

PRAKSISOVERSIGT · STRAFFERETSPLEJE

Praksisoversigt over digital bevisførelse – mobildata og chatudtræk

Beslaglæggelse, ransagning og bevismæssig brug af data fra mobiltelefoner, krypterede platforme og cloud-tjenester

Version 2 Opdateret 24. jun. 2026 15 afgørelser · 2010-2026

[Læs online](#)

INTRODUKTION

Digital bevisførelse – fra ransagning og dataudtræk af mobiltelefoner til anvendelse af krypteret kommunikation fra EncroChat og SKY ECC – udgør i dag den processuelle kerne i de fleste alvorlige straffesager. Retsgrundlaget hviler på retsplejelovens regler om ransagning (§§ 793-799), beslaglæggelse og edition (§§ 802-807) samt proportionalitetskravet i § 797. Højesteret har i en række afgørelser fra 2019-2026 fastlagt de centrale grænser: tvangsmæssig brug af fingeraftryk/Face ID til oplåsning er lovlig som accessorium til ransagning, dataudlæsning af en beslaglagt mobiltelefon er retligt beslaglæggelse (ikke ransagning), og data indhentet af udenlandske myndigheder fra krypterede platforme er ikke undergivet dansk legalitetsprøvelse efter § 746. Selvinkrimineringsbeskyttelsen i § 752 og EMRK art. 6 sætter en klar grænse: sigtede kan tvinges til at afgive biometrisk adgang, men kan ikke kræves at oplyse en kode eller et password.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Tvangsmæssig brug af sigtedes fingeraftryk (Touch ID) eller ansigt (Face ID) til oplåsning af en mobiltelefon er lovlig som accessorium til ransagning og kan gennemtvinges på øjemedet uden forudgående retskendelse, når der er risiko for datatab (Højesteret 2019).
- 02** Sigtede kan ikke tvinges til at oplyse en PIN-kode, et password eller en anden videnbaseret adgangskode – det ville stride mod selvinkrimineringsforbuddet i retsplejelovens § 752 og EMRK art. 6.
- 03** Dataudlæsning af en beslaglagt mobiltelefon (fx via Cellebrite/UFED) udgør retligt en del af beslaglæggelsen efter § 802, stk. 1, og kræver dermed ikke selvstændig ransagningskendelse (Højesteret 2026).
- 04** EncroChat- og SKY ECC-data, der er tilvejebragt af franske og hollandske myndigheder, kan anvendes som bevis i danske straffesager (U.2023.1368 H).
- 05** Legalitetsprøvelse efter retsplejelovens § 746 kan som udgangspunkt ikke kræves for udenlandsk indhentede data, da prøvelsen vedrører dansk politis indgreb, ikke udenlandske efterforskningsskridt (Højesteret 2022).

- 06** Ransagning af mobiltelefoner og digitalt dataudtræk er underlagt proportionalitetskravet i § 797: indgrebet må ikke stå i misforhold til sagens betydning og den krænkelse, undersøgelsen forvolder.
- 07** Anklagemyndigheden skal i sager med krypteret kommunikation fremlægge en varedeklaration, et terminologiskema, en teknisk beskrivelse og en kvalitetskontrolrapport som forudsætning for bevisførelsen (Rigsadvokatmeddelelsen).
- 08** Oplysninger fra krypterede kommunikationstjenester er tekniske beviser, der altid indgår som ét blandt flere beviser og underlægges rettens frie bevisbedømmelse.
- 09** End-to-end-krypterede beskeder fra almindelige applikationer (Signal, WhatsApp, Telegram) er kun tilgængelige for politiet via dataudtræk fra en ulåst enhed eller fra modtagerens enhed – ikke via aflytning af kommunikationsstrømmen.
- 10** Cloud-data hos Apple, Google eller Microsoft kan kræves udleveret via edition efter § 804, eventuelt suppleret med international retshjælp, og vil fra august 2026 kunne indhentes direkte via europæiske editionskendelser efter e-evidence-forordningen (EU) 2023/1543.

§ 1 Retsgrundlag – ransagning, beslaglæggelse og digitale enheder

Digital bevisførelse i straffesager hviler på to parallelle regelsæt i retsplejeloven: reglerne om **ransagning** i [kapitel 73 \(§§ 793-800\)](#) og reglerne om **beslaglæggelse** i [kapitel 74 \(§§ 801-807\)](#).

