, конечно, не только страхом перед надзором, но и множеством иных причин – желанием сберечь время, соблюдать личную цифровую гигиену, регламентировать социальные связи и т. д. [Кунц-

ман и др., 2018]. Выбор таких стратегий отношения к ограничению приватности и цифровому надзору – достаточно хорошо исследованная на эмпирическом материале тема, и в соответствующих исследованиях учитываются такие факторы, как личные фобии, идеологическая позиция человека, отношение к государству, уважение к ценностям безопасности, возраст и социальный статус пользователей различных цифровых инфраструктур [Taewoo Nam, 2019; Mols, Jannsen, 2017].

Данные, полученные в ходе международных исследований, находят свое подтверждение и на российском (в частности, московском) материале. Среди различных поколений москвичей достаточно силен сентимент, предполагающий отказ от предоставления своих данных коммерческим и государственным платформам в связи с опасениями роста контроля с их стороны над частной жизнью пользователей:

> «*Я очень долго не регистрировался, например, в Госуслугах. Просто-таки по причине, потому что огромное количество данных: паспорт и банковский счет, потому что нужно привязывать, например, к Сбербанку свою учетную запись. Она сразу же передается государству, и это тоже как бы не очень хорошо. Сразу напоминает Китай. Это как бы, это не очень хо... То есть как бы вот эта социальная структура – система оценивания, которая в Китае, она реально напоминает антиутопию. Я не знаю, как там на самом деле действительно, потому что если читать новости, то это, конечно, звучит тревожно. Как она работает и как будет работать – непонятно. Но если саму как бы разглядывать ее суть, то это, это реально антиутопия, такой Сбербанк*» (ФГ, мужчина, 24 года, Москва).

В настоящее время не только на уровне теоретических положений, но в ходе социологических исследований установлено, что индивиды в современном обществе все яснее понимают невозможность сокрытия персональных данных: личные данные неизбежно «утекают», открытости становится всё больше, от сбора и анализа цифрового следа спрятаться невозможно. Отдельные информационные «бомбы» (например, разоблачения Сноудена, утечки секретных данных в рамках иных контекстов) могут усиливать эту тенденцию, однако развивается она и без них. В результате можно говорить о формировании в современном обществе реализма надзора (surveillance realism) – рутинизации жизни в ситуации тотального сбора данных и осознания того обстоятельства, что приватность невозможно сохранить. Это приводит к пассивности, самоцензуре и общей установке, которую проще всего выразить соображением типа «мы ни на что не можем повлиять» [Dencik, Cable, 2017]. Понятие «реализм надзора» было введено в рамках анализа материала британского исследования.

Другой коллектив авторов, работавший на корейском материале, вводит понятие усталости от приватности (privacy fatigue). Под этим понимается чувство утомления от всей проблематики приватности, возникающее из-за отсутствия реальных инструментов контроля над собственными персональными данными в интернете [Choi et al., 2018].

Характерным признаком усталости, сопутствующей заботе по сохранению своей приватности в интернете, является желание вовсе отказаться от использования гаджетов и разнообразных цифровых продуктов:

> «*Я на самом деле тоже ссылаюсь к позиции, что оставлять свои личные данные – это сейчас опасно и тревожно. Ну, как бы на душе. И меня сейчас, например, когда я регистрируюсь где-то на очередном, в очередном приложении, сайте или что-то, у меня такой звоночек: сколько я уже данных этих оставил? Потому что, например, вот я недавно устанавливал Viber. С таким скрипом я это делал, потому что еще одно приложение-мессенджер после Telegram, после Facebook мессенджеровского, после WhatsApp. И просто зачем так много этих мессенджеров, почему нельзя один просто взять? Это такой первый момент. А второй момент – я очень сильно устал от прозвона звонков. У меня даже появилась идея поменять телефон, чтобы хотя бы на один год в тишине пожить. Потом, скорее всего, снова бы пришлось менять*» (ФГ, мужчина, 23 года, Москва).

Другой сходный аффект – апатия: опрошенные британским социологом Дарреном Эллисом информанты не просто равнодушны или подчинены процессу нарастающего цифрового контроля (technosecuritization). Их поведение скорее можно описать как попытку научиться управлять своими негативными эмоциями: «Этих систем невозможно избежать, и с ними почти ничего нельзя сделать, и зачем же по собственной воле беспокоиться по их поводу?» [Ellis, 2020: 20].

Апатия и равнодушие относительно негативных эффектов от сбора пользовательских

данных встречаются во всех возрастных группах — и среди людей старшего возраста, и среди молодежи, представители которой испытывают, с одной стороны, бóльшую «цифровую нагрузку» на свою жизнь, а с другой — уделяют значительную долю внимания разнообразным «практикам себя», призванным интенсифицировать контроль над фоновыми психологическими состояниями:

> «*Я не знаю, что скажут мои коллеги и как будет дальше у нас идти дискуссия, но я на самом деле, наверное, один из самых пофигистичных к этому людей, потому что я абсолютно без каких-либо сомнений принимаю все куки, абсолютно готова подписывать любые там какие-то соглашения, давать свои данные. Я за это иногда плачусь тем, что мне постоянно звонят из всяких там этих липовых Сбербанков и присылают кучу рассылок. Вот. Но при этом меня это абсолютно никак в основном не напрягает. И я считаю, что как бы, если о нас захотят что-то узнать, то тут ничего не поможет, и если надо будет, то узнают, то посмотрят, то залезут куда угодно. Вот. Меня за это очень как-то не одобряют мои друзья близкие, мои родители тоже говорят, что я слишком как-то вот беспечна — везде зарегистрировалась, везде свой телефон оставила, вот тебе и звонят. Вот. Но я к этому отношусь абсолютно вот спокойно, прямо максимально*» (ФГ, женщина, 22 года, Москва).

