Политика в отношении персональных данных имеет многоуровневый и кросс-секторальный характер. В нее вовлечены наднациональные, национальные и субнациональные (государственные и неправительственные) акторы, как институциональные, так и индивидуальные.

В чем суть проблемы?

АКТОРЫ

Политика в отношении персональных данных имеет многоуровневый и кросс-секторальный характер. В нее вовлечены наднациональные, национальные и субнациональные (государственные и неправительственные) акторы, как институциональные, так и индивидуальные.

Актор публичной политики – это «действующее лицо», которое принимает активное участие в процессе решения социально значимых проблем и характеризуется, по крайней мере:

- свободой маневра по отношению к принуждениям системы;
- способностью взаимодействия с другими;
- способностью к активному поведению;
- наличием стратегии (цель и способы ее достижения);
- признанием со стороны других акторов[1].

Существуют различные подходы к анализу сложной структуры акторов публичной политики[2]. Наиболее подходящим для первоначального введения в проблематику защиты персональных данных представляется структурирование на основании формальной/официальной позиции, предложенной К. Бенентом и Ч. Раабом[3].

[1] В зависимости от того или иного подхода к политическому анализу, исследователи используют и по-разному определяют термины агент действия, субъект политики, актор и пр. Авторы данного пособия руководствуются дефинициями, обоснованными в книге Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J. and Bots, P. (2010) Policy Analysis of Multi-Actor Systems. P. 79-108. Следует также отметить, что в рамках теории организаций чаще используется термин «стейкхолдер», который исторически предшествовал теоретическому оформлению понятия «актор политики».

[2] Подробно эти подходы описаны здесь Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J. and Bots, P. (2010) Policy Analysis of Multi-Actor Systems.

[3] Raab, C., Koops, B-J (2009), 'Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.edu

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Исследователи, прежде всего, обращают внимание на то, что транснациональное «движение» персональных данных в глобальной сети обуславливает фундаментальное значение международных принципов и, следовательно, определяющую роль **глобальных и региональных межправительственных организаций и объединений**: ООН, ОЭСР, Совета Европы, Европейского Союза, Организации Азиатско-Тихоокеанского сотрудничества, Всемирного банка, Всемирной торговой организации, Международной торговой палаты и др.

Для того, чтобы установить единообразный режим правового регулирования обработки и передачи персональных данных в рамках союза или сообщества стран, представляющая его международная организация, как правило, последовательно выполняет следующее:

- добивается консенсуса стран-участниц данного сообщества относительно тех принципов защиты данных, которые должны применяться в рамках сообщества,
- легитимизирует эти принципы при помощи подписания странами-участницами соответствующего международного соглашения, предусматривающего обязанность стран-участниц гармонизировать свое национальное законодательство в соответствии с вышеуказанными принципами защиты данных,
- устанавливает для стран-участниц, ратифицировавших вышеупомянутое международное соглашение и гармонизировавших национальное законодательство, режим наибольшего благоприятствования в сфере обмена персональными данными,
- запрещает (или, по крайней мере, строго ограничивает) обмен персональными данными со странами, не являющимися участницами данного международного соглашения о защите данных как напрямую, так и через третьи страны[4].

На национальном уровне важнейшую роль в разработке и реализации политики в отношении приватности, безусловно, играют **законодатели, суды и органы высшей государственной власти.**

Очевидно, что и **исполнительные органы, государственные учреждения и организации,** обеспечивающие процессы сбора, хранения и обработки данных, также существенно влияют на политику в отношении защиты персональных данных. Их роль и влияние определяются функциями в различных контекстах (см. таблицу «Пример: функции и контексты акторов политики в отношении защиты персональных данных»).

[4] Иванский, В.П. (1999) Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. Доступно через: http://www.pravo.vuzlib.su/book_z137_page_1.html

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

В процессе принятия решений, разработки и реализации политики складываются и разные конфигурации интересов акторов. Только серьёзный анализ таких кластеров интересов позволяет эффективно решать проблемы защиты прав субъектов данных в конкретных ситуациях. Без учета этого положение будет нестабильным, мозаика несовместимых интересов и ресурсов будет порождать нереализуемые стратегии, каждый инструмент будет использоваться изолированно. Итог – отсутствие единой цели и, следовательно, эффективной политики, основанной на синергии регуляторных воздействий.

К числу ведущих институциональных акторов К. Беннет и Ч. Рааб относят также **уполномоченные органы по защите прав субъектов персональных данных** и их международные объединения.

Функции национального органа (или системы органов) по обеспечению качества персональных данных и защите прав субъектов данных (традиционно такие органы называют кратко – «органы защиты персональных данных»):

- регистрационно-разрешительные,
- контрольно-надзорные,
- арбитражные,
- экспертные.

Неправительственные институциональные акторы – крупные интернет-компании (в лице ответственных или департаментов по защите прав субъектов персональных данных) составляют еще одну влиятельную группу акторов. Так, в 1983 г. была создана Международная рабочая группа по защите персональных данных в сфере телекоммуникаций (Берлинская группа), которая опубликовала ряд влиятельных в рамках европейской политики документов[5]. Альянс онлайновой приватности (Online Privacy Alliance: http://www.privacyalliance.org/)– бизнес-ассоциация, содействующая разработке правил и принципов саморегулирования в целях обеспечения защиты персональных данных потребителей. В 2008 г. была создана ассоциация «Глобальная сетевая инициатива (Global network initiative: https://www.globalnetworkinitiative.org/), члены которой в рамках стратегий социальной корпоративной ответственности разрабатывают критерии и меры обеспечения защиты персональных данных в сфере ИКТ-индустрии. Рабочая группа по приватности и защите персональных данных Международной торговой палаты –

[5] International Working Group on Data Protection in Telecommunications. Доступно через: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt

единственная бизнес-ассоциация, имеющая статус наблюдателя в комитете по защите персональных данных Совета Европы[6].

Группы активистов защиты прав субъектов персональных данных формируются и функционируют на национальном и наднациональном уровнях. Такие организации, как Electronic Privacy Information Center, Privacy International оказывают существенное влияние на формирование принципов и механизмов регулирования. Особый интерес, с точки зрения экспертов, представляет организация «Европейские цифровые права» (European Dgital Rights/EDRI), созданная в 2002 г. и объединяющая 29 групп из 18 европейских стран[7]. В частности, EDRI подготовила популярную брошюру «Защита персональных данных. Введение»[8].

