POLITIET

Politidirektoratet
Postboks 8051 Dep
0031 Oslo

Deres referanse	*Vår referanse*	*Dato*	*Unntatt offentlighet*
2011/02772-2 4398		15.11.2011	§5a

Vedr henvendelse om identitetstyverier

En viser til henvendelse fra Politidirektoratet v/ Morten Hojem Ervik av 7.11.2011vedrørende bistand til besvarelse av en forespørsel fra Justitsministeriet i Danmark omkring temaet identitetstyverier, og da særskilt norske erfaring mht etterforskning og avdekking av enkeltsaker samt eventuelt forebygging.

1. Innledning
   Utgangspunktet for henvendelsen fra Justitsministeriet i Danmark er to problemstillinger: hvordan styrke politiets muligheter for å etterforske saker om identitetstyveri, og hvordan forbedre mulighetene til å hjelpe ofrene for identitetstyveri.

2. Materiell strafferett

   a. Et særskilt lovbrudd?

      Identitetstyverier er et begrep som omfatter flere typer lovbrudd, derunder bedragerier (straffeloven §§ 270 flg), dokumentfalsk (straffeloven § 182 flg), brukt av uriktige legitimasjonspapirer (straffeloven § 372 annet ledd) og sjikane (straffeloven § 390a). Som nevnt nedenfor, ble det i 2010 innført en særskilt bestemmelse (straffeloven § 190a) vedrørende identitetsmisbruk.

      Selv om identitetstyverier er et kjent begrep, viser et søk på Lovdata med "identitetstyveri" som søkeord, kun fire dommer. Alle var subsumert som bedragerier.

   b. Straffeloven av 2005, § 202 (ikke i kraft)

      Da den nye straffeloven ble vedtatt i 2005 (ikke trådt i kraft pr i dag), var identitetskrenkelse omfattet av lovens § 202:

      "Med bot eller fengsel inntil 2 år straffes den som uberettiget setter seg i besittelse av en annens identitetsbevis, eller opptrer med en annens identitet eller med en identitet som er

Kripos
Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet
Brynsalléen 6, Postboks 8163 Dep, 0034 OSLO
Tlf: 23 20 80 00 Faks: 23 20 88 80
E-post: kripos@politiet.no Org.nr.: 974 760 827

lett å forveksle med en annens identitet, med forsett om å
a) oppnå en uberettiget vinning for seg selv eller en annen, eller
b) påføre en annen tap eller ulempe."

Forarbeidene til denne lovbestemmelsen er blant annet NOU-2007-2 "Lovtiltak mot datakriminalitet", bl.a. pkt 5.6.7 (Identitetstyveri), samt Ot.prp. Nr. 22 (2008-2009) pkt. 2.9. Blant annet legger NOU'en og Ot. prp.'en til grunn at identitetsmisbruket også kan gjelde identiteten til et firma eller en annen juridisk person. Dermed vil lovbestemmelsen også verne enkeltpersoner som utsettes for en falsk firmaidentitet, eksempelvis phishing.

c. Straffeloven av 1902, § 190a

Ved lov av 10. desember 2010 nr. 72 ble § 190a i straffeloven av 1902 vedtatt, og denne bestemmelsen har trådt i kraft. § 190a er identisk med § 202 i straffeloven § 2005, men har også et siste ledd:
"Medvirkning straffes på samme måte."

Bakgrunnen for at denne bestemmelsen ble innført, var en dom fra Høyesterett av 14.10.2010 (Rt-2010-1217), hvor en rumensk statsborger var tiltalt for forberedelse av dokumentfalsk, idet han var pågrepet i Norge i besittelse av skimming-utstyr. For dette punktet ble en fellende dom fra Borgarting lagmannsrett opphevet, da Høyesterett kom til at det straffbare forholdet i tilfelle hadde skjedd i utlandet, og at det ikke var noen norsk lovbestemmelse som kunne anvendes på forholdet.

