

PRAKSISOVERSIGT · PENGE OG FINANSVÆSEN

Praksisoversigt over hvidvask via kryptovaluta og digitale aktiver

Straffeloven § 290/§ 290 a, hvidvaskloven og den regulatoriske ramme for digitale aktiver

Version 2 Opdateret 26. jun. 2026 5 afgørelser · 2015-2025

[Læs online](#)

INTRODUKTION

Hvidvask via kryptovaluta og digitale aktiver reguleres i dansk ret primært af straffelovens § 290 (hæleri) og § 290 a (hvidvask), suppleret af hvidvasklovens krav om kundekendskab, underretningspligt og risikostyring for udbydere af kryptoaktivtjenester. Forarbejderne til § 290 a fastslår udtrykkeligt, at virtuelle valutaer som Bitcoin ikke udgør "penge" i bestemmelsens forstand, men at investering af kriminelt udbytte i kryptovaluta er dækket som "konvertering". Den danske retspraksis på området er fortsat i udvikling, med Højesterets dom af 29. januar 2025 (SS-64/2024-HJR) som det centrale præjudikat for fortolkningen af hvidvaskbegrebet under § 290 a, mens den regulatoriske ramme er under markant udbygning med EU's MiCA-forordning og TFR-forordningen om overførsel af kryptoaktiver.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Virtuelle valutaer som Bitcoin udgør ikke "penge" i straffelovens § 290 a's forstand, men investering af kriminelt udbytte i kryptovaluta er dækket som "konvertering" af penge.
- 02** Veksling af kriminelt udbytte til en anden valuta udgør som udgangspunkt hvidvask efter § 290 a, stk. 1, uanset om de omvekslede midler efterfølgende anvendes til ny kriminalitet.
- 03** Selvhvidvask – dvs. at gerningsmanden selv hvidvasker udbyttet af sin egen kriminalitet – er strafbart efter § 290 a, men ikke efter § 290 (hæleri).
- 04** Udbydere af kryptoaktivtjenester er underlagt hvidvaskloven som forpligtede enheder, jf. hvidvasklovens § 1, stk. 1, nr. 22, og skal opfylde krav om kundekendskab, risikovurdering og underretningspligt.
- 05** Underretningspligten i hvidvasklovens § 26 indebærer, at kryptobørser skal underrette Hvidvasksekretariatet ved mistanke om hvidvask eller terrorfinansiering – også inden gennemførelse af transaktioner.
- 06** Konfiskation af kryptovaluta og digitale aktiver kan ske efter straffelovens § 75, stk. 1, som udbytte af en strafbar handling eller som surrogatværdi, og efter § 76 a med omvendt bevisbyrde ved grove forbrydelser.
- 07** Privacy coins (fx Monero), mixers/tumblers og scramblers identificeres i Finanstilsynets vejledning som skærpede risikoindikatorer, der kræver forstærkede kundekendskabsprocedurer.

- 08** EU's TFR-forordning (2023/1113) og MiCA-forordningen (2023/1114) indfører krav om sporbarhed af kryptoaktivoverførsler og tilsynsramme for kryptoaktivtjenesteudbydere – gennemført i dansk ret ved bl.a. bekendtgørelse om risikobegrænsende foranstaltninger ved overførsel af kryptoaktiver.
- 09** Kryptobørser skal anvende DLT-analyseværktøjer ved overførsler til eller fra selvhostede adresser for at vurdere hvidvaskrisiko, jf. bekendtgørelse nr. 1143/2024.
- 10** Ved blandet finansiering af aktiver (delvist kriminelt, delvist lovligt udbytte) kan kun den del der udgør kriminelt udbytte konfiskeres – ikke hele aktivet – jf. Højesterets dom i sag 136/2015.

§ 1 Straffelovens § 290 (hæleri) og § 290 a (hvidvask) – sondringen og kryptoaktivernes placering

Den strafferetlige regulering af hvidvask og hæleri hviler på to parallelle bestemmelser: [straffelovens § 290](#) om hæleri og [§ 290 a](#) om hvidvask. Sondringen mellem de to er afgørende for kryptorelaterede sager.

