НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ИНСТИТУТ КОНКУРЕНТНОЙ ПОЛИТИКИ
И РЕГУЛИРОВАНИЯ РЫНКОВ

Муранов,
Черняков
и партнеры

КОЛЛЕГИЯ АДВОКАТОВ
«МУРАНОВ, ЧЕРНЯКОВ И ПАРТНЕРЫ»

Институт конкурентной политики и регулирования рынков
Коллегия адвокатов «Муранов, Черняков и партнеры»

ПЕРСПЕКТИВЫ И ТЕНДЕНЦИИ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Москвитин О.А. – и.о. директора ИКПРР НИУ ВШЭ, партнер КА «Муранов, Черняков и партнеры»
Сапаров Н.Ч. – главный эксперт ИКПРР НИУ ВШЭ
Березгов А.С. – юрист КА «Муранов, Черняков и партнеры»

Москва, 2022

ВСТУПЛЕНИЕ

Институтом конкурентной политики и регулирования рынков НИУ ВШЭ совместно с КА «Муранов, Черняков и партнеры» было проведено исследование механизмов правового регулирования защиты персональных данных в зарубежных юрисдикциях, в ходе которого исследовались следующие аспекты:

- Международные документы в области защиты персональных данных;
- Правовое регулирование защиты персональных данных в разных странах;
- Основные цели и подходы к регулированию защиты ПД в разных юрисдикциях;
- Сравнение строгости регулирования защиты ПД в зарубежных юрисдикциях;
- Принципы и правовые основания обработки персональных данных;
- Установленные ограничения на трансграничную передачу ПД;
- Анализ зарубежной правоприменительной практики в области защиты ПД;
- Меры ответственности за утечку ПД граждан;
- Анализ «достаточности» нормативного регулирования;
- Анализ полномочий надзорных органов, ответственных за контроль над законодательством о защите ПД.

По итогам проведенного исследования был подготовлен «Обзор регулирования защиты персональных данных в зарубежных юрисдикциях», материалы которого легли в основу настоящего доклада.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ПД

Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 **гг.***

- **Необходимо регламентировать порядок государственной защиты персональных данных граждан**
- **Необходимо обеспечить защиту данных от несанкционированной и незаконной трансграничной передачи иностранным организациям**

***утв. Указом Президента РФ от** 09.05.2017 **№** 203
**** см. также «добросовестность» в понимании ПП ВС РФ от** 23.06.2015 **№** 25 «**О применении судами некоторых положений раздела** I **части первой Гражданского кодекса Российской Федерации**»

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ ЗАЩИТЫ ПД

Конституция Российской Федерации

- Служит гарантом неприкосновенности частной жизни, личной и семейной тайн, прав человека

Конвенция

1981 г.*

- Обеспечивает право на неприкосновенность частной жизни в отношении автоматизированной обработки персональных данных