Lovendringen kom dermed i stand i løpet av kort tid.

d. Straffeloven av 1902 § 186

Samtidig som straffeloven § 190a ble innført, ble straffeloven § 186 (forberedelse av dokumentfalsk) endret, med umiddelbart virkning. Den tidligere lovteksten omfatter den som *"forfærdiger eller anskaffer falsk Segl, stempel eller merke (...) eller i saadan hensikt tilvender seg et ægde Segl, stempel eller merke"*. Den nye lovteksten omfatter den som *"til forberedelse av dokumentfalsk tilvirker, erverver, innfører, utfører, overdrar, besitter eller oppbevarer falsk segl, stempel eller merke (...)"*.

e. Straffeloven av 1902 § 145, 2. ledd

Datainnbruddsbestemmelsen er også relevant i forhold til identitetstyveriet. Denne lovbestemmelsen ble sist endret i 2005, og har nå følgende tekst (hele paragrafen):

Den som uberettiget bryter brev eller annet lukket skrift eller på lignende måte skaffer seg adgang til innholdet, eller baner seg adgang til en annens låste gjemmer, straffes med bøter eller med fengsel inntil 6 måneder eller begge deler.

Det samme gjelder den som uberettiget skaffer seg adgang til data eller programutrustning

som er lagret eller som overføres ved elektroniske eller andre tekniske hjelpemidler.

Volder skade ved erverv eller bruk av slik uberettiget kunnskap, eller er forbrytelsen forøvet i hensikt å skaffe noen en uberettiget vinning, kan fengsel inntil 2 år anvendes.

Offentlig påtale finner bare sted når allmenne hensyn krever det.

Bestemmelsen ble sist endret i 2005, ved at det daværende kravet i annet ledd om beskyttelsesbrudd, ble fjernet. Etter dette er altså datainnbruddsbestemmelsen også være anvendbar i forhold til uberettiget innsamling av data uten at det er skjedd et eksplisitt datainnbrudd; eksempelvis dersom fornærmede har vært utsatt for et sikkerhetshull som andre har utnyttet.

En tilsvarende bestemmelse er inntatt i straffeloven av 2005 (ikke i kraft) § 204, som har følgende innhold:

Med bot eller fengsel inntil 2 år straffes den som ved å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer seg tilgang til datasystem eller del av det.

f. Særlovgivningen

Flere bestemmelser i særlovgivningen kan ha indirekte betydning i forhold til identitetstyverier. Dette gjelder eksempelvis personopplysningsloven. Datatilsynet er ansvarlig tilsynsmyndighet for denne loven, men for de deler av loven som omfattes av straffebudet i § 48, kan påtalemyndigheten reise tiltale på egen hjemmel.

Aktuelle bestemmelser i forhold til identitetstyverier kan være lovens § 19 (informasjonsplikt når det samles inn opplysninger fra den registrerte), § 20 (informasjonsplikt når det samles inn opplysninger fra andre enn den registerte) samt § 231 (meldeplikt til Datatilsynet). Dette er formalregler, men i enkelte tilfeller vil det være lettere å føre bevis for at formallovbrudd har funnet sted, enn å føre bevis for at faktisk misbruk av opplysningene er gjennomført, og at det er den mistenkte som er ansvarlig for misbruket.

Loven har en strafferamme på inntil ett års fengsel, men inntil 3 års fengsel ved særdeles skjerpende omstendigheter, jf. lovens § 48, første ledd og annet ledd. Medvirkning er også straffbart.

3. Straffeprosess

Det er ikke innført endringer i straffeprosessloven spesifikt for å ivareta etterforskning av identitetstyverier eller for å verne fornærmede i slike saker. Imidlertid er det flere bestemmelser som kan ha interesse ved etterforskning på saksområdet.

Dersom id-misbruket har skjedd på en måte som etterlater elektroniske spor, er det behov for å sikre og innhente disse. Straffeprosessloven § 215a gir

påtalemyndigheten adgang til sikringspålegg, jf også Europarådets datakrimkonvensjon artikkel 29. Selv om bakgrunnen for bestemmelsen var knyttet til politianmodninger fra utlandet, vil sikringspålegg også kunne ha interesse i tilfeller hvor politiet må gå til en domstol for å få beslutning på utlevering av elektronisk lagrede opplysninger som befinner seg hos en tredjepart.

