Что угрожает цифровому доверию

ИЗМЕНЯЮЩИЙСЯ ЛАНДШАФТ ПРИВАТНОСТИ

В Республике Беларусь почти 5 миллионов пользователей сети интернет, что составляет 70% населения в возрасте от 15 до 74 лет. Большинство из них (84%) выходят в сеть каждый день. В стране 11 миллионов абонентов сотовой связи и 10 миллионов контрактов на использование услуг доступа в сеть интернет.

График 1. Рост интернет-аудитории в Беларуси в 2014 г.

В сети ищут информацию (90% пользователей), пользуются сетевыми социальными (70%) и видео-сервисами (55%), читают новости (50 %), осуществляют платежи (20%). Представители Белорусской железной дороги 30 декабря 2014 г. вручили памятный

подарок миллионному интернет-пассажиру 2014 года (система продаж билетов через интернет была введена в опытную эксплуатацию в начале 2011 года)[1].

65% беларусских пользователей интернета хоть раз совершали онлайн-покупки. В 2014 г. онлайн-покупки в Беларуси совершил в среднем 1 млн пользователей[2]. По данным Министерства торговли на август 2014 г. в Беларуси было зарегистрировано 9 627 интернет-магазинов[3].

Интернет прочно вошел не только в жизнь граждан, но и в деятельность предприятий и организаций. Почти все субъекты хозяйствования предоставляют налоговые декларации (91%) и ведомственную отчетность (80,6 %) онлайн. 29,7% организаций – таможенные документы. 18,6% субъектов хозяйствования прошли электронную регистрацию[4].

По данным Белстата на 2013 год, наибольший процент организаций с веб-сайтами – среди финансовых учреждений – 95,7%. Больше половины (67%) организаций, предоставляющих коммунальные, социальные и персональные услуги также присутствуют онлайн. 40,9 % организаций получают заказы онлайн и 53,6% – размещают заказы онлайн[5].

В ближайшие 1-1,5 года беларусское правительство планирует существенно расширить сферу возможностей оказания электронных услуг организациям и гражданам посредством интегрирования государственных информационных ресурсов с общегосударственной автоматизированной информационной системой. А к 1 января 2016 года все госорганы, а также юридические лица с долей государства должны будут подключиться к единой системе электронного документооборота. Для того, чтобы услугами электронного правительства смогли воспользоваться все граждане Беларуси, планируется ввести систему электронной идентификации личности. Уже сейчас значительную часть документов в госорганах получают (42, 35%) и отправляют (31,4%) в электронном виде[6].

---

[1] БЖД вручит памятный подарок миллионному интернет-пассажиру 2014 года. Доступно через:http://www.belta.by/ru/all_news/society/BZhD-vruchit-pamjatnyj-podarok-millionnomu-internet-passazhiru-2014-goda_i_690740.html

[2] Data Insight (2014) Какие тренды на белорусском рынке e-commerce в этом году, Доступно через: http://probusiness.by/markets/154-kakie-trendy-na-belorusskom-rynke-e-commerce-v-etom-godu.html

[3] Число интернет-магазинов в Беларуси за 7 месяцев возросло в 1,5 раза. Доступно через: http://www.belta.by/ru/all_news/economics/Chislo-internet-magazinov-v-Belarusi-za-7-mesjatsev-vozroslo-v-15-raza_i_677634.html

[4] Зиновский В. (2014) Информационное общество в Республике Беларусь, 2014. Доступно через: http://belstat.gov.by/bgd/public_compilation?id=520

[5] Там же

[6] Там же

ЧТО УГРОЖАЕТ ЦИФРОВОМУ ДОВЕРИЮ

Государственные органы собирают и хранят огромные массивы сведений о гражданах в базах данных различных министерств и ведомств.

УГРОЗЫ

Использование персональных данных обеспечит огромную отдачу для правительств, организаций и частных лиц. Но распространение информационно-коммуникационных технологий создает как новые возможности, так и новые риски, в том числе в отношении неприкосновенности частной жизни человека.

