

От отдельных лиц, представляющих интерес, к целым популяциям: Индустриализация профилирования

Появление профилирования — от целенаправленного, ручного изучения конкретных «лиц, представляющих интерес» до автоматизированной, непрерывной слежки за целыми популяциями — представляет собой одно из самых глубоких преобразований в осуществлении власти, роли технологий и границах индивидуальной автономии. То, что раньше требовало значительных человеческих усилий, институциональных приоритетов и осознанного отбора, эволюционировало в плавную инфраструктуру, которая генерирует, агрегирует и анализирует поведенческие данные миллиардов людей в реальном времени, часто как случайный побочный продукт повседневной жизни.

Это преобразование не было предопределено одной лишь технологией. Оно возникло из взаимодействия бюрократического расширения, повторяющихся кризисов безопасности, экономических стимулов, связанных с монетизацией данных, и неуклонного снижения предельных издержек сбора, хранения и вывода данных. Результат — не просто «больше слежки», а качественно иной режим: он заменяет естественное трение на безтрениевый масштаб, человеческое усмотрение на алгоритмическую автоматизацию, а исключительное подозрение к немногим — на базовое наблюдение за многими.

В своей основе лежит фундаментальная метаморфоза: профилирование перешло от **ремесленного искусства** — избирательного, трудоёмкого и объяснительного — к **промышленному процессу** — универсальному, автоматизированному и предсказательному. Далее прослеживается это преобразование, выявляя моменты, когда ограничения ослабевали, а новые возможности кристаллизовались в систему непрерывного, охватывающего всё население вывода.

I. Основы: Профилирование как избирательная, ручная практика

Профилирование в своей самой простой форме предполагает систематический сбор и интерпретацию информации для вывода характеристик, прогнозирования поведения или присвоения категорий риска. Его истоки уходят глубоко в древность.

Древние империи проводили переписи не только для налогообложения или призыва, но и для классификации. Римские власти и китайские имперские администраторы сортировали население по профессии, лояльности и статусу, создавая ранние реляционные карты, которые могли выявлять потенциальные угрозы. Религиозные учрежде-

ния вели записи о рождениях, браках, исповедях и моральном поведении, формируя прото-социальные графы, раскрывающие сети влияния и отклонений.

Однако эти системы имели определяющее ограничение: **информация была дорогой**. Сбор, проверка, хранение и интерпретация данных требовали значительного человеческого труда. В результате профилирование оставалось **избирательным, эпизодическим и ограниченным**. Оно фокусировалось на элитах, диссидентах или стратегически важных группах — а не на всём населении.

В ранней современной Европе эта избирательность сохранялась даже по мере расширения государственного аппарата слежки. Разведывательные усилия были направлены против еретиков, политических соперников, контрабандистов и иностранных агентов через информаторов, перехваченную корреспонденцию и физическое наблюдение. Французские и другие «чёрные кабинеты» (*cabinets noirs*) воплощали этот подход: команды клерков вручную вскрывали письма, копировали их и запечатывали обратно для доставки. Эти операции были по своей природе ограничены. Они сосредоточивались на высокоприоритетных целях, поскольку всё более широкое применение было логистически невозможно.

Даже на этом этапе ясно понималась сила **метаданных**. Информация о коммуникации — отправитель, получатель, время и маршрут — могла раскрывать сети и намерения без доступа к содержимому. Британский почтовый шпионский скандал 1844 года ярко высветил это для общественности. Итальянский революционер Джузеппе Мадзини, находившийся в изгнании в Лондоне, подозревал, что его письма вскрываются властями по запросу иностранных держав. Он и его сторонники помещали внутрь конвертов семена мака и песчинки в качестве меток; когда письма приходили потревоженными, Мадзини побудил радикального депутата Томаса Данкэмба поднять вопрос в парламенте. Последовавший скандал раскрыл систематическое вскрытие писем по ордерам, выданным министром внутренних дел сэром Джеймсом Грэмом, вызвав возмущение, парламентские расследования и в итоге упразднение секретного отдела Почтового ведомства. Это стало одним из первых современных приступов паники по поводу приватности и подчеркнуло, как одни лишь реляционные данные могут разрушать сети связей.

В ответ возникли правовые нормы, такие как «тайна переписки» (*Briefgeheimnis, secret de la correspondance*). Эти принципы строго ограничивали использование данных коммуникации исключительно оперативными целями, такими как доставка, запрещая вторичное использование для слежки или профилирования. Основная идея была простой, но глубокой:

Данные, сгенерированные для конкретной функции, не должны переиспользоваться для построения более широких профилей отдельных лиц или сетей.

