ГРИГОРЬЕВА
КСЕНИЯ СЕРГЕЕВНА

кандидат социологических наук,
старший научный сотрудник
Института социологии ФНИСЦ РАН

ПОЧЕМУ ГРАЖДАНЕ НЕ ДОВЕРЯЮТ КОРПОРАЦИЯМ И ПРАВИТЕЛЬСТВАМ, СОБИРАЮЩИМ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

В последнее время в России все чаще звучат опасения относительно государственного и корпоративного надзора за населением. Средства массовой информации заполнены тревожными сообщениями, предупреждающими граждан о наблюдении за ними через компьютеры, смартфоны, фитнес-трекеры и другую «умную» технику[1]. Опросы общественного мнения показывают растущую озабоченность россиян проблемами защиты личных данных. Согласно недавнему исследованию ВЦИОМ, 70% граждан отрицательно относятся к возможности передачи их персональных данных третьим лицам, причем 58% полагают, что это представляет для них личную угрозу[2]. По данным опроса PwC в России, проведенного в 2018 году, лишь 3% респондентов уверены, что контролируют свои персональные данные, в то время как 88% придерживаются противоположной точки зрения. Более 70% опрошенных считают, что компании отслеживают историю посещения ими сайтов и поисковых запросов в интернете, хотя большинство респондентов не хотели бы делиться этой информацией. 78% опрошенных убеждены, что компании собирают данные только для того, чтобы извлечь как

[1] См.: Королев Н. В сложной оперативной остановке. Пассажиров Москвы будут мониторить по смартфонам // Коммерсантъ. 20.10.2020. № 192. URL: https://www.kommersant.ru/doc/4539137?utm_source=yxnews&utm_medium=desktop; Синьков А., Арбатская Л. Ваш любимый смартфон — это тайный шпион: IT-специалист рассказал, как за нами следят благодаря нашим же мобильникам // Комсомольская правда. 05.12.2020. URL: https://www.irk.kp.ru/daily/27107.7/4333016/; Сальникова О. На крючке. Как за нами следят с помощью компьютеров и телефонов // Аргументы и факты. 12.04.2019. URL: https://spb.aif.ru/society/people/na_kryuchke_kak_za_nami_sledyat_s_pomoshchyu_kompyuterov_i_telefonov.

[2] Персональные данные в интернете: угроза утечки и как с ней бороться // ВЦИОМ. 30.11.2020. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/personalnye-dannye-v-internete-ugroza-utechki-i-kak-s-nei-borotsja.

можно больше прибыли[3]. Наконец, согласно опросу ФОМ за 2016 год, 78% россиян полагают, что государственные органы просматривают закрытую личную информацию и переписку в соцсетях и по электронной почте (27% думают, что это массовая практика, а 51% — что это делается в исключительных случаях). Вместе с тем, по мнению 58% граждан, у правительства не должно быть доступа к такой информации, поскольку это нарушает права человека и является вторжением в частную жизнь[4].

Любопытно, что результаты российских опросов общественного мнения имеют выраженное сходство с результатами аналогичных исследований в США — стране, где вопросы конфиденциальности уже давно находятся в центре общественно-политических дебатов. В частности, опрос Исследовательского центра Пью (Pew Research Center) 2019 года показывает, что большинство американцев обеспокоены тем, как их данные используются компаниями (79%) и государством (64%). Более 80% респондентов полагают, что они мало или вообще не контролируют данные, которые собирают о них правительство и корпорации. При этом 72% американцев убеждены: информация почти обо всем или о большей части того, что они делают в интернете или во время использования своего мобильного телефона, собирается коммерческими компаниями. А 47% респондентов считают, что бóльшая часть их онлайн-активности отслеживается государством. С точки зрения подавляющего большинства опрошенных (81%), потенциальные риски, с которыми они сталкиваются из-за сбора персональных данных корпорациями, перевешивают ожидаемые выгоды. 66% американцев придерживаются той же позиции в отношении сбора их личной информации государством[5].

Итак, ни в России, ни в США государственный и корпоративный надзор не встречает энтузиазма со стороны населения. Значительная доля граждан с недоверием относится к декларируемым целям сбора персональных данных (обеспечение безопасности, борьба с преступностью, улучшение сервисов и услуг, предоставляемых потребителям). Каковы причины этого недоверия и имеет ли оно под собой реальные основания?