[§ 290](#) straffer den, der uberettiget modtager eller skaffer sig eller andre del i udbytte opnået ved en strafbar lovovertrædelse. Bestemmelsen dækker *hæleri* i bred forstand, men omfatter **ikke** selvhvidvask – dvs. at gerningsmanden selv skjuler udbyttet af sin egen kriminalitet.

[§ 290 a](#), der blev indsat ved **lov nr. 711 af 8. juni 2018**, kriminaliserer specifikt *hvidvask*: at konvertere eller overføre penge, som direkte eller indirekte er udbytte af en strafbar lovovertrædelse, for at skjule eller tilsløre den ulovlige oprindelse. Selvhvidvask er udtrykkeligt omfattet af denne bestemmelse.

Strafferammen for simpel hvidvask er bøde eller fængsel indtil 1 år og 6 måneder. Ved hvidvask af *særligt grov beskaffenhed* – navnlig pga. erhvervsmæssig eller professionel karakter eller størrelsen af vinding – kan straffen stige til fængsel i 8 år, jf. [§ 290 a, stk. 2](#).

Et centralt fortolkningsspørgsmål for kryptorelaterede sager er, om kryptovaluta udgør "penge" i § 290 a's forstand. Forarbejderne til bestemmelsen tager eksplicit stilling:

De virtuelle valutaer, som kendes i dag (f.eks. bitcoin), har ikke en sådan funktion som almindeligt betalingsmiddel, at de udgør penge i bestemmelsens forstand.

Konsekvensen er, at den *første konvertering til penge* af udbytte i anden form end penge (herunder kryptovaluta) falder uden for § 290 a's ordlyd. Derimod er investering af kriminelt udbytte i kryptovaluta klart dækket:

Investering af pengene, være sig i værdipapirer, fast ejendom eller andet, vil også være en konvertering af pengene, der er strafbar efter den foreslåede bestemmelse, når det sker med det formål at skjule eller tilsløre pengenes ulovlige oprindelse. Dette gælder også ved investering i (køb af) virtuel valuta (f.eks. bitcoin).

Som [Rigsadvokatmeddelelsen om formueforbrydelser](#) præciserer, er den praktiske konsekvens at:

- **Fiat → krypto:** Hvidvask efter § 290 a (investering/konvertering af penge til virtuel valuta)
- **Krypto → fiat:** Kan udgøre hæleri efter § 290 (modtagelse af udbytte), men ikke hvidvask efter § 290 a medmindre det fiat-beløb der modtages derefter konverteres videre
-

Krypto → krypto: Falder i udgangspunktet uden for § 290 a's ordlyd (da krypto ikke er "penge"), men kan efter omstændighederne udgøre hæleri efter § 290

LOV

Straffeloven § 290

Straffeloven § 290a, stk. 1, 2

§ 2 Højesterets dom af 29. januar 2025 – omveksling af narkotikapenge som hvidvask

Det centrale præjudikat for fortolkningen af § 290 a er Højesterets dom af 29. januar 2025 i sag [SS-64/2024-HJR](#). Sagen vedrørte en syrisk statsborger, der i perioden december 2020 til april 2022 modtog og omvekslede pengebeløb i danske kroner stammende fra organiseret narkotikasalg for at skjule udbyttets ulovlige oprindelse.

Oversigt over de pådømte beløb:

Forhold	Karakter	Beløb
1-15	Hvidvask af særligt grov beskaffenhed	9.135.500 kr.
1-15 (delvis)	Forsøg på hvidvask	900.000 kr.
17	Hæleri af særligt grov beskaffenhed	415.200 kr. og 31.700 euro

Forsvarets centrale anbringende var, at § 290 a kun finder anvendelse, når formålet med omvekslingen er at *legalisere* udbyttet – dvs. at kanalisere det ind i lovlige erhvervsaktiviteter. Da de omvekslede penge angiveligt skulle bruges til at købe mere narkotika, kunne det efter forsvarets opfattelse ikke kvalificeres som hvidvask.

Højesteret afviste dette synspunkt:

Højesteret finder, at straffelovens § 290 a efter sin ordlyd og forarbejderne må forstås således, at der som udgangspunkt er tale om hvidvask, når penge, der er udbytte af kriminalitet, veksles til en anden valuta, idet omveksling er egnet til at skjule eller tilsløre udbyttets ulovlige oprindelse. Der er ikke grundlag for at fravige udgangspunktet, når de omvekslede penge skal bruges til at begå ny kriminalitet.