Lov om elektronisk kommunikasjon (ekomloven) § 2-9, tredje ledd gir politiet mulighet til å innhente abonnentopplysninger direkte fra teleselskaper og ISP'er. Regelen omfatter ikke innholdsdata, men gjør det mulig å avklare hvilken kunde som var abonnent for et telefonnummer eller en IP-adresse på et bestemt tidspunkt. Mulighetene for å innhente abonnentopplysninger er imidlertid begrenset av hvor lenge tilbyderne lagrer slike opplysninger. Etter flere vedtak fra Datatilsynet, lagrer ISP'er sine logger i inntil 21 dager, mens mobiloperatører lagrer sine logger inntil 3 måneder. Stortinget vedtok i april 2011 å innføre EU's datalagringsdirektiv i Norge, og lagringstiden vil bli utvidet til 6 måneder når reglene er implementert.

4. Samarbeid mellom offentlig og privat sektor

   a. NorSIS

      NorSIS (Norsk Senter for Informasjonssikring), er faglig underlagt Fornyingsdepartementet, og har som formål å bedre informasjonssikkerheten i Norge, gjennom informasjon og samarbeid mellom privat og offentlig sektor. NorSIS er lokalisert i Gjøvik, i samme miljø som Høgskolen i Gjøvik og samarbeidsprosjektet "Security Valley", som er et kunnskapscluster for datasikkerhet, jf. securityvalley.no.

      i. Id-tyveriprosjektet

         Etter offentlig initiativ, er det etablert et samarbeidsprosjekt for å definere tiltak og virkemidler som forebygger og reagerer på identitetstyverier og svindel som følge av slike tyverier. Prosjektperioden er 2009 til 2011. Nærmere informasjon om dette prosjektet er inntatt på nettsidene til Gjøvik Kunnskapspark. Forkortet lenke til nettsiden for prosjektet er www.goo.gl/Afqjs [1].

         Som det framgår av nettsiden, er prosjektet et samarbeid mellom private virksomheter, private organisasjoner og ulike offentlige virksomheter. Videre er prosjektet inndelt i flere delprosjekter.

      ii. Idtyveri.info

         En del av Id-tyveriprosjektet, er knyttet til etablering og drift av nettsiden idtyveri.info. Det er NorSIS som har ansvaret for denne nettsiden. Siden har informasjon som i stor grad er rettet mot er

[1] Dette er en forkortet nettlenke til prosjektsiden, ved bruk av URL-forkortingstjenesten Goo.gl fra Google.

bredt publikum, blant annet sjekklister for å forebygge risiko for id-tyveri.

Idtyveri.info fikk i 2010 Dataforeningens pris, Rosingsprisen, for IT-sikkerhet.

iii. Sikkert.no

En relatert nettside er sikkert.no , som fokuserer spesifikt på informasjon om datasikkerhet. Også denne nettsiden er i stor grad rettet mot et bredt publikum, blant annet med informasjon om viktigheten av å oppdatere datautstyr for å sikret seg mot sikkerhetshull.

iv. Nasjonal Sikkerhetsmåned

For å skape oppmerksomhet om sitt arbeid for datasikkerhet, har NorSIS etablert oktober måned som "Nasjonal Sikkerhetsmåned", www.norsis.no/nyheter/2011-10-02-Nasjonal-Sikkerhetsmaaned.html Formålet er å ha en årlig holdningskampanje for å oppfordre alle til å beskytte sine datamaskiner og oppfordre det offentlige og næringslivet til å sikre sin data-infrastruktur. EU planlegger en lignende kampanje for oktober 2012.

v. "Stopp Nettsvindelen"

"Stopp Nettsvindelen" er en møteserie som driftes av NorSIS, hvor formålet er å fokusere på hvilke utfordringer private og offentlige virksomheter møter i forhold til internettbedragerier, deriblant id-tyverier. Deltakerne er private og offentlige virksomheter, samt bransjeorganisasjoner.

b. Næringslivets Sikkerhetsråd (NSR)

i. Mørketallsundersøkelsene

NSR utarbeidet hvert annet år en omfattende undersøkelse for å beskrive mørketall for datakriminalitet i Norge. Mørketallsundersøkelsene utarbeides i samarbeid med blant annet NorSIS, Kripos, Nasjonal Sikkerhetsmyndighet, SINTEF, SECODE, Telenor, Det Norske Veritas og Forsvarets Forskningsinstitutt. Datatyverier og tyveri av informasjon er blant de temaer som omfattes av mørketallsundersøkelsene. Undersøkelsene er tilgjengelige på www.nsr-org.no/morketall.htm.