Efter [§ 793, stk. 1](#) kan politiet foretage ransagning af bl.a. "boliger og andre husrum, dokumenter, papirer og lignende samt indholdet af aflåste genstande" (nr. 1) og "andre genstande samt lokaliteter uden for husrum" (nr. 2). En mobiltelefon er en "aflåst genstand" i bestemmelsens forstand, og en gennemgang af dens indhold er dermed formelt en ransagning – medmindre telefonen allerede er beslaglagt, og dataudlæsningen kvalificeres som beslaglæggelsens udøvelse (se nedenfor om Højesterets 2026-afgørelse).

Beslaglæggelse efter [§ 802, stk. 1](#) kræver, at den mistænkte med rimelig grund er mistænkt for en lovovertrædelse undergivet offentlig påtale, og at genstanden "kan tjene som bevis eller bør konfiskeres" eller er fravendt nogen, der kan kræve den tilbage.

Begge indgrebstyper er underlagt **proportionalitetskravet** i [§ 797](#), der bestemmer, at ransagning ikke må foretages, hvis det "efter undersøgelsens formål, sagens betydning og den krænkelse og ulempe, som undersøgelsen må antages at forvolde, ville være et uforholdsmæssigt indgreb." Kravet har særlig praktisk betydning ved digitale indgreb, hvor en komplet dataudlæsning af en mobiltelefon kan blotlægge hele borgerens privatliv.

For yderligere om beslaglæggelsesreglerne i bredere sammenhæng, se [beslaglæggelse og ransagning](#). For historiske teledata og mastelokalisering, se [teledata, cellemast og pejling](#).

LOV

[Retsplejeloven § 793, stk. 1](#)[Retsplejeloven § 797, stk. 1](#)[Retsplejeloven § 802, stk. 1](#)

§ 2 Tvangsmæssig oplåsning af mobiltelefon med fingeraftryk eller Face ID – Højesterets 2019-kendelse

Spørgsmålet om politiets adgang til at tvinge en sigtet til at anvende sit fingeraftryk (Touch ID) eller ansigt (Face ID) for at åbne en aflåst mobiltelefon blev afgjort af Højesteret i februar 2019.

I [Sag 92/2018](#) var en sigtet blevet anholdt og havde fået sin mobiltelefon beslaglagt i forbindelse med en narkotikasag. Politiet tvangsanbragte sigtedes finger på telefonens sensor for at låse den op, hvorefter telefonens indhold kunne gennemses. Forsvareren gjorde gældende, at tvangsmæssig brug af fingeraftryk krævede selvstændig lovhjemmel og stred mod selvinkrimineringsforbuddet.

Højesteret fastslog, at den tvangsmæssige brug af fingeraftryk var et **accessorium til ransagning** af en aflåst genstand, jf. [§ 793, stk. 1, nr. 1](#). Retten bemærkede, at der ikke var tale om at pålægge sigtede at afgive en forklaring eller aktivt bidrage med viden, men alene at anvende et fysisk kendetegn – svarende til at politiet anvender en nøgle til at åbne et aflåst skab. Indgrebet krænkede derfor ikke selvinkrimineringsbeskyttelsen i [§ 752](#).

Højesteret accepterede endvidere, at oplåsningen var sket **uden forudgående retskendelse**, da der var konkret risiko for, at data ville gå tabt (fx ved remote wipe eller timeout af biometrisk adgang). Politiet kunne handle på øjemedet for at sikre det processuelle formål med den allerede iværksatte ransagning.

Denne afgørelse fastslår den grundlæggende sontring i dansk ret:

- **Biometrisk adgang** (fingeraftryk, ansigt): lovlig tvang som accessorium til ransagning.
- **Videnbaseret adgang** (PIN-kode, password, mønster): kan ikke kræves oplyst, da det ville udgøre tvungen selvinkriminering.

LOV	Retsplejeloven § 752, stk. 1	Retsplejeloven § 793, stk. 1
PRAKSIS	Højesteret · Ransagning af mobiltelefon ved tvangsmæssig brug af fingeraftryk (Touch ID) uden retskendelse – proportionalitet og lovhjemmel 14.02.2019	
	Højesteret · Højesteret godkender ransagning af mobiltelefon ved tvungen brug af sigtedes fingeraftryk som accessorium til ransagning 14.02.2019	

§ 3 Dataudlæsning af beslaglagt mobiltelefon – beslaglæggelse, ikke ransagning (Højesteret 2026)

En central afklaring af det retlige fundament for digital bevissikring kom med Højesterets afgørelse [AM2026.06.04H2](#) fra juni 2026.

