



# Персональные данные – информация на вес золота

Каждый день новостные ленты не обходятся без сообщений о пострадавших от кибермошенников. Ущерб, нанесенный преступниками из сети, исчисляется миллионами тенге. С каждым годом их способы обмана становятся все изощреннее. Они придумывают новые схемы, с помощью которых выманивают у простых граждан конфиденциальную информацию, что позволяет взламывать их счета. Таков сценарий и в фильме «На линии», снятом корейскими кинопроизводителями в прошлом году. Просмотр фильма, а также ежедневные новостные сводки порождают массу вопросов: как защитить свои данные, как обезопасить себя в информационном пространстве? И сегодня на эти и ряд других вопросов отвечает докторант PhD, заместитель директора Высшей школы права КазГЮУ имени М.С. Нарикбаева, директор филиала Digital Rights Center Qazaqstan в Нур-Султане Дана Мухамеджанова.

**– Дана, вы являетесь разработчиком учебной дисциплины: «Международные стандарты защиты частной жизни и персональных данных». Что подразумевает под «персональными данными» и почему и от кого их необходимо защищать?**

– Да, часто возникают вопросы о том, что такое персональные данные и что такое частная жизнь, каковы их отличия? Замечу, что частная жизнь носит более широкий характер: это информация о личной, интимной жизни, взаимоотношения с окружающим миром, близкими, родными, коллегами. А также позиционирование себя в социальных сетях, включающее круг друзей, изображения, политические взгляды, сексуальную ориентацию, семейные отношения, взаимоотношения детей и родителей и другое. Если говорить о персональных данных, то это информация, которая идентифицирует субъект, через которую мы можем уточнить, фамилию, имя и отчество, номер телефона, адрес проживания, адрес электронной почты, IP-адрес, а также ИИН, удостоверение личности, паспортные данные. Также есть еще одна категория информации, более чувствительная, это биометрические данные, индивидуальные у каждого субъекта. К ним относятся отпечатки пальцев, радужная оболочка глаз, овал лица, в целом биологические признаки.

Как мы видим, информация, как на бумажных, так и на электронных носителях весьма обширная. Тот же eGov, те же банки, у которых содержится информация о персональных накоплениях, налоговых отчислениях содержат массивный объем персональной информации.

Что касается защиты персональных данных, то очень часто возникают случаи в судебной практике, когда незаконно используется изображение лица. Здесь необходимо отметить, что изображение лица подлежит описанию в статье 145 Гражданского кодекса РК «Право на собственное изображение», в кото-

глобальные угрозы были со стороны Генеральной прокуратуры РК, Центральной избирательной комиссии, eGov, когда персональные данные 18 миллионов пользователей оказались в широком доступе. Об этом стало известно после доклада, обнародованного Центром анализа и расследования кибератак (ЦАРКА). Причиной утечки информации стали низкий уровень защищенности и уязвимость системы. К слову, сами органы, которые несут прямую ответственность за защиту персональных данных, заявили, что не знают, каким образом произошла утечка, закончилось увольнением некоторых сотрудников. На запрос от ЦАРКА в МВД о привлечении к ответственности, пришел

несмотря на то, что это региональный документ, он носит обширный характер. В нем четко прописаны обязательства по соблюдению приватности для всех: для государства, корпоративного сектора, представителей бизнеса, частных лиц... К тому же General Data Protection Regulation GDPR имеет трансграничный эффект, таким образом может повлиять и на Казахстан. Если, к примеру, нарушен процесс обработки персональных данных гражданина Европейского Союза, мы можем получить предписание, а в последующем – штраф. Причем не в тенге, а в евро, и довольно значительный. Ярким примером является предъявление коллективного иска жителей штата Иллинойс

**“ Отдельного внимания заслуживает кадровый вопрос в сфере IT. Ведь прежде чем требовать качественной защиты информации, необходимо обеспечить эту сферу высококвалифицированными специалистами ”**

ответ, что за отсутствием уголовного состава принять какие-либо меры невозможно. А если сравнивать с практикой развитых государств в части защиты персональных данных, то за действия, связанные с их утечкой, нарушениями информационной безопасности, есть уголовная ответственность. Часто слышим такое высказывание, что персональные данные – это современная нефть, поэтому необходимо защищать персональную информацию более строгими мерами и штрафными General Data Protection санкциями.

**– Когда весь мир переходит в цифровую плоскость, и не составляет никакого труда отыскать человека в соцсетях или узнать какую-либо информацию о нем, можно ли вообще говорить об информационной приватности и конфиденциальности?**

в федеральный суд США Северного округа штата Иллинойс двум американским компаниям, в сумме штрафа 6,8 миллиона долларов о незаконном сборе биометрических данных при покупке в торговых автоматах. Данные торговые автоматы хранили отпечатки пальцев покупателей без получения согласия и надлежащего информирования. Вторым известным случаем в Иллинойсе был иск к компании Facebook в сумме 650 миллионов долларов за использование функции распознавания лиц и отметки на изображениях лиц без уведомления пользователей, а также за сбор и хранение биометрических данных пользователей. Данные примеры нечистоплотной практики использования особо чувствительных данных являются основанием для сравнения со штрафными санкциями, применимыми в Казахстане, которые не особо дорого обойдутся для высокотехнологичных компаний.



Закон «О регулировании цифровых технологий».

Отдельного внимания заслуживает кадровый вопрос в сфере IT. Ведь прежде чем требовать качественной защиты информации, необходимо обеспечить эту сферу высококвалифицированными специалистами.

