

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over hacking og uberettiget adgang til IT-systemer (§ 263, § 263 a)

Strafudmåling og kvalificering efter straffelovens §§ 263 og 263 a

Version 2 Opdateret 26. jun. 2026 12 afgørelser · 2014-2026

[Læs online](#)

INTRODUKTION

Straffelovens § 263 kriminaliserer uberettiget adgang til en andens datasystem eller data, mens § 263 a retter sig mod den, der uberettiget skaffer sig eller videregiver adgangsmidler til datasystemer. Bestemmelserne udgør det strafferetlige kernegrundlag for hacking-sager i dansk ret og har en normalstrafferamme på bøde eller fængsel indtil 1 år og 6 måneder, med en kvalificeret strafferamme på fængsel indtil 6 år ved særligt skærpende omstændigheder, herunder industrispionage, systematisk karakter eller betydelige skadevirkninger. Retspraksis spænder fra bøder for enkle overtrædelser til straffe på 3½ års fængsel for de groveste angreb mod samfundsvigtig infrastruktur, og der lægges særlig vægt på adgangsens varighed, mængden af kompromitterede data og udnyttelse af betroet stilling.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Uberettiget adgang til et datasystem er fuldbyrdet allerede ved, at gerningsmanden skaffer sig adgang – det er uden betydning, hvad der efterfølgende foretages i systemet.
- 02** Udtrykket 'datasystem' omfatter computere, smartphones, tablets og ethvert elektronisk udstyr med databehandlingsfunktioner, herunder også data på USB-stik der ikke er tilsluttet et system.
- 03** Flere hackerangreb begået inden for kort tid mod samme mål skal bedømmes samlet ved vurderingen af, om der foreligger 'særligt skærpende omstændigheder' efter § 263, stk. 3.
- 04** Den skærpede strafferamme i § 263, stk. 3, på fængsel indtil 6 år finder ikke kun anvendelse ved industrispionage, men også ved angreb der medfører betydelige skadevirkninger for offentlige eller private interesser.
- 05** Udnyttelse af viden fra en tidligere betroet stilling og brug af en kollegas loginoplysninger kan kvalificere forholdet som begået under 'særligt skærpende omstændigheder'.
- 06** Hacking af samfundsvigtige datasystemer med download af store mængder personfølsomme data – f.eks. politiregistre og CPR-data – straffes i niveauet 3-4½ års fængsel.
- 07** Systematisk fjernstyring af 40+ privatcomputere via malware (f.eks. Netwire) straffes med fængsel i 6 måneder, delvist betinget, med vægt på krænkelserens omfang og varighed.

- 08** Hacking kombineret med identitetstyveri, videregivelse af intime billeder og skjulte optagelser udgør selvstændigt strafbare forhold, der straffes i sammenstød med § 263.
- 09** En arbejdsgiver, der tilgår en fratrådt medarbejders private e-mailkonto uden hjemmel, overtræder både databeskyttelsesforordningen og kan gøre sig skyldig i hacking efter § 263.
- 10** Datahærværk i form af sletning af data i virksomheders IT-systemer kvalificeres efter § 291, stk. 2, når udbedringsomkostningerne overstiger ca. 15.000 kr. eller driften lægges ned.
- 11** Strafferammerne i § 263 blev forhøjet ved lovændringen i 2004 for bedre at afspejle det IT-baserede samfunds sårbarhed og for at undergive IT-kriminalitet samme strafmaksimum som traditionelle formueforbrydelser.
- 12** Ved nyaffattelsen i 2019 blev § 263 omstruktureret, så datakriminalitet (adgang til datasystemer) nu er bestemmelsens hovedregel i stk. 1, mens brevfredskrænkelser er flyttet til stk. 2.

Retsgrundlaget: §§ 263 og 263 a om uberettiget adgang til datasystemer

Den strafferetlige regulering af hacking og uberettiget adgang til IT-systemer hviler på to bestemmelser i straffelovens kapitel 27 om freds- og ærekrænkelser.