Наконец, возможно, наиболее точным и плодотворным обозначением такого комплекса позиций и установок можно считать цинизм по отношению к приватности (privacy cynicism). Цинизм, возникающий как следствие недоверия и скрытого конфликта [Almada et al., 1991], характерен для среды с низким уровнем институционального доверия [Langworthy, 1987]. Еще одним фактором возникновения циничного отношения к реальности является чувство беспомощности: когда человек не может повлиять на решения, которые принимают его контрагенты, у него развивается циничный взгляд на мотивы и интересы последних [Dean et al., 1998].

Наиболее проработана модель цифрового цинизма в исследовании, написанном на немецком материале [Lutz et al., 2020]. Авторы определяют его как «чувство неясности, бессилия и недоверия к тому, как с персональными данными пользователей обращаются цифровые платформы… Капитализм данных, основанный на сборе персональных данных… делает оценку приватности и контроль ее уровня слишком сложными для пользователей… Цинизм в отношении сферы приватности — это когнитивный механизм, позволяющий пользователям, ощущающим свое бессилие, справляться [со своей жизнью в интернете], работать с цифровыми платформами без когнитивного диссонанса. Они вырабатывают рациональное отношение к вопросу защиты приватной сферы, рассматривая ее как нечто бесполезное» [Lutz et al., 2020: 1174].

Информанты недавного исследования, проведенного методами качественной социологии, заявляли, что защита приватности бессмысленна и поэтому они позволяют себе полную беспечность относительно собственных персональных данных. По словам одного из них, «нелогично полагать, что можно как-то скрыть свой цифровой след, учитывая количество действий, которые мы совершаем в сети. Вам придется стать каким-то асоциальным отщепенцем, живущим в горах» [Hoffmann et al., 2016: 7]. Опираясь на эти работы, в США был проведен массовый опрос; выяснилось, что цинизм в отношении приватности статистически связан с тем, что люди все чаще соглашаются с практиками, нарушающими приватность (онлайн-профилирование, доступ приложений к геолокации, установка цифровых «водяных знаков» и проч.) [Segijn, van Ooijen, 2020].

Приведенный выше обзор моделей и понятий, используемых в современных исследованиях угроз сфере приватной жизни, имеет существенное ограничение, связанное с преимущественным вниманием к цифровой среде и поведению в социальных сетях. Однако если исходить из международного контекста обсуждения этой проблематики, именно эти понятия и модели должны быть использованы для концептуализации эмпирических исследований.

Таким образом, при оценке социальных эффектов цифровых городских политик эти концепты, уже достаточно хорошо исследованные и описанные, представляются нам достаточно плодотворными и пригодными для применения в рамках дальнейших эмпирических исследований.

Приватность и цифровые политики в городе: кейсы QR-кодов, распознавание лиц и партисипативные платформы

Среди множества современных технологий, в настоящее время активно используемых в управлении городом (и, шире,

в организации любого рода процессов в городах, от здравоохранения и охраны правопорядка до выборов), мы выделяем три — с нашей точки зрения, одновременно относительно новых, активно затрагивающих проблему цифровой приватности и, наконец, объединяющих недавний московский опыт с опытом других стран. Речь идет о QR-кодах (в привязке к перемещениям и здоровью граждан в пандемию COVID-19), о системе распознавания лиц (вместе с камерами видеонаблюдения) и о цифровых платформах вовлечения граждан (аналогах «Активного гражданина»).

QR-коды относятся к классу технологий автоматической идентификации и сбора данных наряду с биометрией (идентификация по голосу, отпечаткам пальцев, сетчатке глаза) и радиочастотной идентификацией (RFID, например, смарт-карты и бесконтактные мобильные платежи). Эти технологии автоматизируют ручной труд и в целом нацелены на повышение «бесконтактных» взаимодействий.

Онтология QR-кодов предполагает представление о пользователях как о множестве лиц, принимающих решения, одновременно автономных и включенных в систему сбора данных и управления информацией. QR-коды как технология восходят к разработанным еще в середине XX века системам отслеживания перемещений рабочих по цехам (например, с помощью светящихся колец на пальце) в целях оптимизации трудовой дисциплины. С переходом дисциплинирующей логики отслеживания от промышленности к здравоохранению, на стыке медицины и IT-технологий возникает новая система, где люди сами берут на себя обязательства по автоматизации общества [Nguyen, 2022].

Пандемия COVID-19 поставила перед государственными и муниципальными властями всей планеты необычные задачи, которые надо было решать оперативно и в предельно стрессовых условиях. В этих обстоятельствах обращение к специфическим IT-решениям, точнее «склеивание» фабрично-логистической технологии QR-кодов [Denso Wave, 2021], логики «для всего найдется свое приложение» (there's an app for that), смартфонов и подключения по Bluetooth, наряду с традиционными карантинными практиками проверок и блок-постов имело свое основание. В результате произошло стирание различий между медицинскими практиками (надзор над болезнью) и полицейскими (надзор над людьми) [French, Monahan, 2020]. Но самое важное в QR-кодах как технологии эпиднадзора (что отличает ее от, например, видеонаблюдения) заключается в том, что для ее работы необходимо активное согласие граждан — и формирование сетей из граждан, их физических тел и мобильных устройств [Yang et al., 2021].

И практики применения QR-кодов, и отношение к ним граждан варьируют от страны к стране. Так, Китай за несколько недель присвоил 900 млн жителей страны QR-коды, которые они обязаны были предъявлять с помощью мобильного устройства или распечатки, чтобы пользоваться общественным транспортом [Wu et al., 2020]. Присвоение QR-кодов основано на алгоритмах, объединяющих самооценку состояния здоровья людей, статистику и данные из социальных сетей и транспортных систем в режиме реального времени [Shachar, Mahmood, 2021]. Контрольные пункты проверки кодов работали на основных транспортных узлах страны, в том числе внутри городов.