Selv om undersøkelsene ikke direkte omfatter identitetstyverier, er datasikkerhet en viktig faktor for å kunne forebygge og oppklare id-tyverier.

c. Finansnæringens Fellesorganisasjon

Finansnæringen, derunder banker og betalingsformidlere, er en sentral aktor i arbeidet for å forebygge identitetstyverier. Finansnæringens Fellesorganisasjon har utarbeidet et standardskjema ("Melding om identitetstyveri") som gjør det mulig for en kunde i en bank å inngi melding om mulig identitetstyveri til sin bankforbindelse. Som det framgår av skjemaet:

"Gjennom å undertegne på dette dokumentet gir du som kunde din hovedbankforbindelse tillatelse til å varsle andre finansinstitusjoner, private firmaet (som f.eks. kortselskaper) og offentlige institusjoner om at din identitet misbrukes.

Når du har blitt "frastjålet din identitet" har du selv ansvar for aktivt å søke råd og bistand, særlig i forhold til offentlige instanser. Hovedbankforbindelse vil likevel være behjelpelig med å foreta nødvendige tiltak innen egen organisasjon, samt gi informasjon og råd i forhold til hvilke andre instanser som bør kontaktes."

FNO utarbeidet rapporten "Felles utfordringer knyttet til identitetsmisbruk" av 9.10.2008, som gir en nærmere beskrivelse av problemer og mulige løsninger, ut fra finansbransjens ståsted. Både skjemaet og rapporten er tilgjengelig på www.fno.no/no/hoved/fakta/bank .

Ved å etablere bransjerutiner som ivaretar varsling av andre virksomheter, reduseres risikoen for identitetstyverier, og virkningene av gjennomførte identitetstyverier vil også kunne avhjelpes.

d. Andre aktører

Blant annet Datatilsynet og Forbrukerrådet har på sine nettsider informert publikum om risikoen for identitetsmisbruk og gitt råd for å forebygge misbruk, samt deltatt i ulike samarbeidsprosjekter omkring id-tyverier.

5. Statistikk og mørketall

I tillegg til at de handlingene som ofte beskrives som identitetstyverier m.v. dermed omfattes av ulike lovbestemmelser, er det heller ingen samlet registrering i kriminalstatistikken over forhold som kan beskrives om identitetstyverier.

Det er også grunn til å anta at det foreligger mørketall, ettersom ikke alle forhold blir oppdaget, og heller ikke alle forhold som oppdages, blir anmeldt til politiet. Dette framkommer også i mørketallsundersøkelsene fra Næringslivets Sikkerhetsråd (jf pkt 4 litra b over).

En særskilt årsak kan være at flere moduser for id-tyveri skjer fra utlandet til Norge, slik at det blir vanskeligere og mer tidkrevende å innhente beviser mot de ansvarlige, i den grad det lar seg gjøre. Et eksempel på dette er phishing. Et annet eksempel er betalingskortbedragerier, hvor det i en del tilfeller er grunn til å tro at bedrageriene har sitt utgangspunkt i "datalekkasjer" i andre land enn der hvor kortholderen bor.

6. Internasjonalt samarbeid

Identitetstyverier er et internasjonalt problem, og i mange tilfeller fører sporene til andre land. Et eksempel er at norske betalingskort eller data til brukere av betalingskort har blitt ulovlig kopiert og deretter benyttet til kontaktuttak og varekjøp i utlandet. I de sakene som har blitt anmeldt til norsk politi, har den berørte banken normalt gjort undersøkelser på forhånd, men det har ofte vist seg vanskelig eller umulig å følge sporene fram til den/de ansvarlige. Denne type misbruk vil primært kunne begrenses ved bedre sikkerhetsrutiner i bank- og betalingssystemene, men det er sikkert også mer som kan gjøres for sikre bevis fra politiets side samt få til bedre internasjonalt samarbeid om denne type saker. I praksis har en imidlertid erfart at det kan være vanskelig å få til en tilstrekkelig høy prioritet når slike saker leder til etterforskning i utlandet.