Серьезным вкладом в обеспечение прав субъектов персональных данных стали «Международные принципы применения прав человека в отношении мониторинга средств связи», которые были разработаны общественными организациями Access, Article 19, Association for Progressive Communications, Bits of Freedom, Electronic Frontier Foundation, European Digital Rights, Privacy International и др[9].

Правозащитники, усматривающие в отдельных законодательных инициативах и действиях правительства угрозу правам человека (главным образом, праву на неприкосновенность частной жизни). Этих активистов объединяет общая обеспокоенность существующими тенденциями законодательного регулирования обращения персональных данных (при этом указывается, во-первых, на меньшую проработанность соответствующих нормативных инициатив по сравнению с европейским уровнем, а также их несоответствие интересам российских граждан [2]), отсутствием выраженной готовности органов государственной власти к диалогу, низким уровнем правосознания российских граждан.

Среди влиятельных акторов **– организации, устанавливающие технические стандарты**:

- Международная организация стандартизации,
- Форум информационной безопасности (https://www.securityforum.org/)[10],

---

[6]International chamber of commerce (2008) Privacy and Personal Data. Доступно через: http://www.iccwbo.org/advocacy-codes-and-rules/areas-of-work/digitaleconomy/privacy-and-personal-data-protection

[7] Raab, C, Koops, B-J (2009), 'Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.ed.ac.uk/portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy_Protection.pdf

[8]EDRI (2012) Защита персональных данных. Введение». Доступно через: http://www.lawtrend.org/information-access/zashhita-dannyh

[9] International Principles on the Application of Human Rights to Communications Surveillance. Доступно через: https://en.necessaryandproportionate.org/

[10] The Standard of Good Practice for Information Security, Information Security Forum (2003). Доступно через: http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf

- Европейский комитет стандартизации (http://www.cenelec.eu/),
- Британский институт стандартов http://www.bsigroup.com/en-GB/[11].

Обладающие «более, чем средней» степенью правосознания граждане, сетевые активисты, обеспокоенные угрозой нарушения их права на приватность и неприкосновенность персональных данных, также не являются консолидированной стороной. Они обладают различным уровнем компетенции в данном вопросе и участвуют в развитии законодательного процесса с большей или меньшей степенью непостоянства. Тем не менее, представители этой группы играют, возможно, наиболее значительную роль в просвещении интернет-общественности в отношении проблемы обеспечения приватности путем распространения соответствующих публикаций на персональных сайтах и в специализированных изданиях

Таблица 2. Основные акторы политики в отношении персональных данных[12]

Актор	Функция
Разработчик конституции	Обеспечивает право на приватность (и защиту персональных данных)
Законодатель	Разрабатывает закон о защите персональных данных, а также другие законодательные акты с учетом права субъекта данных на защиту персональных данных
Уполномоченный орган по защите прав субъектов персональных данных	Контролирует исполнение законов, способствует распространению лучших практик, инициирует привлечение внимания общественности к вопросам защиты персональных данных
Контролеры данных	Принимают решения относительно целей обработки и типа данных, которые должны быть обработаны
Сотрудники государственных органов	Исполнение законов, обучение персонала правилам и принципом защиты прав субъектов персональных данных
Частные компании	Исполнение законов, обучение персонала правилам и принципом защиты прав субъектов персональных данных, разработка

[11] BS 7799-3:2006.Standard on Information Security Management Systems–Guidelines for Information Security Risk Management. Доступно через: http://www.iso.staratel.com/ISO17799/Doc/BS7799.3.1999/BS%207799-3-2006.pdf

[12] Raab, C., Koops, B-J (2009) 'Privacy Actors, Performances and the Future of Privacy Protection. Доступно через: http://www.research.ed.ac.uk/portal/files/12592176/Privacy_Actors_Performances_and_the_Future_of_Privacy_Protection.pdf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

	и исполнение корпоративных кодексов, лоббирование тех или иных решений
Гражданские ассоциации, группы активистов	Борются за защиту прав субъектов персональных данных, предлагают решения, рекомендуют, привлекают внимание общественности
Академическое сообщество (правоведы, социологи, философы)	Исследование и проблем защиты прав субъектов персональных данных, выявление долговременных тенденций, прогнозы, рекомендации
Журналисты	Освещают события и проблемы, объясняют политику и тенденции развития, обнародуют факты нарушения прав субъектов данных
Субъекты данных (граждане, потребители)	Защищают свое право на приватность информационной сферы, жалуются
Разработчики технических стандартов и технологий	Разрабатывают стандарты и решения, обеспечивающие защиту персональных данных, обучают ИТ- специалистов

В процессе принятия решений, разработки и реализации политики складываются и разные конфигурации интересов акторов. Эксперты утверждают, что только серьёзный анализ таких кластеров интересов позволяет эффективно решать проблемы защиты прав субъектов данных в конкретных ситуациях. Без учета этого положение будет нестабильным, мозаика несовместимых интересов и ресурсов будет порождать нереализуемые стратегии, каждый инструмент будет использоваться изолированно. Итог – отсутствие единой цели и, следовательно, эффективной политики, основанной на синергии регуляторных воздействий

ИНСТРУМЕНТЫ

Международные принципы

Формальный нормативный базис законодательства о защите персональных данных составляют фундаментальные права человека, зафиксированные в международных и региональных документах:

- Всеобщей декларации прав человека (ООН, 1948) ст. 19, 29;
- Международном пакте о гражданских и политических правах (ООН, 1966) ст. 15;
- Международном пакте об экономических, социальных и культурных правах (ООН, 1976);

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Набор инструментов политики в отношении защиты персональных данных включает не только меры законодательного регулирования, но и транснациональные принципы, руководства и соглашения, практики саморегулирования, стандартизации, технологические решения и просветительские мероприятия. Закон должен дополняться кодексами поведения и технологическими мерами, опираться на соответствующую организационную культуру и поддержку общественности