Мы оставляем онлайн огромные массивы персональной информации. Ежедневно через почтовые серверы проходят миллиарды электронных писем. Facebook хранит более сотни мегабайт персональных фотографий и видео на каждого пользователя. Через платежные системы проходят сотни миллиардов персонально помеченных финансовых платежей. Большинство совершеннолетнего населения в развитых странах постоянно транслирует свои текущие координаты через мобильные сети.

Пользователи вручают крупным компаниям колоссальные объемы данных о своей повседневной жизни, в том числе и конфиденциальной при этом считая, что компании будут осторожно обращаться с их данными, однако гарантия есть не всегда. Когда же на основе этой информации принимаются неполезные для нас решения, о них обычно не сообщается[7].

Ошибки, возникающие в результате объединения данных различных государственных структур – источник серьезных угроз информационной сфере частной жизни. Существует мнение, что более половины наборов сведений о гражданах, которые собирают правительства, содержат ошибки. Некоторые из этих ошибок, такие как неправильный адрес, несущественны, их легко заметить и исправить. В других случаях может совместиться кредитная информация о двух совершенно разных людях с похожими именами и т.п. При таких обстоятельствах бывает сложно понять основания тех или иных решений, принимаемых соответствующими учреждениями.

Массовая систематическая слежка за гражданами – одна из серьезнейших угроз неприкосновенности частной жизни онлайн. Суть функционирования системы массового систематического слежения сводится к процедуре поиска и выборки персональных данных конкретного субъекта из различных файлов (которые могут храниться в компьютерных банках данных, дислоцированных в разных концах страны) и слияния этих персональных данных в единый файл, содержащий исчерпывающие сведения о данном субъекте данных (data matching – совмещение,

[7] Паризер, Э. (2012) за стеной фильтров. Что интернет скрывает от нас. Москва, Альпина

стыковка, согласование данных). Создание системы «Большого брата» на базе применения процедур типа data matching предполагает наличие единого поискового признака – универсального идентификационного кода.

С развитием систем анализа больших массивов данных (Big Data) угроза усиливается, поскольку объединяться может, не только информация, содержащаяся в базах данных, но и видео, аудиоинформация, наши следы в интернете и пр. Такие системы позволяют установить уникальный профиль человека даже без слежки, а просто путем анализа его перемещений по координатам GSM-телефона и изображению с общедоступных камер наружного наблюдения, а также с помощью анализа интернет-трафика. Сохранить анонимность при генерации столь огромного массива информации становится практически невозможно.

По данным глобальных исследований, большинство лиц, ответственных за защиту персональных данных в компаниях, не имеют достаточно времени для выполнения своих обязанностей, а отчеты руководителям предоставляются нерегулярно. Исследование выявило, что 60% сотрудников компаний чаще всего допускают нарушения именно при обработке персональных данных, и наиболее часто жертвой подобных нарушений является клиент; 50% наиболее распространенных причин, которые приводят к нарушению принципов защиты персональных данных в пределах компании, является небрежность, а в 51% случаев такие нарушения не регистрируются и не наказываются соответствующим образом[8].

Превращение персональной информации в товар – еще одна угроза информационному самоопределению личности. «Идентифицирующая личность информация: имя, профессия, хобби и другие мелочи, делающие человека уникальным, превращается в объект владения, – пишет Э. Паризер. – Но владеют этим объектом не конкретные индивидуумы, контролирующие информацию о себе, а крупный бизнес, постоянно использующий его для получения прибыли и захвата рынка. Как можно ощущать собственную ценность, не владея в полной мере даже собственным именем?»[9].