En annen type saker som typisk forutsetter internasjonalt samarbeid, er phishing-sakene. Eksempelvis har norske bankkunder mottatt e-poster som tilsynelatende var fra deres bankforbindelse, og de ble bedt om å logge seg på en nettside for å bekrefte sin nettbankkode. Nettsiden var imidlertid kontrollert av tredjeparter, og formålet var å innhente ulike typer personinformasjon. Phishing er et internasjonalt problem, og få saker blir oppklart.

Vi anser at det er viktig å ha kontakt med Europol og Interpol på dette saksområdet, både i forhold til enkeltsaker og i forhold til modusopplysninger.

7. Sakseksempler

Nedenfor vil en kort gå gjennom enkelte saker, som illustrerer ulike aspekter ved identitetstyverier

a. Skimming-saker

Norske domstoler har pådømt flere saker om skimming. Sakene var i utgangspunktet subsumert som forsøk på dokumentfalsk, men i 2010 kom Høyesterett til at denne lovbestemmelsen ikke var anvendbar jf nærmere redegjørelse over, pkt .2 litra c). I ettertid har det vært enkelte saker med tiltale basert på den nye straffeloven § 190a. Et sakskompleks med fire tiltalte ble pådømt i Sarpsborg tingrett 18. oktober 2011 (saksnr 11-104868MED-SARP) og er nå rettskraftig for tre av de fire tiltalte.

Skimmingen var subsumert som flere tilfeller av datainnbrudd, som organisert kriminalitet (straffeloven § 145 annet ledd, jf første og tredje ledd, jf § 60a), henholdsvis forsøkt på datainnbrudd, og flere tilfeller av forberedelse av dokumentfalsk (straffeloven § 186, jf. § 60a), flere tilfeller av benyttelse av falske dokumenter (straffeloven § 183, jf. § 60a), flere tilfeller av grove tyverier (straffeloven § 257, jf. § 258, jf. §60a), henholdsvis forsøk på grove tyverier.

Dette framkommer av dommen:
"Straffeloven § 186 ble endret per 10.12.2010 med umiddelbar ikraftsetting, noe som

avfødte en endring av tiltalebeslutningen på dette punkt rett før hovedforhandlingen. Enkelt sagt rammet denne bestemmelsen i sin opprinnelige ordlyd bare anskaffelse av nevnte type gjenstander/utstyr i Norge.
Etter lovendringen rammes enhver besittelse uavhengig av hvor slik anskaffelse har skjedd. Slik retten oppfatter lovendringen, er nedslagsfeltet utvidet slik at bestemmelsen etter desember 2010 favner atskillig videre enn tidligere."

b. Sjikane via falsk nettprofil

I Personvernkommisjonens rapport NOU 2009:1 pkt. 14.3.4 er en sak omtalt.

"På et populært nettsted i Norge har det blitt laget en falsk profil over en 13 år gammel jente hvor det opplyser at hun ønsker sex med voksne menn og fantaserer om å bli voldtatt hjemme. Profilen inneholder konkrete og utfyllende personopplysninger. Saken ble politianmeldt, og det viste seg at profilen var opprettet av en person i jentas omgangskrets som hevn og resultat av en uenighet."

Denne saken ble oppklart av politiet, med bistand fra Kripos, gjennom en sporing av IP-adressen til den som hadde opprettet den falske profilen. Fra profilen var opprettet, til profilen ble oppdaget og senere søkt oppsport via politiet, var det gått mer enn 21 dager, men mindre enn 6 måneder. På grunn av Datatilsynets pålegg i 2009 om sletting av IP-logger etter maksimalt 21 dager, ville denne saken ikke vært mulig å oppklare i dag, mens det var mulig på det tidspunktet saken ble etterforsket.

Dersom gjerningspersonen hadde vært over den kriminelle lavalder, ville forholdet på det aktuelle tidspunktet vært subsumert etter straffelovens § 390a (sjikane), men den nye straffebestemmelsen om identitetsmisbruk (straffelovens § 190a) ville formentlig også vært anvendbar i konkurrens med strl.§ 390a.

c. "Kvearner"-saken

Høyesterett behandlet i 2003 (Rt. 2003-825) en straffesak basert på at to tiltalte hadde mottatt konfidensiell forretningskorrespondanse til det børsnoterte norske firmaet Kværner, som eide domenet kvaerner.com. De to tiltalte hadde domenet kvearner.com, og mottok e-post hvor mottakers adresse var stavet feil.