Договор о Евразийском экономическом союзе

- Гарантирует развитие евразийской интеграции в цифровом секторе

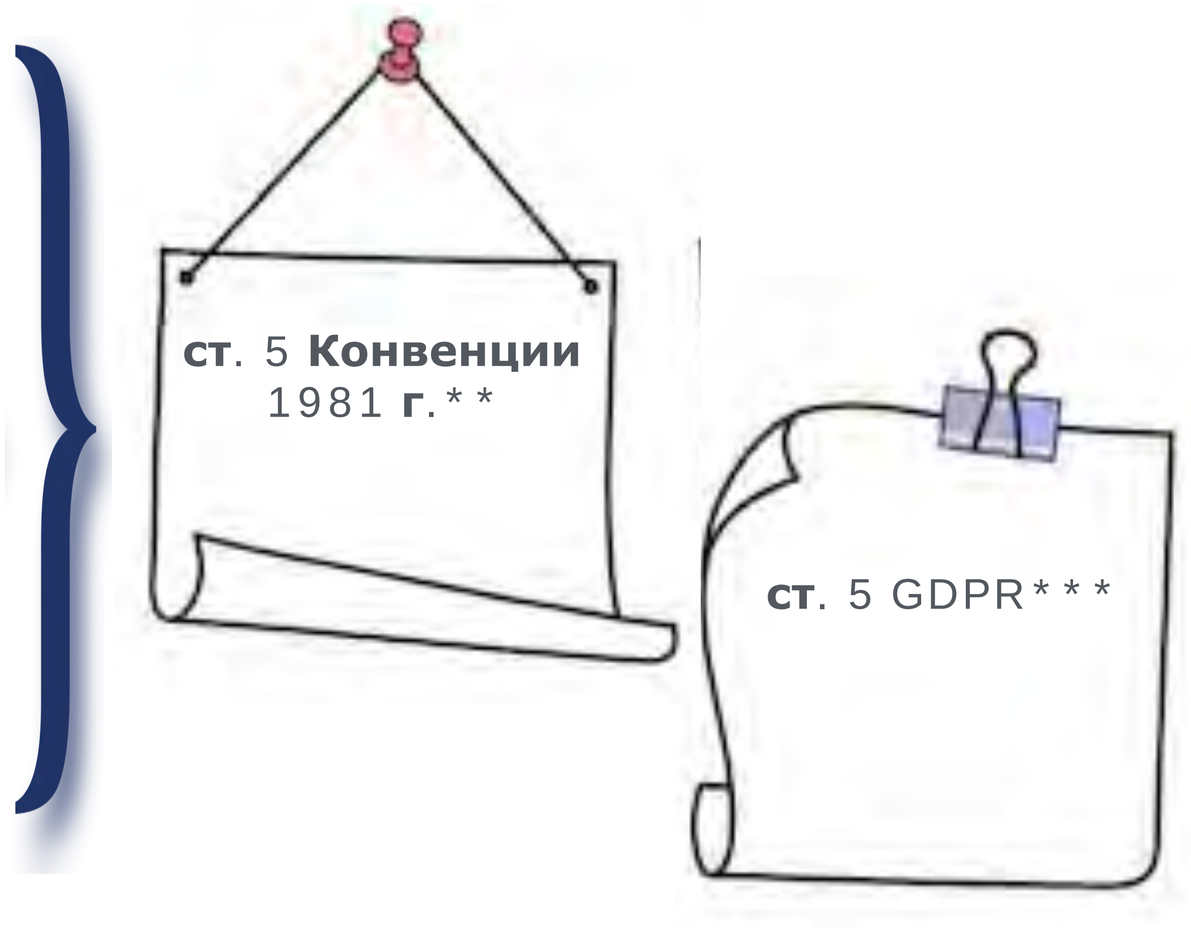
Закон о персональных данных**

- Обеспечивает эффективными механизмами защиты персональные данные граждан

* **Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных** (**заключена в Страсбурге** 28.01.1981)
****Федеральный закон от** 27 **июля** 2006 **г. № 152-ФЗ** «**О персональных данных**»

ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ*:

1. **Законность и справедливость обработки**
2. **Ограничение целью**
3. **Точность**
4. **Минимизация данных**



*ст. 5 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
** Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в Страсбурге 28.01.1981)
*** General Data Protection Regulation, Общий регламент по защите персональных данных

ПОПРАВКИ В ЗАКОН О ПЕРСОНАЛЬНЫХ ДАННЫХ*

- **Уполномоченные органы вправе вмешаться в вопросы обработки персональных данных российских граждан на территории других государств**
- **Регламентируется порядок трансграничной передачи персональных данных**
- **Операторы обязаны обеспечивать непрерывное взаимодействие с ГосСОПКА****
- **Операторы обязаны информировать уполномоченные органы об инцидентах с принадлежащими им базами персональных данных**
- **Операторы обязаны уведомлять уполномоченные органы о намерении осуществлять обработку персональных данных** (за исключением осуществления обработки без использования средств автоматизации)

*предусмотрены Федеральным законом от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»
** Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Институт конкурентной политики и регулирования рынков
Коллегия адвокатов «Муранов, Черняков и партнеры»