Существуют специализированные компании, которые собирают общедоступные данные и привязывают их к профилям конкретных людей, с указанием имени, адреса и

[8] 2B Advice (2012) Data Protection Practice 2012. Доступно через: https://www.2b-advice.com/GmbH-en/Study-Data-Protection-Practice-2012

[9] Паризер, Э. (2012) за стеной фильтров. Что интернет скрывает от нас. Москва, Альпина

ЧТО УГРОЖАЕТ ЦИФРОВОМУ ДОВЕРИЮ

Основные типы угроз приватности в цифровом мире:

недобросовестная политика обращения с персональными данными со стороны держателей данных (прежде всего, представителей бизнеса, а также со стороны государственных органов), которым были доверены персональные данные со стороны граждан (в том числе и утечка персональных данных);

сбор, систематизация и распространение персональных данных из различных источников, позволяющих составить многосторонний «профиль» соответствующего субъекта данных: от религиозных убеждений и особенностей характера до покупательских предпочтений и сведений об имуществе;

киберпреступность (сетевое мошенничество, вредоносные программы и программы-шпионы, кражи, совершенные посредством использования информационно-коммуникационных технологий).

т.д. Например, американская компания Acxiom уже накопила базу данных по 1500 классификаторам на 500 миллионов пользователей со всего мира. Компания заявляет, что по составленным профилям может прогнозировать реакцию потребителей на различные раздражители (товары, бренды и проч.)[10]. Такие компании способны даже автоматически предсказывать местонахождение пользователей, анализируя архивные GPS-метки. По последним экспериментальным данным, точность составляет 80% в течение 80 недель[11].

Данные, на основании которых можно идентифицировать индивида, собираются не только правительствами и коммерческими компаниями. Пользователи различных ресурсов и сервисов глобальной сети интернет – это сотни тысяч «маленьких братьев», которые поставляют видео, аудио и текстовую информацию о людях онлайн.

Еще одна опасность – это персонализация потоков сообщений, которая лишает человека возможности контролировать информацию, которую он получает. Код, лежащий в основе персонализации, довольно прост, поясняет Э. Паризер: «Фильтры нового поколения изучают то, что вам, судя по всему, нравится: ваши предшествующие действия или то, что нравится людям, похожим на вас, – и пытаются экстраполировать эти данные. Это механизмы предсказаний, постоянно уточняющие теорию о том, кто же вы на самом деле, что вы сделаете и чего захотите дальше. Вместе они творят уникальную информационную вселенную для

[10] Tucker, P. (2013) Has Big Data Made Anonymity Impossible?.Доступно через: http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible

[11] Sadilek, A., Krumm, J.(2012) Far Out: Predicting Long-Term Human Mobility. Доступно через: http://www.cs.rochester.edu/~sadilek/publications/Sadilek-Krumm_Far-Out_AAAI-12.pdf

каждого из нас — я называю этот процесс возведением «стены фильтров» — и фундаментально меняют наш подход к восприятию информации»[12]. Тем самым стирается граница между удобством сервиса и вмешательством – контролем поведения и непосредственным влиянием на личность.

Демократизация деструктивных технологий, информационные войны, создающие угрозу национальной безопасности, побуждают правительства все в большей степени использовать системы массированного систематического наблюдения. События последних лет показали, насколько опасной для сохранения неприкосновенности частной жизни может быть такая деятельность при отсутствии надлежащих инструментов регулирования.

Непосредственную угрозу информационной приватности представляют различные виды компьютерных преступлений. Большинство из них – это «старые» нарушения неприкосновенности частной жизни, совершенные с использованием информационно-коммуникационных технологий. Некоторые же, например, кража личности – это совершенно новые явления, которые требуют разработки новых мер регулирующего воздействия.

Таким образом, типы угроз приватности в цифровом мире можно обозначить следующим образом:

- недобросовестная политика обращения с персональными данными со стороны держателей данных (прежде всего, представителей бизнеса, а также со стороны государственных органов), которым были доверены персональные данные со стороны граждан (в том числе и утечка персональных данных);
- сбор, систематизация и распространение персональных данных из различных источников, позволяющих составить многосторонний «профиль» соответствующего субъекта данных: от религиозных убеждений и особенностей характера до покупательских предпочтений и сведений об имуществе;
- киберпреступность (сетевое мошенничество, вредоносные программы и программы-шпионы, кражи, совершенные посредством использования информационно-коммуникационных технологий).