Et sentralt aspekt i forhold til faktum, framgår av avsnitt 17 i dommen:
"Domenet var også satt opp med e-post, dit feilsendt e-post kom selv om den var adressert til personer som ikke befant seg hos "Kvearner". Dette førte til at A jevnlig mottok feilsendt e-post; ifølge hans forklaring for byretten kunne det dreie som 10-20 pr dag til Kvearner.com.

Det var således langt fra noen tilfeldighet at feilsendt e-post kom inn på As datamaskin. Tvert imot var dette noe han selv hadde lagt til rette for, ved en virksomhet som idet minste må karakteriseres som innpåsliten. Dette stiller særlige krav til håndteringen av slik feilsendt e-post."

I lagmannsretten ble de frifunnet for forsøk på utpresning. De ble også frifunnet for brudd på straffelovens § 405a ("den som på urimelig måte skaffer seg eller søke å skaffe seg kunnskap om eller rådighet over en bedriftshemmelighet"). Frifinnelse for den sistnevnte tiltaleposten ble opphevet Høyesterett pga uriktig lovanvendelse, dog uten at Høyesterett avsa ny dom.

"Kvearner"-saken er nevnt i lovforarbeidene til den nye § 190a i straffeloven som et eksempel på mulig identitetstyveri av et firmanavn. Fra Ot.prp. nr. 22 (2008-2009) pkt. 2.9.6 (endringer i straffeloven § 2005):

"Ved å sette straff for fiktiv identitet, unngår man å trekke grensen mellom fiktiv og uriktig identitet. Utvalget illustrerer problemet med saksforholdet i Kværner-kjennelsen inntatt i Rt. 2003 s. 825. (...)
For en datamaskin er det opplagt av Kvaerner og Kvearner representerer to ulike navn med den følge av Kvearner vil anses som en fiktiv og ikke stjålet identitet. Utvalget utkast gjelder imidlertid bruk av uriktig identitet overfor mennesker, og for mennesker er navnene lettere å forveksle. Er identiteten som benyttes lett å forveksle med en annens identitet, bør det ikke gjøre noen forskjell for straffbarheten om den ikke er helt identisk med den andres identitet. For å gjøre det tilstrekkelig klart at også slike tilfeller er omfattet av straffebudet, foreslår departementet at det i forslaget til § 202 presiseres at straffansvaret også gjelder den som uberettiget opptrer med en identitet som er lett å forveksle med en annens identitet. Holder gjerningspersonen det for sikkert eller overveiende sannsynlig at identiteten lett kan forveksles med en annen, foreligger straffansvar."

d. Tele2 og Combitel-sakene

I slutten av juli 2007 opplevde flere norske mobiltelefonioperatører uberettiget innsamling av personinformasjon via deres nettsider. Dette skyldtes et sikkerhetshull, som gjorde det mulig å hente ut persondata (fødselsnummer, navn og adresse) på flere tusen personer. Sakene ble pådømt av Borgarting lagmannsrett (LB-2010-181392 og LB-2010-18170) samt Frostating lagmannsrett (LF-2009-202167). Fra ingressen på førstnevnte avgjørelse:

"Siktede lastet ned persondata (fødselsnummer, navn og adresser) på flere tusen personer fra en teletilbyders nettside ved bruk av et særskilt dataprogram. Siktede ble dømt for overtredelse av straffeloven § 145 annet ledd [datainnbrudd] og personopplysningsloven § 48, jf § 31 og § 20 til 30 dager betinget fengsel og en bot på kr 20 000."

Det er mulig at den nye straffeloven § 190a ville vært anvendbar i disse sakene. Som det framgår av Ot.prp. nr. 22 (2008-2009) pkt. 2.9.6 (endringer i straffeloven § 2005):

"Med "identitet" menes navn, fødselsnummer, organisasjonsnummer, e-postadresse og andre opplysninger som, alene eller sammen med annen informasjon, kan identifisere en fysisk eller juridisk person."

e. Hotmail-dommen

Follo tingrett har avsagt en dom vedrørende "hacking" av en webmailkonto, TFOLL-2008-93551. Fra ingressen:

"39 år gammel mann ble dømt til en bot på kr. 7.000 for uberettiget å ha skaffet seg adgang til sin kones e-postkonto [datainnbrudd, straffeloven § 156, annet ledd] og for å ha gjort brukernavn og passord tilgjengelig for en annen person [straffeloven § 145b] slik at denne kunne lese e-posten på fornærmedes konto."