Straffelovens § 263 er bestemmelsens kerneregulering. Efter den gældende affattelse (der trådte i kraft 1. januar 2019) straffes i **stk. 1** med bøde eller fængsel indtil 1 år og 6 måneder den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem. **Stk. 2** vedrører den subsidiære brevfredskrænkelser (åbning af lukkede meddelelser og skjult aflytning). Den kvalificerede strafferamme i **stk. 3** hæver strafmaksimum til fængsel indtil 6 år, når forholdet begås:

- med forsæt til at skaffe sig erhvervshemmeligheder, eller
- under andre *særligt skærpende omstændigheder*, eller
- (for stk. 1-overtrædelser) når der er tale om overtrædelser af *mere systematisk eller organiseret karakter*.

Straffelovens § 263 a kriminaliserer den, der uberettiget sælger, udbreder eller videregiver adgangsmidler (koder, passwords mv.) til datasystemer. Bestemmelsen blev nyaffattet ved freds- og ærekrænkelserloven i 2019 og samler den tidligere § 263 a (ikke-kommercielle systemer) og § 301 a (kommercielle systemer) i én bestemmelse. Stk. 2 indeholder en skærpet strafferamme på fængsel indtil 6 år ved særligt skærpende omstændigheder.

Hacking medfører regelmæssigt samtidig overtrædelse af § 291 om hærværk, når der slettes eller beskadiges data. Angreb på *samfundsvigtige* datasystemer kan desuden rammes af § 193 om omfattende forstyrrelse i driften af offentlige kommunikationsmidler, IT-systemer m.v., med en strafferamme på fængsel indtil 6 år.

Afgrænsning mod beslægtede praksisoversigter: Når den uberettigede adgang bruges til økonomisk udnyttelse (f.eks. pengeoverførsler), overgår forholdet typisk til [databedrageri](#) efter § 279 a. Misbrug af ulovligt opnåede NemID/MitID-legitimationsoplysninger til transaktioner er behandlet i [mitid-nemid-misbrug](#).

LOV

Straffeloven § 263, stk. 1, 3

Straffeloven § 263a, stk. 1

Straffeloven § 291, stk. 2

§ 2 Lovhistorik: Fra brevhemmelighed til cyberforbrydelse

Straffelovens § 263 har gennemgået en markant udvikling fra sin oprindelse som beskyttelse af brevhemmeligheden til i dag at udgøre det primære strafferetlige værn mod IT-kriminalitet.

Bestemmelsens oprindelse (1930) var knyttet til fredskrænkelser – brud på brevhemmelighed og krænkelse af private gemmer. Hacking var naturligvis ukendt på dette tidspunkt.

1985-lovændringen indførte den daværende § 263, stk. 2, om uberettiget adgang til en andens *oplysninger eller programmer*, der er bestemt til at bruges i et *informationssystem*. Hermed blev datakriminalitet for første gang direkte kriminaliseret i dansk ret.

2004-lovændringen forhøjede strafferammerne markant. Som Højesteret bemærkede i [Sag 219/2017](#):

"Det fremgår af forarbejderne til lovændringen i 2004, hvorved strafferammerne i § 263, stk. 2 og 3, blev forhøjet, at dette skete for bl.a. bedre at afspejle forbrydelsens alvor under hensyn til det it-baserede samfunds sårbarhed og for at undergive kriminalitet rettet mod informationer samme strafmaksimum som kriminalitet rettet mod mere traditionelle værdier i form af penge og ting."

2019-nyaffattelsen – gennemført med baggrund i [Straffelovrådets betænkning nr. 1563/2017 om freds- og ærekrænkelser](#) – omstrukturerede bestemmelsen grundlæggende. Datakriminalitet (adgang til datasystemer) blev rykket fra stk. 2 til stk. 1, mens brevfredskrænkelser blev subsidieret i stk. 2. Terminologien blev moderniseret: "informationssystem" blev til "datasystem", og "oplysninger eller programmer" til "data".

Forarbejderne til nyaffattelsen præciserer udtrykkeligt, at bestemmelsens gerningsindhold er bredt:

"Den foreslåede bestemmelse vil således omfatte meget forskelligartede forhold, herunder at en gerningsmand skaffer sig adgang til en andens computer eller smartphone [...], at en gerningsmand logger på en andens e-mailsystem [...], eller at en gerningsmand skaffer sig adgang til et usb-stik."