В Австралии, напротив, QR-коды применяли в общественных заведениях, где сами граждане должны были сканировать эти коды при помощи телефона — такое решение облегчало жизнь организациям (в противном случае им приходилось записывать информацию о посетителях на бумагу). В Китае QR-коды помогали государству решать свои задачи по сдерживанию эпидемии, в Австралии — были скорее подспорьем, позволяющим автоматизировать бюрократические процедуры. Главным же цифровым решением в стране стало приложение по отслеживанию контактов COVIDSafe, работающее на основе технологии Bluetooth. Оно фактически отслеживало перемещения пользователей — и именно это вызвало наибольшие опасения и недовольство граждан, опасавшихся за неприкосновенность своей частной жизни (и того, что данные об их перемещениях попадут в руки хакеров). Эта реакция, во-первых, заставила власти страны отказаться от требования обязательного скачивания и использования приложения (по китайскому пути) и, во-вторых, законодательно запретить передачу любых данных COVIDSafe каким-либо организациям или использование их для любых целей, кроме отслеживания контактов [Asghar et al., 2021].

Наконец, Новая Зеландия пошла третьим путем: ее основное решение — приложение NZ COVID Tracer, также для отслеживания контактов, не применяет ни Bluetooth, ни NFC, а работает через QR-коды. Коды Минздрава наносились внутри помещений, чтобы посетители ска-

нировали и добавляли местоположение в свой «дневник» перемещений (он же траектория контактов). В отличие от Китая, этот процесс является добровольным. Более того, «узлами» сети здесь выступают не люди, а географические точки (как места потенциальной опасности заражения).

Наиболее масштабное исследование социальных эффектов QR-кодов на сегодняшний день было проведено в Китае (и государственного приложения «Дзянькан ма», 健康码, обязательного для скачивания, с его трехуровневой системой индикации здоровья пользователя — красный, желтый, зеленый, — только последний дает право пользоваться общественным транспортом и посещать любые заведения). Авторы исследования [Tai et al., 2021] предлагают следующую типологию реакций и поведенческих стратегий граждан на внедрение подобной инициативы:

1) лишение прав и технологическое исключение — те, у кого вообще нет смартфонов и кто полностью выпадает из системы и, соответственно, заблокирован и отчужден от пользования городом;

2) «отказники» — те, кто отказался его установить и пользоваться им (слишком сложное и неудобное приложение);

3) «пользователи поневоле» — те, кто скачал и пользуется приложением, но пребывает в перманентной фрустрации (Что, если на смартфоне сядет батарейка? А если пропадет связь? А если случится сбой и «зеленый» статус по ошибке станет «красным»?);

4) «те, кто обхитрил систему» — группа пользователей, которая обладает IT-компетенциями выше среднего и выяснила, как работает приложение и как обратить в свою пользу все лазейки; наиболее распространенная хитрость — покупка второго смартфона с установкой приложения на него (это устройство все время лежит дома, что снижает риск попадания в «красную» зону);

5) «взломщики» — еще менее распространенный тип поведения, который предполагает взлом приложения для получения поддельного QR-кода.

Если говорить о том, какие эффекты от введения QR-кодов во время пандемии коронавируса наблюдаются в России, то следует указать, что на момент активного обсуждения этой инициативы и ее последующего внедрения (лето–осень 2021 года) чуть больше половины россиян (56%) — как среди тех, кто на тот момент был вакцинирован, так и тех, кто вакцинирован не был, — поддерживали меры по ограничению прав тех граждан, которые не имели QR-кода (например, недопуск на массовые мероприятия, в общественный транспорт и т.д.). В то же время 40% опрошенных в исследовании ВЦИОМ были против подобных ограничений. Важно отметить, что результаты по этому же вопросу, но только среди вакцинированных, демонстрируют иные цифры: в этой аудитории доля тех, кто был бы готов поддержать ограничительные меры в адрес сограждан, не имеющих QR-кодов, оказалась значительно выше и достигла 74%. Если же оценивать динамику мнений опрошенных по этому вопросу не в федеральном масштабе, а среди жителей крупных городов, в том числе Москвы, то окажется, что жители мегаполисов относятся к введению QR-кодов с бóльшим доверием, чем жители глубинки [ВЦИОМ, 2021].

Тем не менее, какой бы значимой ни была история с распространением коронавируса и практик по борьбе с ним, на долгой дистанции основным социальным эффектом от внедрения системы QR-кодов стало их повсеместное проникновение: вначале в качестве документа, удостоверяющего факт наличия прививки, а затем — в качестве часто применяемого средства распространения информации и удобного инструмента, интегрированного в систему повседневных платежных практик. Все это, в свою очередь, стало особенно значимым после прекращения работы различных бесконтактных платежных сервисов в России в 2022 году. Другими словами, можно утверждать, что негативное отношение к введению QR-кодов на старте работы этой технологии не помешало операторам соответствующих цифровых инфраструктур внедрить их в жизнь, сделав большинство граждан РФ «пользователями QR-технологии поневоле».

Использование автоматизированного визуального наблюдения и слежки — неотъемлемая черта современных средств охраны правопорядка и общественной безопасности. Ставшие уже привычными в глобальном масштабе и повсеместными (особенно в городских условиях) камеры видеонаблюдения дополняются мобильными устройствами (беспилотники, носимые камеры у сотрудников полиции). Применение *технологии распознавания лиц* — еще один виток развития данного подхода.

В Европе и США уже давно разворачивается общественная дискуссия об использовании камер видеонаблюдения. Сторонники подчеркивают пользу этой технологии как источника доказательств для выявления подозреваемых в преступлениях, а также

отмечают эффект сдерживания правонарушений в общественных местах, оборудованных видеокамерами [Ashby, 2017]. Противники же недовольны тем, что камеры ограничивают развитие бизнеса в общественных местах (кафе, рестораны, фланерство и проч.) и угрожают частной жизни граждан. Также опасения вызывают возможные злоупотребления со стороны полицейских, имеющих доступ к чувствительным данным, страх перед властью «большого брата», недовольство ощущением постоянного наблюдения) [Bennett, Gelsthorpe, 1996]. Активно обсуждаются пути достижения баланса между борьбой с преступностью и защитой приватности [Sheldon, 2011].

