Отговорност на доставчиците на услуги на информационното общество

Изготвил: Пенка Куршумова

Учител по КМИТ и информатика

Въведение

В днешния дигитален свят интернет и информационните технологии играят централна роля в нашия живот. От платформите за социални медии до онлайн магазините, доставчиците на услуги на информационното общество предлагат разнообразие от услуги, които използваме всеки ден. Но какви са техните отговорности и как те влияят на нашата безопасност и права?В този урок ще разгледаме какво представляват тези доставчици, какви са техните отговорности и как можем да се защитим, когато използваме техните услуги.

1. Какво представляват доставчиците на услуги на информационното общество?

Доставчиците на услуги на информационното общество са компании или физически лица, които предоставят услуги чрез интернет. Това може да включва:

- **Интернет доставчици**: Компании, които предоставят достъп до интернет.
- **Социални мрежи**: Платформи като Facebook, Instagram и Twitter.
- **Онлайн магазини**: Сайтове като Amazon и eBay.
- **Платформи за споделяне на съдържание**: YouTube, TikTok.
- **Услуги за хостинг на уебсайтове (**GoDaddy, Bluehost)
- **Имейл услуги** (Gmail, Yahoo Mail) и други

2. Отговорност на доставчиците.

Отговорността на тези доставчици е регулирана от различни закони и регламенти, като например директива за електронната търговия и новия Регламент за цифровите услуги (DSA).

2.1 Правна отговорност

- Защитаване на личните данни: Доставчиците са задължени да защитават личните данни на потребителите. Например, платформи като Facebook трябва да спазват Общия регламент за защита на данните (GDPR) в Европейския съюз.
- Премахване на незаконно съдържание: Ако в платформата се разпространяват незаконни материали, доставчиците трябва да действат бързо за тяхното премахване.

Пример: YouTube премахва видеа, които нарушават авторските права.

Контрол на личните данни на Facebook

Ситуация: Представете си, че използвате Facebook и искате да управлявате каква информация се събира за вас и как тя се използва. Под GDPR, Facebook е задължен да предостави на потребителите повече контрол върху техните лични данни.

Как Facebook спазва GDPR:

1**. Настройки за конфиденциалност и контрол върху данните**

Facebook предоставя на потребителите инструменти за управление на техните данни чрез раздела „Настройки на конфиденциалност“. Тук можете да видите и променяте кой има достъп до вашата информация. Например, можете да решите да ограничите видимостта на публикациите си само до определени хора или да спрете споделянето на информация с трети лица.

2. Права на достъп и корекция на данните

Под GDPR имате право да поискате достъп до информацията, която Facebook е събрала за вас, както и да поискате корекции или изтриване на данните, ако те са неточни или не са необходими. Facebook предоставя опцията „Изтегли информацията си“, която ви позволява да получите копие на всички данни, които платформата събира за вас.

3. Процедура за изтриване на данни

Ако решите да изтриете акаунта си, Facebook трябва да се увери, че вашите данни са изтрити, освен ако не съществуват законови задължения за тяхното съхраняване. Това е част от правото ви на изтриване (или правото да бъдете забравени) по GDPR.

4. Уведомяване за нарушения на сигурността

В случай на нарушение на сигурността на данните, Facebook е задължен да уведомява съответния надзорен орган и, при необходимост, самите потребители, за да могат те да предприемат съответни действия за защита на собствената си информация.

Тези мерки са част от усилията на Facebook да спази GDPR и да осигури, че личните данни на потребителите са защитени и управлявани по начин, който съответства на законодателството

2.2 Етична отговорност

- Предотвратяване на вредно съдържание: Платформи като Instagram работят върху алгоритми за разпознаване на съдържание, което може да бъде вредно или обидно, като например насилие или омраза.
- Прозрачност и честност: Доставчиците трябва да бъдат прозрачни относно как събират и използват данните на потребителите. Пример: Google предоставя информация на потребителите за използването на техните данни чрез панела за активност на акаунта.

Пример за премахване на незаконно съдържание

Ситуация: Потребител публикува в социалната мрежа Facebook пост, който съдържа реч на омразата и подбужда към насилие срещу определена група хора.

Действия на доставчика:
Уведомление за нарушението: Друг потребител или организация уведомява Facebook за поста, като подава жалба чрез системата за докладване на съдържание.

