Logo

Description automatically generatedImmagine che contiene testo, clipart

Descrizione generata automaticamenteA picture containing diagram

Description automatically generated

Text

Description automatically generated

**MODUL FOR DIGITALT MEDBORGERSKAP**

**UTVIKLET AV ANTALYA VIZYON COLLEGE**



**DIGITALT MEDBORGERSKAP**

**MODUL**

**ENHET 7: DIGITAL LOV**

|  |
| --- |
| ***SAMMENDRAG AV MODULEN*** |
| I løpet av denne modulen vil elevene bli introdusert definisjonen av digital lov, eksempler på ulovlig og lovlig teknologibruk. De vil absorbere viktigheten av digitale lover. De vil lære å unngå plagiarisme. Elevene vil kunne forstå betydningen av nettmobbing i en vanlig sammenheng basert på teknologi og å takle vanskelighetene de kan ha møtt. |

INNHOLDSFORTEGNELSE

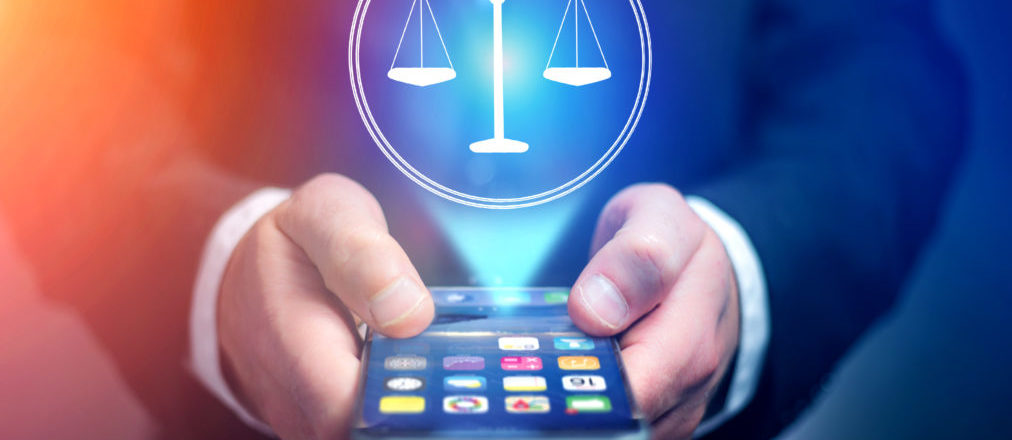
* 3,4 Definisjon av digital lov og funn
* Eksempler på ulovlig teknologibruk 5,6
* Eksempler på juridisk teknologi Bruk 6
* Plagiat 7,8
* Nettmobbing 9
* Digitale rettsspørsmål 10
* Digital lov nøkkelord 10
* Evalueringsspørsmål 11
* Referanser 12

DEFINISJON

Digital lov er det elektroniske ansvaret for handlinger, gjerninger som enten er etiske eller uetiske.

Uetisk bruk manifesterer seg i form av tyveri og/eller kriminalitet. Etisk manifesterer seg i form av å overholde samfunnets lover. Det handler i utgangspunktet om hva du er og ikke har lov til å gjøre mens du surfer og bruker Internett. Alle bør respektere loven og overholde den. Å ikke følge loven kan føre til alvorlig straff.

Internett har gjort det enkelt å legge ut, finne og laste ned et stort utvalg av materialer. Faktisk er denne evnen til å dele informasjon enkelt en av styrkene til Internett. Imidlertid vurderer brukere ofte ikke hva som er passende, upassende eller til og med ulovlig når de legger ut eller får tilgang til informasjon på Internett. Brukere bemerker ofte: "Vi trodde ikke det var galt - alt vi gjorde var å dele informasjon."



Spørsmålene om immaterielle rettigheter og opphavsrettsbeskyttelse er svært reelle, og har svært reelle konsekvenser for brudd. Disse problemene ble brakt i forgrunnen da Recording Industry Association of America (RIAA) bøtelagt studenter og andre for å laste ned musikk ulovlig (Wired News, 2003). Denne handlingen fikk noen teknologibrukere til å tenke to ganger om hva som er passende og ulovlig for online fildeling. I 2009 fant imidlertid en treårig samling av 16 land av International Federation of the Phonographic Industry (IFPI) at 95% av musikkfilene ble ulovlig delt (IFPI, 2009). Ironisk nok, en 2003 undersøkelse utført av Ipsos (et marked

forskningsselskap) for Business Software Alliance indikerte at to tredjedeler av høyskolefakulteter og administratorer sa at det er galt å laste ned eller bytte filer, mens mindre enn en fjerdedel av studentene følte det samme (CyberAtlas, 2003).