ПОПРАВКИ В ЗАКОН О ПЕРСОНАЛЬНЫХ ДАННЫХ*

Согласуются с современным правовым регулированием в зарубежных странах

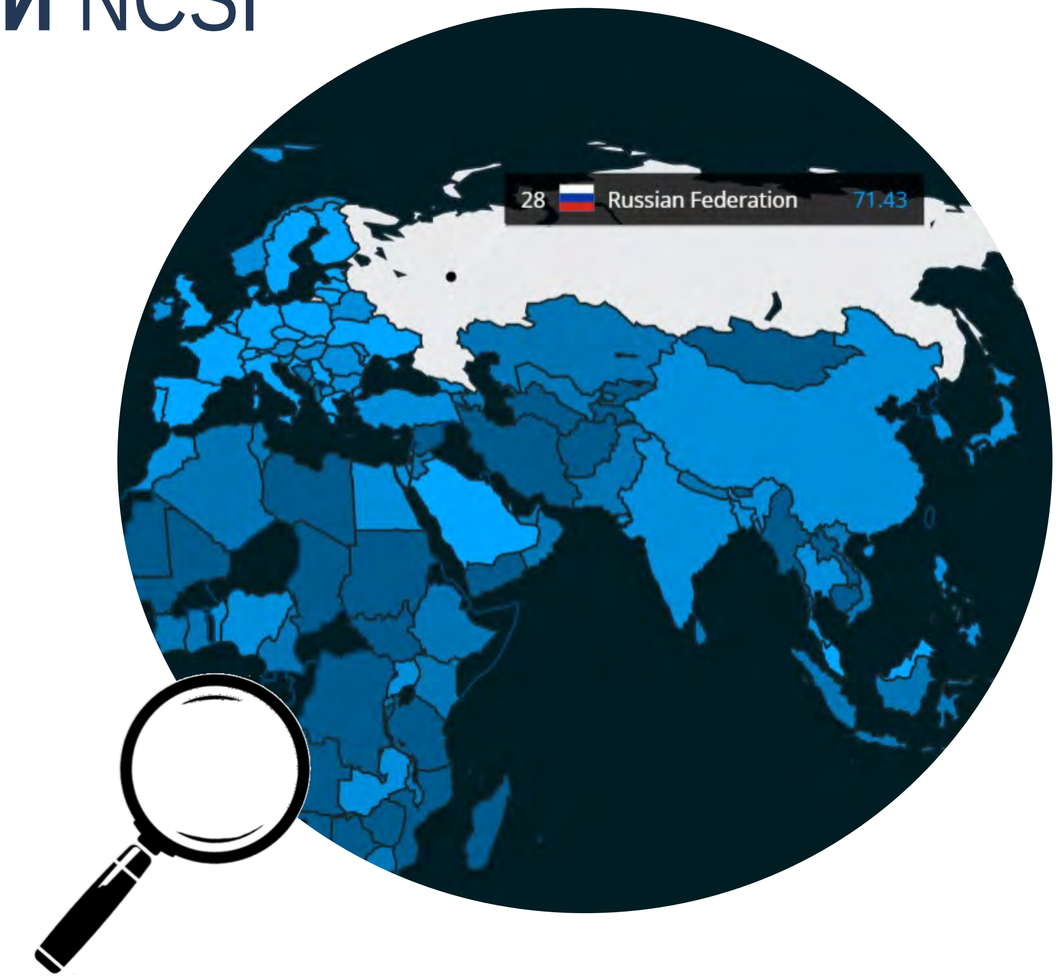
статья 33 GDPR**	• оператор обязан незамедлительно уведомить надзорный орган об утечке персональных данных
статья 56 GDPR	• основы трансграничной обработки персональных данных

*предусмотрены **Федеральным законом от** 14.07.2022 **№** 266-**ФЗ** «**О внесении изменений в Федеральный закон** «**О персональных данных**»
General Data Protection Regulation, **Общий регламент по защите персональных данных

ИНДЕКС КИБЕРБЕЗОПАСНОСТИ NCSI*

Россия занимает 28-**е место из** 160 **государств**

Одной из самых злободневных проблем России в сфере цифровизации остается **массовая утечка персональных данных**



*National Cybersecurity Index // NCSI // URL: https://ncsi.ega.ee/ncsi-index/?order=rank

МАССОВАЯ УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ

С начала 2022 года в России было зафиксировано **около** 60 **крупных утечек персональной информации**.

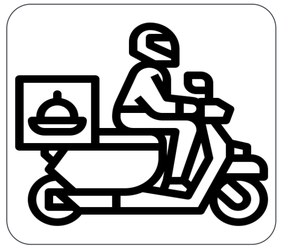
В результате в открытом доступе оказались **более** 230 **млн записей с персональными данными россиян**.

Только за период весна-лето 2022 года произошло **более** 14 **крупных утечек**.