Как видно из данных исследований общественного мнения, наблюдение со стороны коммерческих компаний вызывает отторжение, по меньшей мере, из-за двух обстоятельств:

[3] «Защити меня». Кибербезопасность, защита данных, конфиденциальность информации, доверие и регулирование Всестороннее исследование предпочтений российских потребителей, их опасений, а также способов завоевать их доверие и привлечь на сторону компаний // Pw C. 2018. URL: www.pwc.ru/protectme2018.

[4] Приватность в интернете. Должен ли быть у государства доступ к личной информации интернет-пользователей? // ФОМ. 29.01.2016. URL: https://fom.ru/SMI-i-internet/12496.

[5] Auxier B., Rainie L., Anderson M., Perrin A., Kumar M., Turner E. (2019) Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. *Pew Research Center. Internet&Technology*. URL: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

1) граждане ощущают неспособность контролировать сбор информации о себе и, при необходимости, ограничивать доступ к тем сведениям, которыми они не хотят делиться;

2) у них создается впечатление, что их личная информация, получаемая компаниями, рассматривается последними как товар и продается третьим лицам.

Эмпирические исследования это подтверждают. Хотя компании часто указывают, что сбор персональных данных сопровождается уведомлением (всем известны всплывающие окна с оповещением об использовании файлов cookies) и «информированным согласием», аналитики подчеркивают: в действительности речь не идет о реальном выборе, доступном пользователю. Первая проблема заключается в том, что тексты о политике конфиденциальности часто трудны для понимания и фактически недоступны для тех, кто не обладает юридическим образованием. Кроме того, такие соглашения недостаточно детализированы, они просто не могут содержать в себе исчерпывающие сведения обо всех возможных видах использования персональных данных. Процессы сбора и передачи пользовательской информации крайне сложны. В них участвует множество действующих лиц — профилировщики, рекламные агентства, рекламные биржи, веб-сайты, где размещается целевая реклама, компании, которые приобретают на аукционах возможность представить пользователям таргетированные объявления. Весь процесс аналитики и торговли занимает доли секунды. Информационные потоки находятся в непрерывном движении, в систему постоянно заходят новые компании, заключаются очередные сделки. Описать этот процесс с достаточным количеством конкретных деталей о том, как именно собираются данные, с какой целью и кому они передаются, практически невозможно. Помимо этого, информация о пользователях хранится неопределенно долго и в будущем может быть использована для целей, которые нельзя предсказать заранее[6].

Вторая проблема состоит в самом качестве формально предоставляемого выбора. Соглашения о доступе к персональным данным устроены таким образом, что все иные варианты, кроме согласия, приводят к серьезным негативным последствиям для пользователя. Отказавшись, он может не только лишиться определенных выгод, товаров и услуг, но и оказаться исключенным из социального участия, практически неосуществимого без использования современных средств связи и информационных технологий[7]. Таким образом, выбор, предоставляемый гражданам, по сути, фиктивен, а контроль над личными данными действительно от них ускользает.

[6] Sloan R. H., Warner R. (2013) Beyond Notice and Choice: Privacy, Norms, and Consent. *Suffolk University Journal of High Technology Law, Forthcoming*. Chicago-Kent College of Law Research Paper No. 2013—16. https://www.doi.org/10.2139/ssrn.2239099.

[7] Helm P., Seubert S. (2020) Normative Paradoxes of Privacy: Literacy and Choice in Platform Societies. *Surveillance & Society*. Vol. 18. No. 2. P. 185—198. https://www.doi.org/10.13140/RG.2.2.19578.11202.

Помимо перечисленных есть и другие проблемы. Многие исследователи указывают на то, что погоня за накоплением все новых и новых данных, позволяющих делать все более и более точные прогнозы потребительского поведения, подталкивает интернет-корпорации к использованию поведенческих манипуляций[8]. Шошанна Зубофф, автор концепции надзорного капитализма, называет такие стратегии «инструментализмом», подчеркивая, что они нацелены на формирование человеческого поведения в интересах третьих сторон[9].