De nye digitale teknologiene bringer med seg et helt nytt rike av problemer som mest sannsynlig ikke ble forestilt av skaperne. Ofte oppstår disse problemene fra uforutsette og utilsiktede bruk av den nye teknologien. For eksempel har spørsmålet om sexting (å ta og dele seksuelt eksplisitt materiale, for eksempel naken eller halvnakne bilder) blitt stort for tenåringer. Hvis deltakeren er under 16 år, kan dette anses som barnepornografi selv om avsenderen er en villig deltaker eller har sendt et selvportrett. Hvis dette materialet mottas av en telefon (eller annen enhet), kan personen som eier enheten bli kriminelt belastet for bare å ha materialet (selv om personen ikke ønsket det i utgangspunktet). Den som sender bildene til andre kan bli arrestert for distribusjon av barnepornografi (igjen, selv om mindreårige tar og sender bilder av seg selv). Domfellelse for en av disse forbrytelsene kan ødelegge noens rykte permanent, og vil kreve at personen registrerer seg som en seksualforbryter. Hver stat og land er forskjellig, men mange har allerede vedtatt slike lover.

Selv om lovene i ditt område ennå ikke dekker sexting som en forbrytelse, kan mottakerne (eller avsenderen) være i et område der slike lover gjelder.

Det vil alltid være mennesker som ikke følger samfunnets regler og som engasjerer seg i aktiviteter som strider mot idealene i samfunnet som helhet. I denne forbindelse er det digitale samfunnet ikke annerledes. Som sådan blir det etablert konsekvenser for de som opptrer som upassende digitale borgere - brukere som stjeler andres informasjon, hacker seg inn på servere, oppretter og frigjør virus, og så videre. Etter hvert som nye lover utarbeides, er det viktig at digitale borgere er med på å bestemme hvordan de skal håndtere disse aktivitetene når de oppstår. Hvis medlemmer av det digitale samfunnet ikke gir informasjon for å bestemme disse gode statsborgerskapspolitikkene, vil lovene som er vedtatt av politikere ikke gjenspeile en god forståelse av det digitale samfunnet.







Lover knyttet til teknologibruk blir mer av et problem for skoledistrikter. Selv om det kan oppstå problemer utenfor skolens vegger eller ikke på skolens datamaskiner, kan effektene fortsatt måtte tas opp i løpet av skoledagen. Administratorer må gi lærere og elever ressurser og veiledning om hva som er lovlig og ulovlig.

De juridiske aspektene ved bruk av studentteknologi kan være en stor bekymring for skoleadministratorer. Teknologiledere og lærere må bidra med ressurser for å hjelpe administratorer med å ta gode beslutninger. På samme måte hjelper det ikke bare elevene å lære elevene å ta gode valg, men skoleadministratorene. Studentene må innse at det de gjør i dag kan påvirke dem i fremtiden.

De må også avgjøre om deres teknologiregler og retningslinjer støttes lovlig. Digitalt medborgerskap hjelper alle teknologibrukere med å bli mer oppmerksomme på de juridiske konsekvensene av teknologibruk.

Eksempler på ulovlig teknologibruk

• Studentene laster ned opphavsrettsbeskyttet musikk fra sosiale nettverk eller fildelingssider (f.eks. Kazaa).

• Studenter skripting (ved hjelp av datakode) for å omgå brannmurer eller annen nettverksbeskyttelse.

• hacking i folks personlige opplysninger, piratprogramvare og oppretting av virus eller trojanske hester.

**Identitetstyveri** er i ferd med å bli et økende problem. Studier viser at en av fem familier har vært ofre for dette i USA. Tyvene kan stjele kredittkortnummeret ditt slik at de kan kjøpe eller leie forskjellige produkter ved hjelp av informasjonen din. Det verste er at du ikke skjønner hva som skjer før du får tilsendt regninger eller mottar samtaler om ulike transaksjoner. Det tar måneder å gjenopprette all informasjonen din og sikre alt. Derfor bør alle ta forholdsregler.

**Spoofing** betyr generelt å overbevise folk om å oppgi personlig eller økonomisk informasjon som lar hackeren begå kredittkort-/banksvindel eller andre former for identitetstyveri. Spamkriminelle bruker ofte spoofing som et forsøk på å komme inn på andres datamaskin.





**IP Spoofing** er en teknikk som brukes til å få tilgang til datamaskiner, hvor inntrengeren sender en melding til en datamaskin med en IP-adresse som forteller dem at meldingen kommer fra en pålitelig maskin og person. For å stoppe IP Spoofing-pakkefiltrering er en programmering som blokkerer andre pakker som kommer inn i nettverket ditt. Dette forhindrer at en ekstern angriper får tilgang til en intern maskin.