Dommen fastslår således, at det er selve *handlingen* – vekslingen – der konstituerer hvidvask, når den er egnet til at skjule den ulovlige oprindelse. Formålet med de omvekslede midler (om de bruges lovligt eller til ny kriminalitet) er uden betydning.

Straffen blev fastsat til 2 år og 6 måneders fængsel med udvisning og indrejseforbud i 6 år. Konfiskation af 31.700 euro, 415.200 kr., elektronisk pengetæller og mobiltelefon blev stadfæstet i medfør af § 75.

Dommens principielle betydning for kryptosager er, at *enhver veksling* af kriminelt udbytte – herunder veksling fra fiat til kryptovaluta – som udgangspunkt er hvidvask, forudsat at vekslingen er egnet til at skjule eller tilsløre den ulovlige oprindelse. Det kræves ikke, at formålet er "legalisering".

LOV

Straffeloven § 75

Straffeloven § 290a, stk. 1, 2

PRAKSIS

Højesteret · Højesteret stadfæster dom for hvidvask af narkotikapenge efter Straffelovens § 290 a

29.01.2025

§ 3

Hvidvasklovens dækning af kryptoaktivtjenesteudbydere

Hvidvaskloven (lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme) pålægger en række forpligtede enheder krav om kundekendskab, risikovurdering, overvågning og underretning. Kryptoaktivtjenesteudbydere er udtrykkeligt omfattet.

[Hvidvasklovens § 1, stk. 1, nr. 22](#) fastslår, at loven gælder for:

Udbydere af kryptoaktivtjenester.

Bestemmelsen suppleres af nr. 23 og nr. 24, der omfatter henholdsvis udstedere af aktivbaserede tokens og udstedere af e-pengetokens. Dermed er hele bredden af kryptoaktivtjenester – fra veksling og handel til deponering og porteføljepleje – underlagt hvidvasklovens forpligtelsesregime.

De centrale forpligtelser for kryptobørser og andre kryptoaktivtjenesteudbydere omfatter:

- **Kundekendskabsprocedurer (KYC):** Identifikation og verifikation af kunders identitet, herunder reelle ejere, jf. hvidvasklovens kapitel 3
- **Risikovurdering:** Løbende vurdering af risikoen for hvidvask og terrorfinansiering forbundet med kundeforhold og transaktioner
- **Overvågning:** Løbende overvågning af transaktioner med henblik på at opdage usædvanlige eller mistænkelige mønstre
- **Underretningspligt:** Pligt til at underrette Hvidvasksekretariatet ved mistanke om hvidvask eller terrorfinansiering, jf. [§ 26](#)

[Hvidvasklovens § 26, stk. 1](#) bestemmer, at virksomheder og personer omfattet af loven skal underrette Hvidvasksekretariatet, hvis de er vidende om, har mistanke om eller rimelig grund til at formode, at en transaktion, midler eller en aktivitet har eller har haft tilknytning til hvidvask eller terrorfinansiering. Underretningen skal som udgangspunkt ske *inden* transaktionen gennemføres, jf. [§ 26, stk. 4](#), og transaktionen må ikke gennemføres uden Hvidvasksekretariatets samtykke, medmindre det er umuligt at undlade at gennemføre den.

Denne underretningspligt har særlig praktisk betydning for kryptobørser, da kryptoaktivoverførsler kan gennemføres hurtigt og irreversibelt – i modsætning til traditionelle banktransaktioner, der lettere kan tilbageholdes.

LOV

[Hvidvaskloven § 1, stk. 1](#)

[Hvidvaskloven § 26, stk. 1, 4](#)

Finanstilsynets vejledning om kryptospecifikke risikofaktorer – § 4 privacy coins, mixers og tumblers

[Finanstilsynets vejledning om hvidvaskloven](#) indeholder detaljerede retningslinjer for kryptoaktivtjenesteudbyderes håndtering af hvidvaskrisici. Vejledningen identificerer en række teknologiske og transaktionsmæssige risikofaktorer, der er særegne for kryptovalutamarkedet.