МАССОВАЯ УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ В РФ

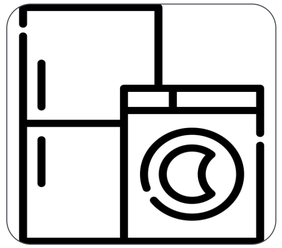
Июль 2022 **г.**

- Логистическая компания сообщила об утечке персональных данных миллионов клиентов
- Известный сервис доставки еды привлекался к ответственности за незаконное распространение персональных данных курьеров сервиса



Август 2022 **г.**

- Известный сервис доставки еды был оштрафован на 60 тыс. руб. за утечку персональных данных клиентов



Октябрь 2022 **г.**

- Ритейлер, управляющий сетью магазинов бытовой техники и электроники, обнаружил утечку персональных данных клиентов и сотрудников сети магазинов бытовой техники и электроники

ОТВЕТСТВЕННОСТЬ ЮРИДИЧЕСКИХ ЛИЦ В СФЕРЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

впервые совершенное правонарушение*	• от 60 тыс. до 100 тыс. рублей (или незначительно выше – в зависимости от вида нарушения)
повторное правонарушение	• от 100 тыс. до 300 тыс. рублей (или незначительно выше – в зависимости от вида нарушения)

Не вполне соответствует принципам справедливости, неотвратимости и целесообразности юридической ответственности.

Способно спровоцировать операторов на пренебрежительное отношение к Закону и дальнейшее совершение правонарушений, не мотивирует к инвестициям в защиту ПД.

*статья 13.11 КоАП РФ

ЗАРУБЕЖНАЯ ПРАКТИКА

Ирландская комиссия по защите данных (DPC) оштрафовала американскую компанию Twitter на 450 **тыс**. **евро** в связи с недостаточно быстрым раскрытием информации об утечке данных

- На протяжении более четырех лет система безопасности Twitter позволяла получать доступ к закрытым сообщениям некоторых пользователей

- В соответствии с GDPR организация должна была уведомить регулятора об утечке данных в течение 72 часов после ее обнаружения

ЗАРУБЕЖНАЯ ПРАКТИКА

- Управлением комиссара по информации Великобритании (ICO) был наложен штраф в размере 204,6 **млн евро** на British Airways за утечку 420 тысяч записей персональных данных её пассажиров и работников
- Инцидент произошел из-за слабой системы защиты информации, на которую была совершена хакерская атака.

- Сингапурская Комиссия по защите персональных данных (PDPC) оштрафовала медицинского ИТ-провайдера Integrated Health Information Systems (IHiS) и группу клиник SingHealth в общей сложности **на** 1 **млн местных долларов** (**около** $740 **тыс**.) за уязвимость в защите персональных данных пациентов.
- В результате кибератаки из сети SingHealth была похищена личная информация более 1,5 млн пациентов.

ЗАРУБЕЖНАЯ ПРАКТИКА

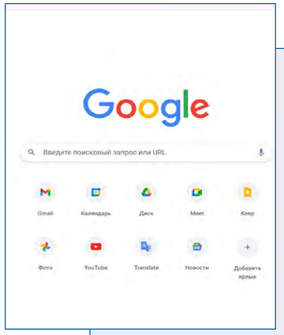
Во многих странах санкции в области утечки персональных данных являются более жесткими по сравнению с российскими за аналогичные правонарушения:

На $22,6 **млн**

Оштрафовали в Великобритании компанию распознавания лиц Clearview AI

$124 **млн**

Размер штрафа, назначенный бренду отелей и курортов Marriot за утечку данных



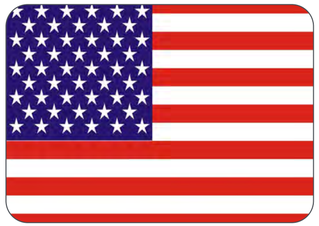
На 50 **млн евро**

оштрафован Google во Франции по максимально допустимому уровню наказания в соответствии с нормами GDPR

МЕРЫ ОТВЕТСТВЕННОСТИ ЗА УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН В ЗАРУБЕЖНЫХ ЮРИСДИКЦИЯХ

Великобритания	• административная ответственность: штраф в размере 500 тыс. фунтов; • уголовная ответственность: лишение свободы при преднамеренном характере нарушений, которые привели к серьезным последствиям;
Япония	• гражданская ответственность: деликт; • уголовная ответственность: ответственность за нарушение права на неприкосновенность частной жизни; • закон о защите персональных данных: лишение свободы сроком на 6 месяцев или штрафа в размере не более чем 300 тыс. иен.
Китай	• закон о защите персональных данных: штраф на сумму более 50 млн юаней (7,74 млн долларов США) или до 5% годового оборота компании.
Сингапур	Штраф в размере до 5000 долларов США или лишение свободы на срок до 2 лет за: • несанкционированное раскрытие персональных данных; • ненадлежащее использование персональных данных; • несанкционированная повторная идентификация анонимной информации.