Этот принцип будет эхом отзываться на протяжении веков — однако в итоге он будет размыт под технологическим и институциональным давлением.

II. Бюрократический век: Масштабирование без автоматизации

XX век значительно расширил профилирование, сохраняя при этом многие из прежних ограничений. Требования тотальной войны потребовали беспрецедентного сбора информации. Цензура почты, радиоэлектронная разведка и дешифровка расширили слежку за пределы элит на более широкие слои населения. Такие учреждения, как Агентство национальной безопасности, институционализировали масштабный перехват, в то время как внутренние агентства составляли обширные досье на политические группы, подозреваемых радикалов и преступные сети.

Тем не менее профилирование оставалось **по сути целевым**. Прослушка привязывалась к конкретным лицам или линиям. Разведывательные досье составлялись человеческими аналитиками. Даже при росте объёма **человеческое внимание оставалось узким местом**.

Ранние компьютерные системы (1950-е — 1970-е годы) начали менять масштаб ведения записей. Правительства и корпорации оцифровывали списки получателей пособий, кредитные истории и криминальные базы данных, позволяя быстрее извлекать и сопоставлять информацию. Однако эти системы всё ещё работали с **дискретными записями**, а не с непрерывными потоками поведения.

К 1970-м годам опасения по поводу централизованных «банков данных» вызвали правовые ответы. Закон США о приватности 1974 года и ранние европейские законы о защите данных ввели принципы ограничения цели, минимизации данных и прозрачности. Эти рамки распространили логику тайны переписки на цифровую эпоху.

Однако они были построены на ключевом допущении: что сбор данных **ограничен и эпизодичен**. Они регулировали записи — а не потоки. Это допущение вскоре рухнет.

III. Переломный момент: От записей к выхлопу данных

Решающий разрыв происходит в конце 1990-х — начале 2000-х годов с подъёмом интернета — не просто как средства коммуникации, а как инфраструктуры, которая непрерывно производит данные.

Цифровые системы генерируют **выхлоп данных**: метаданные, автоматически создаваемые как побочный продукт обычной активности. Каждое соединение, запрос, клик и перемещение производит следы, которые можно регистрировать, хранить и анализировать с ничтожной стоимостью.

Это знаменует решающий сдвиг:

Профилирование перестаёт быть деятельностью, выполняемой над данными, и становится инфраструктурой, которая непрерывно их

производит.

Провайдеры интернет-услуг фиксируют логи соединений, запросы DNS и информацию о маршрутизации, раскрывая модели поведения даже без доступа к содержимому. В отличие от почтовых метаданных — эфемерных и децентрализованных — цифровые метаданные постоянны, централизованы и тривиально доступны для поиска.

На основе этой инфраструктуры платформы вроде Google и Meta превратили профилирование в основную экономическую модель. Поисковые системы фиксируют намерения; социальные сети картографируют отношения; мобильные экосистемы отслеживают перемещения. Встроенные трекеры расширяют видимость на огромные части веба. Пиксели отслеживания Meta, присутствующие примерно на одной трети популярных сайтов мира, мониторят активность далеко за пределами собственных платформ, часто захватывая чувствительные сигналы из сфер здоровья, финансов или политики.

В этой среде возникает критическое осознание:

Содержимое в значительной степени становится избыточным. Во многих случаях реляционные паттерны — это не просто заменители смысла, они аналитически полезнее самого содержимого.

Метаданные не просто указывают, что коммуникация произошла; они позволяют **вероятностную реконструкцию содержимого**. Кто с кем общается, когда, как часто и в каком более широком контексте — всё это сильно сужает то, о чём идёт речь. Публично доступная информация — общие принадлежности, профессиональные роли, политические позиции, социальные связи — ещё больше сужает пространство возможных интерпретаций.

Со временем эти ограничения становятся предсказательными. Метаданные не просто описательны; они генеративны. Они не просто сопровождают содержимое — они часто **приближают или выводят его**, особенно при агрегации в большом масштабе.

Поисковые запросы раскрывают намерения. Частота коммуникации раскрывает силу отношений. Совместное местоположение раскрывает связи. При достаточном масштабе эти сигналы сходятся в высокоточные поведенческие модели, которые часто делают прямой доступ к содержимому ненужным.

Корпоративные системы оптимизируют поведение для монетизации; государственные системы ограничивают его для контроля — но оба полагаются на одну и ту же базовую машину: **прогнозирование через крупномасштабный поведенческий вывод**.

IV. Идентичность без возможности скрыться: Постоянные якоря

Определяющей чертой промышленного профилирования стало появление **постоянной идентичности**.