Vejledningen fremhæver følgende som skærpede risikoindikatorer:

- **Privacy coins** (fx Monero, Zcash): Kryptovalutaer med indbyggede anonymiseringsmekanismer, der vanskeliggør sporbarhed
- **Mixers/tumblers/scramblers**: Tjenester der blander kryptovalutaoverførsler fra flere brugere for at tilsløre forbindelsen mellem afsender og modtager
- **Peer-to-peer (P2P) overførsler**: Direkte overførsler uden mellemmand, der vanskeliggør identifikation
- **Decentraliserede børser (DEX)**: Handelsplatforme uden central kontrol eller KYC-krav
- **Selvhostede wallets** ("unhosted wallets"): Kryptovaluta opbevaret i brugerens egen wallet uden en tjenesteudbyders kontrol

Ved forekomst af disse risikofaktorer skal kryptoaktivtjenesteudbydere anvende *forstærkede kundekendelsesprocedurer*, herunder:

- Indhentning af yderligere oplysninger om kundens formål med handlen
- Skærpet overvågning af transaktionsmønstre
- Analyse af blockchain-transaktioner med DLT-analyseværktøjer
- Vurdering af om underretningspligten er udløst

Vejledningen omtaler specifikt, at vekslingstjenester for virtuelle valutaer skal være opmærksomme på kunder, der foretager hyppige overførsler mellem forskellige kryptovalutaer (cross-chain-overførsler), store engangsoverførsler til selvhostede wallets, eller overførsler med tilknytning til jurisdiktioner med svag AML-regulering.

LOV

Hvidvaskloven § 1, stk. 1

Bekendtgørelsen om selvhostede adresser og krav om § 5 DLT-analyseværktøjer

Bekendtgørelse nr. 1143 af 14. november 2024 ([bekendtgørelse om gennemførelse af risikobegrænsende foranstaltninger ved overførsel af kryptoaktiver rettet mod eller stammende fra en selvhostet adresse](#)) gennemfører i dansk ret EU's krav om sporbarhed af kryptoaktivoverførsler til og fra selvhostede adresser.

Bekendtgørelsen er udstedt med hjemmel i hvidvaskloven og pålægger udbydere af kryptoaktivtjenester at:

- **Anvende DLT-analyseværktøjer** (Distributed Ledger Technology-analyse, fx Chainalysis, Elliptic) til at vurdere risikoen ved overførsler til eller fra selvhostede adresser
- **Indhente oplysninger** om ordregiverens eller ordremodtagerens identitet ved overførsler til/fra selvhostede adresser
- **Foretage risikovurdering** af om den selvhostede adresse er forbundet med kriminelle aktiviteter, sanktionslister eller andre risikofaktorer
- **Dokumentere analyseresultater** og stille dem til rådighed for tilsynsmyndigheder

Kravet om DLT-analyseværktøjer er bemærkelsesværdigt, da det formaliserer den praksis, som retshåndhævende myndigheder som SØIK (Statsadvokaten for Særlig Økonomisk og International Kriminalitet) allerede anvender i efterforskningen af kryptorelateret kriminalitet. Blockchain-analyseværktøjer som Chainalysis gør det muligt at spore kryptoaktivoverførsler på offentlige blockchains, identificere klynger

af adresser tilhørende samme entitet, og flagge forbindelser til kendte kriminelle wallets eller sanctionerede adresser.

Supplerende er [bekendtgørelse om indberetningspligt for udbydere af kryptoaktivtjenester](#) (nr. 1155/2025) indført, som pålægger udbyderne indberetningspligt til skattemyndighederne vedrørende kunders kryptoaktivtransaktioner.

LOV

[Hvidvaskloven § 1, stk. 1](#)[Hvidvaskloven § 26](#)

Konfiskation af kryptovaluta og digitale aktiver efter straffelovens §§ 75-76 a

Konfiskation af kryptovaluta og digitale aktiver kan ske efter de almindelige konfiskationsregler i [straffelovens § 75](#) og de udvidede konfiskationsregler i [§ 76 a](#).

[§ 75, stk. 1](#) hjemler konfiskation af "udbytte, der er opnået ved en strafbar lovovertrædelse", herunder genstande der er trådt i stedet for udbyttet. Kryptovaluta, der repræsenterer kriminelt udbytte – fx Bitcoin købt med narkotikapenge – kan således konfiskeres som surrogatværdi.