Bestemmelsen omfatter også den, der udnytter en svaghed i et datasystem, der giver en videre adgang end tilsigtet – f.eks. URL-manipulation eller udnyttelse af en softwaresårbarhed.

LOV

Straffeloven § 263, stk. 1, 2

PRAKSIS

Højesteret · Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads 27.02.2018

§ 3 De groveste sager: Hacking af samfundsvigtig infrastruktur (3-4½ års fængsel)

De strengeste straffe i dansk praksis er idømt for systematisk hacking af samfundsvigtige IT-systemer, hvor store mængder personfølsomme data er blevet kompromitteret.

CSC-hackersagen er den mest alvorlige hackingsag, der har været behandlet ved danske domstole. Sagen vedrørte et omfattende og teknisk kompliceret angreb i 2012 mod en stor IT-virksomheds mainframe, der

driftede bl.a. Kriminalregisteret, CPR-registeret, Kørekortregisteret og Schengen Informationssystemet for Rigspolitiet.

Angriberen etablerede tre bagdøre i systemet og downloadede i alt ca. 19 GB data til servere i Iran, Cambodia og Tyskland over en periode fra februar til august 2012. Byretten ([SS-5591/2014-FRB](#)) idømte tiltalte fængsel i 3 år og 6 måneder. Østre Landsret ([SS-3126/2014-OLR](#)) stadfæstede enstemmigt dommen og fastslog:

"Sagen er den hidtil alvorligste af sin karakter, hvor der i forbindelse med angreb, der foregik systematisk og havde en lang tidsmæssig udstrækning, blev downloadet en betydelig mængde stærkt personfølsomme oplysninger til servere i Tyskland, Cambodja og Iran."

Forholdet blev henført under [§ 263, stk. 3](#) (skærpet strafferamme) og [§ 291, stk. 2](#) (hærværk af betydeligt omfang), men retten fandt det ikke godtgjort, at angrebene havde fremkaldt en *omfattende forstyrrelse* i driften, hvorfor tiltalen efter [§ 193](#) ikke førte til domfældelse. Tiltalte blev desuden udvist.

Bevistemaet om fjernstyring er af særlig interesse. Tiltalte forklarede, at hans computere havde været fjernstyret af ukendte tredjeparter. Landsretten fandt, at muligheden for fjernstyring ikke helt kunne udelukkes, men at den samlede bevisførelse – herunder krypterede containere med de stjålne data, chatlogs og personspecifikke søgninger – "samlet set helt oplagt og entydigt" godtgjorde tiltaltes medvirken. Retten bemærkede, at en person med indgående IT-kendskab ikke ville have undladt at opdage en uautoriseret fjernstyring over en periode på 6 måneder.

LOV	Straffeloven § 193	Straffeloven § 263, stk. 3	Straffeloven § 291, stk. 2
PRAKSIS	Landsretten · Østre Landsret stadfæster dom i CSC-hackersagen: 3 år og 6 måneders fængsel og udvisning for hacking af samfundsvigtigt informationssystem 17.06.2015 Byretten · Hacking af Forurettede A/S' mainframe med politiregistre – Tiltalte 1 og Tiltalte 2 (Retten på Frederiksberg 2014) 31.10.2014		

§ 4 Hacking mod tidligere arbejdsplads: Udnyttelse af betroet stilling

Højesterets dom i [Sag 219/2017](#) er den ledende afgørelse om hacking begået af en tidligere ansat med udnyttelse af viden fra en betroet IT-stilling.

Tiltalte – en tidligere IT-chef – gennemførte i november 2014 tre målrettede angreb mod sin tidligere arbejdsgivers IT-systemer:

Dato	Angreb	Konsekvens
8. nov. 2014	Sletning af data i SAN-lagringsenhed	Virksomhedens drift lammet
9. nov. 2014	Sletning af indholdsfortegnelse på NAS	Backups ødelagt
16. nov. 2014	Sletning af intranet	Genetableret via papirkurv

Angrebene medførte, at virksomheden reelt blev "lagt ned", medarbejdere hjemsendt og udbedringsomkostninger på over 400.000 kr.