- Международной конвенции о ликвидации всех форм расовой дискриминации (ст.5);
- Международной конвенции о ликвидации всех форм дискриминации женщин (1965 г.);
- Конвенции о защите прав человека и основных свобод (Совет Европы, 1950) ст. 10, 15, 16, 17;
- Американской декларации прав и свобод человека (1948) ст. 6;
- Американской конвенции о правах человека (Пакт Сан-Хосе, 1969) ст. 13;
- Африканской Хартии прав человека и народов (Организация африканского единства, 1981) ст. 9, 27, 29;
- Хартии социальных прав и гарантий граждан независимых государств (СНГ, 1994);
- Хартии Европейского союза об основных правах человека (ЕС, 2000);
- Арабской хартии прав человека (Лига арабских государств, 2004);
- Конвенции Содружества Независимых Государств о правах и основных свободах человека (СНГ, 2011);
- Азиатской хартии по правам человека (АСЕАН, 2012);
- Бишкекской декларации ОБСЕ.

Международное соглашение на глобальном уровне о принципах защиты персональных данных до сих пор отсутствует, хотя эксперты все более настойчиво говорят о необходимости разработки такого документа. В настоящее время эту лакуну заполняют:

- Резолюция Генеральной ассамблеи ООН «Право на приватность в цифровую эпоху» (2014);
- Резолюция Генеральной ассамблеи ООН «Руководящие принципы, касающиеся компьютеризированных картотек, содержащих данные личного характера» (1990);

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

- Конвенция № 108 Совета Европы о защите индивидуумов (частных лиц) по отношению к автоматизированной обработке персональных данных (1981) и Дополнительный протокол, который вышел за рамки регионального документа и открыт для подписания неевропейскими странами;
- «Рекомендации в отношении Руководящих принципов по защите неприкосновенности частной жизни и трансграничных потоков персональных данных» Организации экономического сотрудничества и развития.

Особое место в этом контексте занимает Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных»[13], которая, по мнению экспертов, определяет основные тенденции законодательного регулирования защиты персональных данных, поскольку:

- принцип адекватности национальных законов требованиям Директивы определяет возможности обмена данными со странами Европейского Союза;
- требования Директивы N 95/46/ЕС дублируются в Дополнительном протоколе Конвенция № 108 Совета Европы.

В рамках СНГ к настоящему моменту существует четыре документа:

Модельный закон СНГ, принятый Межпарламентской ассамблеей в 1999 г.

Решение Координационного Совета государств-участников СНГ по информатизации при РСС от 1 июля 2003 г. N 3/1. «Стратегия сотрудничества стран СНГ в сфере информатизации»

Решение Совета глав правительств Содружества Независимых Государств «О внесении дополнений в Стратегию сотрудничества государств - участников СНГ в сфере информатизации и в План действий по реализации Стратегии сотрудничества государств - участников СНГ в сфере информатизации на период до 2010 года»

Соглашение о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии, и использовании в государствах – участниках СНГ (2009)

[13] Директива Европейского Парламента и Совета Европейского Союза 95/46/ЕС от 24 октября 1995 г.о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (в редакции Регламента Европейского парламента и Совета ЕС 1882/2003 от 29 сентября 2003 года) http://pd.rkn.gov.ru/docs/Direktiva_Evropejskogo_Parlamenta_i_Soveta_Evropejskogo_Sojuz_95_46_ES.rtf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Таблица 3. Принципы защиты данных в международных документах[14].

Принципы защиты данных	Конвенция Совета Европы	Руководящие принципы ОЭСР	Директива ЕС о защите данных
Честные и законные средства сбора данных	✓	✓	✓
Указанные и законные цели сбора данных	✓	✓	✓
Соответствие данных цели их сбора	✓	✓	✓
Точность данных	✓	✓	✓
Хранение данных только до момента достижения цели их сбора	✓	-	✓
Особый режим обращения с «уязвимыми данными»	✓	-	✓
Безопасность обработки и хранения данных	✓	✓	✓
Информирование субъекта данных об осуществлении обработки его данных	✓	✓	✓
Доступ субъекта данных к своим личным данным и возможность их изменения	✓	✓	✓
Подотчетность при обработке данных	✓	✓	✓

Международные принципы защиты персональных данных – не статичный инструмент. С появлением новых технологий, осознанием новых вызовов производится их периодический пересмотр.

В 2013 г. были опубликована новая редакция Руководящих принципов ОЭСР[15].

В новой редакции сохранены все основные принципы:

- законный и ограниченный сбор персональных данных, получаемых с ведома и согласия физического лица,

[14] Tan J (2008) A comparative study of the APEC privacy framework: A new voice in the data protection dialogue?. In Asian Journal of Comparative Law, 3(1). http://www.degruyter.com/dg/viewarticle/j$002fasjcl.2008.3.1$002fasjcl.2008.3.1.1071$002fasjcl.2008.3.1.1071.xml;jsessionid=F36717919BBF04391AC61CF44A516545

[15] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) доступна по адресу: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf .

- данные собираются в соответствии с целями обработки, обеспечивается их полнота и актуализация,
- использование данных для новых целей должно быть либо совместимо с первоначальной целью обработки, либо требуется согласие на новые виды использования или раскрытия информации,
- разумные меры безопасности для защиты данных, обеспечение подотчетности всех операторов данных,
- у субъекта персональных данных есть право на доступ к хранящимся о нём данным, а также право на их уничтожение или исправление.

Вместе с тем в новой редакции усиливаются требования к подотчётности оператора данных независимо от местонахождения данных, а также независимо от того, обрабатываются ли данные самим оператором, его представителями или передаются другому оператору.

ОЭСР рекомендует:

- использовать адаптированные под особенности организации программы управления защитой персональных данных и оценки последствий утечек для управления связанными с утечками рисками;
- включать в контракты положения, требующие соблюдения политики оператора данных по вопросам защиты персональных данных;
- устанавливать протоколы оповещения в случае инцидентов безопасности;
- разрабатывать план реагирования на инциденты безопасности и запросы со стороны субъекта персональных данных.

В настоящее время в число основных принципов защиты персональных данных входят:

1. **Принцип ограничения объема собираемых данных**

Объем собираемых персональных данных должен иметь пределы; все эти данные должны быть получены законным и честным образом – если возможно, то с ведома или согласия субъекта данных.

