Регулирование вопросов защиты данных: международная практика

Ольга Исмагилова, Карина Кудакаева

Вопросы регулирования трансграничных потоков данных и обеспечения защиты конфиденциальности данных занимают не последнее место в международной цифровой повестке, а увеличение случаев утечек персональных и других категорий чувствительных данных и/или их использования в социальной инженерии продолжают привлекать интерес экспертов по всему миру. Это доказывает необходимость выработки таких механизмов обработки персональных и других типов данных, которые одновременно обеспечивали бы их надежную защиту и способствовали техническому прогрессу и инновациям (посредством предоставления легитимного доступа к данным для развития таких технологий, как Большие данные, искусственный интеллект и Интернет вещей).

В этой связи ОЭСР принял рекомендации по развитию искусственного интеллекта, поддержанные затем G20 и утвержденные в приложении к «Заявлению Министров торговли и цифровой экономики», 8–9 июня 2019 г. Рекомендации включают необходимость создания открытых баз данных (с привлечением государственных и частных инвестиций) и поощрение создания фондов данных для развития искусственного интеллекта. Одновременно, при формировании новых механизмов рекомендуется обеспечивать защиту персональных данных и соблюдение требований информационной (цифровой) безопасности с тем, чтобы новые технологии не навредили человеку и не создавали угроз его безопасности.

Тенденции последних лет показывают, что все больше стран занимаются регулированием потоков персональных данных путем внедрения либо отдельного закона о защите персональных данных, либо внесения положений о защите персональных данных в соответствующие секторальные законы, например в законы об информационной безопасности, телекоммуникациях, электронной коммерции (см. таблицу ниже). Основные вопросы касаются того, кто будет владеть данными (персональными, государственными и корпоративными) и как обеспечить их безопасный сбор, хранение, обработку и удаление, одновременно обеспечив возможность для их использования при дальнейшей оптимизации всех процессов, сохранив необходимую степень конфиденциальности данных. В 1990-х гг. в мире насчитывалось около 20 стран, регулирующих потоки персональных данных, однако уже к 2015 г. их количество превысило 100. И их количество только растет из года в год.

Подходы стран к регулированию вопросов защиты персональных данных

<table>
<tr><th>Всеобъемлющий подход</th><th colspan="2">Секторальный подход</th><th>Комплексный подход</th></tr>
<tr><td rowspan="2">Отдельный закон о защите персональных данных</td><td colspan="2">Нет отдельного закона о защите персональных данных, положения о защите персональных данных включены в секторальные законы</td><td rowspan="2">Защита персональных данных регулируется как отдельным законом, так и положениями в секторальных законах, а также законами отдельных штатов и/или территорий</td></tr>
<tr><td>Различия по штатам (регионам) при секторальном подходе в целом</td><td>Секторальный подход на всей территории страны</td></tr>
<tr><td>Россия, ЕС[1] («Общий регламент защиты персональных данных» (GDPR)), Израиль, Малайзия, Мексика, Сингапур, Турция, Южная Корея, Япония.</td><td>Индия, Китай (отдельно в Гонконге и на Тайване), ОАЭ (отдельно для свободных экономических зон), США.</td><td>Бразилия, Бруней-Даруссалам, Вьетнам, Индонезия (единый закон обсуждается), Иран, Нигерия, Чили.</td><td>Канада (отдельное регулирование принято в провинциях Альберта, Британская Колумбия и Квебек, наряду с всеобщим законом о защите конфиденциальности данных и электронных документах (PIPEDA), Австралия.</td></tr>
</table>

[1] Подход ЕС является примером для многих стран. При этом, что вопросы локализации данных рассматриваются каждой страной отдельно.