Ранние системы полагались на изменяемые идентификаторы — имена, документы, адреса, — которые можно было изменить или скрыть. Современные системы реконструируют идентичность через пересекающиеся сигналы:

- Отпечатки устройств
- Поведенческие паттерны
- Социальные графы
- Биометрические маркеры (лица, походка, голос)

Публично размещённые изображения служат прочными якорями. Даже когда люди меняют аккаунты или используют псевдонимы, системы распознавания лиц — особенно в государственных или разведывательных контекстах — могут воссоединять идентичности через разные наборы данных. Совместное появление на фото или в общих событиях ещё больше укрепляет выводимые связи.

Последствие глубоко:

Идентичность больше не то, что человек заявляет, а то, что непрерывно выводится.

Это устраняет большую часть трения, которое когда-то ограничивало слежку. Идентификация больше не зависит от одного сигнала; она возникает из избыточности многих.

V. Слияние: От точек данных к онтологиям

Кульминацией этой эволюции стало **слияние данных**: интеграция разрозненных наборов данных в унифицированные аналитические системы.

Платформы вроде Palantir Technologies агрегируют государственные записи, финансовые транзакции, активность в социальных сетях, данные о местоположении и метаданные коммуникаций в coherentные модели отдельных лиц и сетей. Эти системы строят динамические онтологии, позволяющие аналитикам запрашивать отношения, выявлять паттерны и генерировать прогнозы.

Конкретный пример иллюстрирует сдвиг. В сфере иммиграционного контроля инструмент Palantir ELITE (Enhanced Leads Identification and Targeting for Enforcement) заполняет карты потенциальными целями, опираясь на визовые записи, данные о занятости, метаданные телефонов, социальные связи и даже информацию об адресах из Medicaid или NHS, чтобы присваивать «оценки уверенности в адресе» и генерировать досье. Офицеры могут выявлять «богатые целями» районы для операций, пометая людей не только на основе прямых доказательств, но потому, что их **поведенческая и реляционная сигнатура** напоминает ранее выявленные случаи. Аналогичное слияние наблюдается в инструментах вроде ImmigrationOS, которые интегрируют историю поездок, биометрию и социальные данные для приоритизации.

Подозрение больше не обнаруживается — оно **генерируется**.

Профилирование не просто документирует реальность; оно активно конструирует её, выводя на поверхность вероятностные ассоциации, которые становятся операционно применимыми.

VI. От объяснения к упреждению

Традиционное профилирование было преимущественно ретроспективным. Оно стремилось объяснить прошлые действия — кто совершил преступление, кто организовал заговор, кто представлял угрозу.

Промышленное профилирование предсказательно и упреждающе. Оно выявляет:

- Кто может совершить преступление
- Где может произойти преступление
- Кто может допустить дефолт, радикализироваться или отклониться

Эту логику часто сравнивают с видением, изображённым в «Особом мнении», где людей задерживают до совершения преступлений. Хотя современные системы лишены детерминистического предвидения, структурное сходство очевидно: инструменты предиктивной полиции анализируют исторические данные, вызовы 911, считыватели номерных знаков и социальные сигналы для генерации «горячих списков» или оценок риска.

Современные системы работают на вероятности. Людей помечают не потому, что они совершат действие, а потому, что они **статистически похожи на тех, кто уже совершил**.

Сдвиг тонкий, но глубокий:

Людей больше не судят в первую очередь по их действиям, а по их положению в вероятностном ландшафте.

Подозрение становится структурным — оно генерируется непрерывно, а не запускается дискретными событиями.

VII. Право в эпоху вывода

Правовые рамки, такие как Общий регламент по защите данных (GDPR), пытаются наложить ограничения через согласие, прозрачность и минимизацию. Однако они сталкиваются со структурными ограничениями.

Большинство правовых систем регулируют **данные как объект**. Современное профилирование черпает силу из **отношений и выводов**, которые гораздо сложнее определить, наблюдать или ограничить.

Дополнительные вызовы включают:

- Непрерывные потоки данных через юрисдикции
- Широкие исключения для национальной безопасности и «законных интересов»
- Непрозрачные алгоритмические системы, устойчивые к надзору

Результат — устойчивое несоответствие:

Правовые рамки, разработанные для эпохи записей, с трудом управляют эпохой непрерывного, предсказательного вывода.

VIII. Асимметрия власти

Промышленное профилирование создаёт структурный дисбаланс.

Люди непрерывно генерируют данные через участие в современной жизни. Избежать этого возможно, но дорого и не полностью. В то же время:

- Корпорации поддерживают непрозрачные системы, защищённые секретностью
- Государства получают доступ к данным и интегрируют их через правовые полномочия или партнёрства
- Техническая сложность скрывает подотчётность

Результат — очевидная асимметрия:

Многие становятся прозрачными; сильные мира сего остаются сравнительно непрозрачными.