СРАВНЕНИЕ РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАРУБЕЖНЫХ ЮРИСДИКЦИЯХ



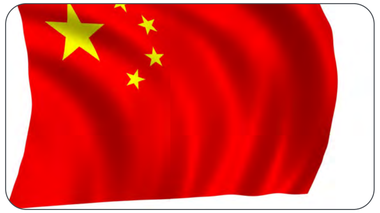
США

- Нет федерального закона, специально касающегося персональных данных. Действуют два нормативных акта, определяющие обязанности государственных органов в сфере работы с персональными данными;
- Обеспечение защиты данных в отдельных областях базируется на федеральном, отраслевом законодательстве, рекомендациях по защите информации.

Великобритания

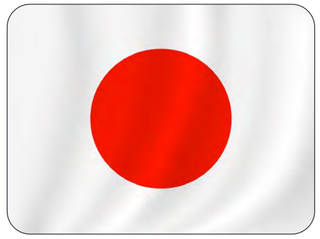
- Систематизация регулирования;
- Широта полномочий контрольно-надзорных органов в сфере информации и жесткость санкций за нарушения законодательства о персональных данных;
- Контрольно-надзорные органы в сфере защиты информации в Великобритании обладают значимым авторитетом в вопросах регулирования обработки персональных данных;
- Компании обязаны проработать внутреннюю систему обеспечения безопасности обработки информации, в том числе персональных данных.

СРАВНЕНИЕ РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАРУБЕЖНЫХ ЮРИСДИКЦИЯХ



Китай

- Систематизация регулирования;
- Создание в компаниях независимых надзорных органов для обеспечения управления пользовательской информацией в соответствии с законом;
- Схоже с законодательством Великобритании в указанной области;
- Регулирование в большей степени ориентировано на юридических лиц, которые обладают базой данных и осуществляют обработку персональных данных.



Япония

- Санкции за нарушение законодательства о защите персональных данных являются более жесткими;
- Регулирование относится преимущественно к организациям, обладающим базами данных, работающим с персональными данными и персональной информацией;
- Закон о защите персональных данных Японии не применяется к государственным органам, учреждениям, администрациям.

СРАВНЕНИЕ РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАРУБЕЖНЫХ ЮРИСДИКЦИЯХ

Израиль

- Наличие базового закона, а также отдельные НПА;
- Использование персональных данных основывается на базовом требовании – необходимости получения согласия субъекта персональных данных;
- Обязательная регистрация базы данных;
- Риск-ориентированный подход при установлении требований к безопасности информации, содержащейся в базах данных.

Бразилия

- Общий закон о защите данных (LGPD) представляет собой шаг вперед в области безопасности персональных данных, устанавливая высокие стандарты защиты информации;
- Использование персональных данных основывается на базовом требовании – необходимости получения согласия субъекта персональных данных;
- Обязательное наличие в организации сотрудника по защите данных.

АНАЛИЗ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ

Бразилия	• Общий закон о защите данных (Lei Geral de Proteção de Dados, LGPD); • Закон охватывает, среди прочего, права субъектов данных, обязанности агентов по обработке данных и сотрудников по защите данных, параметры информационной безопасности, требования к международной передаче личных данных, а также регламенты работы Национального управление по защите данных.
Израиль	• Закон о защите конфиденциальности 5741-1981 (Protection of Privacy Law, 5741 – 1981, PoPL и иные НПА; • Регулирует сбор, использование и распространение персональных данных, хранящихся в электронных базах данных на территории Израиля; • Устанавливает стандарты и требования к безопасности для определенных типов персональных данных, включая кредитную историю, медицинские записи и биометрические данные.
Япония	• Закон о защите персональных данных (APPI) и иные НПА; • Законодательство о защите персональных данных применимо к любым лицам, обрабатывающим персональную информацию (физические лица, юридические лица, индивидуальные предприниматели, государственные органы, иные организации).

АНАЛИЗ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ

Китай

- Закон о защите личной информации 2021 г. (Personal Information Protection Law of the People's Republic of China, PIPL);
- Правовое регулирование защиты персональных данных в Китае не отличается принципиально от подходов, например, Великобритании;
- Основывается на положениях Европейского регламента о защите персональных данных.