Иными словами, угрозы информационной приватности порождаются не применением новых цифровых и телекоммуникационных технологий, а ненадлежащими способами

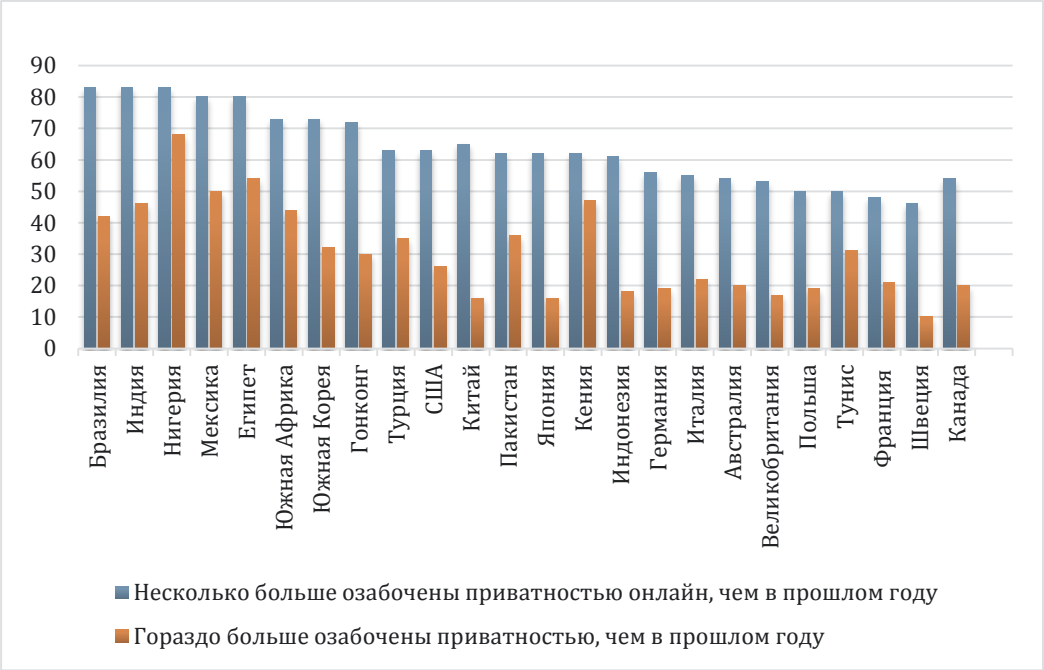
[12] Там же

сбора информации (массовое систематическое слежение, перехват сообщений, опросы, анкеты и пр.) и несоблюдением необходимых мер защиты при обработке информации.

….И КАК МЫ НА НИХ РЕАГИРУЕМ

По данным глобальных исследований, люди все больше ощущают угрозы неприкосновенности частной жизни онлайн.

График 2. Ответы на вопросы о приватности онлайн. Распределение по странам (%) [13]



В Беларуси не проводилось полномасштабных исследований того, как на практике государственные и частные организации обращаются с теми объемами персональных данных, которые оказываются в их распоряжении. Не исследовались и установки пользователей ресурсов и сервисов сети интернет в отношении права на неприкосновенность частной жизни онлайн. Однако есть все основания предположить, что Беларусь в этом отношении не является исключением и многие тенденции, обозначенные в предыдущем разделе, проявляются и в нашей стране.

Результаты опроса 40 активистов общественных организаций, проведённого аналитической группой ЦЕТ совместно с Центром правовой трансформации,

[13] CIGI-IPSOS Global Survey on Internet Security and Trust. Доступно через https://www.cigionline.org/internet-survey

позволяют отметить наличие озабоченности в отношении защиты цифровой приватности.

График 3. Обеспокоенность в отношении защиты персональных данных

При этом практически все предложенные к оценке области использования интернет, по мнению респондентов, несут в себе потенциальные опасности, связанные с возможностью злоупотребления персональной информацией пользователей.