Højesteret fastslog tre afgørende principper:

1. **Samlet bedømmelse:** De tre angreb skal bedømmes samlet – ikke isoleret – ved vurderingen af, om der foreligger "særligt skærpende omstændigheder".

2. **Ikke kun industrispionage:** Udtrykket "andre særligt skærpende omstændigheder" i § 263, stk. 3 rummer også tilfælde, der vanskeligt kan angives mere præcist, herunder tilfælde med betydelige skadevirkninger for private interesser – selv uden formål om erhvervshemmelighedsspionage.
3. **Strafniveau:** Straffen for hackingforholdene og hærværket isoleret set bør ligge omkring **2 års fængsel**. Den samlede straf for alle 81 forhold (herunder 78 bedrageriforhold) blev fastsat til **fængsel i 3 år og 6 måneder**.

Højesteret afviste betinget dom og samfundstjeneste henset til straffens længde og kriminalitetens alvor.

LOV

Straffeloven § 263, stk. 3

Straffeloven § 291, stk. 2

PRAKSIS

Højesteret · Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads 27.02.2018

Hacking af private computere og identitetstyveri:

§ 5 Normalstrafniveauet

Under den skærpede strafferamme ligger en betydelig gruppe sager, hvor privatpersoners computere eller konti kompromitteres – typisk via fjernstyringsprogrammer, stjalne passwords eller social engineering. Strafniveauet ligger her i intervallet 3-6 måneders fængsel, ofte delvist betinget.

Netwire-sagen (S-323-15) vedrørte en tiltalte, der over ca. ét år uberettiget skaffede sig adgang til 40 private computere via fjernstyringsprogrammet Netwire. Programmet gav adgang til filkopiering, keylogging, skærmbilleder og remote shell. Østre Landsret skærpede byrettens straf fra 4 til **6 måneders fængsel**, hvoraf 3 måneder betinget med 3 års prøvetid:

"Efter arten og omfanget af lovovertrædelserne, der har strakt sig over en periode på omkring 1 år, samt henset til den krænkelse, som lovovertrædelserne har medført for de forurettede, finder landsretten, at straffen [...] bør forhøjes til fængsel i 6 måneder."

Hacking kombineret med seksuelle krænkelser (S-1264-18) viser sammenstødet mellem § 263 og andre bestemmelser. Tiltalte havde over en længere periode udnyttet sin IT-tekniske viden til at hacke flere kvinders konti, videregivet intime billeder og foretaget skjulte videooptagelser af samleje. Østre Landsret skærpede straffen til **5 måneders ubetinget fængsel** med følgende begrundelse:

"Ved straffastsættelsen er der navnlig lagt vægt på sagens karakter og omfang, herunder at der er tale om adskillige og systematiske krænkelser, hvor tiltalte gennem en længere periode har udnyttet og misbrugt sin it-tekniske viden til at begå alvorlige og krænkende lovovertrædelser."

Trods tiltaltes ustraffethed fandt retten ikke grundlag for betinget dom. Der blev desuden tilkendt tortgodtgørelse til de forurettede på 5.000-20.000 kr. pr. person.

LOV

Erstatningsansvarsloven § 26, stk. 1

Straffeloven § 263, stk. 1

Straffeloven § 264d

PRAKSIS

Landsretten · Skærpet fængselsstraf i landsretten for omfattende hacking, identitetstyveri, videregivelse af intime billeder og skjult videooptagelse af samleje 26.09.2018

Landsretten · Hacking af 40+ computere via fjernstyringsprogram: Landsretten skærper straffen og forlænger prøvetiden 30.03.2015

§ 6 Gerningsindholdet: Hvad udgør 'uberettiget adgang'?

Et centralt fortolkningsspørgsmål i praksis er, hvornår en adgang er "uberettiget" i bestemmelsens forstand. Forarbejderne til 2019-nyaffattelsen præciserer, at bestemmelsen er formuleret bredt, og at der *regelmæssigt* skal ske en udskillelse af legale handlinger fra det strafbare.

Adgangen er fuldbyrdet ved selve indtrængen. Det er uden betydning, hvad gerningsmanden efterfølgende foretager sig i systemet – om data kopieres, ændres, slettes eller blot betragtes. Allerede det at skaffe sig adgang fuldender gerningen.