Sagen angik, om politiets dataudlæsning (typisk foretaget med forensic-værktøjer som Cellebrite UFED eller MSAB XRY) af en allerede beslaglagt mobiltelefon udgjorde en selvstændig ransagning – med de skærpede krav til retskendelse, der følger af [§§ 794-795](#) – eller om det var en del af den allerede gennemførte beslaglæggelse efter [§ 802](#).

Højesteret fastslog, at **dataudlæsningen udgør en del af beslaglæggelsen**, ikke en selvstændig ransagning. Begrundelsen var, at når politiet lovligt har beslaglagt en mobiltelefon med henblik på, at dens indhold kan tjene som bevis, jf. [§ 802, stk. 1, nr. 2](#), er den tekniske udlæsning af data et nødvendigt led i gennemførelsen af

beslaglæggelsens formål. At kopiering af data sker ved hjælp af forensic-software ændrer ikke indgrebets retlige karakter.

Afgørelsen har praktisk stor betydning, idet den fastslår, at:

- Dataudlæsning **ikke kræver selvstændig ransagningskendelse**, når telefonen allerede er lovligt beslaglagt.
- Proportionalitetsvurderingen efter [§ 805](#) (beslaglæggelsens proportionalitet) – ikke [§ 797](#) – er den relevante ramme.
- Forsvarerens prøvelsesmulighed vedrører beslaglæggelsens lovlighed efter [§ 806](#), herunder om omfanget af dataudlæsningen er proportionalt.

Sagen skal ses i sammenhæng med den generelle praksis om beslaglæggelse af mobiltelefoner i alvorlige straffesager, jf. fx [AM2026.01.30H](#), hvor Højesteret stadfæstede beslaglæggelse og ransagning af en mobiltelefon i en våbensag, hvor kildeoplysninger og fund af skydevåben begrundede indgrebet.

LOV	Retsplejeloven § 802, stk. 1	Retsplejeloven § 805	Retsplejeloven § 806
PRAKSIS	Højesteret · Højesteret: Dataudlæsning af beslaglagt mobiltelefon udgør del af beslaglæggelsen – ikke ransagning (AM2026.06.04H2) 04.06.2026		
	Højesteret · Højesterets stadfæstelse af beslaglæggelse og ransagning af mobiltelefon i sag om ulovlig våbenbesiddelse 30.01.2026		

§ 4 EncroChat og SKY ECC – krypteret kommunikation som bevis i straffesager

Siden 2020 har krypterede kommunikationsplatforme – navnlig EncroChat og SKY ECC – været et dominerende bevisinstrument i sager om organiseret narkotikakriminalitet, våbenhandel og banderelateret vold. Platformene adskiller sig fundamentalt fra almindelige krypterede apps (Signal, WhatsApp, Telegram), idet de kræver særligt tilvirkede telefoner med deaktiveret kamera, mikrofon og samtalefunktion, og er designet med hurtige slettefunktioner til brug ved anholdelse.

Efter [Rigsadvokatmeddelelsen om krypteret kommunikation fra særlige tjenester](#) modtager National enhed for Særlig Kriminalitet (NSK) data fra de franske og hollandske myndigheder via det internationale politisamarbejde. I marts 2020 lykkedes det de franske myndigheder at dekryptere EncroChat, og i marts 2021 blev SKY ECC kompromitteret i et samarbejde mellem belgiske, hollandske og franske myndigheder.

Højesteret har i [U.2023.1368 H](#) fastslået, at oplysninger fra EncroChat, der er tilvejebragt af udenlandske myndigheder, **kan bruges som bevis** i en dansk straffesag. Sagen angik en bandefuldbyrdsessag, hvor Højesteret stadfæstede politiets beslaglæggelse af mobiltelefoner trods visse formelle fejl.

I praksis fra landsretterne er EncroChat/SKY ECC-data anvendt bredt som bevis:

- I [SS-1306/2022-OLR](#) blev en omfattende narkotikasag ført på grundlag af krypteret kommunikation fra begge platforme.
- I [S-123-22](#) stadfæstede Østre Landsret, at EncroChat- og SKY ECC-data indhentet via international retshjælp kan anvendes som bevis.
- I [S-3450-23](#) afsagde Østre Landsret kendelse om dokumentation af krypteret korrespondance under hovedforhandlingen.