Наконец, накопление больших данных в руках узкого круга организаций, имеющих преимущественный доступ к пользовательской информации, ведет к монополизации знаний и власти, созданию ситуации, когда корпорации знают о пользователях больше них самих, оставаясь при этом непрозрачными для внешней аудитории[10].

Все перечисленное, очевидно, не может способствовать повышению доверия населения к коммерческим компаниям, собирающим персональные данные.

Что касается государственного надзора, то наиболее распространенной причиной негативного отношения к нему является вызываемое им нарушение прав на неприкосновенность частной жизни. Существование высокотехнологичных программ правительственного шпионажа, таких как американские MISTIC, CO-TRAVELLER и PRISM, ставшие известными благодаря разоблачениям Эдварда Сноудена, или российская СОРМ[11], свидетельствует о том, что представления о масштабной «правительственной слежке» не являются плодом воображения. Более того, как показывают международные исследования государственного надзора, его повсеместный стремительный рост, начавшийся после 11 сентября 2001 года, имел весьма плачевные последствия не только для стандартов конфиденциальности, но и для других прав и свобод. В частности, в некоторых случаях он сопровождался похищениями, бессрочными содержаниями под стражей, жестоким обращением и даже убийствами, санкционированными государствами. Причем некоторые правительства разработали правовые обоснования, направленные на признание подобных действий в качестве легитимных средств

[8] Degli Esposti S. (2014) When Big Data Meets Dataveillance: The Hidden Side of Analytics. *Surveillance & Society*. Vol. 12. No. 2. P. 209—225. https://www.doi.org/10.24908/ss.v12i2.5113; Palmås K. (2011) Predicting What You'll Do Tomorrow: Panspectric Surveillance and the Contemporary Corporation. *Surveillance & Society*. Vol. 8. No. 3. P. 338—354. https://doi.org/10.24908/ss.v8i3.4168.

[9] Zuboff S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs.

[10] Zuboff S. (2015) Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*. Vol. 30. No. 1. P. 75—89. https://doi.org/10.1057/jit.2015.5; Palmås K. (2011) Predicting What You'll Do Tomorrow: Panspectric Surveillance and the Contemporary Corporation. *Surveillance & Society*. Vol. 8. No. 3. P. 338—354. https://doi.org/10.24908/ss.v8i3.4168.

[11] Система технических средств для обеспечения функций оперативно-разыскных мероприятий.

борьбы с терроризмом. Такая политика описана в научной литературе как «правдоподобная законность» и «легальная незаконность»[12].

Исследователи также обращают внимание на то, что наряду с угрозами конфиденциальности, порождаемыми неограниченным сбором информации о гражданах, существуют не менее серьезные проблемы усугубления социального неравенства. Так, Дидье Биго, анализируя государственный надзор, направленный на обеспечение безопасности, приходит к выводу, что он превосходит простую логику наблюдения за всеми. При помощи сбора информации, поступающей из области социального обеспечения, налоговой сферы, страхования, кредитных организаций, супермаркетов, других коммерческих компаний, и перекрещивания ее с файлами полиции осуществляется фильтрация тех, кого, по мнению силовых структур и правительств, следует поместить под «особый контроль». Эта стратегия нацелена на то, чтобы действовать до совершения преступлений, ожидаемых со стороны «опасных» групп, и ведет к распространению так называемого актуарного правосудия[13]. Дэвид Лион также обращает внимание на классифицирующую силу надзора, подчеркивая, что способы, которыми он осуществляется сегодня, приводят к новым видам исключения и росту социального неравенства[14].

Таким образом, избыточный и неконтролируемый правительственный надзор за гражданами весьма проблематичен, а вызываемое им беспокойство населения нельзя назвать безосновательным.

Стоит добавить, что в последние годы границы между государственным и корпоративным надзором все больше размываются. Активное взаимодействие правительств и корпораций приводит к созданию разветвленных частно-государственных сетей наблюдения, нередко имеющих трансграничный характер[15].

