

Как защитить свои персональные данные в интернете ?



Сегодня защита персональных данных в интернете стала актуальным вопросом для многих россиян. Различные виды сведений о физических передаются, обрабатываются и накапливаются государственными органами и частными компаниями. При этом наиболее нежелательным сценарием для любого гражданина является утечка персональных данных в сеть и их попадание к злоумышленникам. Рассмотрим подробнее, что такое персональные данные и как их уберечь от незаконного использования.

Что включают в себя персональные данные?

Если кратко, то к данному виду информации относят любые виды личных сведений, которые могут быть прямо соотнесены с конкретным физическим лицом и содержат определенную информацию, характеризующую это физическое лицо. Условно можно выделить следующие виды персональных данных:

- Реквизиты физического лица: ФИО, номер паспорта, дата рождения, адрес регистрации и прочие данные, позволяющие идентифицировать человека.
 - Сведения о материальном положении человека, трудоустройстве и достатке. Сюда относится уровень доходов, подробные данные о трудоустройстве (сведения из трудовой книжки) и т.п.
 - Данные об имуществе, включая недвижимость и другие виды имущества, проходящего государственную регистрацию (автомобили, доли в ООО, ценные бумаги и т.п.).
 - Медицинская информация, сведения о перенесенных и текущих заболеваниях (сведения из медицинской карточки).
 - Специфические сведения о физическом лице: информация о его интимной жизни, вовлеченности в религиозные организации и т.п.
 - Биометрические личные данные: сканы отпечатков пальцев, анализ ДНК и т.п.
- Большинство из этой информации достаточно часто передается нами добровольно, поэтому обезопасить себя от утечки бывает сложно.

Как передаются персональные данные?

По законодательству РФ процессинг персональных данных может осуществляться только с согласия физического лица, которого эти данные касаются. Существует три основных канала передачи:

- Заполнение различных анкет. Когда человек заполняет сведения о себе и передает представителям некой компании, он соглашается на обработку своих данных.
 - Добровольное сообщение сведений о себе в Интернете. Например, это могут быть сведения в социальных сетях и других ресурсах, где человек может добровольно опубликовать данные, которые подходят под определение персональных.
 - Сбор информации о пользователях на основе косвенных признаков. К примеру, сайт может отслеживать сферу интересов пользователя и анализировать ее.
- По этим каналам данные от физического лица передаются агрегаторам, которые потом уже могут распоряжаться этими данными по своему усмотрению, однако с соблюдением положений 152-ФЗ от 27.07.2006.

Как пользователю сохранить свои данные от утечек и слежки?

Чтобы не допустить неконтролируемое распространение сведений о себе третьим лицам в первую очередь нужно следить за тем, какие данные вы сами добровольно отдаете. Подобные проблемы гораздо проще предупредить, чем потом решать. Старайтесь сообщать сведения о себе только проверенным операторам с хорошей репутацией. Кроме того, не стоит в открытых ресурсах вроде социальных сетей публиковать информацию, которая может быть чувствительной к утечке.

Однако если вы обнаружили факт незаконного распространения ваших личных данных в Интернете, злоумышленников можно привлечь к ответственности. Для этого нужно запросить у нотариуса обеспечение доказательств в Интернете и преследовать нарушителя ваших прав по закону, вплоть до обращения в суд.