Oplysningerne fra krypterede kommunikationstjenester karakteriseres som et **teknisk bevis**, der i overensstemmelse med princippet om den frie bevisbedømmelse underlægges rettens konkrete vurdering. Som Rigsadvokatmeddelelsen udtrykker det:

Tekniske beviser vil altid indgå som ét blandt flere beviser i en straffesag, og betydningen af et bevis i form af oplysninger fra de krypterede kommunikationstjenester vil altid bero på en konkret vurdering af det enkelte bevis samt sagens samlede omstændigheder i øvrigt.

LOV

Retsplejeloven § 802, stk. 1

PRAKSIS

- | | |
|--|------------|
| Højesteret · Højesteret stadfæster anvendelse af EncroChat-data og godkender politiets beslaglæggelse af mobiltelefoner trods formelle fejl i bandefuldbyrdelsessag | 11.01.2023 |
| Landsretten · Kendelse om dokumentation af krypteret korrespondance fra EncroChat og SKY ECC i Østre Landsret | 18.09.2025 |
| Landsretten · Dom over omfattende narkotikanetværk: Smugling og videresalg af kokain og hash via skjulte rum og krypteret kommunikation | 07.09.2023 |
| Landsretten · Østre Landsret stadfæster byretskendelse: Encrochat og Sky ECC data indhentet via international retshjælp kan anvendes som bevis | 10.02.2022 |

§ 5 Legalitetsprøvelse af udenlandsk indhentede data – § 746

Et centralt procesretligt spørgsmål er, om forsvareren kan kræve **legalitetsprøvelse** efter [§ 746](#) af udenlandske myndigheders indhentelse af data fra krypterede platforme.

Højesteret afgjorde spørgsmålet i [SS-2/2022-HJR](#) i september 2022. Forsvareren gjorde gældende, at de franske myndigheders dekryptering af EncroChat-data udgjorde et efterforskningsindgreb, der skulle prøves efter danske processuelle regler, før data kunne fremlægges som bevis.

Højesteret afviste denne argumentation og fastslog, at [§ 746](#) alene vedrører **dansk politis** efterforskningsskridt. Franske myndigheders indhentelse af data fra EncroChat's servere i Frankrig var et fransk efterforskningsindgreb, gennemført efter fransk ret. Spørgsmålet om dette indgrebs lovlighed henhørte under franske domstole, ikke under danske.

Højesteret bemærkede endvidere, at legalitetsprøvelse efter [§ 746](#) som udgangspunkt ikke kan kræves **før hovedforhandlingen**. Det er under hovedforhandlingen, at retten tager stilling til bevisernes tilladelse og vægt, jf. [§ 841](#) (bevistilladelighed).

I landsretspraksis er dette princip fulgt konsekvent. I [SS-2559/2021-OLR](#) afviste Østre Landsret et kæremål vedrørende bevisførelse af EncroChat-data.

Princippet afspejler en grundlæggende forudsætning i international retshjælp: et efterforskningsskridt gennemført i en fremmed stat foretages i overensstemmelse med den fremmede stats love og regler. Danmark prøver ikke lovligheden af den fremmede stats interne processer.

Rigsadvokatmeddelelsen præciserer dog, at det franske kendelsesmateriale, der ligger til grund for indhentningen fra EncroChat og SKY ECC, som udgangspunkt **kan udleveres** til forsvareren – en fravigelse af det sædvanlige princip om, at udenlandsk kendelsesmateriale ikke indhentes. Baggrunden er, at de franske myndigheder allerede har udleveret materialet til brug for straffesager i andre europæiske lande.

LOV

[Retsplejeloven § 746](#)[Retsplejeloven § 841](#)

PRAKSIS

Højesteret · Højesterets kendelse om legalitetsprøvelse af EncroChat-bevis efter retsplejelovens § 746

27.09.2022

Landsretten · Kære af afgørelse om bevisførelse vedrørende Encro-chat data

07.10.2021

§ 6 Selvinkriminering – grænsen mod tvungen udlevering af kodeord og passwords

Selvinkrimineringsbeskyttelsen sætter en afgørende grænse for, hvad politiet kan kræve af en sigtet i forbindelse med digital bevissikring. Retsgrundlaget er [§ 752, stk. 1](#), der bestemmer, at sigtede "ikke er forpligtet til at udtale sig", samt EMRK art. 6 om retten til en retfærdig rettergang.

