

Кугай Александр Иванович

д-р филос. наук, профессор

Северо-Западный институт управления

ФГБОУ ВО «Российская академия народного хозяйства

и государственной службы при Президенте РФ»

г. Санкт-Петербург

ПАНОПТИЧЕСКИЕ ТЕХНОЛОГИИ И КОНФИДЕНЦИАЛЬНОСТЬ В СОВРЕМЕННОМ ОБЩЕСТВЕ

***Аннотация:** статья посвящена особому аспекту конфиденциальности, часто называемому информационной конфиденциальностью, т.е. праву на неприкосновенность личной информации, включая информацию о своих действиях, и преднамеренному вторжению государства в частную жизнь. Достижения в области технологий и изменения в способах общения и хранения информации сопровождаются неуклонным ростом уязвимости информационной конфиденциальности. Эта уязвимость усугубляется сочетанием повышенных опасений по поводу безопасности граждан в контексте разработок в области электронного правительства, направленных на улучшение государственных услуг и реформирования государственного сектора. Против рисков терроризма и преступности необходимо заново сбалансировать риск для частной жизни. Без подходящих механизмов для защиты в долгосрочной перспективе свобод общества рискуют оказаться в ситуации, из которой будет трудно повернуть вспять.*

***Ключевые слова:** паноптикум, информационная конфиденциальность, частная жизнь, государство, риск.*

Введение

«Те, кто готов пожертвовать насущной свободой ради кратковременной безопасности, не достойны ни свободы, ни безопасности». Бенджамин Франклин.

Большинство людей, вероятно, хотя бы смутно осознают растущее вмешательство государства в их жизнь. Вероятно, только силовики знают всю полноту

средств наблюдения и информации, находящейся сейчас в распоряжении современного государства.

Неприкосновенность частной жизни, как и свобода слова и свобода собраний, является правом человека [1] Право на неприкосновенность частной жизни признается в статье 12 ООН «Хартия прав человека». На протяжении всей письменной истории всегда существовала напряженность между правом человека на неприкосновенность частной жизни и правом государства на защиту себя и общества в целом. Проблема сегодня в том, что технологии изменения масштабов и размеров способности государства делать это растут с угрожающей скоростью [2].

Можно стать параноиком по поводу вторжения в частную жизнь. Существует множество организаций, выступающих за конфиденциальность, которые можно найти в Интернете и в других местах, которые разжигают такие страхи [3], многое из того, что публикуется на эту тему, носит не критический и/или полемический характер. Сохранять академическую отстраненность, не говоря уже об объективности, в такой напряжённой атмосфере отнюдь непросто. Один из способов попытаться достичь объективной точки зрения состоит в том, чтобы посмотреть на баланс рисков в этом контексте.

Право на неприкосновенность частной жизни

Конфиденциальность [6] – не простое явление [4], оно допускает множество значений. Оно включает в себя не только право на свободу от вторжения в нашу жизнь, оно может распространяться на такие понятия, как личное пространство, собственное тело или право на брак, использование противозачаточных средств или сделать аборт. Формальные юридические определения были расширены и «растянуты до общеупотребительного языка», чтобы охватить даже такие идеи, как доверие и свобода от преступлений, что «ни для кого ничего не значат» [4, с. 35].

Государство может напрямую вторгаться в частную жизнь из соображений безопасности, но оно также может злоупотреблять информацией, предоставляе-

мой государству добровольно гражданами или полученной при оказании государственных услуг (например, налоговая информация или медицинские записи). Также многие третьи стороны на законных основаниях владеют частными и добровольно раскрытыми данными, к которым государство может получить доступ (легально или незаконно). Все чаще институтам требуется по закону сообщать информацию государству, например, банки должны сообщать о кассовых операциях в течение определенного предела, авиакомпании должны сообщать данные о пассажирах и так далее.

Таксономия вторжения

Благодаря технологиям возможность шпионить за другими или вторгаться в частную жизнь увеличилась на порядки за последние два десятилетия [7]. При рассмотрении влияния технологий на конфиденциальность полезно классифицировать вторжения в частную жизнь на три категории: просмотр, перехват, чтение и интерпретация.

Каждый из них имеет свои особенности.