IX. Интериоризация: Профилирование и саморегуляция поведения

Помимо институциональных и технологических аспектов, индустриализация профилирования производит глубокое психологическое преобразование. Слежка больше не действует исключительно как внешняя сила; она становится интериоризированной.

Эту динамику предвидел Мишель Фуко в своём анализе паноптикума: теоретической тюремной конструкции Джереми Бентама, в которой заключённые, видимые центральному наблюдателю, которого они не видят, интериоризируют дисциплину и самостоятельно регулируют своё поведение под неопределённостью постоянного наблюдения. Сила паноптикума заключается не в непрерывном наблюдении, а в **ожидании** его.

Промышленное профилирование резко расширяет эту логику. Люди действуют в средах, где их действия могут быть записаны, проанализированы и интерпретированы непрозрачными способами — платформами, оптимизирующими вовлечённость, или государствами, оценивающими риск. Результат — сдвиг в сторону **саморегуляции**.

Это проявляется в:

- Самоцензуре в постах, поисках или ассоциациях

- Избегании определённых групп, тем или мест
- Выравнивании поведения под воспринимаемые нормы для минимизации оценок риска
- Изменении поведения в цифровых и физических контекстах

Важно, что эти адаптации не требуют явного принуждения. Они возникают из ожидания.

Контроль осуществляется не только через то, что делают системы, но и через то, чего люди избегают делать.

Эффекты выходят за пределы отдельных лиц. По мере того как люди самоцензурируются и само-сортируются, генерируемые данные усиливают паттерны, формируя будущие прогнозы. Система не только наблюдает реальность — она тонко перестраивает её, создавая петли обратной связи, которые нормализуют конформизм.

X. Конец избирательной слежки

Профилирование прошло фундаментальное преобразование:

- От **целевого** к **универсальному**
- От **ручного** к **автоматизированному**
- От **ретроспективного** к **предсказательному**
- От **фрагментированного** к **интегрированному**

Ранние системы были ограничены трением — стоимостью, временем, человеческим вниманием. Промышленные системы устраняют эти ограничения. Слежка становится фоновой. Включение становится умолчанию.

Принцип, согласно которому данные должны служить только своей непосредственной цели, уступил место парадигме, в которой **все данные потенциально exploitable**.

XI. Заключение: Цена участия

Долгая дуга от почтовой тайны до слияния цифровых данных раскрывает последовательный паттерн: каждое технологическое расширение увеличивает масштаб профилирования, в то время как правовые и социальные ответы отстают. Отличительной чертой настоящего является структурный характер. Профилирование больше не деятельность, направленная на конкретных лиц — это инфраструктура, внутри которой существуют люди.

Категория «лица, представляющего интерес» растворяется. Каждый становится объектом непрерывной оценки.

Это преобразование поддерживается не только государственной властью, но и экономическими стимулами. Платформы, которые кажутся бесплатными, работают через извлечение поведенческих данных. Фраза *«если вы не платите за продукт, вы и есть продукт»* передаёт интуицию — но недооценивает реальность.

Производится не сам индивид, а **предсказательная модель** индивида — портативная, применимая на практике и часто недоступная тому, кого она представляет.

Центральный вызов лежит в разрыве между восприятием и реальностью.

Во-первых, люди недооценивают **воздействие** того, что известно. Профилирование работает через ассоциации. Отношения — прошлые, слабые или косвенные — могут формировать исходы. Связь с кем-то, кто позже становится нежелательным, может повлиять на возможности. Человека судят не только индивидуально, но и реляционно.

Во-вторых, люди недооценивают **масштаб** того, что можно узнать. Системы выводят чувствительные атрибуты — политические, религиозные, сексуальные, экономические — не из явного раскрытия, а из паттернов. Эти выводы становятся операционными независимо от их точности.

Людей оценивают не только по тому, что они раскрывают, но и по тому, что можно вывести — и по тому, с кем они связаны.

Участие в цифровой жизни, таким образом, подразумевает неявный обмен: удобство на legibility. Этот обмен не прозрачен и не подлежит обсуждению.

Задача состоит не в том, чтобы остановить датификацию, а в том, чтобы ограничить её — восстановить трение, обеспечить соблюдение границ и гарантировать подотчётность.

Центральный вопрос ясен:

Произойдёт ли вмешательство до того, как инфраструктура постоянного профилирования укоренится слишком глубоко, чтобы её можно было meaningfully оспорить?

В отсутствие такого вмешательства цена участия — это не только данные, но и постепенное размывание границы между наблюдением, выводом и, в конечном итоге, определением.