Ambassaden har indhentet følgende oplysninger til besvarelse af de nedennævnte spørgsmål fra Politidirektoratet i Oslo, som har indhentet oplysninger fra Kriminalpolitiet, som er det nationale ekspertorgan på området.

Ad. 1: Ved spørgsmål 38 og 39 - hvordan håndterer man i Norge problemstillingen vedrørende personer, der f.eks. på grund af trusler om æresrelateret vold eller partnervold har behov for en særlig adressebeskyttelse.

«Politiet fikk overført beslutningsmyndighet for beskyttelsestiltaket adressesperre fortrolig/strengt fortrolig i 2012, fra Skattedirektoratet. Kripos ble tildelt oppgaven som metodeutvikler og koordinator i slike saker. Kripos er også postmottak for trusselutsatte med adressesperre strengt fortrolig.

Innenfor statsforvaltningen reguleres behandlingen av geolokaliserende data knyttet til trusselutsatte med adressesperre av beskyttelsesinstruksen, sikkerhetslovens forskrift om informasjonssikkerhet og personopplysningsloven med forskrift. Utenfor statsforvaltningen reguleres behandlingen utelukkende av personopplysningsloven med forskrift.

Det finnes to graderinger innen adressesperre jf. Beskyttelsesinstruksens § 2:

Adressesperre fortrolig(kode 7)
Benyttes dersom det vil kunne skade offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende jf. Beskyttelsesinstruksens § 4.

Adressesperre fortrolig innebærer at den trusselutsattes adresse ikke skal utgis til private. Adresseopplysningen er imidlertid tilgjengelig for alle offentlige myndigheter som har tilgang til opplysninger fra folkeregisteret eller fra kopiene hos en av distributørene. I tilknytning til adresseopplysningen fremgår det at adressen skal behandles fortrolig. Adressesperringen fungerer m.a.o. som et varsel til de offentlige myndigheter om at adresseopplysningen ikke skal utgis til private. Private institusjoner vil imidlertid ikke få frem en sperret adresse når de søker i registeret.

Adressesperre strengt fortrolig(kode 6)
Benyttes dersom det vil forårsake betydelig skade for offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende jf. Beskyttelsesinstruksens § 4.

Adressesperre strengt fortrolig innebærer at opplysninger om den trusselutsattes adresse i utgangspunktet ikke skal gis ut til noen. Personer med adressesperre strengt fortrolig vil ved overføring av folkeregisterkopiene til distributørene være registrert med en postboksadresse. Den reelle adressen vil bare være tilgjengelig for et fåtall autoriserte ansatte i Skattedirektoratet.

En sak som omhandler adressesperre kan ha ulike utspring. I all hovedsak ser en at sakene starter ved en anmeldelse til politiet, henvendelse fra barnevernet til politiet eller at den trusselutsatte selv oppsøker politiet og anmoder om en vurdering av en akutt eller langvarig trusselsituasjon.

Det er dedikerte ansatte i hvert politidistrikt som er ansvarlig for utarbeidelse av trusselvurdering. Trusselvurderingen skal konkludere med hvilke(t) beskyttelsestiltak som eventuelt er mest hensiktsmessig. Dette fremlegges den i politidistriktet som har beslutningsmyndighet, politimester eller den han/hun har bemyndiget, som beslutter om beskyttelsestiltak(ene) skal iverksettes.

Dersom beskyttelsestiltaket som skal iverksettes er adressesperre fortrolig/strengt fortrolig oversendes saken Kripos v. Nasjonalt kontaktpunkt for adressesperre, som har den direkte kontakten med Skattedirektoratet. Skattedirektoratet har utpekt et fåtall personer som kan registrere/avregistrere disse sakene i folkeregisteret. Adressesperren gjelder for 3 år, med mulighet for opphevelse under perioden, evt. etter en ny vurdering kan adressesperren forlenges med ytterligere 3 år.

Det er det enkelte politidistrikt som er ansvarlig for oppfølgingen av den/de trusselutsatte. Hvilken oppfølging som kreves i den enkelte sak varierer ettersom sakens kompleksitet og alvorlighetsgrad er ulik i hvert enkelt tilfelle. Den trusselutsattes forutsetning for å klare å leve med beskyttelsestiltaket vil også være avgjørende for hvilken oppfølging som kreves.»

Ad. 2. Ved spørgsmål 39 - redegøre for, om man i Norge i visse tilfælde tilbyder personer udsat for trusler om f.eks. æresrelateret vold at skifte personnummer, og hvordan man i så fald håndterer det tab af registrerede personlige data, som et skifte af personnummer indebærer, f.eks. lægejournaloplysninger eller lignende.