2. **Принцип качества данных**

Персональные данные должны соответствовать целям, в которых они будут использоваться; в той мере, в которой это необходимо в соответствии с упомянутыми целями, персональные данные должны быть точными, полными и регулярно обновляемыми.

3. Принцип конкретизации целей

Цели, в которых собираются персональные данные, должны быть конкретизированы не позднее момента сбора указанных данных, а их последующее использование должно ограничиваться достижением упомянутых либо сходных (совместимых) целей, которые должны указываться каждый раз, когда эти цели пересматриваются.

4. Принцип ограничений на использование данных

Персональные данные не должны разглашаться, предоставляться в пользование или иным образом использоваться в отличных от перечисленных в пункте 3 целях, за исключением случаев, когда:

a) субъект данных дает на то свое согласие;
b) это разрешено законом.

5. Принцип обеспечения безопасности

Персональные данные должны быть обеспечены должными механизмами защиты от рисков, связанных с потерей, несанкционированным доступом, уничтожением, использованием, изменением или разглашением данных.

6. Принцип открытости

Процесс развития, а также практика и политика в отношении персональных данных должны осуществляться в рамках общей политики открытости. В постоянной готовности должны быть средства для установления факта наличия и характера персональных данных, основных целей их использования, а также личности и обычного местонахождения распорядителя данных.

7. Принцип индивидуального участия

Индивидуум должен иметь право:

а) получать от распорядителя данных либо иным образом, подтверждения того, имеются ли у распорядителя данных персональные данные, относящиеся к упомянутому индивидууму;

б) получать относящиеся к нему персональные данные:

- в разумные сроки;
- если взимается плата, то по тарифу, не являющемуся чрезмерно высоким;
- в рамках разумной процедуры;
- в удобной для понимания форме;

в) в случае отказа от удовлетворения заявки, не предоставление информации, поданной в соответствии с пунктами (а) и (б), получать разъяснения о мотивах отказа и опротестовывать такой отказ;

г) опротестовывать относящиеся к нему данные; в случае удовлетворения протеста требовать того, чтобы таковые данные были уничтожены, исправлены или дополнены.

8. Принцип ответственности

Распорядитель данных должен нести ответственность за принятие мер, обеспечивающих соблюдение вышеперечисленных принципов. [16]

28 ЯНВАРЯ 2014 ГОДА В ОТМЕЧАВШИЙСЯ В ЕВРОПЕ ДЕНЬ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ВИЦЕ-ПРЕЗИДЕНТ ЕВРОПЕЙСКОЙ КОМИССИИ, УПОЛНОМОЧЕННЫЙ (ЕВРОКОМИССАР) ПО ВОПРОСАМ ЮСТИЦИИ ВИВИАН РЕДИНГ ВЫСТУПИЛА С РЕЧЬЮ, В КОТОРОЙ СФОРМУЛИРОВАЛА ВОСЕМЬ ПРИНЦИПОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, В СООТВЕТСТВИИ С КОТОРЫМИ ДОЛЖНА ОСУЩЕСТВЛЯТЬСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ КАК В ГОСУДАРСТВЕННОМ, ТАК И В ЧАСТНОМ СЕКТОРАХ.

Принцип 1: ***Европа должна создать надежную правовую базу*** для защиты персональных данных, которая могла бы стать для всего мира образцом и стандартом. В противном случае другие страны нас опередят и навяжут свои стандарты Европе.

Принцип 2***: Правовая база защиты персональных данных не должна проводить различие между частным и государственным секторами***. Граждане просто не поймут такое различие в условиях, когда государственный сектор собирает, сопоставляет, а иногда даже хочет продавать персональные данные.

Принцип 3. ***В ходе подготовки законодательства о защите персональных данных необходимо проводить его общественное обсуждение***, поскольку оно затрагивает гражданские свободы в онлайн-среде. Защита персональных данных должна быть темой кампании по информированию общественности,

[16] Рекомендации в отношении Руководящих принципов по защите неприкосновенности частной жизни и трансграничных потоков персональных данных» Организации экономического сотрудничества и развития (· OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) Доступно через: http://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en

направленной на совместное обсуждение вопроса гражданами, правозащитными группами, коммерческими компаниями и государственными органами.

Принцип 4: ***Ничем не ограниченный перехват электронных коммуникаций неприемлем***. Сбор данных в интересах наблюдения и контроля (surveilance) должен быть нацеленным и ограничен рамками, пропорциональными целям такого наблюдения.

Принцип 5: ***Законы должны быть четкими, и должна поддерживаться их актуальность.*** Нельзя, чтобы страны-члены Евросоюза, устанавливая рамки современных программ контроля и наблюдении, полагались на устаревшие законы, разработанные в другую технологическую эпоху. Такие законы мало или вообще ничего не говорят гражданам о том, что на самом деле происходит.

Принцип 6: ***Исключения со ссылкой на интересы национальной безопасности должны использоваться экономно***. Они должны быть именно исключениями, а не правилом. Необходимость защиты национальной безопасности может оправдать особые нормы. Однако не всё, что относится к внешним связям, является вопросами национальной безопасности. Иной подход подрывает легитимность законов, имеющих жизненно важное значение для нашей безопасности.

Принцип 7: ***Судебный надзор необходимо для того, чтобы избежать слишком сильного «раскачивания маятника» в разные стороны***. Надзор со стороны исполнительной власти – дело хорошее. Парламентский контроль необходим. Судебный же надзор является ключевым фактором.

Принцип 8: ***Законодательство о защите персональных данных должно применяться независимо от гражданства заинтересованных лиц***. Применение различных стандартов в зависимости от того, является ли лицо гражданином данной страны, не имеет никакого смысла ввиду открытой природы Интернета[17]

[17] Eecke, P. (2014) EUROPE: EU Commissioner Reding introduces her Eight Principles of Data Protection. Доступно через: http://www.jdsupra.com/legalnews/europe-eu-commissioner-reding-introduc-85150/

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Национальное законодательство

Первые законодательные акты в отношении персональных данных принимались в связи с созданием централизованных государственных баз данных уже в 1960-х гг. Однако нормы, принимавшиеся до 1970 г. носили, в основном, технический характер. В законах второй половины 1970-х гг. намного больше внимания уделялось правам индивидов. Третье поколение норм связано с реакцией на введение концепта «информационное самоопределение личности» в немецком законодательстве. Четвертое поколение норм связано с разработкой секторальных законов, дополняющих общие законы о защите персональных данных.

