ВАРНЕНСКИ СВОБОДЕН УНИВЕРСИТЕТ “ЧЕРНОРИЗЕЦ ХРАБЪР”

Специалност: ПРАВО

КУРСОВА РАБОТА

Тема: "Съвременните връзки между правото и информацията”

Изговил:

I-ви курс, задочно обучение

фак. №

Темата "Съвременните връзки между правото и информацията" се фокусира върху взаимодействието и влиянието, което бързото развитие на информационните технологии и обработката на информацията оказват върху правната сфера и обществото като цяло. Тук са някои аспекти, които могат да бъдат разгледани в рамките на тази тема:

Защита на личните данни:

Защитата на личните данни е станала особено важна в цифровата епоха, където събирането, обработката и съхранението на големи количества лична информация са станали стандартна практика. Регулирането на тези процеси играе ключова роля в запазването на правата и поверителността на гражданите. GDPR (Общ регламент относно защитата на личните данни) в Европейския съюз е един от основните законодателни актове, насочени към установяване на стандарти за защита на личните данни.

Ето някои от основните принципи на GDPR и как се регулират събирането, обработката и съхранението на лични данни:

Съгласие: Определението за съгласие е усилено, и организациите трябва да получат ясно и информирано съгласие от субектите на данните за събиране и обработка на техните лични данни.
Права на субектите: GDPR предоставя на лицата по данните по-големи права за контрол и достъп до техните лични данни, както и възможността за тяхното коригиране или изтриване.
Отговорност и прозрачност: Организациите са задължени да бъдат отговорни и прозрачни по отношение на начина, по който събират, обработват и съхраняват личните данни.
Ограничение на целите: Личните данни трябва да се събират само за конкретни, законосъобразни цели и не могат да се обработват по начин, несъвместим с тези цели.
Минимизация на данните: Организациите трябва да събират само минималното количество лични данни, необходими за постигане на определени цели.
Сигурност на данните: Организациите трябва да прилагат подходящи мерки за сигурност, за да предотвратят неоторизиран достъп, загуба, разкриване или унищожение на личните данни.

Сътрудничество с регулаторните органи: Организациите са задължени да сътрудничат с регулаторните органи и да предоставят информация за обработката на лични данни, когато това се налага.

Наред с GDPR, много страни и региони също имат свои закони за защита на личните данни, които спазват подобни принципи. По-голямата част от тези закони се фокусират на постигане на баланс между необходимостта от събиране и обработка на данни за различни цели и правата на гражданите върху техните лични данни.

Киберсигурност и киберпрестъпност:

Киберсигурността и борбата с киберпрестъпността представляват сериозни предизвикателства в света на съвременните технологии. Правото се развива, за да се адаптира към тези предизвикателства и да предостави рамки за ефективна защита на информационната сигурност и противодействие на киберпрестъпността. Ето някои от начините, по които правото реагира на тези предизвикателства:

Законодателство за киберсигурност: Мнозина правителства приемат закони и регулации, които налагат задължения за поддържане на високи стандарти на киберсигурност за организации и критична информационна инфраструктура. Тези законодателства определят минимални изисквания за защита на данни и личната информация.

Наказателно преследване на киберпрестъпността: Съдебната система играе важна роля в преследването и наказването на киберпрестъпници. Множество страни са въведли законодателство, което предвижда наказателна отговорност за хакерски атаки, кражба на данни, измама и други форми на киберпрестъпност.

Международно сътрудничество: Поради характера на киберпрестъпността, която често преминава през граници, сътрудничеството между страните е от решаващо значение. Международни организации, като Interpol, и международни договорености, насочени към борба с киберпрестъпността, се разработват и приемат.

Киберсигурност на корпоративно ниво: Организациите също трябва да прилагат правни мерки за предпазване от кибератаки. Законодателството насърчава корпорациите да вграждат киберсигурност в своите бизнес процеси и да предприемат мерки за защита на данните на своите клиенти.

Развитие на технически стандарти и иновации: Правните рамки често се допълват с технически стандарти и иновации, предназначени да повишат сигурността на информационните системи. Това включва използването на шифроване, двуфакторна автентикация и други технически мерки за защита.

Изграждане на капацитет: Образователни програми и тренинги се предлагат с цел подготовка на кадри и увеличаване на капацитета за борба с киберпрестъпността както на индивидуално, така и на институционално ниво.