Великобритания

- Закон о защите данных (Data Protection Act 2018);
- Основывается в большей степени на наднациональном законодательстве в сфере защиты персональных данных, чем на внутригосударственных положениях;
- С 2021 г. разрабатывает собственный механизм трансграничной передачи данных между Королевством и другими странами, включая механизм признания адекватности (Standard Contractual Clauses), а также механизм, обеспечивающий обмен данными с США.

СИСТЕМА НАДЗОРНЫХ ОРГАНОВ

Австралия

- Австралийское управление связи и средств массовой информации (Australian Communications and Media Authority, ACMA);
- Группа реагирования на чрезвычайные ситуации в кибербезопасности (Australian Computer Emergency Response Team, AusCERT).

Великобритания

- Департамент цифровых технологий, культуры, средств массовой информации и спорта (Department for digital, culture, media & sport);
- Комиссар Великобритании по информации;
- Международный Экспертный Совет (далее – IDTEC) по трансграничной передаче данных (International Data Transfers Expert Council).

СИСТЕМА НАДЗОРНЫХ ОРГАНОВ

Бразилия

- Национальное управление по защите данных (ANPD) - является независимой организацией, способной самостоятельно рассматривать и разрешать вопросы защиты персональных данных и конфиденциальности.

Европейский Союз

- Европейский Совет по защите данных (контрольная, исполнительная, консультативная функции, функции по координации и взаимодействию);
- Европейский Уполномоченный по защите данных (информационная, консультативная, организационная, охранительная и контрольная функции);
- Национальные надзорные органы (информационной, охранительной, исполнительной, контрольной функции, функции по координации и взаимодействию).

ЗАКОНОПРОЕКТ ОБ ОБОРОТНЫХ ШТРАФАХ ЗА УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ*

Предлагаются следующие поправки:

- ввести определение «объект утечки персональных данных», а также критерии, по которым будет устанавливаться вина конкретной организации;
- установить соразмерность штрафов за утечки объемам и критичности персональных данных, появившихся в незаконном обороте;
- ввести дифференцированные штрафы:
  - за первую утечку штраф будет фиксированным (в зависимости от объема данных, утечку которых допустила компания),
  - в случае повторной утечки будет применяться оборотный штраф с четко установленными границами.

*__Минцифры готовит новую версию законопроекта об оборотных штрафах за утечку персональных данных__ // URL: https://t.me/mintsifry/1296.

ИНЫЕ АКТУАЛЬНЫЕ И ДЕЙСТВЕННЫЕ МЕРЫ ПРОТИВ УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Активная пропаганда и поддержка со стороны государства по внедрению корпоративных систем комплаенса в сфере персональных данных, как это делается в антимонопольной сфере и (или) сфере противодействия коррупции.

- Дополнительным механизмом защиты может быть и периодический добровольный независимый аудит соблюдения законодательства и мер по защите персональных данных со стороны независимых аудиторов, экспертов.

- Страхование ответственности с выплатами пострадавшим.

НЕЗАКОННОЕ РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ С ЦЕЛЬЮ ПОЛУЧЕНИЯ ПРИБЫЛИ

статья 137 **УК РФ** (**нарушение неприкосновенности частной жизни**)

Пример:

Сотрудница салона связи была признана виновной в незаконном сборе и распространении сведений о частной жизни лица, составляющих его личную тайну, без его согласия, с использованием служебного положения.

Нарушение выразилось в передаче неустановленному лицу за вознаграждение персональных данных клиентов салона связи, в том числе фамилии, имени, отчества, даты рождения, паспортных данных, семейного положения через один из мессенджеров.

Обвиняемой был назначен штраф в размере 110 тыс. руб.

ПРИМЕЧАНИЕ: **В настоящее время обсуждаются идеи введения уголовной ответственности за реализацию и приобретение ПД**.

Спасибо за внимание!

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ИНСТИТУТ КОНКУРЕНТНОЙ ПОЛИТИКИ И РЕГУЛИРОВАНИЯ РЫНКОВ

КОЛЛЕГИЯ АДВОКАТОВ «МУРАНОВ, ЧЕРНЯКОВ И ПАРТНЕРЫ»

icpmr.hse.ru Телефон: +7 (495) 772-95-90

Адрес: г. Москва, Покровский б-р, д. 11, каб. М205