К слову, Министерство цифрового развития, инноваций и аэрокосмической промышленности объявило тендер по разработке цифрового кодекса. Планируется, что один нормативный документ – Цифровой кодекс – будет регулировать общественные отношения с использованием прорывных digital-технологий, такие как цифровые активы, AI, блокчейн, роботы и масштабную обработку данных, порядок функционирования цифровых платформ и экосистем, Big Data, а также закрепил цифровые права граждан страны.

**– С какого времени этот вопрос поднимается в Казахстане и каковы достижения на сегодня?**

– В Казахстане в этом направлении небольшие шаги были предприняты в 2013 году, когда был принят Закон «О защите персональных данных». В ряде стран СНГ к тому времени такого закона не было. К примеру, в Беларуси он появился буквально год-два назад. Следующий шаг, более масштабный и продуктивный, был предпринят в 2020 году. В это время пошли первые предпосылки, были обсуждения в экспертной среде о том, что необходимо создать отдельный институт по защите пер-

работать. Яркое тому свидетельство – утечки данных в Uber, Яндекс.Еда. Поэтому с 2018 года работа по усилению защиты персональных данных активизировалась. В каждой организации была разработана политика конфиденциальности, положение по сбору и обработке персональных данных.

В нашей же стране эти процессы пока не контролируются и находятся на уровне рекламной деятельности, то есть вам звонят и предлагают прийти на салонные процедуры или приобрести товары по низким ценам. Поэтому здесь нужно говорить о кибергиgiene и правовой грамотности населения.

**– Дана, и пару слов расскажите о курсах, проводимых в Центре цифровых прав.**

– Центр цифровых прав был открыт в январе этого года в Алматы и в столице. С 15 августа Digital Rights Center Qazaqstan в Нур-Султане совместно с КазГЮУ имени М.С. Нарикбаева проводит 10-дневные курсы в первой в истории Казахстана Школе киберправа. В школе будут рассмотрены актуальные практические кейсы, вопросы регулирования в цифровой среде согласно законодательству Казахстана и международному праву, сформированы навыки работы с правовыми отношениями, складывающимися в киберпространстве. Школа ориентирована на специалистов в области информационной безопасности, юристов, и будет включать в себя вопросы интеллектуальной собственности, защиты персональных данных

**“ Персональные данные – это современная нефть, поэтому необходимо защищать персональную информацию более строгими мерами и штрафными General Data Protection санкциями ”**

сональных данных. И результатом проведенных работ стало Агентство по защите персональных данных при Министерстве цифрового развития, инноваций и аэрокосмической промышленности Казахстана. Новому ведомству были переданы полномочия Генеральной прокуратуры.

**– После просмотра упомянутого корейского фильма «На линии» начинаешь понимать, насколько человек уязвим и беззащитен перед современными технологиями. Какие есть способы обезопасить себя в информационном пространстве?**

– Конечно, нужно усиливать законодательство, формы ответственности. На мой взгляд, нынешние штрафы, санкции не отвечают современным критериям. Причем, понимая, что любая информационная система уязвима, будь то государственный орган или частная организация, их сотрудники знают, что нарушения повлекут за собой максимум увольнения, а как минимум, штрафы, которые можно погасить и дальше

и многое другое. Отмечу, что сегодня недостаточно быть дипломированным специалистом только в сфере IT, требуется и знание правовых основ. Таковы и требования современного рынка труда: в равной степени владение IT навыками и юридическими знаниями.

Учитывая реалии современного общества, КазГЮУ постоянно мониторит изменения на рынке труда, изучает потребность в квалифицированных кадрах, тем самым регулярно совершенствует образовательные программы. К примеру, были введены ряд новых дисциплин, связанных с кибербезопасностью, computer science, digital system and network, IT and business, а также в прошлом учебном году была апробирована магистерская программа Право IT совместно с компанией EY Kazakhstan.

**Гулжанат ЖУБАНИЯЗОВА, фото из личного архива Д. Мухамеджановой и открытых источников**



рой указано, что относится к изображению лица, когда можно использовать, фотографировать. Судебная практика сформировалась так, что больше всего исков подавалось в отношении публичных лиц, это фотографирование в общественных местах, без его согласия или разрешения. Вторая часть связана с контактными телефонами: постоянный обзвон мошенников, онлайн-мошенники, фишинг.

Как мы видим, видов преступлений очень много, но с эпизодами с использованием персональных данных мы сталкиваемся в нескольких случаях. Первый – это утечки, самые

– Да, понятие приватности больше используется за рубежом – «privacy». Политика конфиденциальности используется при входе на сайты, использовании приложений, социальных сетей. Это говорит о том, что при использовании любого приложения будет гарантирована сохранность данных, а при их утечке – предприняты соответствующие меры. И говоря о передовом опыте в этой сфере я всегда в качестве примера привожу General Data Protection Regulation GDPR, который был принят в 2018 году и является своего рода золотым стандартом по защите персональных данных в Европе.

**– Какова международная практика и применяется ли она в нашей стране?**

– В 2018 году в нашей стране была принята концепция «Киберщит Казахстана», направленная на защиту электронных информационных ресурсов, информационными систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз. Документ основывался на политике кибербезопасности Сингапура, Австрии, Великобритании и других стран, находящихся на передовой в борьбе с киберпреступностью. Далее в 2020 году был принят