Som Højesterets 2019-kendelse om Touch ID fastslog, adskiller dansk ret mellem to typer adgang:

Adgangstype	Retlig kvalifikation	Kan kræves tvangsmæssigt?
Fingeraftryk / Face ID (biometrisk)	Fysisk kendetegn – accessorium til ransagning	Ja
PIN-kode / password / mønster (videnbaseret)	Forklaring / vidensafgivelse	Nej – selvinkriminering

Sondringen bygger på den internationalt anerkendte distinktion mellem "real evidence" (fysiske kendetegn som fingeraftryk, DNA, blodprøve) og "testimonial evidence" (vidnesbyrd/forklaringer). En kode eller et password er en **videnshandling** – sigtede bliver bedt om at kommunikere noget, han ved – og er dermed beskyttet af selvinkrimineringsforbuddet.

Denne grænse har konkret betydning:

- Politiet kan **ikke** kræve, at en sigtet oplyser sin PIN-kode, sit password, sit låsemønster, sin krypteringsnøgle til VeraCrypt/BitLocker, eller adgangskoden til en cloud-konto.
- Politiet **kan** – under de rette betingelser – tvinge sigtede til at anbringe sin finger på en sensor eller sit ansigt foran kameraet.
- End-to-end-krypterede beskeder i Signal, Telegram og WhatsApp er kun tilgængelige, hvis politiet kan åbne enheden via biometri eller forensic-bypass, eller indhente beskederne fra modtagerens enhed.

For en bredere behandling af EMRK art. 6 i dansk procesret, se [EMRK art. 6 – retfærdig rettergang](#).

LOV

[Retsplejeloven § 752, stk. 1](#)

PRAKSIS

Højesteret · Ransagning af mobiltelefon ved tvangsmæssig brug af fingeraftryk (Touch ID) uden retskendelse – proportionalitet og lovhjemmel

14.02.2019

§ 7 Proportionalitetskravet ved digitale tvangsindgreb og bulkudtræk

Proportionalitetsprincippet i § 797, stk. 1 har en særlig intensitet ved digitale ransagninger. En komplet dataudlæsning af en moderne smartphone kan blotlægge tusindvis af billeder, hele beskedhistorikker, GPS-lokationer, søgehistorik, helbredsdata og finansielle transaktioner – en langt mere indgribende undersøgelse end en traditionel husransagning.

Forarbejderne til 1997-reformen af retsplejelovens kapitel om ransagning (lov af 11. juni 1997) understreger, at proportionalitetsvurderingen skal inddrage:

- **Undersøgelsens formål:** hvad søges konkret bevist?
- **Sagens betydning:** lovovertrædelsens karakter og strafferamme.
- **Krænkelser og ulemper:** det privatlivsindgreb, ransagningen påfører.

I praksis fører dette til, at domstolene ved digitale indgreb skal vurdere, om et **begrænset udtræk** (fx kun beskeder i en bestemt tidsperiode eller kun bestemte applikationer) er tilstrækkeligt, eller om hele telefonens indhold skal udlæses.

I sager om organiseret kriminalitet – typisk narkotikahandel og bandekriminalitet – accepterer domstolene som udgangspunkt komplet dataudlæsning, fordi kriminalitetens systematiske karakter nødvendiggør en bred søgning. I [SS-65/2025-HJR](#) beslaglagde politiet mobiltelefoner fra flere tiltalte i en bandesag, og Højesteret stadfæstede indgrebet.

Også i landsretspraksis ses denne tendens, jf. [S-440-25](#), hvor beslaglæggelse af mobiltelefoner i en bandekonflikt blev godkendt.

For mindre alvorlige forhold – fx simpelt tyveri, færdselsovertrædelser eller dokumentfalsk – vil et komplet bulkudtræk af hele telefonens indhold derimod lettere kunne anses for uforholdsmæssigt. Her bør politiet søge at begrænse udtrækket til de data, der er relevante for det konkrete efterforskningsformål.

Privatlivets beskyttelse efter [EMRK art. 8](#) forstærker proportionalitetsvurderingen i det omfang, indgrebet berører korrespondance og privat kommunikation.