В целом относительно новые технологии распознавания лиц вызывают ровно те же эмоции и дискуссии. Снова подчеркивается их очевидная эффективность в общественной безопасности. И так же они подвергаются критике за «заморозку» живой, спонтанной активности в публичных пространствах города за злоупотребления со стороны полицейских и других силовых структур, а также за неизбежное покушение на приватность и частную жизнь при сборе и использовании данных [Naker, Greenbaum, 2017].

Данные социологических исследований отражают такой разброс мнений. Опрос населения в трех странах (США, Великобритания, Австралия) показал, что более 80% респондентов поддерживают реактивное применение систем распознавания лиц в рутинной полицейской работе (например, поиск преступников, людей, пропавших без вести, расследование преступлений). Однако менее 30% респондентов одобряют проактивное использование этих систем (например, мониторинг и слежку за гражданами). По данным другого исследования, проведенного в США, большинство респондентов (59%) поддерживают использование систем распознавания лиц правоохранительными органами для снижения угроз безопасности в общественных местах, 73% считают, что они могут помочь в поиске правонарушителей и снижении уровня преступности, а 56% заявили о доверии к тому, что сотрудники правоохранительных органов будут ответственно использовать полученные данные [Pew Research Center, 2019]. Также выяснилось, что поддержка или, наоборот, подозрительное отношение к данной технологии связаны с политическими взглядами человека, степенью его доверия к властям и с его представлениями о полиции. Люди старшего возраста, мужчины, белые и республиканцы (в США) чаще всего поддерживают дальнейшее распространение систем распознавания лиц [Bromberg et al., 2020].

Ситуация с внедрением в городскую повседневность систем распознавания лиц в России близка к общемировой. Актуальные исследования [ВЦИОМ, 2022] демонстрируют, что большинство граждан (57%) согласны с развитием таких технологий в быту только в том случае, если эта практика не будет нарушать право граждан на личную жизнь, а персональные данные будут надежно защищены. Важно отметить, что около пятой части опрошенных (18%) не согласны с использованием технологии распознавания лиц вовсе, так как даже с соблюдением всех предосторожностей подобная мера является очевидным вторжением в сферу приватного. При этом примерно такой же процент граждан (19%) считают, что доверять любым системам, базирующимся на технологиях искусственного интеллекта, не следует по той причине, что эти технологии не являются носителями человеческой этики и морали.

Платформа Mos.ru и связанные с ней сервисы (система электронных опросов «Активный гражданин», Московская электронная школа, система дистанционного электронного голосования и др.) — один из примеров все более популярного в современных городских экосистемах внедрения *цифровых платформ*. Только в Европе уже 120 муниципалитетов применяют такие платформы [EU SCIS, 2022]. Программа-максимум таких проектов — не просто выстроить умный город, цифровизировать существующие сервисы и интерфейсы, но перейти к модели «управление как платформа», опирающейся на принципы прозрачности, соучастия и сотрудничества [O'Reilly, 2010].

Реальный опыт использования городских платформ, роль властей как владельцев платформ, отношение к ним граждан, способы участия — все это только начинает осмысляться и исследоваться [Haveri, Anttiroiko, 2023]. Однако уже возникло понимание, что успех зависит от установок и решений тех, кто проектирует «город как платформу», и от политической обстановки. Немаловажно и то, что цифровые платформы нередко «выключают» из участия в жизни города целые группы жителей, которые или сами не имеют к ним доступа, или считаются проектировщиками «неудобными» и «отсталыми» — так, в африканских умных городах это бедняки и в целом неформальный сектор экономики [Peter, Meyer, 2022: 9].

Аналоги «Активного гражданина» давно и эффективно используются в городах Западной Европы, США, Австралии и Южной

Азии [Swist et al., 2017; Falco, Kleinhans, 2018] – это цифровые партисипаторные платформы, или платформы вовлечения общественности (participatory platforms, public engagement platforms). Они отчасти разделяют функционал социальных сетей и форумов, но при этом специально нацелены на учет мнений горожан по выдвинутым властями вопросам, а также включают инструменты визуализации данных, геймификации и картографирования [Feeney, Brown, 2017].

Основным аналитическим инструментом для исследования таких платформ и их места в жизни горожан считается «партисипаторный куб» [Poplin, Fereira, Rocha, 2013]. У него три измерения: это доступ к участию, тип коммуникации и власть, позволяющая принимать решения. Доступ может предоставляться или конкретным организациям, или тем, кто проходит определенный фильтр, или вообще всем желающим. Второе измерение определяет, коммуницируют ли граждане на платформе только с властью (организатором опросов и обсуждений), с другими организациями или также и друг с другом. Третье измерение – это то, какие полномочия есть у лиц или учреждений, участвующих в активностях платформы: консультационные (информировать городские власти о своих предпочтениях), возможность решать (выбирать между предложенными опциями в уверенности, что результаты выбора будут реализованы) и, наконец, предлагать свои идеи для будущих обсуждений.

В целом мировой опыт показывает, что цифровые платформы повышают вовлеченность граждан в жизнь города, прежде всего благодаря удобству использования (они доступны круглосуточно и не требуют специальной поездки к определенному времени). Отмечается, что они активно привлекают молодежь, обычно менее склонную к гражданской активности [Nam-Jin et al., 2013]. Вместе с тем отмечается, что обсуждение онлайн хуже, чем очное (лицом к лицу), позволяет понять и обсудить альтернативные точки зрения на проблему [Hindman, 2008]. Та же геймификация, формы обратной связи и другие особенности интерфейса могут привести к тому, что осмысленные обсуждения и принятие решений будут тонуть в «белом шуме» [Farina et al., 2014].

Заключение

Современные цифровые технологии, являющиеся неотъемлемой частью множества социальных политик, разворачивающихся в пределах мегаполисов по всему миру и в том числе, безусловно, в Москве, играют в жизни горожан двоякую роль. С одной стороны, бурное развитие разнообразных дигитальных сервисов возможно в силу того удобства, которое их работа привносит в повседневность. Бесшовность взаимодействия горожан друг с другом, с властями, с инфраструктурами – основной аргумент пропонентов подобных систем. С другой стороны, растущая скорость таких взаимодействий, их обезличенность и непрозрачность для рядовых пользователей формируют новые, недоизученные в российском контексте социальные эффекты, характеризующиеся, в первую очередь, отчуждением – как отчуждением людей друг от друга (снижение уровня солидарности на фоне минимизации личных контактов, разобщение), так и отчуждением от самих себя в связи с невротизацией повседневности (рост недоверия технологиям, тревожности, интенсивности опасений относительно тотального контроля за сферой приватного и т.п.).