Overskridelse af autoriseret adgang kan også være strafbar. Forarbejderne nævner udtrykkeligt:

- En medarbejder, der har berettiget adgang til arbejdsgiverens system, men som tilgår data, der ikke er arbejdsmæssigt behov for – navnlig hvis medarbejderen har videregående forsæt til at videregive data.
- En kunde, der har berettiget adgang til en brugerflade, men som udnytter en fejl eller svaghed i systemet til at kopiere, ændre eller slette data.

URL-manipulation er et særligt relevant eksempel. Datatilsynet har i flere afgørelser fastslået, at "Broken Access Control" via URL-manipulation er en velkendt sårbarhed – klassificeret som A5:2017 på OWASP Top 10-listen – og at systemer, der tillader uberettiget adgang via URL-ændringer, ikke opfylder kravene til behandlingssikkerhed efter [GDPR art. 32](#).

Adgang til private e-mailkonti er behandlet i Datatilsynets afgørelse [2024-31-0529](#), hvor en virksomhed tilgik en fratrådt medarbejders personlige e-mailkonto, som stod åben i en webbrowser på en afleveret arbejdscomputer. Datatilsynet udtalte alvorlig kritik og bemærkede, at spørgsmålet om en eventuel overtrædelse af [§ 263](#) ikke henhørte under Datatilsynets kompetence – hvilket antyder, at forholdet efter omstændighederne også kan være strafbart.

I sagen om [Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser](#) (2024-32-0482) fandt Datatilsynet, at en offentlig myndighed lovligt kan inddrage oplysninger, der er skaffet i strid med [§ 263, stk. 2](#), af en privat tredjepart – men kun fordi myndigheden selv ikke havde medvirket til den ulovlige handling, og fordi hensynet til barnets bedste og officialpligten vejede tungere.

LOV

[Databeskyttelsesforordningen § 32, stk. 1](#)
[Straffeloven § 263, stk. 1](#)

PRAKSIS

Datatilsynet · Alvorlig kritik til privat virksomhed for uberettiget adgang til tidligere ansats e-mails og filer 25.10.2024

Datatilsynet · Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag 13.09.2024

§ 7 Samspillet med GDPR-håndhævelse og datasikkerhed

Hacking-sager har en vigtig pendant i databeskyttelsesretten. Mens straffeloven retter sig mod gerningsmanden, kan den dataansvarlige organisation – der har undladt at sikre sine systemer tilstrækkeligt – også drages til ansvar efter [GDPR art. 32](#) om behandlingssikkerhed.

Bødestraf til dataansvarlige for utilstrækkelig IT-sikkerhed er blevet en fast del af praksis:

- Vestre Landsret idømte i [SS-113/2025-VLR](#) en region en bøde på **500.000 kr.** for en URL-sårbarhed i en spørgeskemadatabase, der eksponerede 23.000 borgeres helbredsoplysninger i over halvandet år.

- Østre Landsret stadfæstede i [S-2302-23](#) en **bøde på 50.000 kr.** til en kommune for manglende adgangskontrol i et tandplejesystem, der risikerede at afsløre adressebeskyttede borgeres oplysninger.
- Datatilsynet politianmeldte [Lyngby-Taarbæk Kommune](#) og indstillede til en bøde på 350.000-400.000 kr. for manglende flerfaktorautentifikation og brugerrevokation, efter at en uvedkommende tredjepart udnyttede svage loginoplysninger til at tilgå 5.000 borgeres data.

Erstatning for immateriel skade efter databrud er fortsat svær at opnå. I sagen om Gladsaxe Kommunes databrud ([BS-19616/2021-OLR](#)) fastslog Østre Landsret, at kommunen havde overtrådt [GDPR art. 32](#), men at de seks sagsøgende borgere ikke havde godtgjort at have lidt immateriel skade efter [GDPR art. 82](#). Retten lagde bl.a. vægt på, at computeren var stjålet sammen med andre genstande og pantflasker, at der ikke var bevis for, at uvedkommende faktisk havde tilgået dataene, og at to borgeres efterfølgende identitetstyverier ikke var dokumenteret at have årsagssammenhæng med det konkrete databrud.