LOV

[Retsplejelovent § 797, stk. 1](#)

PRAKSIS

Højesteret · Højesteret stadfæster beslaglæggelse af tre mobiltelefoner hos bandetilknyttet i sag om overtrædelse af knivloven

06.02.2026

Landsretten · Østre Landsret stadfæster beslaglæggelse af mobiltelefoner i sag om bandekonflikt trods dissens

06.05.2025

§ 8 Anklagemyndighedens dokumentationskrav – varedeklaration og kvalitetskontrol

I sager hvor bevismaterialet stammer fra krypterede kommunikationstjenester, stiller [Rigsadvokatmeddelelsen om krypteret kommunikation fra særlige tjenester](#) krav om, at anklageren sikrer udarbejdelsen af fire dokumenter:

- **Varedeklaration:** beskriver tilvejebringelsen og behandlingen af data fra den krypterede tjeneste, herunder eventuelle fejl og usikkerheder ved brugen af oplysningerne som bevis. Rigspolitiet har udarbejdet selvstændige varedeklarationer for henholdsvis [EncroChat](#) og [SKY ECC](#).
- **Terminologiskema:** forklarer tekniske begreber for straffesagens aktører.
- **Teknisk beskrivelse:** redegør for den standardiserede databehandling af den pågældende platform.
- **Kvalitetskontrolrapport:** dokumenterer politiets kontrol af data i den konkrete sag, herunder hvilke data der er indhentet, hvordan kvaliteten er kontrolleret, og hvilke relevante usikkerheder og fejlkilder der er identificeret.

Alle fire dokumenter skal bilagere sagen og dokumenteres under hovedforhandlingen i relevant omfang, **inden** der gøres brug af oplysninger fra den krypterede tjeneste.

Rigsadvokatmeddelelsen fremhæver en række [opmærksomhedspunkter ved anvendelsen af oplysningerne](#):

- Dekrypteringen af data foregår ofte løbende, og de datapakker politiet modtager, er ikke nødvendigvis fuldt dækkende for al kommunikation på en brugerprofil.
- Oplysningerne kan indeholde teledata, og de samme opmærksomhedspunkter som ved øvrige teledata gælder – se [Rigsadvokatmeddelelsen om teledata i straffesager](#).
- Hvis teledata stammer fra udenlandske teleudbydere, skal der ikke foretages en vurdering af, om det pågældende lands regler er i overensstemmelse med EU-Domstolens logningsafgørelser.

Under hovedforhandlingen skal de **bearbejdede** oplysninger dokumenteres. De originale data fra "ejerlandet" bør dog være til stede i retten til brug for behandling af eventuelle spørgsmål om uoverensstemmelser.

PRAKSIS **Højesteret** · Højesteret stadfæster anvendelse af EncroChat-data og godkender politiets beslaglæggelse af mobiltelefoner trods formelle fejl i bandefuldbyrdelsessag 11.01.2023

Cloud-data og edition – adgang til data hos Apple, Google og Microsoft

En stigende andel af digitalt bevismateriale befinder sig ikke på selve den fysiske enhed, men i cloud-tjenester hos store teknologivirksomheder (Apple iCloud, Google Drive/Gmail, Microsoft OneDrive/Outlook, Dropbox m.fl.). Data kan også være synkroniseret mellem flere enheder eller slettet lokalt men fortsat tilgængeligt i skyen.

Adgangen til cloud-data reguleres primært via **edition** efter [§ 804](#), der giver retten mulighed for at pålægge tredjemænd at udlevere genstande eller dokumenter af betydning for efterforskningen. Editionsplæg kan rettes mod den dataansvarlige – typisk teleudbyderen eller cloud-tjenesteudbyderen.

Når tjenesteudbyderen befinder sig i udlandet – hvilket er tilfældet for Apple (Irland/USA), Google (Irland/USA) og Microsoft (Irland/USA) – rejser sig spørgsmålet om **international retshjælp**. Traditionelt har Danmark skullet anmode det pågældende lands myndigheder om assistance, hvilket kan indebære betydelige forsinkelser.

E-evidence-forordningen (EU) 2023/1543 og det ledsagende direktiv (EU) 2023/1544 – der finder anvendelse fra 18. august 2026 – indfører en ny mekanisme med **europæiske editionskendelser** og **sikringskendelser**, der kan rettes direkte mod tjenesteudbydere med forretningssted eller retlig repræsentant i EU. Forordningen eliminerer det mellemliggende nationale myndighedsled og reducerer dermed forsinkelserne betydeligt.