Проверка на жалбата: Facebook проверява съдържанието на поста и установява, че той нарушава правилата на платформата и законите за реч на омразата.

Премахване на съдържанието: Facebook премахва поста или блокира достъпа до него, за да предотврати разпространението на незаконното съдържание.

Резултат: Facebook изпълнява своите задължения, като премахва незаконното съдържание след получаване на уведомлението. Това помага за поддържането на безопасна и законна онлайн среда.

Този пример илюстрира как доставчиците на услуги на информационното общество трябва да реагират на уведомления за незаконно съдържание и да предприемат действия за неговото премахване или блокиране.

Пример за прозрачност и отговорност

Ситуация: Онлайн платформа за споделяне на съдържание, като YouTube, иска да гарантира, че потребителите разбират как се справя с незаконното съдържание и какви са нейните политики и процедури.

Действия на доставчика:

Публикуване на политики: YouTube публикува на своя уебсайт подробни политики и насоки за съдържанието, което е позволено и забранено на платформата. Тези политики включват информация за това какво се счита за незаконно съдържание, като например реч на омразата, нарушаване на авторски права и насилие.

Процедури за докладване: YouTube предоставя ясни инструкции за това как потребителите могат да докладват съдържание, което смятат за незаконно. Това включва лесни за използване форми за подаване на жалби и информация за процеса на разглеждане на жалбите.

Отчетност и прозрачност: YouTube публикува редовни отчети за прозрачност, в които предоставя статистика за броя на получените жалби, предприетите действия и резултатите от тях. Тези отчети помагат на потребителите да разберат как платформата се справя с незаконното съдържание и какви мерки предприема за поддържане на безопасна онлайн среда.

Резултат: YouTube демонстрира прозрачност и отговорност, като предоставя ясна информация за своите политики и процедури, както и редовни отчети за своите действия. Това помага на потребителите да се чувстват уверени, че платформата се грижи за тяхната безопасност и спазва законите.

Този пример показва как доставчиците на услуги на информационното общество могат да бъдат прозрачни и отговорни, като предоставят ясна информация и редовни отчети за своите действия.

2.3 Техническа отговорност

- Осигуряване на сигурност: Доставчиците трябва да осигурят технически защити срещу хакерски атаки и други заплахи. Например, онлайн банкирането на банка предоставя двуфакторна автентикация за допълнителна защита.
- Поддръжка на системите: Те трябва редовно да обновяват системите си, за да предотвратят уязвимости. Пример: Актуализациите на софтуерни платформи помагат за защита от нови видове атаки.

3. Права на доставчиците на електронни услуги

3.1 Принцип на „безопасен пристан“

- Определение и приложение

Определение: Принципът на „безопасен пристан“ осигурява защита за доставчиците на услуги от правна отговорност за съдържание, публикувано от потребители, при условие че не знаят за нарушението и действат бързо след уведомление.

Приложение: Съществува в различни законодателства, като Директивата за електронна търговия на ЕС и Закона за цифрово милениум авторските права (DMCA) в САЩ.

Пример за “Безопасен пристан”

Ситуация: Потребител качва видео в YouTube, което съдържа музика, защитена с авторски права, без разрешение от притежателя на правата.

Действия на доставчика: YouTube не знае за нарушението: Видеото е качено и достъпно за гледане, но YouTube не е наясно, че съдържа незаконно използвана музика.

Уведомление за нарушението: Притежателят на авторските права или друг потребител уведомява YouTube за нарушението чрез системата за уведомяване и премахване (например, чрез подаване на жалба за нарушаване на авторски права).

Бърза реакция: След получаване на уведомлението, YouTube проверява жалбата и, ако тя е основателна, премахва видеото или блокира достъпа до него.

Резултат: YouTube не носи отговорност за нарушението, защото:

- Не е знаел за незаконното съдържание преди уведомлението.
- Реагирал е бързо и е премахнал съдържанието след получаване на уведомлението.

Този пример показва как принципът на “безопасен пристан” защитава доставчиците на услуги на информационното общество, като същевременно гарантира, че незаконното съдържание се премахва бързо и ефективно.

3.2 Право на собствена политика и условия за ползване

➢ Право на създаване на правила

Установяване на правила за използване на платформата.

Определяне на политики относно съдържанието и поведението на потребителите.

➢ Модериране на съдържание

- Премахване на съдържание, което нарушава условията за ползване.
- Блокиране на потребители, които систематично нарушават правилата.