Противоречие между технократическими цифровыми практиками управления городской средой, являющимися по своей сути организованными вертикально (держатели цифровых платформ находятся на вершине этой вертикали, а атомизированные пользователи, не имеющие представления о том, как технически эти платформы функционируют, – в ее основании) и горизонтальными практиками самоорганизации горожан, в настоящий момент находится в состоянии хрупкого равновесия. С точки зрения многих исследователей, работы которых цитировались выше, а также тех, кто не попал в наш обзор, несмотря на авторитет в академических кругах (см., например, работу Ш. Зубофф «Эпоха надзорного капитализма»), это равновесие не должно качнуться в сторону дегуманизации социального взаимодействия.

В этом отношении тревогу у наших респондентов-москвичей вызывают не только те цифровые городские сервисы, которые уже доказали свою эффективность («Госуслуги», mos.ru и т.п.), но и те, чье внедрение в городскую повседневность еще только предстоит в будущем – например, системы социального рейтингования и оценивания. Несмотря на то что перспектива разворачивания таких систем в законченном виде (по китайской модели, как мы представляем ее себе по профильным публикациям) пока неочевидна, это не мешает москвичам проводить напрашивающиеся параллели:

«Для меня оценивать людей — это как-то не всегда гуманно, что ли. То есть я понимаю — оценивать товар. Грубо говоря, товар, продукт какой-то финальный. То есть, например, я не знаю, там фильм — это финальный продукт, ты его оцениваешь со всех сторон, ты можешь как-то его осмыслить. […] А когда ты оцениваешь человека, это немножко напоминает… супермаркет. То есть ты просто выбираешь товар, который тебе подходит или не подходит. И у тебя в итоге никакого общения с человеком не формируется, как правило, в этих приложениях. И они, как правило, оказываются невероятно мусорными. То есть они просто тратят твое время» (ФГ, мужчина, 26 лет, Москва).

Подводя итог сказанному, важно отметить, что городским властям как основным держателям цифровых платформ необходимо застраховаться от того, чтобы социальные эффекты разработки и внедрения цифровых городских политик не превратились в антисоциальные в строгом смысле слова — разобщающие, невротизирующие и разрушающие горизонтальные связи горожан.

Источники

Кунцман А., Богданова Е.О., Пономарева Э.Я., Щетвина А.А. (2018) Отказ и ограничение использования интернета в среде российских IT-специалистов // Социология власти. № 3. С. 144–164.

ВЦИОМ (2021) Отношение россиян к мерам по борьбе с коронавирусом. Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/otnoshenie-rossijan-k-meram-po-borbe-s-koronavirusom (дата обращения 17.04.2023).

ВЦИОМ (2022) Искусственный интеллект: угроза или светлое будущее? Режим доступа: https://wciom.ru/analytical-reviews/analiticheskii-obzor/iskusstvennyi-intellekt-ugroza-ili-svetloe-budushchee (дата обращения 17.04.2023).

Almada S.J., Zonderman A.B., Shekelle R.B. et al. (1991) Neuroticism and Cynicism and Risk of Death in Middle-Aged Men // Psychosomatic Medicine. No. 53. P. 165–175.

Asghar H., Farokhi F., Kaafar D., Rubinstein B. (2021) On the Privacy of TraceTogether, the Singaporean COVID-19 Contact Tracing Mobile App, and Recommendations for Australia. Режим доступа: https://eng.unimelb.edu.au/ingenium/technology-and-society/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia (дата обращения: 17.04.2023).

Ashby M.P. J. (2017) The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis // European Journal of Criminology Policy Research. No. 23. P. 441–459.

Bennett T., Gelsthorpe L. (1996) Public Attitudes Toward CCTV (Closed Circuit Television) in Public Places // Studies on Crime and Crime Prevention. Vol. 5 (1). P. 72–90.

Bromberg D.E., Charbonneau E., Smith A. (2020) Public Support for Facial Recognition via Police Body-Worn Cameras: Findings from a List Experiment // Government Information Quarterly. Vol. 37 (1). P. 1–8.

Choi H., Park J.,Jung Y. (2018) The Role of Privacy Fatigue in Online Privacy Behaviour // Computers in Human Behavior. No. 81. P. 42–51.

Dean J.W., Brandes P., Dharwadkar R. (1998) Organizational Cynicism // Academy of Management Review. No. 23. P. 341–352.

Dencik L., Cable J. (2017) The Advent of Surveillance Realism // International Journal of Communication. No. 11. P. 763–781.

Denso Wave (2021) QR Code Development Story vol. 1. Режим доступа: https://www.denso-wave.com/en/technology/vol1.html (дата обращения: 17.04.2023).

Ellis D. (2020) Techno-Securitisation of Everyday Life and Cultures of Surveillance-Apatheia // Science as Culture. Vol. 29 (1). P. 11–29.

EU SCIS (2022) EU Smart Cities Information System: Projects and Sites Overview. Режим доступа: https://smart-cities-marketplace.ec.europa.eu/projects-and-sites (дата обращения: 17.04.2023).

Falco E., Kleinhans R. (2018) Digital Participatory Platforms for Co-Production in Urban Development: A Systematic Review // International Journal of E-Planning Research. Vol. 7 (3). P. 1–27.

Farina C.R., Epstein D., Heidt J., Newhart M.J. (2014) Designing an Online Civic Engagement Platform: Balancing ‘More’ vs. ‘Better’ Participation in Complex Public Policymaking // International Journal of E-Politics. Vol. 5 (1). P. 16–40.