Таблица 1. Основные угрозы цифровой приватности

В каких ситуациях использования сети интернет Вы чувствуете наибольшую угрозу, связанную с возможными злоупотреблениями Вашей персональной информацией? (возможно несколько вариантов ответа)	**Абсолютная частота**
При использовании почтовых сервисов	24
Когда Вы заходите на сайт, который требуют регистрации	23
При пользовании социальными сетями	22
При покупке товаров или услуг	20
Не чувствую никаких угроз	0

Большинство (64 %) при этом осознает, что угрозы не очевидны, имеют скрытый характер.

График 4. Нарушения приватности онлайн

Как показывают ответы на последующие вопросы, эти злоупотребления связаны чаще всего с передачей и использованием не по назначению контактных данных (телефон, адрес электронной почты) или отслеживанием информации в социальных сетях.

В ходе работы фокус-групп так же было озвучено несколько кейсов и несколько наиболее распространенных типов злоупотреблений персональными данными с последствиями разной степени тяжести: от огромного количества навязчивой рекламы в социальных сетях, поисковиках или непосредственно в электронной почте, до финансовых потерь (воровство денег с карточек) и попадания в почти уголовную историю.

В то же время, во многих случаях некорректное обращение с персональными данными происходит не по злому умыслу и не в целях личной выгоды (или «государственных интересов»), а просто по незнанию и от безграмотности. В ходе работы фокус-групп были озвучены несколько случаев такого рода: региональная газета публиковала персональные данные всех «новых граждан города» (то есть личные данные новорожденных и матерей), пока одна из матерей не пригрозила журналистам судом; сайт государственной поликлиники, который ввел возможность заказывать талоны на посещение врача онлайн, сделал информацию о том, кто к какому врачу записывается общедоступной и пр.

График 5. Уровень доверия организациям в сфере защиты персональных данных

Никто из респондентов не имеет полной уверенности, что организации (государственные и частные), собирающие, хранящих и обрабатывающих информацию, обеспечивают необходимый уровень защиты персональных данных.

Интересно, что опрошенные гражданские активисты не имеют однозначного и твёрдого мнения по вопросу о публичном раскрытии информации о частной жизни конкретных людей: примерно половина (16 из 35) считают, что в некоторых случаях нарушение тайны частной жизни допустимо, тогда как только немного меньше (13 из 35) считают, что необходим законодательный запрет на публичное раскрытие личной информации.

Что касается способов зашиты персональной информации, то среди гражданских активистов равно распространены следующие:

- осторожность – избегать сомнительных сайтов, не оставлять самим личных данных в открытом доступе, использовать анонимизаторы, управление паролями,
- использование специального ПО: PGP, TrueCrypt,
- изменение законодательства – например, законы, запрещающие компаниям (интернет-провайдерам и др.) предоставлять «на сторону» личные данные граждан,

- смирение – или отказаться от использования интернета и современных технологий, или просто иметь в виду риски и опасности; пользоваться интернетом на свой страх и риск.

Анализ результатов опроса активистов общественных организаций и работы в фокус-группах (журналисты и представители бизнеса) показал:

- обыденные примеры «социального дискомфорта» не связываются с правом на неприкосновенность частной жизни онлайн;
- термин «персональные данные» становится все более узнаваемым, однако интерпретации его неоднозначны и иногда далеки от реального содержания;
- степень защищённости персональных данных, собираемых государственными и коммерческими учреждениями, вызывает серьезные опасения, которые, в силу специфики регулирования этой сферы в Беларуси, трудно подтвердить или опровергнуть;
- отсутствие общих регламентов и правил, регулирующих обращение с персональными данными, их хранение, передачу или распространение, только в незначительной степени компенсируется некодифицированными нормами (здравый смысл, моральные нормы, журналистская этика) или внутрикорпоративными регламентами;
- в качестве мер, которые могли бы способствовать улучшению ситуации и повышению защищенности граждан, респондентами исследования предлагалось введение единого законодательного регулирования процессов сбора, хранения и распространения персональных данных, а также просветительские и образовательные действия, направленные на повышение компетенций граждан в обращении с личной информацией.