> В 1969 г. Парламент Великобритания принял «Билль о наблюдении за данными», устанавливающий контроль за собранной информацией. Первым целевым законодательным актом по защите персональных данных является немецкий Закон Земли Гессен 1970 года «О защите данных». Закон «О данных», принятый в Швеции в 1972 г. стал первым общенациональным законодательным актом,

Хотя процедурные нормы излагаются по-разному, в соответствии с правовой системой каждой страны, существует широкое согласие в отношении целей, которые должны быть обеспечены этими нормами. Национальные законодательства, включают, как минимум, следующие принципы, зафиксированные в международных документах:

- открытость – общество должно быть проинформировано о наличии баз персональных данных, которые находятся в распоряжении правительственных органов, организаций и учреждений;
- возможность доступа субъекта данных к данным о себе и возможность корректировать неточные или устаревшие данные;
- сбор персональных данных и объем этих данных должен быть ограничен в соответствии с целями сбора;
- ограничение использования – персональные данные должны использоваться только в целях, для которых они собирались;
- ограничения раскрытия – персональные данные могут быть раскрыты только в законных целях и с согласия субъекта данных[18].

[18] Bennett, C. Grant, R. (1999) Visions of Privacy: Policy Choices for the Digital Age. Toronto: University of Toronto Press;

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Рекомендации ОЭСР (2013)

Управление глобальными рисками требует разработки национальных стратегий стран с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных

- безопасность – данные должны быть защищены от потери, несанкционированного доступа, уничтожения, использования или модификации[19].

Национальные правовые системы защиты персональных данных могут основываться на двух принципиально отличающихся подходах:

- Генеральный – заключается в стремлении к созданию единого и всеобъемлющего закона о защите сферы частной жизни на основе права на невмешательство в частную жизнь. Некоторые страны включили право на защиту персональных данных в Конституцию (Швеция, Бельгия, Греция, Нидерланды).

- Секторный (или отраслевой) – состоит в создании специализированных законов либо для каждого типа посягательств на сферу частной жизни, либо для каждой отрасли или сектора человеческой деятельности, являющейся потенциальным источником угроз для права человека на невмешательство в его частную жизнь (например, для почты и средств связи, для бюро кредитной информации, для средств массовой информации и рекламной сферы, для частных детективов, для компьютерных банков данных). Отраслевые законы представляют собой дополнительные законоположения, конкретизирующие положения базового национального закона о защите данных и обеспечивающие защиту персональных данных в отраслях человеческой деятельности, связанных с обработкой, передачей или использованием таких данных и несущих потенциальные угрозы посягательства на сферу частной жизни граждан. «Секторный» («отраслевой») подход, при котором новые «отраслевые» законы принимались по мере

[19] Hert, P. (2013) Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency? Доступно через: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert-Papakonstantinou.pdf

накопления прецедентной базы, указывающей на новый источник угроз для сферы частной жизни, приводил к бессистемности, дублированию и противоречивости законоположений.

Уже в конце 1990-х гг. эксперты отмечали, что в чистом виде и тот, и другой подходы оказались непродуктивными. В подавляющем большинстве стран современные национальные системы правового регулирования обработки и использования персональных данных применяют так называемый смешанный принцип, объединяющий определенные аспекты «генерального» и «отраслевого» подходов. Такой подход может быть эффективным только при наличии национальных стратегий стран с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных.

В странах-членах Европейского Союза в настоящее время ведется работа по модернизации регулирования защиты персональных данных.

Таблица 4. Ключевые изменения в рамках реформы законодательства стран-членов Европейского Союза в области защиты данных[20].

Общий свод правил защиты данных, действующий на всей территории ЕС. Ненужные административные требования, например, обязанность компаний направлять уведомления, будут отменены.
Вместо действующего сегодня требования, обязывающего все компании уведомлять органы по надзору за соблюдением защиты данных обо всех действиях по защите данных, регламентом предусмотрено повышение уровня ответственности и подотчетности лиц, осуществляющих обработку данных.
Компании и организации обязаны в максимально короткий срок (по возможности не позднее 24 часов) уведомлять национальный надзорный орган о серьезных нарушениях требований по защите данных.
Организации будут иметь дело только с одним национальным органом по защите данных в стране ЕС по месту основной регистрации. Аналогичным образом люди могут обращаться в орган по защите данных в своей стране, даже если обработку их данных осуществляет компания, находящаяся за пределами ЕС. Во всех случаях, когда требуется согласие на обработку данных, четко прописано, что такое согласие необходимо недвусмысленно получить, а не предполагать возможность его получения.

[20] European Commission (2012) Proposal for a regulation of the European parliament and of the Council щn the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Доступно через: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Право «быть забытым» поможет людям более эффективно устранять угрозу защите данных в сети интернет – им будет предоставлена возможность удалять свои данные, если нет законных оснований для их сохранения.

Компании, работающие на рынке ЕС и предлагающие свои услуги гражданам ЕС, будут обязаны при обработке данных за пределами ЕС руководствоваться правилами ЕС.

Независимые национальные органы по защите данных будут усилены, чтобы иметь возможность эффективнее добиваться соблюдения правил ЕС в своих странах. Они будут наделены полномочиями налагать штраф на компании, нарушающие правила ЕС в области защиты данных. Размер штрафных санкций может достигать €1 млн. или 2 % от суммы годового оборота компании.