«Spørsmål nr. 2 relaterer seg til beskyttelsestiltaket "Fiktiv identitet" som beskrives i Politilovens kap.II, §§ 14a – 14i. (https://lovdata.no/dokument/NL/lov/1995-08-04-53/KAPITTEL_3#KAPITTEL_3) Loven gir anledning til at den trusselutsatte benytter det som vi i Norge kaller "fingerte personopplysninger", og vil i praksis si at personen får et nytt fødselsnummer (fødselsdato + personnummer).

Beskyttelsestiltaket er det mest inngripende tiltaket vi har i Norge, og opplysninger om hvordan denne metoden håndteres er gradert "Strengt fortrolig" etter Beskyttelsesinstruksen. Jeg beklager derfor at jeg ikke i detalj kan beskrive gjennomføringen av tiltaket. Tiltaket benyttes ikke ofte. Jeg skal likevel forsøke å gi et godt svar på spørsmålet.

Beskyttelsestiltaket kan brukes overfor flere grupper av trusselutsatte og ikke bare i forhold til personer som blir utsatt for æresrelaterte trusler og vold. Det skal alltid ligge en konkret trusselvurdering til grunn, og denne skal konkludere med at fiktiv identitet er det korrekte tiltaket å iverksette. Det er komplisert å leve med, og den trusselutsatte må vurderes til å være i stand til å ivareta sin fiktive identitet. I motsetning til adressesperre er dette et tiltak som i utgangspunktet er ment å vare livet ut, selv om det er mulig å reversere det.

I denne sammenheng er det viktig å nevne at loven setter krav til at vedkommende søker "står i fare for å bli utsatt for alvorlig kriminalitet rettet mot liv, helse eller frihet". Det er også et krav om at det er fare for fremtidig vold eller trusler. Det er altså ikke anledning til å innvilge fiktiv identitet for eksempel i forbindelse med id-tyveri.

Da loven trådt i kraft 1. januar 2004 var det lovgivers intensjon at dette skulle være et tiltak som skulle brukes når det er behov, men ikke utover det. Loven sier derfor at det kun er anledning til å gi tillatelse til bruk av fingerte personopplysninger "dersom andre tiltak ikke kan gi tilstrekkelig vern".

I praksis er det den trusselutsatte som søker om fiktiv identitet. Dersom søknaden kommer direkte til Kripos, vil den bli sendt til det lokale politidistriktet for å starte saksbehandlingen der. Lokalt politi vil skrive en trusselvurdering og enten anbefale fiktiv identitet eller ikke anbefale tiltaket. Saken går deretter videre til Kripos, som siden 2006 har hatt det operative ansvaret for metoden, men som også saksforbereder søknaden for Politidirektoratet.

Den trusselutsatte vil bli intervjuet for både å kartlegge trusselen, men også for å forsøke å forutse hvordan den trusselutsatte vil klare å leve med en fiktiv identitet. Kripos vil sende sin innstilling til Politidirektoratet som har avgjørelsesmyndighet i saken. Avgjørelsen kan påklages til Justisdepartementet.

Dersom det blir gitt tillatelse for den trusselutsatte til å benytte fingerte personopplysninger er det Kripos som har ansvaret for gjennomføringen. Tiltaket skal ikke ha noen annen rettsvirkning enn beskyttelse. I praksis vil dette si at Kripos i den grad det er mulig skal bistå søkeren til å speile sin historikk over i ny identitet. I denne anledning kan "Politidirektoratet (les Kripos etter 1. januar 2006) uten hinder av taushetsplikt, kreve utlevert fra andre myndigheter de opplysninger som anses nødvendige".

For å kunne speile disse opplysningene har vi spesielt utpekte kontaktpersoner i offentlig sektor og i flere private bedrifter.

I tillegg til å bistå søkeren med å få overført personlige data fra gammel identitet til ny identitet skal Kripos ifølge loven også "bistå offentlige myndigheter eller private rettssubjekter som har et rettmessig behov for å komme i kontakt med den som har fått tillatelse til å benytte fingerte personopplysninger".

Tillatelsen til å benytte fingerte personopplysninger kan trekkes tilbake for eksempel dersom truslene opphører, og også dersom den trusselutsatte ber om det. Vedkommende vil da få tilbake sitt opprinnelige fødselsnummer, og vil også få bistand til å "speile" sine personlige data tilbake til den opprinnelige identiteten.»

- - 0 - -

Ambassaden kan i øvrigt henvise til følgende links::

Beskyttelsesinstruksen: https://lovdata.no/dokument/INS/forskrift/1972-03-17-3352

Sikkerhedslovens forskrift om informationssikkerhed:
https://lovdata.no/dokument/SF/forskrift/2001-07-01-744

Personoplysningsloven med forskrift: https://lovdata.no/dokument/NL/lov/2000-04-14-31?q