LOV	Databeskyttelsesforordningen § 32, stk. 1	Databeskyttelsesforordningen § 82, stk. 1
	Databeskyttelsesforordningen § 83, stk. 2	Databeskyttelsesloven § 41, stk. 1
PRAKSIS	Landsretten · Region idømt bøde på 500.000 kr. for brud på datasikkerhed – URL-sårbarhed i CBCL-database	23.03.2026
	Landsretten · Kommune idømt bøde på 50.000 kr. for utilstrækkelig IT-sikkerhed i tandpleje-system, der risikerede at afsløre beskyttede adresser	19.02.2025
	Landsretten · Landsretten stadfæster: Kommune dømt for brud på datasikkerhed, men ingen erstatning til borgere	19.11.2024
	Datatilsynet · Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb	27.11.2024

§ 8 Strafudmålingens centrale momenter

På tværs af den foreliggende praksis kan følgende momenter identificeres som afgørende for strafudmålingen:

Skærpende omstændigheder:

- Angreb på samfundsvigtige systemer (politiregistre, sundhedsdata, CPR)
- Stor datamængde kompromitteret (tusindvis eller millioner af personers data)
- Lang varighed – systematisk angreb over uger eller måneder
- Udnyttelse af betroet stilling eller insiderviden
- Betydelige skadevirkninger (driftsstans, udbedringsomkostninger over 400.000 kr.)
- Anvendelse af sofistikerede metoder (bagdøre, kryptering, scripts)
- Viderealg eller videregivelse af kompromitterede data

Formildende omstændigheder:

- Tilståelse og samarbejde med myndigheder
- Ung alder eller gode personlige forhold
- Begrænset varighed eller omfang af det uberettigede adgang
- Ingen videregivelse af opnåede data

Oversigt over straffniveauer i praksis:

Sagstype	Typisk straf	Eksempel
Hacking af samfundsvigtig infrastruktur med datanedlastning	3-4½ års fængsel	CSC-sagen (3½ år)
Groft datahærværk mod arbejdsgivers IT-system med bedrageri	2-3½ års fængsel	Sag 219/2017 (3½ år samlet)
Systematisk fjernstyring af mange private computere	4-6 måneders fængsel, delvist betinget	Netwire-sagen (6 mdr.)
Hacking + identitetstyveri + digitale sexkrænkelser	5-8 måneders fængsel	S-1264-18 (5 mdr.)

Det er værd at bemærke, at de mest alvorlige sager – CSC og Sag 219/2017 – begge resulterede i præcis 3 år og 6 måneders fængsel, hvilket i praksis synes at udgøre det øverste straffniveau for hackingsager i dansk ret. Strafferammens maksimum på 6 år er endnu ikke nået.

LOV	Straffeloven § 263, stk. 3	
PRAKSIS	Højesteret · Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads 27.02.2018 Landsretten · Skærpet fængselsstraf i landsretten for omfattende hacking, identitetstyveri, videregivelse af intime billeder og skjult videooptagelse af samleje 26.09.2018 Landsretten · Østre Landsret stadfæster dom i CSC-hackersagen: 3 år og 6 måneders fængsel og udvisning for hacking af samfundsvigtigt informationssystem 17.06.2015 Landsretten · Hacking af 40+ computere via fjernstyringsprogram: Landsretten skærper straffen og forlænger prøvetiden 30.03.2015	

§ 9 Sammenfatning og udviklingstendenser

Retspraksis om hacking og uberettiget adgang til IT-systemer viser en klar udvikling i retning af strengere sanktioner og en bredere forståelse af gerningsindholdet.

Straffniveauet er steget markant siden bestemmelsens indførelse. De to ledende afgørelser – CSC-hackersagen og Sag 219/2017 – ligger begge på 3½ års fængsel og markerer den øvre grænse i praksis. For mindre alvorlige overtrædelser ligger straffniveauet typisk i intervallet 3-6 måneders fængsel, delvist betinget.

Gerningsindholdet er blevet udvidet ved 2019-nyaffattelsen, der moderniserede terminologien og placerede datakriminalitet som bestemmelsens hovedregel. Forarbejderne understreger den brede forståelse af "uberettiget adgang", der også omfatter overskridelse af autoriseret adgang.