Восемь основных принципов защиты персональных данных, выявленных ЮНКТАД

Открытость	•организации обязаны быть открытыми в отношении порядка сбора и использования персональных данных (ПД)
Ограничения на сбор ПД	•сбор ПД должен быть ограниченным, законным и справедливым, обычно с оповещением и/или с согласия субъекта ПД
Указание цели	•цели сбора и разглашения ПД должны быть четко обозначены в момент сбора ПД
Ограничения по использованию	•использование или раскрытие ПД должно быть ограничено обозначенной целью или тесно связанными целями
Безопасность	•ПД должны быть обеспечены надлежащей степенью защиты
Качество данных	•ПД должны быть актуальными, точными и вовремя обновляться
Ответственность	•операторы обработки ПД обязаны соответствовать принципам обеспечения защиты ПД

Согласно «Индексу ограничительности торговли услугами в секторе телекоммуникаций» ОЭСР, 37 стран применяют более строгое законодательство по сравнению с «Рекомендациями ОЭСР по защите персональных данных и трансграничным потокам персональных данных».

Передача отдельных видов данных (финансовой, медицинской и бухгалтерской информации, а также корпоративных данных), как правило, регулируется отдельными секторальными нормативно-правовыми актами, как в странах с всеобъемлющим, так и в странах с секторальным подходом.

ЮНКТАД определил 8 основных принципов защиты персональных данных, характерных для всех стран (см. рисунок выше).

На международных площадках ведутся активные дискуссии о целесообразности локализации отдельных категорий данных, а также других мер регулирования трансграничных потоков данных в контексте возможных ограничений для бизнеса в цифровую эпоху. Однако в ходе исследования ИМЭФ ВАВТ были выявлены другие аспекты политики защиты персональных данных, которые могут усложнять торговлю компаний в цифровую эпоху:

— Нетранспарентность и разрозненность нормативно-правовой базы. Например, в США нет федерального закона о персональных данных. Данная сфера регулируется рядом отдельных законодательных актов, таких как «О неприкосновенности частной жизни», отдельными законами штатов (в одной только Калифорнии принято около 25 законов в данной области), а также секторальными законами (например, о финансовой и медицинской информации). Помимо этого, отдельные ведомства выпускают руководства для бизнеса, например, «Рекомендации для бизнеса и регуляторов о защите персональных данных потребителей в эпоху быстрых изменений» Комиссии США по торговле.

— Высокая стоимость сертификации компаний о соответствии требованиям законодательства в области защиты персональных данных.

— Высокая стоимость мер обеспечения соответствия законодательству (например, для соответствия GDPR, согласно расчетам Ernst & Young, 500 крупнейших компаний мира должны будут потратить $7,8 млрд).

— Слишком высокие штрафные санкции за несоблюдение мер и отсутствие досудебного порядка разрешения возникших разногласий и споров. Например, Uber согласился выплатить $148 млн штрафа за утечку данных в 2018 г., а в ЕС компании обязали выплатить штрафы, общим объемом в €56 млн (из них €50 млн — Google) за 9 месяцев действия GDPR.

— Отсутствие регулирования или недостаточная степень его проработанности, что создает повышенные риски утечки данных на территории некоторых стран (особенно актуально для наименее развитых стран).

С учетом высокой значимости и необходимости законодательных инициатив в защите персональных и других категорий чувствительных данных, в связи с наличием рисков для национальной и ин-

формационной безопасности, обеспечения прав интеллектуальной собственности, защиты прав потребителей и конкуренции на рынке целесообразно принятие следующих мер для снижения издержек:

— формирование общих принципов защиты данных в зависимости от их категории;

— координация действий для предотвращения утечек данных;

— выработка единых стандартов обеспечения защиты данных и качества соответствующих услуг;

— внедрение мер по снижению стоимости услуг по обеспечению защиты данных;

— продвижение международных инициатив по гармонизации и взаимному признанию законодательства в области защиты персональных и других категорий данных (например, «Конвенция 108 +» Совета Европы или двухсторонние и многосторонние соглашения)[2];

— повышение транспарентности законодательства стран, обмен опытом и практиками.

[2] Подробнее о подобных международных инициативах в Вестнике АТЭС (Выпуск 6, январь 2019 г.) «Цифровая экономика: от общего к частному» (статья «Защита персональных данных в АТЭС: подходы экономик и международные инициативы»).