Просмотр. Первая категория вторжения в частную жизнь – это физическое наблюдение/мониторинг того, что делают люди. Физическое наблюдение является трудоемким и представляет для государства сложные материально-технические и людские ресурсы. Развитие технологий за последнее десятилетие значительно расширил масштабы, удешевил и в целом упростил этот процесс. Наиболее очевидным проявлением этого является камера замкнутого телевидения (ССТV) [8].

Перехват. Вторая категория вторжения в частную жизнь – это перехват сообщений. Это так же старо, как сама история. Существует давняя традиция ловить курьеров, вскрывать конверты паром и прослушивать телефонные звонки. Важной стратегией в большинстве случаев является перехват информации без передачи, стороны знают, что их сообщение было прочитано. Поскольку общение становится все более электронным, возможность и легкость перехвата сообщений между гражданами и организациями трансформировалась.

Меры противодействия перехвату так же стары, как и сам перехват [5]. Передняя линия обороны, это шифрование, в котором ведутся непрерывные сражения между шифровальщиками и дешифровщиками, с точки зрения простых граждан, эти сражения отдалены. Уровень техники, доступный обычным людям для шифрования своей электронной почты может быть достаточным, для противодействия хакеру, но он не предлагает полной защиты от сил безопасности современного государства.

Чтение и интерпретация. Третий тип вторжения в частную жизнь – это доступ к существующим личным данным, независимо от того, являются ли эти данные общедоступными. (например, государственным учреждением), в частной собственности (например, у семейного врача) или в личном владении (например, на домашний компьютер). Понятно, что технологии не только значительно увеличили способность государства приобретать огромные объемы полученных данных, знания о своих гражданах, но и его способность в своих интересах ее интерпретировать, манипулировать, управлять людьми.

Заключение

Неприкосновенность частной жизни, как и свобода, является ценным товаром, который можно добровольно обменять на другие товары или выгоды. Эти преимущества включают в себя как частные блага, общественные услуги, безопасность и членство в обществе. Способность граждан коллективно и правильно судить об этом компромиссе лежит в основе свободного общества.

Традиционное ограничение власти государства вторгаться в частную жизнь заключалось в том, что нас было много, а их мало. Пока еще кажется маловероятным, что технология окончательно преодолет это ограничение в ближайшем будущем. Но, если и когда это произойдет, паноптическое государство станет реальностью, и обществу останется участь размышлять над вопросом Ювенала: «Кто наблюдает за наблюдателями?».

«Каждый человек, – писал английский поэт Джон Донн, – есть часть континента, часть великого». То, что делается сегодня для частной жизни одного, завтра может быть сделано для всех. Против рисков терроризма и преступности

необходимо заново сбалансировать риск для частной жизни. Без подходящих механизмов для защиты в долгосрочной перспективе свобод граждан, общества рискуют оказаться в ситуации, из которой будет трудно повернуть вспять. Прежде чем уступить какую-либо свободу или право, всегда мудро помнить вызывающие воспоминания слова Джони Митчелл: «Вы не знаете, что у вас есть, пока это не исчезнет».

Список литературы

1. Кугай А.И. Права человека: от теории – к политике / А.И. Кугай // Управленческое консультирование. – 2021. – №5. – С. 32–44.
2. Кугай А.И. «Цифровое поколение»: угрозы и надежды в эпоху информационно-цифровой цивилизации / А.И. Кугай // Управленческое консультирование. – 2019. – №7. – С. 90–99.
3. Ball K. Element of surveillance: a new framework and future directions, *Information, Communications and Society*. 2002. N 5 (4), pp. 573–590.
4. Cate F. Principles for Protecting Privacy, *Cato Journal Spring/Summer*, 2002. N 22 (1), pp. 33–57.
5. Carroll J. *Computer Security*, Butterworth-Heinemann, Boston, 1996.
6. Introna L. and Pouloudi A. Privacy in the information age: Stakeholders, interests and values, *Journal of Business Ethics*, 1999. N 22 (1), pp. 27–38.
7. McArthur R. Reasonable expectations of privacy, *Ethics and Information Technology*, 2001. N 3 (2), pp. 123–128.
8. Webster C. Changing Relationships Between Citizens and the State: The Case of Closed Circuit Television Cameras, in: *Public Administration in and Information Age*, I. Snellen and W. van de Donk, eds, IOS Press, Amsterdam, 1998, pp. 79–96.