Danmark har med [bekendtgørelse om udpegning af central myndighed](#) implementeret dele af direktivet. Politiet kan pålægge tjenesteudbydere tvangsbøder ved manglende efterlevelse af påbud.

For en bredere behandling af editionsreglerne, se [editionspålæg](#). For logning og sletning af teledata, se [Rigsadvokatmeddelelsen om logning](#) og [Rigsadvokatmeddelelsen om sletning af teledata](#).

LOV

[Retsplejeloven § 804](#)

PRAKSIS

Højesteret · Højesterets kendelse om edition og beslaglæggelse i skattesag vedrørende udenlandske betalingskort

09.02.2010

§ 10 End-to-end-krypterede beskeder og forsvarerens aktindsigt

End-to-end-krypterede beskeder i almindelige applikationer (Signal, Telegram, WhatsApp, iMessage) adskiller sig grundlæggende fra EncroChat/SKY ECC-data. Kommunikationen er krypteret mellem afsender og modtager, og hverken tjenesteudbyder eller politiet kan læse beskederne ved aflytning af kommunikationsstrømmen. For den processuelle praksis om [telefon- og rumaflytning](#) er dette en afgørende begrænsning.

Politiet kan kun få adgang til end-to-end-krypterede beskeder via:

- **Dataudtræk fra en ulåst enhed** – enten ved biometrisk tvangsoplåsning eller ved forensic-bypass (Cellebrite/UFED kan i visse tilfælde udlæse data fra låste enheder afhængigt af model og softwareversion).
- **Dataudtræk fra modtagerens enhed** – beskederne findes typisk på begge parter enheder.
- **Cloud-backup** – hvis afsender eller modtager har backup af beskeder i iCloud, Google Drive eller lignende (disse backups er ikke nødvendigvis end-to-end-krypterede og kan kræves udleveret via edition).

Forsvarerens aktindsigt i råudtrækket er et tilbagevendende procesretligt spørgsmål. Når politiet foretager en komplet dataudlæsning af en mobiltelefon, genereres en omfattende forensic-rapport (typisk fra Cellebrite UFED eller MSAB XRY), der indeholder alle udlæste data – herunder billeder, beskeder, GPS-lokationer, appdata m.v. Forsvareren kan efter omstændighederne kræve aktindsigt i hele råudtrækket, ikke kun de dele politiet har udvalgt som relevante for sagen.

I sager med EncroChat/SKY ECC-data gælder særlige regler om forsvarerens aktindsigt. Efter [§ 729 c](#) kan visse oplysninger undtages fra forsvarerens adgang, hvis hensynet til efterforskningens gennemførelse, beskyttelse af fortrolige oplysningskilder eller lignende hensyn taler for det. Rigsadvokatmeddelelsen fastslår dog, at det franske kendelsesmateriale som udgangspunkt kan udleveres til forsvareren i EncroChat/SKY ECC-sager.

LOV

[Retsplejeloven § 729c](#)

§ 11 Sammenfatning – centrale retningslinjer for digital bevisførelse

Retspraksis og Rigsadvokatmeddelelserne tegner et klart billede af rammerne for digital bevisførelse i dansk strafferet:

Fysisk adgang til enheden:

- Mobiltelefoner kan beslaglægges efter § 802 som genstande, der kan tjene som bevis.
- Biometrisk tvangsoplåsning (fingeraftryk/Face ID) er lovlig som accessorium til ransagning.
- Krav om kodeord/PIN er forbudt som selvinkriminering.

Dataudlæsning:

- Dataudlæsning af en beslaglagt enhed er retligt en del af beslaglæggelsen (ikke selvstændig ransagning).
- Proportionalitetskravet nødvendiggør en vurdering af udlæsningens omfang i forhold til sagens karakter.

Krypteret kommunikation fra særlige tjenester:

- EncroChat/SKY ECC-data kan anvendes som bevis i danske straffesager.
- Legalitetsprøvelse efter § 746 retter sig mod dansk politis indgreb, ikke udenlandske myndigheders.
- Anklagemyndigheden skal fremlægge varedeklaration, kvalitetskontrolrapport, terminologiskema og teknisk beskrivelse.