Саморегулирование и со-регулирование

В отличие от многих других сфер управления специфика возникновения и развития интернета как распределенной, «саморегулирующейся» и «саморазвивающейся» сети не позволяет сводить вопросы упорядочивания соответствующих общественных отношений к формулированию «желательных» управляющих воздействий и их фиксации в виде норм права. Иначе говоря, управление путем принятия неких норм национального законодательства или международных соглашений абсолютно бесперспективно[21]. Поэтому саморегулирование в рамках интернет-бизнеса и различных организаций (в том числе и государственных) является одним из важнейших инструментов в политике защиты персональных данных. Связано это прежде всего с тем, что в ситуации быстрых технологических изменений, неопределённости отношений юрисдикций при трансграничной передаче персональных данных посредством глобальных телекоммуникационных сетей, национальное законодательство в принципе не в состоянии обеспечить надлежащий уровень информационной приватности человека.

Основные формы саморегулирования в сфере защиты персональных данных– это обязательства, кодексы, стандарты, корпоративные правила.

Основные формы саморегулирования – это обязательства, кодексы, стандарты, корпоративные правила.

[21] Курбалийя, Й. (2010)- Управление Интернетом. Доступно через: http://cctld.ru/files/IG-2010.pdf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Мотивации саморегулирования в сфере защиты персональных данных можно суммировать следующим образом. Различные учреждения и институты посредством саморегулирования стремятся:

- избежать законодательных мер;
- предупредить разработку законодательных мер;
- заполнить пробелы в законодательстве;
- более эффективно реализовать нормы законодательства.

Инструменты саморегулирования могут разрабатываться на уровне:

- организации (государственной, частной, общественной, международной, национальной);
- сектора экономики;
- профессионального сообщества (например, для технических специалистов, которые занимаются обработкой информации, технологические кодексы предписывают определённые нормы для разного рода приложений).

Существуют различные пути принятия компаниями, организациями или отраслями мер саморегулирования в области защиты персональных данных:

- информирование об обязательствах;
- введение внутренних руководящих указаний или принципов;
- принятие Кодексов практики или поведения;
- учреждение должности специального ответственного.

Обязательства (commitments) -это краткие констатации минимальных мер по защите персональных данных, обеспечение которых гарантирует та или иная организация (государственная, частная, общественная).

Обязательства – это краткие констатации минимальных мер по защите персональных данных, обеспечение которых гарантирует та или иная организация (государственная, частная, общественная).

Кодексы поведения – важнейший инструмент политики даже в тех странах, где существует достаточно эффективное законодательство, поскольку:

- позволяют организациям публично представить свою политику и обеспечить необходимую прозрачность с персональными данными;
- содействуют правильному применению мер, определённых законодательством;

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Кодексы поведения – важнейший инструмент политики даже при наличии эффективного законодательства, поскольку

позволяют организациям публично представить свою политику и обеспечить необходимую прозрачность с персональными данными;

содействуют правильному применению мер, определённых законодательством;

процедура обсуждения кодексов содействует более глубокому пониманию проблем защиты персональных данных в различных сферах;

достаточно гибкие инструменты и легко могут изменяться с изменением технологических или экономических условий

- процедура обсуждения кодексов содействует более глубокому пониманию проблем защиты персональных данных в различных сферах;
- кодексы – достаточно гибкие инструменты и легко трансформируются с изменением технологических или экономических условий.

Директива ЕС от 24 октября 1995 о защите персональных данных выводит кодексы практики/поведения на международный уровень. В ст. 20 говорится:

«…страны-участницы должны поощрять заинтересованные деловые круги к участию в разработке европейских Кодексов поведения или профессиональной этики в отношении определенных отраслей деятельности на основе принципов, установленных в настоящей Директиве»[22].

В области защиты персональных данных форма, содержание и основная направленность кодексов практики/поведения не являются единообразными.

Анализ, проведенный ОЭСР, показывает, что в основе большинства кодексов лежит принцип «соблюдай или объясни». Пускай они, и содержат некоторые обязательные принципы, большинство рекомендаций по своей сути не носят обязательного характера и позволяют выбрать иной подход; в этом случае компании должны дать надлежащие объяснения[23].

Одним из ключевых элементов любого кодекса практики/поведения должен быть его добровольный характер. Соответственно, любой кодекс не предоставляет никаких законных прав другим сторонам, вовлеченным в процесс обработки, передачи и использования

[22] European Union. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Brussels: European Commission, OJ No. L281.24, October 1995

[23] Ваимерш, Э. (2013) Европейские кодексы корпоративного управления и их эффективность. Доступно через: http://www.oecd.org/daf/ca/2013OECDRussiaCorporateGovernanceRoundtableEuropeanCodesRus.pdf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Если кодекс поведения просто, провозглашает широкие принципы защиты данных, но не предлагает мер для соблюдения этих принципов, то такой кодекс не является средством защиты данных

персональных данных. Например, субъекты данных или лицо, передающее данные, не обретают никаких прав против держателя данных, который создал конкретный кодекс. Однако это не препятствует кодексу быть обязательным для исполнения внутри данной отрасли или корпорации. Например, нарушение отраслевых стандартов, содержащихся в кодексах, может привести к прекращению членства их нарушителя в соответствующей отраслевой или профессиональной ассоциации.

Если кодекс просто провозглашает широкие принципы защиты данных, но затем не предлагает мер для соблюдения этих принципов, то такой кодекс не является средством защиты данных.

Следует отметить, что кодексы поведения/практики являются обычно инструментами частного сектора. Этому способствуют несколько причин:

- регулирование защиты данных государственного сектора обычно осуществляется на основании правил, установленных внутренними инструкциями;
- в большинстве стран защита данных частного сектора остается сравнительно нерегулируемой, что предоставляет отраслям и корпорациям возможности для саморегулирования.

Исторически сложилось так, что многие кодексы ограничиваются рамками отдельных секторов бизнеса. Прежде всего, в банковской и страховой отраслях, поскольку именно здесь собирают огромные количества персональных данных и располагают технологическими возможностями для их обработки. Кроме того, эти отрасли могут быть внутренне взаимосвязаны через корпоративное право собственности и могут иметь интересы в смежных областях бизнеса

(например, службы безопасности торговли), тем самым потенциально способствовать еще большей концентрации данных. В рамках индустрии прямого маркетинга, строящегося на использовании информации о потребителях, создание кодексов практики/поведения также стало общепринятой практикой.