[§ 75, stk. 2](#) hjemler konfiskation af "genstande, der har været brugt eller bestemt til at bruges ved en strafbar lovovertrædelse", herunder hardware wallets, computere med kryptografiske nøgler og elektroniske enheder anvendt til at gennemføre hvidvasktransaktioner.

Højesterets dom af 29. januar 2025 ([SS-64/2024-HJR](#)) stadfæstede konfiskation af pengetællemaskine, mobiltelefon og kontante midler i medfør af [§ 75](#) i en hvidvaksag.

Ved grove forbrydelser (med strafferamme på 6 års fængsel eller mere) kan [§ 76 a, stk. 1](#) anvendes med omvendt bevisbyrde: alle formuegoder tilhørende den domfældte kan konfiskeres, medmindre den pågældende sandsynliggør, at de er erhvervet på lovlig måde. Denne bestemmelse er særlig relevant for kryptorelaterede sager, da kryptovaluta i en selvhostet wallet ofte er vanskelig for anklagemyndigheden at spore til et specifikt kriminelt forhold.

Højesterets dom af 3. december 2015 ([Sag 136/2015](#)) fastslog en vigtig begrænsning ved blandet finansiering:

På baggrund af forarbejderne til straffelovens § 76 a sammenholdt med de nævnte omstændigheder finder Højesteret, at det uanset oplysningerne om T1's beskedne indtægtsforhold må anses for tilstrækkeligt sandsynliggjort, at den del af købesummen for ejendommen [...] som overstiger 3,1 mio. kr., er betalt med lovligt erhvervede midler.

Dommen illustrerer, at når et aktiv (fx en kryptovalutabeholdning) er anskaffet med en blanding af kriminelt og lovligt erhvervede midler, kan kun den kriminelle andel konfiskeres. Det er anklagemyndighedens bevisbyrde at godtgøre den kriminelle andels omfang, med mindre [§ 76 a](#)'s omvendte bevisbyrde finder anvendelse.

Praktisk konfiskation af kryptovaluta kræver adgang til den domfældtes private nøgler (private keys). Uden disse er det teknisk umuligt at overføre kryptovalutaen. Politiet kan beslaglægge hardware wallets og elektroniske enheder, men hvis nøglerne er memoriserede eller opbevaret uden for dansk jurisdiktion, kan konfiskationen i praksis blive vanskelig at gennemføre.

LOV

[Straffeloven § 75, stk. 1, 2](#)[Straffeloven § 76a, stk. 1, 4](#)

Højesteret: Højesteret stadfæster dom for hvidvask af narkotikapenge efter [Straffelovens § 290 a](#) om konfiskation af fast ejendom købt med midler fra grovt særlig.

udbyttekonfiskation

Hvidvask via kryptovaluta og digitale aktiver

09.12.2025

PRAKSIS

§ 7 Bitcoin som kriminalitetsinstrument – afpresning og hacking

Ud over hvidvask optræder kryptovaluta i dansk retspraksis som betalingsmiddel i forbindelse med anden kriminalitet, navnlig afpresning og IT-kriminalitet.

I byretssagen [SS 1-31954/2015](#) blev tiltalte dømt for omfattende afpresning og hacking mod behandlingssteder og forsikringsselskaber, hvor kravet om betaling blev stillet i Bitcoin. Sagen illustrerer det fænomen, der er velkendt fra *ransomware*-angreb: kryptovalutaens pseudonyme karakter gør det muligt at modtage betalinger uden at afsløre modtagerens identitet.

I sådanne tilfælde kan kryptovalutaen udgøre:

- **Udbytte** af den strafbare handling (afpresningsbeløbet betalt i Bitcoin) → konfiskation efter [§ 75, stk. 1](#)
- **Redskab** til den strafbare handling (den wallet-adresse der anvendes til at modtage betaling) → konfiskation efter [§ 75, stk. 2](#)

Blockchain-analyse spiller en central rolle i efterforskningen af sådanne sager, da politiet via offentligt tilgængelige transaktionsdata på blockchains kan spore betalingsstrømme fra ofrets wallet til den kriminelles wallet og videre til eventuelle kryptobørser, hvor identifikation kan ske via KYC-oplysninger.