**Piratkopiering av programvare** er kopiering og salg av uautorisert dataprogramvare, filmer osv. Dette skjer mye i Mexico, Kina, Indonesia, Russland, Brasil og Zimbabwe, men mange andre land er også involvert. De fleste av disse landene har lover om brudd på opphavsretten, men mange borgere overholder dem ikke, men noen land er strengere om dem enn andre.

Det er 4 typer piratkopiering av programvare:

• Industriell piratkopiering: En person eller gruppe forsøker duplisering og distribusjon i stor skala for profitt.

• Bedriftspiratkopiering: Ubeskyttet innhold deles gjennom nettverk som peer-topeer, LAN og Internett.

• Forhandlerpiratkopiering: Involverer maskinvareselskaper som selger maskiner med ulovlige kopier av programvare forhåndsinstallert på harddisken.

• Home Piracy: Inkluderer alt fra handelsdisker med venner til å kjøre en ideell oppslagstavle med det formål å ulovlig programvaredistribusjon.

**Datahacking** er praksisen med å endre maskinvare og programvare. Folk som er involvert i slike aktiviteter kalles ofte hackere. Siden ordet "hack" lenge har vært brukt til å beskrive noen som ikke er i stand til å gjøre jobben sin veldig bra. Noen hackere hevder at dette begrepet er støtende, siden de er veldig dyktige i emnene sine.



Datahacking er mest vanlig blant tenåringer og unge voksne, selv om det også er mange eldre hackere. Mange hackere anser datahacking som en "kunst" -form. De liker ofte programmering og har ferdigheter på ekspertnivå i et bestemt program.

**Eksempler på bruk av juridisk teknologi**

• Studentene forstår hva som kan lastes ned uten kostnad og hva som anses som opphavsrettsbeskyttet materiale og bør betales for.

• Studentene informerer en voksen om andre som deler naken- eller halvnakne bilder (sexting).

**Plagiat**

I følge Merriam-Webster online ordbok betyr å "plagiere":

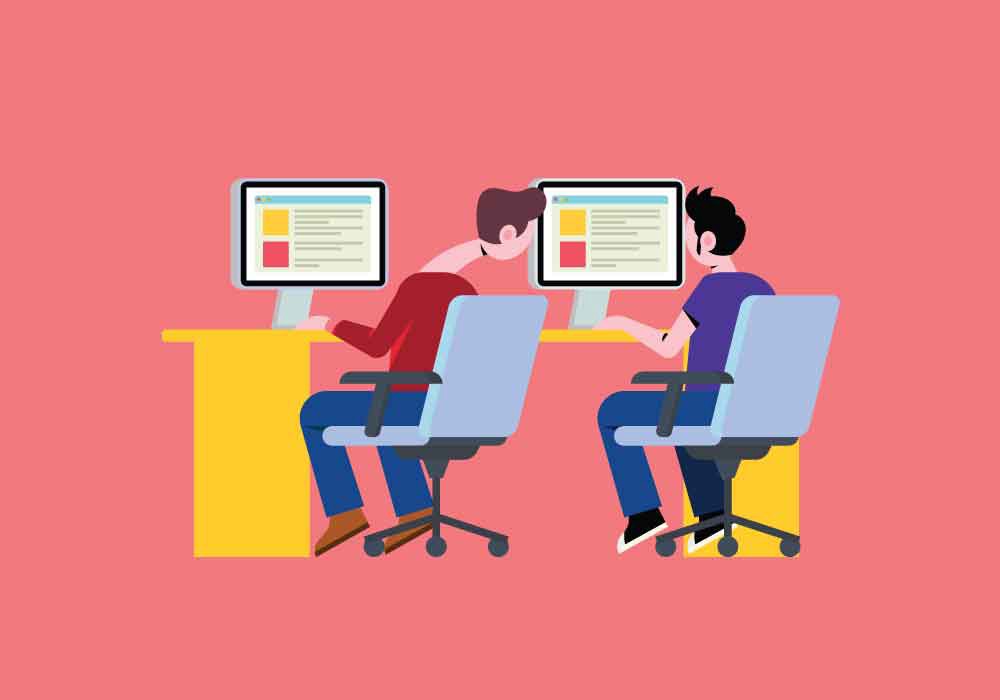
• å stjele og gi fra seg (ideene eller ordene til en annen) som ens egne

• å bruke (en annens produksjon) uten å kreditere kilden

• å begå litterært tyveri

• å presentere som ny og original en idé eller et produkt avledet fra en eksisterende kilde.