Feeney M.K., Brown A. (2017) Are Small Cities Online? Content, Ranking, and Variation of US Municipal Websites // Government Information Quarterly. Vol. 34 (1). P. 62–74.

Flaherty D.H. (1989) Protecting Privacy in Surveillance Societies. Chapel Hill, NC: University of North Carolina Press.

French M., Monahan T. (2020) Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19? // Surveillance and Society. No. 18. P. 1–11.

Floridi L. (2014) Open Data, Data Protection, and Group Privacy // Philosophy & Technology. No. 27. P. 1–3.

Floridi L. (2016) On Human Dignity as a Foundation for the Right to Privacy // Philosophy & Technology. No. 29. P. 307–312.

Gavison R. (1980) Privacy and the Limits of the Law // Yale Law Journal. Vol. 89 (4). P. 421–471.

Haveri A., Anttiroiko A.-V. (2023) Urban Platforms as a Mode of Governance // International Review of Administrative Sciences. Vol. 89 (1). P. 3–20.

Hindman M. (2008) The Myth of Digital Democracy. Princeton: Princeton University Press.
Hoffmann C.P., Lutz C., Ranzini G. (2016) Privacy Cynicism: A New Approach to the Privacy Paradox//Journal of Psychosocial Research. Vol. 10 (4). DOI: 10.5817/CP2016-4-7.
Langworthy R.H. (1987) Police Cynicism: What We Know from the Niederhoffer Scale//Journal of Criminal Justice. Vol. 15 (1). P. 17–35.
Löfgren K., Webster C.W. R. (2020) The Value of Big Data in Government: The Case of 'Smart Cities.'//Big Data & Society. Vol. 7 (1). DOI: https://doi.org/10.1177/2053951720912775.
Lutz C., Hoffmann C.P., Ranzini G. (2020) Data Capitalism and the User: An Exploration of Privacy Cynicism in Germany// New Media & Society. Vol. 22 (7). P. 1168–1187.
Mann S. (2005) Sousveillance and Cyberglogs. A 30-year Empirical Voyage Through Ethical, Legal and Policy Issues//Presence: Teleoperators and Virtual Environments. Vol. 14 (6). P. 625–646.
McStay A. (2020) Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy//Big Data & Society. No. 7. DOI: https://doi.org/10.1177/2053951720904386.
Mols A., Janssen S. (2017) Not Interesting Enough to be Followed by the NSA//Digital Journalism. No. 5:3. P. 277–298.
Naker S., Greenbaum D. (2017) Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy//Boston University Journal of Science and Technology Law. Vol. 23 (1). P. 88–122.
Nam-Jin L., Shah Dh. V., McLeod J.M. (2013) Processes of Political Socialization: A Communication Mediation Approach to Youth Civic Engagement//Communication Research. Vol. 40 (5). P. 669–97.
Nguyen D. (2022) Convenient efficiency: A media genealogy of QR codes//New Media & Society, 0(0) DOI: https://doi.org/10.1177/14614448221141086.
Norberg P.A, Horne D.R., Horne D.A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors//Journal of Consumer Affairs. Vol. 41 (1). P. 100–126.
Pew Research Center (2019) More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly. Режим доступа: https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ (дата обращения: 17.04.2023).
Peter C., Meyer C. (2022) Organizing for the Smart African City: Leveraging the Urban Commons for Exerting the Right to the City//Organization Studies, 0 (0) DOI: https://journals.sagepub.com/doi/10.1177/01708406221089609.
Poplin A., Pereira G.C., Rocha M.C.F. (2013) The Participatory Cube: A Framework for Analysis of Online Participation Platforms./In: Geertman, S., Toppen, F., Stillwell, J. (eds)//Planning Support Systems for Sustainable Urban Development. Lecture Notes in Geoinformation and Cartography, vol 195. Springer, Berlin, Heidelberg.
Prainsack B. (2019) Logged out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons//Big Data & Society. Vol. 6 (1). DOI: https://doi.org/10.1177/2053951719829773.
O'Reilly T. (2010) Government as a Platform. In: Lathrop Daniel, Ruma Laurel (Eds.), Open Government: Collaboration, Transparency, and Participation in Practice (P. 11–39). Sebastopol, CA: O'Reilly Media.
Segijn C.M., van Ooijen I. (2020) Perceptions of Techniques Used to Personalize Messages Across Media in Real Time//Cyberpsychology Behaviour and Social Networking. Vol. 23 (5). P. 329–337.
Shachar A., Mahmood A. (2021) The Body as the Border//Historical Social Research Historische Sozialforschung. Vol. 46 (3). P. 124–150.
Sheldon B. (2011) Camera Surveillance Within the UK: Enhancing Public Safety or a Social Threat?//International Review of Law, Computers & Technology. No. 25. P. 193–203.
Solove Daniel J., Privacy Self-Management and the Consent Dilemma (November 4, 2012). 126 Harvard Law Review 1880 (2013). GWU Legal Studies Research Paper No. 2012–141, GWU Law School Public Law Research Paper No. 2012-141. Режим доступа: https://ssrn.com/abstract=2171018.
Swist T., Magee L., Phuong J., Sweeting D. (2017) The Labour of Communicating Publics: Participatory Platforms, Socio-Technical Intermediaries and Pluralistic Expertise//Communication and the Public. No. 2. P. 210–225.
Taewoo Nam (2019) What Determines the Acceptance of Government Surveillance? Examining the Influence of Information Privacy Correlates//The Social Science Journal. No. 56:4. P. 530–544.
Tai Z., Yu X., He B. (2021) Locked Down Through Virtual Disconnect: Navigating Life by Staying on/off the Health QR Code During COVID-19 in China//Convergence. Vol. 27 (6). P. 1648–1662.
Taylor L., Floridi L., van der Sloot B. (2016) Group Privacy: New Challenges of Data Technologies. Berlin: Springer.
Westin A.F. (1967) Privacy and Freedom. New York: Athenaum.
Wu J., Wang J., Nicholas S. et al. (2020) Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations//Journal of Medical Internet Research. Vol. 22 (10): e21980.
Yang F., Heemsbergen L., Fordyce R. (2021) Comparative Analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: A New Corona of Public Health Governmentality?//Media International Australia. Vol. 178 (1). P. 182–197.