Существуют и межотраслевые кодексы. Национальный компьютерный центр Великобритании разработал ряд кодексов, относящихся к: (1) службам безопасности; (2) компьютерным бюро; (3) данным о наемных служащих; (4) управлению собственностью; (5) информации о потребителях и поставщиках.

Кодексы поведения в отношении защиты персональных данных имеют и международные организации. Свод практических правил Международной Организации Труда (International Laboui Organization- ILO) по защите персональных данных работника был принят на совещании экспертов в 1996 г. Кодекс не имеет обязательной силы, но может быть использован при разработке национального законодательства. В нем изложены основные принципы сбора, обработки, использования и хранения личной информации о работниках, а также о лицах, обращающихся к работодателю в целях трудоустройства. Специальные разделы Свода посвящены личным правам работника, возникающим в связи со сбором персональных данных, в частности, праву на уведомление о сборе персональных данных, на ознакомление в рабочее время со сведениями о себе, которые имеются у работодателя, на получение копий документов, право на доступ к медицинским документам через своего врача-представителя и др. Эти требования могут служить надежным ориентиром при принятии конкретных решений в отношении защиты личных данных работников и содействовать разработке соответствующего национального законодательства.

Как и законодательное регулирование, кодексы поведения имеют свои ограничения. Анализ достоинств и недостатков этой формы саморегулирования, проведенный ОЭСР, остается актуальным и сейчас.

Достоинства саморегулирования:

- кодексы поведения доказали, что они могут быть весьма гибкими инструментами для внедрения закона в конкретные отрасли и сектора экономики;
- релевантные процедуры обладают весьма позитивным воздействием на взаимосвязь палаты с различными отраслями и секторами экономики;
- и те, и другие ведут к улучшенному осознанию и пониманию проблем и вопросов защиты персональных данных, которые являются специфическими для каждой отрасли или сектора экономики;
- кодексы поведения предоставляют определенным отраслям удобную возможность продемонстрировать реальную заботу о вопросах защиты права на невмешательство в частную жизнь;

- отрасли и сектора, подлежащие регулированию кодексом, наделенным правовой санкцией, могут служить примером и посредником для других.

Недостатки саморегулирования:

- регулирование при помощи кодексов может быть ограничено условиями конкуренции и другими аспектами некоего конкретного сектора или отрасли;
- кодексы поведения могут усложнить или запутать правовые рамки, которые применяются в конкретном секторе или отрасли;
- субъекты данных не всегда осведомлены о статусе конкретного кодекса поведения: наделен он правовой санкцией или нет;
- требование адекватных консультаций может создать проблемы с поиском достаточно компетентного партнера;
- практический эффект любого кодекса может зависеть соответственно от сферы его компетенции и статуса, а также иных специфических условий[24].

Стандарты

Стандарты – это не только технические критерии надежности степени защиты персональных данных, но и инструменты реализации политики в этой сфере. Ведь стандартизация, по сути, представляет собой общепринятую процедуру оценки, которая позволяет определить, действительно ли организация делает то, что провозглашает в качестве правил, и включает три компонента:

- установление технических стандартов;
- установление стандартов процедур обработки (менеджмента);
- процедуры оценки влияния тех или иных технологий на защиту персональных данных[25].

Разработкой стандартов в этой сфере, наряду с Международной организацией стандартизации (ISO), занимается Европейский комитет по стандартизации (The Centre Européanne de Normalisations (CEN). Вместе с рабочей группой Article 29 они контролируют выполнение Директивы ЕС 1995 г., устанавливая и контролируя стандарты в трех сферах:

- общий стандарт защиты персональных данных (практические меры, которые организации должны реализовать для выполнения требований Директивы);
- секторальные стандарты (информация в сфере здравоохранения и пр.);

[24] OECD documents. Privacy and data protection: Issues and Challenges", Information Computer Communication Policy. Organization for Economic Cooperation and Development, Paris, 1966, p. 46 -47.

[25] ISO 22307:2008 on Financial Services: Privacy Impact Assessment (ISO 22307:2008 Финансовые услуги. Оценка влияния конфиденциальности); ISO 9564-1:2002, Banking–PIN Management and Security–Part 1: Basic Principles and Requirements for Online PIN Handling in ATM and POS Systems; ISO 18043:2006, Information Technology–Security Techniques–Selection, Deployment and Operations of Intrusion Detection Systems ИСО/МЭК 18043:2006 'Информационные технологии – Методы гарантии безопасности. Доступно через: http://vsegost.com/Catalog/57/5736.shtml

- стандарты для специфических задач (главным образом, в онлайновой среде).

Сертификация

Сертификация (получение сертификатов соответствия стандартам) конкретизирует требования и делает более продуктивной процедуру аудита и проверки на соответствие требованиям[26].

Оценка влияния на защиту персональных данных

Оценка влияния на защиту персональных данных – это, по сути, оценка возможных рисков. Ясные критерии оценки риска для защиты данных при введении тех или иных процедур частными и государственными учреждениями позволяют предупредить возможные нарушения законодательства, а общественности предусмотреть возможные угрозы информационной приватности.

Такая оценка должна осуществляться в соответствии с определёнными правилами и учитывать:

- тип персональных данных, которые подвергаются риску,
- источник, из которого будет получаться информация,
- обстоятельства сбора информации,
- процесс обработки персональных данных,
- предполагаемое использование имеющихся или производимых персональных данных,
- предполагаемых реципиентов и способы использования ими информации,
- обстоятельства, при которых производится информация,
- возможные условия использования и раскрытия информации,
- меры по недопущению неавторизованного доступа, раскрытия, модификации или уничтожения. [27]

[26] Winn, J. (2008) Technical Standards as Data Protection Regulation. Доступно через: http://dx.doi.org/10.2139/ssrn.1118542

[27] Bennett, C. (2001) What government should know about privacy: a foundation paper. Доступно через: http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

Технологии

Заложенная при проектировании защита персональных данных (privacy by design) - это концепция, которая исходит из того, что. защита личной информации, не может быть обеспечена исключительно соблюдением нормативно-правовых актов. Такая защита должна стать «правилом по умолчанию» в работе любой организации

К инструментам политики защиты персональных данных аналитики относят и технологии, обеспечивающие приватность на основе принципа «проектируемой конфиденциальности».