Cloud-data og international dimension:

- Cloud-data kan indhentes via edition efter § 804, evt. suppleret med international retshjælp.
- E-evidence-forordningen (EU) 2023/1543 vil fra august 2026 muliggøre direkte europæiske editionskendelser mod tjenesteudbydere i EU.

Området er i hastig udvikling – nye krypterede platforme erstatter nedlukkede, forensic-værktøjerne udvikles konstant, og EU-reglerne om grænseoverskridende e-beviser træder i kraft i 2026. Retspraksis kan forventes at adressere yderligere spørgsmål om proportionalitet ved bulkudtræk, bevisægtighed af genskabte slettede data og grænserne for forsvarerens aktindsigt i komplette dataudtræk.

LOV	Retsplejeloven § 746	Retsplejeloven § 802	Retsplejeloven § 804
PRAKSIS	Højesteret · Højesteret: Dataudlæsning af beslaglagt mobiltelefon udgør del af beslaglæggelsen – ikke ransagning (AM2026.06.04H2) 04.06.2026		
	Højesteret · Højesteret stadfæster anvendelse af EncroChat-data og godkender politiets beslaglæggelse af mobiltelefoner trods formelle fejl i bandefuldbyrdsessag 11.01.2023		
	Højesteret · Højesterets kendelse om legalitetsprøvelse af EncroChat-bevis efter retsplejelovens § 746 27.09.2022		
	Højesteret · Ransagning af mobiltelefon ved tvangsmæssig brug af fingeraftryk (Touch ID) uden retskendelse – proportionalitet og lovhjemmel 14.02.2019		

REFERENCE Lovgrundlag

6 paragraffer

Retsplejeloven § 746	Retsplejeloven § 752 stk. 1
Retsplejeloven § 793 stk. 1	Retsplejeloven § 797 stk. 1
Retsplejeloven § 802 stk. 1	Retsplejeloven § 804

MATERIALE Citerede afgørelser

14 afgørelser

HØJESTERET · ØVERSTE INSTANS

8

04.06.2026	Højesteret: Dataudlæsning af beslaglagt mobiltelefon udgør del af beslaglæggelsen – ikke ransagning (AM2026.06.04H2)	5/2026
06.02.2026	Højesteret stadfæster beslaglæggelse af tre mobiltelefoner hos bandetilknyttet i sag om overtrædelse af knivloven	10436-12289
30.01.2026	Højesterets stadfæstelse af beslaglæggelse og ransagning af mobiltelefon i sag om ulovlig våbenbesiddelse	AM2026.01.30H
11.01.2023	Højesteret stadfæster anvendelse af EncroChat-data og godkender politiets beslaglæggelse af mobiltelefoner trods formelle fejl i bandefuldbyrdelsessag	U.2023.154 H
27.09.2022	Højesterets kendelse om legalitetsprøvelse af EncroChat-bevis efter retsplejelovens § 746	2237-2664
14.02.2019	Ransagning af mobiltelefon ved tvangsmæssig brug af fingeraftryk (Touch ID) uden retskendelse – proportionalitet og lovhjemmel	Sag 92/2018
14.02.2019	Højesteret godkender ransagning af mobiltelefon ved tvungen brug af sigtedes fingeraftryk som accessorium til ransagning	
09.02.2010	Højesterets kendelse om edition og beslaglæggelse i skattesag vedrørende udenlandske betalingskort	Sag 138/2009

LANDSRETTE · ANKEINSTANS

5

18.09.2025	Kendelse om dokumentation af krypteret korrespondance fra EncroChat og SKY ECC i Østre Landsret	S-3450-23
06.05.2025	Østre Landsret stadfæster beslaglæggelse af mobiltelefoner i sag om bandekonflikt trods dissens	9967-11661
07.09.2023	Dom over omfattende narkotikanetværk: Smugling og videresalg af kokain og hash via skjulte rum og krypteret kommunikation	5758-6877
10.02.2022	Østre Landsret stadfæster byretskendelse: Encrochat og Sky ECC data indhentet via international retshjælp kan anvendes som bevis	S-123-22
07.10.2021	Kære af afgørelse om bevisførelse vedrørende Encro-chat data	2227-2651

PARKERINGSKLAGENÆVNET · NÆVN / KLAGEINSTANS

1

30.08.2024	Afgift annulleret: Defekt kvitteringsfunktion forhindrede kontrol af p-billet ved Cabinn Metro	park-2664
------------	--	-----------