THE SOCIAL EFFECTS OF DIGITAL URBAN POLICIES: THE MOSCOW EXPERIENCE IN A GLOBAL CONTEXT

Vladimir V. Kartavtsev, Director, Centre for Applied and Field Research, Institute of Cultural Studies, Faculty of Urban and Regional Development, HSE University; 21/4 Staraya Basmannaya str., Moscow, 101000, Russian Federation.
E-mail: vkartavcev@hse.ru
Artyom A. Kosmarski, Senior researcher, Centre for Applied and Field Research, Institute of Cultural Studies, Faculty of Urban and Regional Development, HSE University; 21/4 Staraya Basmannaya str., Moscow, 101000, Russian Federation.
E-mail: akosmarskii@hse.ru

Abstract. This review article examines privacy as a key issue that arises when urban digital policies collide with residents' lifeworlds. The authors describe the different effects of privacy that characterize people's digital behavior and their attitudes to new technologies—the privacy paradox, digital escapism, apathy, and privacy cynicism. A comparative analysis is made of international and Russian experiences (primarily using the example of Moscow) in using such technologies as QR codes, face recognition, and digital participatory platforms. The authors conclude that the contradiction between technocratic digital practices of urban environment management, which are inherently vertically organized, and the horizontal practices of individual self-organization, is currently in a state of fragile equilibrium.
Key words: Moscow; oversight; privacy; digital policies; QR codes.
Citation: Kartavtsev V.V., Kosmarski A.A. (2023) Social Effects of Digital Urban Policies: The Moscow Experience in the Global Context. *Urban Studies and Practices*, vol. 8, no 1, pp. 61-73. DOI: https://doi.org/10.17323/usp81202361-73 (in Russian)

References

Almada S.J., Zonderman A.B., Shekelle R.B. et al. (1991) Neuroticism and Cynicism and Risk of Death in Middle-Aged Men. *Psychosomatic Medicine*, vol. 53, pp. 165–175.

Asghar H., Farokhi F., Kaafar D., Rubinstein B. (2021) On the Privacy of TraceTogether, the Singaporean COVID-19 Contact Tracing Mobile App, and Recommendations for Australia. Available at: https://eng.unimelb.edu.au/ingenium/technology-and-society/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia (accessed 17 April 2023).

Ashby M.P.J. (2017) The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. *European Journal of Criminology Policy Research*, vol. 23, pp. 441–459.

Bennett T., Gelsthorpe L. (1996) Public Attitudes Toward CCTV (Closed Circuit Television) in Public Places. *Studies on Crime and Crime Prevention*, vol. 5 (1), pp. 72–90.

Bromberg D.E., Charbonneau E., Smith A. (2020) Public Support for Facial Recognition via Police Body-Worn Cameras: Findings from a List Experiment. *Government Information Quarterly*, vol. 37 (1), pp. 1–8.

Choi H., Park J., Jung Y. (2018) The Role of Privacy Fatigue in Online Privacy Behaviour. *Computers in Human Behavior*, vol. 81, pp. 42–51.

Dean J.W., Brandes P., Dharwadkar R. (1998) Organizational Cynicism. *Academy of Management Review*, vol. 23, pp. 341–352.

Dencik L., Cable J. (2017) The Advent of Surveillance Realism. *International Journal of Communication*, vol. 11, pp. 763–781.

Denso Wave (2021) QR Code Development Story (vol. 1). Available at: https://www.denso-wave.com/en/technology/vol1.html (accessed 17 April 2023).

Ellis D. (2020) Techno-Securitisation of Everyday Life and Cultures of Surveillance-Apatheia. *Science as Culture*, vol. 29 (1), pp. 11–29.

EU SCIS (2022) EU Smart Cities Information System: Projects and Sites Overview. Available at: https://smart-cities-marketplace.ec.europa.eu/projects-and-sites (accessed 17 April 2023).

Falco E., Kleinhans R. (2018) Digital Participatory Platforms for Co-Production in Urban Development: A Systematic Review. *International Journal of E-Planning Research*, vol. 7 (3), pp. 1–27.

Farina C.R., Epstein D., Heidt J., Newhart M.J. (2014) Designing an Online Civic Engagement Platform: Balancing 'More' vs. 'Better' Participation in Complex Public Policymaking. *International Journal of E-Politics*, vol. 5 (1), pp. 16–40.

Feeney M.K., Brown A. (2017) Are Small Cities Online? Content, Ranking, and Variation of US Municipal Websites. *Government Information Quarterly*, vol. 34 (1), pp. 62–74.

Flaherty D.H. (1989) Protecting Privacy in Surveillance Societies. Chapel Hill, NC: University of North Carolina Press.

Floridi L. (2014) Open Data, Data Protection, and Group Privacy. *Philosophy & Technology*, vol. 27, p. 1–3.

Floridi L. (2016) On Human Dignity as a Foundation for the Right to Privacy. *Philosophy & Technology*, vol. 29, pp. 307–312.

French M., Monahan T. (2020) Disease Surveillance: How Might Surveillance Studies Address COVID-19? *Surveillance and Society*, vol. 18, pp. 1–11.

Gavison R. (1980) Privacy and the Limits of the Law. *Yale Law Journal*, vol. 89 (4), pp. 421–471.

Haveri A., Anttiroiko A.-V. (2023) Urban Platforms as a Mode of Governance. *International Review of Administrative Sciences*, vol. 89 (1), pp. 3–20.

Hindman M. (2008) *The Myth of Digital Democracy*. Princeton: Princeton University Press.

Hoffmann C.P., Lutz C., Ranzini G. (2016) Privacy Cynicism: A New Approach to the Privacy Paradox. *Journal of Psychosocial Research*, vol. 10 (4). DOI: 10.5817/CP2016-4-7.