Заложенная при проектировании защита персональных данных (privacy by design) – это концепция, которая исходит из того, что защита личной информации, не может быть обеспечена исключительно соблюдением нормативно-правовых актов. Такая защита должна стать «правилом по умолчанию» в работе любой организации, что означает:

- **Встраивание конфиденциальности в конструкцию системы должно быть активным, а не ограничиваться лишь мерами по устранению последствий.** Личная информация должна быть защищена до того, как система запущена в работу, а не после выявления нарушений конфиденциальности.
- **Конфиденциальность как стандартная установка.** Параметры по умолчанию часто являются определяющими (многие пользователи вообще их никогда не меняют). Поэтому необходимо обеспечить максимальный «автоматизм» в той или иной информационной системе или деловых отношениях. Не требуется никаких действий со стороны индивидуума для защиты личной информации, — система уже изначально содержит в себе необходимые установки.
- **Конфиденциальность как часть структуры**. Защита личной информации должна стать неотъемлемой частью архитектуры любой информационной системы или деловых отношений.
- Полная функциональность с суммарным положительным результатом – **учет всех законных интересов и целей «беспроигрышным» способом, без ненужных компромиссов** (например, укрепление безопасности системы в противовес защите личной информации демонстрирует, что можно обеспечить и то, и другое).
- **Защита личной информации на протяжении всего цикла** ее сбора, хранения, обработки и уничтожения.
- **Доступность и открытость – гарантии того, что система действительно работает в соответствии с заявленными принципами и целями** (это должно быть подтверждено независимой проверкой). Все компоненты и операции остаются

открытыми и доступными, как для пользователей, так и для тех, кто обеспечивает сервис.

- **Соблюдение конфиденциальности пользователей**. Система должна быть ориентирована, в первую очередь, на пользователя: защита личной информации по умолчанию, своевременное уведомление о сборе личной информации, предоставление пользователю свободы выбора в удобной и понятной форме[28].

Наиболее распространённые технологические инструменты, обеспечивающие защиту персональных данных – это шифрование, технологии анонимизации и «псевдонимизации», фильтры.

Технологии, как и другие инструменты политики защиты персональных данных, имеют недостатки. Прежде всего, пользователю иногда бывает сложно узнать или понять, правильно ли работает технология. Можно заметить сигналы нарушения приватности: сомнительные электронные сообщения, появление персональной информации в интернете и пр. Но вряд ли возможно с абсолютной уверенностью утверждать, что с технической точки зрения приватность обеспечена. Более того, даже если ошибки и сбои обнаруживаются и исправляются специалистами, обычно сложно узнать, внесены ли изменения технически корректным способом.

Просвещение

Законы, кодексы, технологический дизайн не в состоянии обеспечить защиту персональных данных, если индивиды не умеют предотвратить вмешательство в цифровую сферу частной жизни. Информирование и образование граждан – важный инструмент в работе регулирующих органов, неправительственных организаций, политических партий. Однако просвещение в сфере защиты персональных данных – это не только обучение технологиям, но и пропаганда социальных норм, ответственного поведения в отношении как своих данных, так и информации о других.

РЕЗЮМЕ

Политика в отношении персональных данных имеет многоуровневый и кросс-секторальный характер. В нее вовлечены наднациональные, национальные и субнациональные (государственные и неправительственные) акторы, как институциональные, так и индивидуальные

В процессе принятия решений, разработки и реализации политики складываются и разные конфигурации интересов акторов. Только серьёзный анализ таких кластеров

[28] Кавукиан, Э. (2011) Privacy by Design 7 основополагающих принципов. Доступно через: http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-russian.pdf

интересов позволяет эффективно решать проблемы защиты прав субъектов данных в конкретных ситуациях. Без учета этого положение будет нестабильным, мозаика несовместимых интересов и ресурсов будет порождать нереализуемые стратегии, каждый инструмент будет использоваться изолированно. Итог – отсутствие единой цели и, следовательно, эффективной политики, основанной на синергии регуляторных воздействий.

Набор инструментов политики в отношении защиты персональных данных включает не только меры законодательного регулирования, но и транснациональные принципы, руководства и соглашения, практики саморегулирования, стандартизации, технологические решения и просветительские мероприятия. Закон должен дополняться кодексами поведения и технологическими мерами, опираться на соответствующую организационную культуру и поддержку общественности.

Управление глобальными рисками информационной приватности требует:

- соблюдения принципов законности, конкретизации целей, минимизации сбора и использования персональных данных, контроля субъекта данных, ответственности распорядителя данных и обеспечения безопасности данных;
- *разработки национальных стратегий* с целью координирования усилий всех акторов на государственном уровне и активизации сотрудничества между уполномоченными органами по защите персональных данных;
- *подотчётности оператора (распорядителя, контролера) данных* независимо от местонахождения данных, а также независимо от того, обрабатываются ли данные самим оператором, его представителями или передаются другому оператору.

В ходе подготовки законодательства о защите персональных данных необходимо проводить его общественное обсуждение, поскольку оно затрагивает гражданские свободы в онлайн-среде. Защита персональных данных должна быть темой кампании по информированию общественности, направленной на совместное обсуждение вопроса гражданами, правозащитными группами, коммерческими компаниями и государственными органами.

Правовая база защиты персональных данных не должна проводить различие между частным и государственным сектором. Граждане просто не поймут такое различие в условиях, когда государственный сектор собирает, сопоставляет, а иногда даже хочет продавать персональные данные.

Исключения со ссылкой на интересы национальной безопасности должны использоваться экономно. Они должны быть именно исключениями, а не правилом. Необходимость защиты национальной безопасности может оправдать особые нормы. Однако не всё, что относится к внешним связям, является вопросом национальной безопасности. Иной подход подрывает легитимность законов, имеющих жизненно важное значение для нашей безопасности.

В ЧЕМ СУТЬ ПРОБЛЕМЫ?

В сфере защиты персональных данных надзора со стороны исполнительной власти недостаточно. Необходим парламентский и судебный контроль.

Правозащитники и гражданские активисты, наряду с представителями государственных органов и бизнеса, могут и должны быть активными участниками диалога о стратегиях, приоритетах и балансе в сфере защиты персональных данных