Plagiat er med andre ord en svindelhandling. Det innebærer å stjele andres arbeid og inkludering av enhver ide fra noen andre uten å gi behørig kreditt ved å sitere og referere til den kilden i hans / hennes arbeid. (P.org, 2017)



Alt av følgende betraktes som plagiering:

• Å levere inn andres arbeid som ditt eget

• kopiere ord eller ideer fra noen andre uten å gi kreditt

• oppsummere eller omskrive arbeidet eller ideene til en annen uten å sitere og referere til den opprinnelige kilden som ikke setter et anførselstegn

• gi feil informasjon om kilden til et sitat

• endre ord, men kopiere setningsstrukturen til en kilde uten å gi kreditt

• kopiere så mange ord eller ideer fra en kilde at det utgjør størstedelen av arbeidet ditt, enten du gir kreditt eller ikke

• bruke statistikk, tabeller, figurer, formler, diagrammer, spørreskjemaer, bilder, musikknotasjon, datakode etc. laget av andre uten å sitere og referere til den opprinnelige kilden

• kopiering av arbeidet til en annen student, med eller uten deres samtykke. (P.org, 2017)

Plagiat kan oppstå av flere årsaker:

• Rett og slett ikke forstå hva plagiering er.

• Ikke sitere eller referere riktig i arbeidet ditt.

• Press fra tidsfrister og/eller dårlig tidsstyring som fører til en "klipp og lim" tilnærming til forskning.

• Uorganisert forskning og notater fører til forvirring mellom dine egne tanker og ideer hentet fra andre kilder.

• Mangel på tillit til å sette ting i dine egne ord.



Kopiering av andres arbeid kan få alvorlige konsekvenser. Disse kan være personlige eller profesjonelle og også lovlige. De fleste tilfeller av plagiering kan imidlertid unngås ved å sitere kilder. Bare å erkjenne at bestemt materiale er lånt og gi publikum den informasjonen som er nødvendig for å finne den kilden, er vanligvis nok til å forhindre plagiering. (Universitetet i Bristol, 2022)



**Nettmobbing eller** netthets er en form for mobbing eller trakassering ved hjelp av elektroniske midler. Det har blitt stadig mer vanlig, spesielt blant tenåringer. Skadelig mobbeatferd kan omfatte å legge ut rykter, trusler, seksuelle bemerkninger, ofrenes personlige opplysninger eller nedsettende etiketter (dvs. hatefulle ytringer). Nettmobbing ligner ofte på tradisjonell mobbing, med noen bemerkelsesverdige forskjeller. Ofre for nettmobbing vet kanskje ikke identiteten til mobberen sin, eller hvorfor mobberen retter seg mot dem. Trakasseringen kan ha vidtrekkende effekter på offeret, da innholdet som brukes til å trakassere offeret, kan spres og deles lett blant mange mennesker og ofte forblir tilgjengelig lenge etter den første hendelsen.



Begrepene "cyberharassment" og "cyberbullying" brukes noen ganger synonymt, selv om noen bruker sistnevnte til å referere spesifikt til trakassering blant mindreårige eller i en skoleinnstilling. Et flertall av stater har lover som eksplisitt inkluderer elektroniske kommunikasjonsformer innenfor stalking- eller trakasseringslover. Fra midten av 2015 er land i EU som Storbritannia i ferd med å lage lover spesielt relatert til nettmobbing.

Forskere foreslår at programmer settes på plass for forebygging av nettmobbing. Disse programmene vil bli innlemmet i skolens læreplaner og vil inkludere online sikkerhet og instruksjon om hvordan du bruker Internett riktig.

Digitale lovspørsmål

• Bruke fildelingsnettsteder

• Piratkopiering programvare

• Undergrave teknologier for digital rettighetsadministrasjon (DRM)

• Hacking i systemer eller nettverk

• Stjele noens identitet

• Sexting og deling av ulovlige bilder



Digital Law Nøkkelord

• lover om opphavsrett til teknologi

• Person-til-person-programvare (P2P)

• Piratkopiering





EVALUERING SPØRSMÅL

* Hva tenker du når du hører «digital lov»-frase?

* Kan du gi et eksempel på ulovlig teknologibruk?

* Er du klar over resultatene av ulovlig bruk av teknologi?

* Hva er plagiering?
* Hva betyr «nettmobbing»? Har du blitt mobbet før?

**Referanser**

Digital lov. <https://digiteen.wikispaces.com/Digital+Law>

Ribble, M. (2015). Digitalt medborgerskap i skolen: Ni elementer alle elever bør kjenne til. 3. utg. ISTE.

Universitetet i Bristol Bibliotek <https://www.bristol.ac.uk/library/support/findinginfo/plagiarism/>

Hva er plagiering? <http://www.plagiarism.org/article/what-is-plagiarism>