Kuntsman A., Bogdanova E.O., Ponomareva E. Ya., Shchetvina A.A. (2018) Otkaz i ogranicheniye ispol'zovaniya interneta v srede rossiyskikh IT-spetsialistov [Renunciation and Self-Restraint in Internet Use Among Russian IT-Specialists]. *Sotsiologiya vlastti* [Sociology of power], vol. 3, pp 144–164. (in Russian)

Langworthy R.H. (1987) Police Cynicism: What We Know from the Niederhoffer Scale, *Journal of Criminal Justice*, vol. 15 (1), pp. 17–35.

Löfgren K., Webster C.W. R. (2020) The Value of Big Data in Government: The Case of 'Smart Cities.'. *Big Data & Society*, vol. 7 (1). DOI: https://doi.org/10.1177/2053951720912775.

Lutz C., Hoffmann C.P., Ranzini G. (2020) Data Capitalism and the User: An Exploration of Privacy Cynicism in Germany. *New Media &*

Society, vol. 22 (7), pp. 1168–1187.
Mann S. (2005) Sousveillance and Cyberglogs.
A 30-year Empirical Voyage Through Ethical, Legal and Policy Issues//Presence: Teleoperators and Virtual Environments, vol. 14 (6), pp. 625–646.
McStay A. (2020) Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy. *Big Data & Society*, vol. 7. DOI: https://doi.org/10.1177/2053951720904386.
Mols A., Janssen S. (2017) Not Interesting Enough to be Followed by the NSA. *Digital Journalism*, vol. 5 (3), pp. 277–298.
Naker S., Greenbaum D. (2017) Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy. *Boston University Journal of Science and Technology Law*, vol. 23 (1), pp. 88–122.
Nam-Jin L., Shah Dh. V., McLeod J.M. (2013) Processes of Political Socialization: A Communication Mediation Approach to Youth Civic Engagement. *Communication Research*, vol. 40 (5), pp. 669–97.
Nguyen D. (2022) Convenient Efficiency: A Media Genealogy of QR Codes. *New Media & Society*, 0 (0). DOI: https://doi.org/10.1177/14614448221141086.
Norberg P.A, Horne D.R., Horne D.A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *Journal of Consumer Affairs*, vol. 41 (1), pp. 100–126.
Pew Research Center (2019) More than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly. Available at: https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ (accessed 17 April 2023).
Prainsack B. (2019) Logged Out: Ownership, Exclusion and Public Value in the Digital Data and Information Commons. *Big Data & Society*, vol. 6 (1). DOI: https://doi.org/10.1177/2053951719829773.
Peter C., Meyer C. (2022) Organizing for the Smart African City: Leveraging the Urban Commons for Exerting the Right to the City. *Organization Studies*, 0 (0). DOI: https://journals.sagepub.com/doi/10.1177/01708406221089609.
Poplin A., Pereira G.C., Rocha M.C.F. (2013) The Participatory Cube: A Framework for Analysis of Online Participation Platforms/ Geertman, S., Toppen, F., Stillwell, J. (Eds.) *Planning Support Systems for Sustainable Urban Development*. Lecture Notes in Geoinformation and Cartography, vol. 195. Springer, Berlin, Heidelberg.
O'Reilly T. (2010) Government as a Platform/Lathrop, D., Ruma, L. (Eds.), *Open Government: Collaboration, Transparency, and Participation in Practice* (pp. 11–39). Sebastopol, CA: O'Reilly Media.
Segijn C.M., van Ooijen I. (2020) Perceptions of Techniques Used to Personalize Messages Across Media in Real Time. *Cyberpsychology Behavior and Social Networking*, vol. 23 (5), pp. 329–337.
Shachar A., Mahmood A. (2021) The Body as the Border. *Historical Social Research/Historische Sozialforschung*, vol. 46 (3), pp. 124–150.
Sheldon B. (2011) Camera Surveillance Within the UK: Enhancing Public Safety or a Social Threat? *International Review of Law, Computers & Technology*, vol. 25, pp. 193–203.
Solove Daniel J., Privacy Self-Management and the Consent Dilemma (November 4, 2012). 126 Harvard Law Review 1880 (2013). GWU Legal Studies Research Paper Vol. 2012–141, GWU Law School Public Law Research Paper Vol. 2012-141, Available at SSRN: https://ssrn.com/abstract=2171018.
Swist T., Magee L., Phuong J., Sweeting D. (2017) The Labour of Communicating Publics: Participatory Platforms, Socio-Technical Intermediaries and Pluralistic Expertise. *Communication and the Public*, vol. 2, pp. 210–225.
Taewoo Nam (2019) What Determines the Acceptance of Government Surveillance? Examining the Influence of Information Privacy Correlates. *The Social Science Journal*, vol. 56:4, pp. 530–544.
Tai Z., Yu X., He B. (2021) Locked Down Through Virtual Disconnect: Navigating Life by Staying on/off the Health QR Code During COVID-19 in China. *Convergence*, vol. 27 (6), pp. 1648–1662.
VSTIOM (2021) Otnoshenie rossiyan k meram po bor'be s koronavirusom [Attitudes of Russian Citizens Towards Measures Against Covid-19]. Available at: https://wciom.ru/analytical-reviews/analiticheskii-obzor/otnoshenie-rossijan-k-meram-po-borbe-s-koronavirusom (accessed 17 April 2023). (in Russian)
VSTIOM (2022) Iskusstvennyi intellect: urgoza ili svetloe buduschee [Artificial Intelligence: Menace or Bright Future?]. Available at: https://wciom.ru/analytical-reviews/analiticheskii-obzor/iskusstvennyi-intellekt-ugroza-ili-svetloe-budushchee (accessed 17 April 2023). (in Russian)
Westin A.F. (1967) Privacy and freedom. New York: Athenaum.
Wu J., Wang J., Nicholas S. et al. (2020) Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations. *Journal of Medical Internet Research*, vol. 22 (10): e21980.
Yang F., Heemsbergen L., Fordyce R. (2021) Comparative Analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: A New Corona of Public Health Governmentality? *Media International Australia*, vol. 178 (1), p. 182–197.