LOV

[Straffeloven § 75, stk. 1, 2](#)

PRAKSIS

Byretten · Betinget fængsel for omfattende afpresning og hacking mod behandlingssted og forsikringsselskaber

09.05.2016

§ 8 EU-regulering: MiCA-forordningen og TFR-forordningen om kryptoaktiver

Den EU-retlige ramme for kryptoaktiver og bekæmpelse af hvidvask gennem digitale aktiver er fundamentalt omlagt med vedtagelsen af to forordninger i 2023:

MiCA-forordningen ([forordning \(EU\) 2023/1114](#)) – Markets in Crypto-Assets Regulation – indfører et samlet tilsynsregime for kryptoaktivtjenesteudbydere i EU. Forordningen kræver bl.a.:

- Tilladelse til udbydere af kryptoaktivtjenester (veksling, deponering, handel, porteføljepleje mv.), jf. [art. 60](#)
- Krav om interne kontrolmekanismer og politikker til forebyggelse af hvidvask i overensstemmelse med 4. hvidvaskdirektiv
- Kundekendskabskrav (KYC) ved optagelse af kunder på handelsplatforme, jf. [art. 76](#)
- Krav om hvidbøger (white papers) ved udbud af kryptoaktiver

TFR-forordningen ([forordning \(EU\) 2023/1113](#)) – Transfer of Funds Regulation, også kaldet EU's "Travel Rule" for krypto – udvider de eksisterende sporbarhedskrav for pengeoverførsler til også at gælde overførsler af kryptoaktiver. Forordningen kræver, at:

- Ordregiverens og ordremodtagerens identitetsoplysninger medsendes ved overførsler af kryptoaktiver, jf. [art. 1](#)

- Udbydere af kryptoaktivtjenester verificerer disse oplysninger og opbevarer dem
- Transaktioner kan spores af retshåndhævende myndigheder og FIU'er (Financial Intelligence Units)

I dansk ret er TFR-forordningens krav om selvhostede adresser gennemført ved [bekendtgørelse om gennemførelse af risikobegrænsende foranstaltninger ved overførsel af kryptoaktiver rettet mod eller stammende fra en selvhostet adresse](#).

FATF (Financial Action Task Force) har i sin evaluering af Danmark vurderet landet som "Partially Compliant" med hensyn til regulering af VASP'er (Virtual Asset Service Providers) under FATF Anbefaling 15. Dette signalerer et behov for fortsat styrkelse af den regulatoriske ramme og tilsynsindsatsen over for kryptoaktivtjenesteudbydere.

LOV

Hvidvaskloven § 1, stk. 1

§ 9 Organiseret kriminalitet, krypteret kommunikation og hvidvask – samspillet i praksis

Moderne hvidvasksager involverer ofte en kombination af traditionelle pengeoverførsler og digitale kommunikationsmetoder. Nyere dansk retspraksis illustrerer, hvordan krypterede kommunikationsplatforme anvendes til at koordinere hvidvasknetværk.

I Højesteretssagen [SS-64/2024-HJR](#) blev politiets dokumentation af hvidvaskaktiviteterne understøttet af GPS-observationer, teleoplysninger og krypteret korrespondance på SKY og WhatsApp. Ligeledes byggede sagen [AM2025.03.12H](#) bl.a. på dekrypterede meddelelser fra krypterede kommunikationsplatforme.

SØIK (Statsadvokaten for Særlig Økonomisk og International Kriminalitet) – siden 2023 opdelt i NSK (National enhed for Særlig Kriminalitet) og en ny bagmandsafdeling – varetager efterforskningen af komplekse hvidvasksager med internationale forgreninger. Kryptoaktiver tilføjer yderligere kompleksitet til disse efterforskninger:

- **Pseudonymitet:** Kryptovalutaadresser er pseudonyme, men ikke anonyme – blockchain-analyse kan afsløre transaktionsmønstre og forbindelser til kendte entiteter
- **Grænseoverskridende karakter:** Kryptoaktiver kan overføres globalt uden mellemmand, hvilket kræver internationalt samarbejde om bevisoptagelse og beslaglæggelse
- **Volatilitet:** Værdien af beslaglagte kryptoaktiver kan ændre sig markant mellem beslaglæggelse og dom, hvilket rejser spørgsmål om opgørelse af konfiskationsbeløb
- **Teknisk kompleksitet:** Effektiv efterforskning kræver specialiseret viden om blockchain-teknologi, DeFi-protokoller og privacy-enhancing technologies

Samarbejdet med udenlandske myndigheder og kryptobørser er afgørende, da mange kryptobørser opererer fra jurisdiktioner uden for dansk jurisdiktion. European Judicial Cooperation Network og Europol's European Cybercrime Centre (EC3) faciliterer dette samarbejde.