Стратегическое партнерство между бизнесом и государством в области надзора обусловлено взаимным стремлением к достижению тотального знания, которое позволило бы выйти на небывалый уровень эффективности в экономике и управлении. Эта мечта объясняет стремление ко все большему накоплению данных, которые (по крайней мере в настоящий момент) даже не могут быть полностью

[12] Sanders R. (2018) Plausible Legality: Legal Culture and Political Imperative in the Global War on Terror. New York, NY: Oxford University Press; Austin L. M. (2015) Lawful Illegality: What Snowden Has Taught us About the Legal Infrastructure of the Surveillance State. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2524653.

[13] Bigo D. (2009) Du panoptisme au Ban-optisme. Les micros logiques du contrôle dans la mondialisation. In: Chardel P.-A., Rockhill G. (eds.) Technologies de contrôle dans la mondialisation: enjeux politiques, éthiques et esthétiques. Paris: Editions Kimé. P. 59—80.

[14] Lyon D. (2009) Surveillance, Power, and Everyday Life. In: *The Oxford Handbook of Information and Communication Technologies*. Avgerou Ch., Mansell R., Quah D., Silverstone R. (eds.) New York: Oxford University Press. P. 449—472.

[15] Burke C. (2020) Digital Sousveillance: A Network Analysis of the US Surveillant Assemblage. *Surveillance & Society*. Vol. 18. No. 1. P. 74—89. https://doi.org/10.24908/ss.v18i1.12714; Baird T. (2016) Surveillance Design Communities in Europe: A Network Analysis. *Surveillance & Society*. Vol. 14. No. 1. P. 34—58. https://doi.org/10.24908/ss.v14i1.5622.

обработаны. Установлено, например, что так называемый закон Ирины Яровой в действительности практически не работает, поскольку существенно опережает технологическое развитие России[16]. Несравненно более мощная американская система сбора и обработки информации, включающая в себя огромное хранилище данных площадью до 140 м^2 и стоимостью около 1,5 млрд долларов, оснащенное аппаратным и программным обеспечением, оцениваемым еще в 2 млрд долларов, также пока не способна реализовать замысел американского правительства и силового блока о доминировании полного спектра, дающего контроль над всеми реальными и потенциальными угрозами[17].

Соблазнительная греза о тотальном знании остается недостижимой и там, где она зародилась, — в коммерческом секторе. Впрочем, здесь стремление к ее осуществлению дает гораздо более ощутимые дивиденды по сравнению со сферой безопасности. Информация о действиях пользователей в сети давно и успешно монетизирована, она приносит огромные прибыли таким интернет-гигантам, как Google, Facebook и Microsoft. Точность прогнозов о потребительских стратегиях существенно повысилась, а «невидимая рука рынка» заметно скукожилась. По словам главного экономиста Google Хэла Вариана, опосредованность транзакций компьютером сделала возможным наблюдение за поведением, которое ранее было ненаблюдаемым, позволив создавать совершенно новые бизнес-модели с нулевым уровнем неопределенности. К примеру, страховые компании могут использовать системы мониторинга, чтобы выяснить, как клиент ведет себя за рулем, и решить, следует ли продолжать оказывать ему услуги или оплачивать его претензии. Однако, как справедливо замечает Ш. Зубофф, устранение неопределенности, которое энергично рекламирует Х. Вариан, одновременно ликвидирует необходимость, а значит, и возможность доверия между компаниями и клиентами. В результате контракты перестают быть социальными, превращаясь в рутинные машинные операции[18].

Как бы то ни было, правительства и корпорации еще далеки от воплощения своей мечты об идеальном управлении и экономике, лишенных неизвестности, непредсказуемости и рисков. Весьма вероятно, что она никогда не исполнится. И хотя неограниченный массовый государственный и коммерческий сбор данных о населении имеет некоторые позитивные результаты (например, более эффективное расследование преступлений или повышение качества услуг), кажется, участники опроса Исследовательского центра Пью правы: потери перевешивают приобретения.

[16] Ermoshina K., Musiani F. (2017) Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. *Media and Communication*. Vol. 5. No. 1. P. 42—53.
[17] Munkholm J. L. (2020) The Pursuit of Full Spectrum Dominance: The Archives of the NSA. *Surveillance & Society*. Vol. 18. No. 2. P. 244—256. https://doi.org/10.24908/ss.v18i2.13266.
[18] Zuboff S. (2015) Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*. Vol. 30. No. 1. P. 75—89. https://doi.org/10.1057/jit.2015.5