Faktum slik det beskrives i dommen:
"Ved å velge muligheten for alternativ pålogging ble tiltalte presentert for et spørsmål generert av hans kone ved opprettelsen av epostkontoen, hvorved man ved korrekt svar får oppgitt et passord for pålogging. Etter 18 års ekteskap visste tiltalte svaret på spørsmålet som fremkom, hvoretter han fikk oppgitt et passord til sin kones private epostkonto. Han logget seg deretter inn på hennes epostkonto og kunne lese hennes private epost."

En antar at dette faktum også kunne vært omfattet av straffeloven § 190a. Brukernavn og passord er nevnt i Datakrimutvalgets delinnstilling II (NOU 2007:2 pkt. 3.5.12) som eksempler på identitetsopplysninger som kan være gjenstand for identitetstyveri.

f. To dommer om personopplysningsloven

Gulating lagmannsrett behandlet i 2007 (LG-2006-184922) en straffesak, hvor tiltalte ble dømt for brudd på personopplysningsloven § 48, første ledd bokstav a, e og f, jf § 31 første ledd bokstav a og annet ledd, § 26, fjerde ledd og § 20. Faktum var at tiltalte hadde samlet inn over 60.000 amerikanske personnavn og adresser og over 650.000 e-postadresser, uten å angi kilden for personopplysningene. Dette registeret ble benyttet til å sende ut e-postreklame (spam).

På samme måte som i spam-dommen, ble tiltalte i Combitel-saken (jf litra d over) dømt blant annet for overtredelse av personopplysningsloven § 48, jf § 31 og § 20, jf dom fra Borgarting lagmannsrett LB-2010-181392.

Fra dommen:
"Tingretten har beskrevet det som "kunstig" å anvende personopplysningslovens regler om forhåndsmelding og varsling i en situasjon som den foreliggende, og forsvareren har anført det samme i prosedyren. Lagmannsretten forstår forsvareren slik at det anføres at reglene om meldeplikt og varslingsplikt må forutsettes å rette seg mot ellers lovlige virksomheters behandling av personopplysninger, hvor reglene gir mening, og ikke mot den som for demonstrasjonsformål og i den hensikt å styrke personvernet, henter ut personopplysninger fra slike virksomheter.

Lagmannsretten kan ikke se at det er grunnlag for å foreta en innskrenkende tolkning av bestemmelsene selv om det legges til grunn at siktede hadde et aktverdig motiv. Personopplysningslovens regler retter seg mot enhver for å oppnå en effektiv beskyttelse av personvernet, og har dermed også en funksjon i situasjoner som den foreliggende.(...)

Det legges etter dette til grunn at de objektive straffbarhetsvilkårene er oppfylt. Siktede har som behandlingsansvarlig behandlet personopplysninger uten å gi forhåndsmelding til Datatilsynet og uten å varsle de berørte personene."

Personopplysningslovens historiske utgangspunkt var dataregistre hos etablerte firmaer og offentlige virksomheter. Dommene beskrevet over er eksempler på at ulovlig innsamlede personopplysninger kan omfattes av personopplysningsloven, også i tilfeller hvor tiltalte var en privatperson som ikke drev noen næringsvirksomhet.

En legger etter dette til grunn at personopplysningsloven kan være relevant i tilfeller av ulovlig innsamling av personopplysninger, selv om det ikke føres bevis for at opplysningene rent faktisk er misbrukt i ettertid.

g. "Spy-Net"-saken

Haugaland tingrett avsa 28.4.2011 (saksnr 11-015223MED-HAUG) dom i en sak om omfattende, delvis databasert kriminalitet, deriblant datainnbrudd og etterfølgende kredittkortbedragerier. Det framkommer av dommen, side 59:

"Ved bruk av [programvaren] SpyNet har tiltalte gjennom egne opprettede nettsider som blant annet www.politiet.eu spredt virus i form av trojanere, som igjen har infisert et stort antall datamaskiner til intetanende eiere. (...) Gjennom slike datainnbrudd har tiltalte hatt full tilgang til vedkommendes datamaskiner og har bl.a. ved hjelp av keylogg kunnet tilegne seg dennes kredittkortopplysninger, som i neste omgang er misbrukt. Misbruket har ikke bare medført at tiltalte urettmessig har fått utlevert varer og tjenester, men han har på en utspekulert måte ved bruk av fiktive handler på finn.no også beriket seg med store kontantbeløp. Tiltalte har operert med ulike navn, adresser og har brukt proxyservere for å skjule sin egne IP-adresse. Retten viser også til at tiltalte hacket seg inn på kundekonsulent hos IF, hvorfra han fikk tilgang til Ifs kunderegister med kundenavn, adresse og personnummer. En rekke av Ifs kunder ble misbrukt av tiltalte ved at han bl.a. opprettet kundekontoer i nettbutikker i deres navn.

Tiltaltes handlemåte er etter rettens oppfatning av svært samfunnsskadelig karakter idet dette er et angrep på de etablerte betalingsordninger og – kanaler som samfunnet har gjort seg helt avhengige av. Denne straffbare virksomhet er vanskelig å avdekke og det er slik retten ser det av allmennpreventive grunner helt essensielt å reagere strengt på slike straffbare forhold."

Dommen er ikke rettskraftig, da en er påanket av domfelte til Gulating lagmannsrett.

Forholdene fant sted før straffeloven § 190a trådte i kraft.

Med hensyn til politiets etterforskning, kommer det fram av dommen av sentrale beviser ble funnet ved analyse at datamaskinen tilhørende tiltalte. Politiet hadde aksjonert etter klager fra flere som hadde vært i kontakt med tiltalte gjennom nettstedet Finn.no, et annonsemarked tilsvarende danske dba.dk. Modus var (sitert fra dommen) :*"et objekt var lagt ut for salg og at kjøper,*

da avtale om kjøp var inngått, hadde overført hele eller deler av kjøpesummen på forskudd, men ikke mottatt varen. Det viste seg ved nærmere undersøkelse av selgeren ikke eksisterte og ikke lenger svarte på oppgitt e-post eller mobilnummer."

Lokalt politi og Kripos foretok nærmere undersøkelser av tiltaltes datamaskin, og fant spor etter datainnbrudd og kredittkortbedragerier. Saken er dermed et illustrerende eksempel på betydningen av at politiet har kompetanse og ressurser til å kunne foreta *computer forensics* når slike saker etterforskes, ettersom de forhold som var anmeldt var av mindre omfang enn hva tiltalen og dommen til slutt omfattet.

h. Oppsummering basert på sakserfaringer

Selv om mange tilfeller av hva som ofte beskrives om identitetstyveri kan løses via andre straffebestemmelser, som dokumentfalsk, bedrageri, sjikane eller datainnbrudd, eventuelt vil disse bestemmelsene ikke alltid være anvendbare. I tilfellet Kvearner-saken som nevnt under pkt 7 litra c), ville den anvendbare straffebestemmelsen (straffeloven § 405a, inntil 3 måneders fengsel) ha en betydelig lavere strafferamme enn nye § 190a (inntil 2 års fengsel). Dette har betydning i forhold til flere straffeprosessuelle vilkår, og i forhold til terskler ved internasjonalt samarbeid.

Selv om det hittil har vært få saker hvor straffeloven § 190a har vært et tema, viser eksempelet fra skimmingsaken nevnt under pkt. 7 litra a) at endringen av strl.§ 186 fikk betydning nærmest umiddelbart.

Det er også et poeng at særlovgivning som personopplysningsloven kan være relevant også i forhold til identitetstyverier. Som nevnt over kan personopplysningsloven gi hjemmel for reaksjoner mot den som har foretatt ulovlig innsamling av personopplysninger. Et annet aspekt er at lovens krav om informasjonssikkerhet ved databehandling (jf personopplysningsloven § 13) setter standarder for virksomheter som behandler andres personopplysninger, og som kan være en kilde for identitetstyverier.

Med hilsen

Odd Reidar Humlegård
Sjef Kripos

Berit Børset
seksjonssjef

Saksbehandler:
Eirik Trønnes Hansen
Tlf.: 23 20 82 67