LOV

Straffeloven § 290a, stk. 2

PRAKSIS

Højesteret · Højesteret skærper straffen til 4 års fængsel, men nedsætter indrejseforbud til 6 år i sag om medvirken til narkotikakriminalitet (kokain)

13.03.2025

§ 10 Sammenfatning og regulatorisk udvikling

Dansk ret er i en løbende tilpasningsproces for at adressere hvidvask via kryptovaluta og digitale aktiver. De centrale retlige rammer kan opsummeres således:

- **Strafferetligt** er hvidvask via kryptovaluta dækket af § 290 a som "konvertering" af penge, når kriminelt udbytte investeres i kryptovaluta. Omvendt falder konvertering *fra* kryptovaluta til penge som udgangspunkt uden for § 290 a's ordlyd, men kan straffes som hæleri efter § 290. Højesterets dom af 29. januar 2025 har bekræftet, at veksling af kriminelt udbytte er hvidvask uanset formålet med de omvekslede midler.
- **Regulatorisk** er kryptoaktivtjenesteudbydere underlagt hvidvasklovens fulde forpligtelsesregime, herunder kundekendskab, risikovurdering, overvågning og underretningspligt. Bekendtgørelsen om selvhostede adresser kræver anvendelse af DLT-analyseværktøjer.
- **EU-retligt** sætter MiCA-forordningen og TFR-forordningen en ny ramme for tilsyn med og sporbarhed af kryptoaktiver.
- **Konfiskationsmæssigt** kan kryptovaluta konfiskeres som udbytte efter § 75 eller med omvendt bevisbyrde efter § 76 a, men praktisk gennemførelse kræver adgang til private nøgler.

Der er ingen vedtagne men ikke-konsoliderede ændringer til hverken straffelovens § 290 a (senest konsolideret 14. november 2025) eller hvidvaskloven (senest konsolideret 21. april 2026).

Den publicerede retspraksis om hvidvask *specifikt via kryptovaluta* er endnu begrænset i Danmark. Hovedparten af de pådømte hvidvasksager involverer traditionel valutaveksling eller kontantoverførsler. I takt med at kryptovalutamarkedet modnes og den regulatoriske ramme styrkes – herunder kryptobørsernes underretningspligt og Hvidvasksekretariatets analysekapacitet – må det forventes, at antallet af kryptorelaterede hvidvasksager vil stige.

LOV

Hvidvaskloven § 1, stk. 1

Hvidvaskloven § 26

Straffeloven § 75

Straffeloven § 76a

Straffeloven § 290a

Straffeloven § 290

PRAKSIS

Højesteret · Højesteret stadfæster dom for hvidvask af narkotikapenge efter Straffelovens § 290 a

29.01.2025

REFERENCE Lovgrundlag

6 paragraffer

Hvidvaskloven § 1	stk. 1	Hvidvaskloven § 26	
Straffeloven § 75	stk. 1	Straffeloven § 76a	stk. 1
Straffeloven § 290		Straffeloven § 290a	

MATERIALE Citerede afgørelser

4 afgørelser

HØJESTERET · ØVERSTE INSTANS

3

13.03.2025	Højesteret skærper straffen til 4 års fængsel, men nedsætter indrejseforbud til 6 år i sag om medvirken til narkotikakriminalitet (kokain)	AM2025.03.12H
29.01.2025	Højesteret stadfæster dom for hvidvask af narkotikapenge efter Straffelovens § 290 a	7062-8491
03.12.2015	Konfiskation af fast ejendom købt med midler fra groft hæleri: Afgørelse om grænsen for udbyttekonfiskation	Sag 136/2015
BYRET TEN · FØRSTE INSTANS		1
09.05.2016	Betinget fængsel for omfattende afpresning og hacking mod behandlingssted og forsikringsselskaber	SS 1-31954/2015