3.3 Право на защита на интелектуалната собственост

- **Закрила на патенти и търговски марки**

Защита на иновации и технологии чрез патенти и търговски марки.

Съдебна защита срещу нарушения на собствените права.

- **Разпознаване и защита на авторските права**

Използване на технологии за разпознаване на нарушаващо съдържание.

Управление на права на интелектуална собственост на трети лица.

3.4 Право на защита от неправомерно съдебно преследване

- Забрана за отговорност за съдържание на потребители

Не носят отговорност за съдържание, качено от потребители, освен ако не са информирани и не са реагирали на уведомления за нарушение.

3.5 Права по отношение на личните данни на потребителите

- Събиране и обработка на данни

Право да събират и обработват лични данни в съответствие с приложимите закони за защита на данните (напр. GDPR).Осигуряване на прозрачност относно начина на събиране и използване на данните.

- Права на потребителите

Предоставяне на опции за достъп до данните и корекция или изтриване на лична информация по искане на потребителя.

3.6. Права на сътрудничество с правоприлагащи органи

- **Съдействие при разследвания**

Предоставяне на информация на правоприлагащи органи при разследвания на престъпления или злоупотреби.

Спазване на съдебни заповеди и изисквания на закона за предоставяне на данни.

3.7 Право на иновация и развитие

- **Развитие на нови услуги и функции**

Разработване на нови технологии и функции за подобряване на потребителския опит.

Реагиране на променящите се нужди на пазара и потребителите чрез иновации.

Тази структура включва принципа на „безопасен пристан“ като основна точка и показва как той взаимодействува с правата и задълженията на доставчиците на услуги на информационното общество.

4. Как можем да се защитим?

4.1 Използване на силни пароли

Пример: Вместо „123456“, използвайте комбинация от букви, цифри и специални символи, например „!G7t$hM9*q“.

4.2 Проверка на настройките за конфиденциалност

Пример: В социалните медии проверявайте настройките на профила си, за да контролирате кой може да вижда вашите публикации и лични данни.

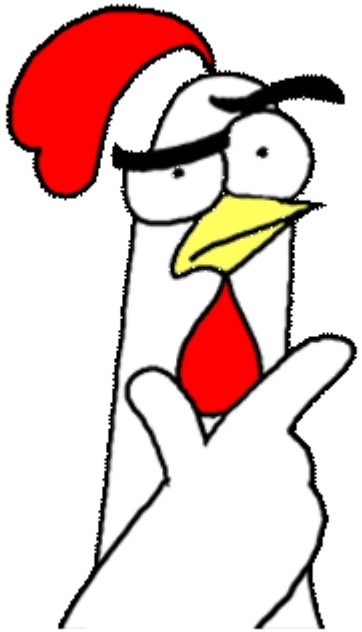
4.3 Избягване на съмнителни линкове и прикачени файлове

Пример: Никога не кликвайте на линкове в имейли от непознати източници, особено ако те изглеждат подозрителни или искат да въведете лична информация.

Ролева игра

Въпрос: Представете си, че сте администратор на платформа за видео споделяне. Потребител подава жалба за съдържание, нарушаващо авторски права. Какви стъпки ще предприемете, за да спазите принципа на „безопасен пристан“ и как ще реагирате на потребителя, който е подал жалбата?

Решение:



Въпроси към урока:

1. Определете и дайте примери за три различни типа доставчици на услуги на информационното общество.
Доставчици на интернет услуги (ISP) – предоставят достъп до интернет на потребителите. Пример: "Виваком".
Хостинг доставчици – съхраняват и поддържат уебсайтове на техни сървъри. Пример: "SuperHosting".
Платформи за споделяне на съдържание – предоставят услуги за създаване и разпространение на цифрово съдържание. Пример: "YouTube".

2. Обяснете какви са правните отговорности на доставчиците на услуги и дайте пример за конкретна ситуация, когато те трябва да предприемат действия.
Доставчиците на услуги са длъжни да осигуряват сигурността на личните данни, да информират потребителите за обработката на техните данни и да премахват незаконно съдържание при уведомяване. Например, ако доставчик на хостинг услуга получи сигнал за хоствано незаконно съдържание, той е длъжен да го премахне, за да не носи отговорност.

3. Посочете две мерки, които можете да предприемете, за да се защитите при използване на онлайн услуги, и обяснете защо са важни.

Благодаря за внаманието!