Samspelet med databeskyttelsesretten er et centralt træk ved moderne hackingsager. Hvor straffeloven retter sig mod angriberen, kan den utilstrækkelig sikre dataansvarlige nu også bødestraffes – med bøder der i praksis kan nå 500.000 kr. for offentlige myndigheder. De to regelsæt supplerer hinanden og skaber samlet set et stærkere sanktionssystem.

Kritisk infrastruktur nyder en særlig beskyttelse. NIS-direktivet og den danske implementering i [NIS-bekendtgørelsen](#) stiller krav om, at operatører af væsentlige tjenester indfører passende sikkerhedsforanstaltninger. Angreb på sådanne systemer kvalificeres regelmæssigt under den skærpede strafferamme i § 263, stk. 3.

Bevisspørgsmål står centralt i hackingsager. CSC-sagen illustrerer, at forsvarets typiske indvending – at computeren var fjernstyret – kræver stærk teknisk dokumentation for at bære igennem. Domstolene lægger vægt på den samlede bevissituation, herunder digitale spor som krypterede containere, chatlogs, IP-adresser og tidsmæssig sammenhæng mellem aktivitet og anholdelse.

Der er ingen vedtagne men endnu ikke konsoliderede ændringer til [§ 263](#) pr. juni 2026.

LOV	Straffeloven § 263, stk. 1, 3	Straffeloven § 263a	
PRAKSIS	Højesteret · Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads		27.02.2018
	Landsretten · Østre Landsret stadfæster dom i CSC-hackersagen: 3 år og 6 måneders fængsel og udvisning for hacking af samfundsvigtigt informationssystem		17.06.2015
	Byretten · Hacking af Forurettede A/S' mainframe med politiregistre – Tiltalte 1 og Tiltalte 2 (Retten på Frederiksberg 2014)		31.10.2014

REFERENCE Lovgrundlag

4 paragraffer

Straffeloven § 193	Straffeloven § 263	stk. 1, 3
Straffeloven § 263a	stk. 1, 2	Straffeloven § 291
		stk. 2

MATERIALE Citerede afgørelser

11 afgørelser

HØJESTERET · ØVERSTE INSTANS		1
27.02.2018	Højesterets dom om skærpede strafferammer for hacking og datahærværk mod tidligere arbejdsplads	219-2017
LANDSRETTEEN · ANKEINSTANS		6
23.03.2026	Region idømt bøde på 500.000 kr. for brud på datasikkerhed – URL-sårbarhed i CBCL-database	10573-12480
19.02.2025	Kommune idømt bøde på 50.000 kr. for utilstrækkelig IT-sikkerhed i tandpleje-system, der risikerede at afsløre beskyttede adresser	S-2302-23
19.11.2024	Landsretten stadfæster: Kommune dømt for brud på datasikkerhed, men ingen erstatning til borgere	6704-8053
26.09.2018	Skærpet fængselsstraf i landsretten for omfattende hacking, identitetstyveri, videregivelse af intime billeder og skjult videooptagelse af samleje	S-1264-18
17.06.2015	Østre Landsret stadfæster dom i CSC-hackersagen: 3 år og 6 måneders fængsel og udvisning for hacking af samfundsvigtigt informationssystem	10786-13836

30.03.2015 Hacking af 40+ computere via fjernstyringsprogram: Landsretten skærper straffen og forlænger prøvetiden S-323-15

BYRETTEEN · FØRSTE INSTANS 1

31.10.2014 Hacking af Forurettede A/S' mainframe med politiregistre – Tiltalte 1 og Tiltalte 2 (Retten på Frederiksberg 2014) 10740-12764

DATATILSYNET · NÆVN / KLAGEINSTANS 3

27.11.2024 Politianmeldelse af Lyngby-Taarbæk Kommune for utilstrækkelig it-sikkerhed efter hackerangreb

25.10.2024 Alvorlig kritik til privat virksomhed for uberettiget adgang til tidligere ansats e-mails og filer 2024-31-0529

13.09.2024 Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag 2024-32-0482

FORARBEJDE Betænkninger 1 reference

Straffelovrådets betænkning om freds- og ærekrænkelser

nr. 1563 · 2017 · Justitsministeriet