- Hva er en personopplysning?

Biometri

Biometri brukes for å bekrefte identitet. Brukt riktig kan biometri være et godt og effektivt verktøy ved identifisering, men det er viktig å være bevisst på fordeler og ulemper ved metodene.

Hva er biometriske kjennetegn?

Biometriske kjennetegn kan beskrives som kjennetegn som utgår fra kroppen, som er unike for deg som enkeltperson og samtidig permanente eller stabile over tid. Ved å måle disse kjennetegnene kan de benyttes til å gjenkjenne en person, eller bekrefte en persons påståtte identitet.

De mest kjente formene for biometriske kjennetegn er fingeravtrykk, håndavtrykk og ansiktsform, samt de to øyeteknologiene netthinne- og irisavlesning. I utgangspunktet kan alle målbare og unike egenskaper ved deg benyttes. Dette kan for eksempel være i form av stemmegjenkjenning, DNA, eller hvilken tastefrekvens du benytter når du skriver på et tastatur.

Biometri beskrives ofte som "noe vi er" når det sammenlignes med de tradisjonelle metodene for å gjenkjenne eller bekrefte en persons identitet. De tradisjonelle metodene omfatter "noe du vet", for eksempel et passord, og "noe du har", for eksempel en kodebrikke.

Biometri har sin egenart, det er uløselig knyttet til kroppen vår, på godt og vondt.

Biometri brukes til å fastslå eller bekrefte identitet

Biometri er et viktig hjelpemiddel i politietterforskning. Politiet bruker slike kjennetegn for å fastslå identitet og knytte gjerningspersoner til et åsted. Biometri kan også benyttes i mer hverdagslige sammenhenger for å bekrefte identitet, for eksempel for å fastslå at du er medlem i et treningsstudio.

Mange betrakter biometri som en rask, effektiv og sikker løsning for å bekrefte at du er den du er eller utgir deg for å være. Du trenger ikke ha med deg noe (kort) eller huske noe (kode).

Bruk av biometri kan være et godt bidrag til å utvikle sikre løsninger, men da normalt i kombinasjon med andre metoder for å bekrefte at en person er den han gir seg ut for å være (*autentisering*). For eksempel kan tradisjonelle passord eller kodekort brukes i kombinasjon med en biometrisk løsning. Der kortet kan bli stjålet og koden gitt videre, er biometrien uløselig knyttet til deg. Dersom løsningen og bruken av denne er god, kan biometri gi bedre sikkerhet.

Biometri benyttes også i situasjoner der det ikke nødvendigvis er den høye sikkerheten man er på jakt etter. Eksempler her er bruk av fingeravtrykk i timeregistrering, for å hindre at ansatte registrerer timer for hverandre. Annen bruk kan ha som formål å nettopp gjøre det enkelt for deg som bruker, slik som for eksempel at du kan åpne og lukke garderobeskap i en svømmehall ved hjelp av øyegjenkjenning.

Biometri må brukes riktig

Brukt riktig kan biometri være et godt og effektivt verktøy for sikkerhet. Løsninger som baserer seg på biometri for å oppnå bedre sikkerhet og presisjon, nyter høy tillit i befolkningen. Det er derfor viktig å forhindre uriktig bruk av slike verktøy. Når tilliten til metoden er høy, kan et eventuelt misbruk få store konsekvenser. Det er derfor viktig å huske at en løsning som benytter biometri ikke nødvendigvis fører til bedre sikkerhet. Det også grunn til å være skeptisk til bruk av biometriske løsninger i sammenhenger hvor man hittil ikke har sett noe som helst behov for å identifisere enkeltpersoner.

To situasjoner er særlig aktuelle:

1. Metoden kan være teknisk svak. Biometrisk avlesning skiller seg i utgangspunktet ikke vesentlig fra andre tekniske sikkerhetsløsninger. Det finnes gode og dårlige løsninger, og det vil være et teknologikappløp mellom sikre løsninger og angrep på disse. Dårlige fingeravtrykkslesere kan for eksempel akseptere avkappede fingre og gummihansker med påmontert falske fingeravtrykk.
2. Mangelfull identitetskontroll ved førstegangs-registrering. Dersom feil person blir registrert i utgangspunktet, kan en ikke si at løsningen er sikker, selv om den benytter seg av biometri.

Den viktigste grunnen til å være varsom med bruk av biometri er at biometriske kjennetegn unikt beskriver det enkelte individ, og er uløselig knyttet til denne. En persons biometriske kjennetegn kan ikke skiftes ut. Dersom kriminelle finner metoder for identitetstyveri og utnyttet svakheter i de biometriske løsningene, vil ofrene for dette bli utsatt for betydelige problemer.

Biometriske kjennetegn kan også være bærer av annen informasjon enn det rent identifiserende. DNA er et eksempel på dette. Biometrisk avlesning av øynene, ansiktet eller benbygningen kan i tillegg til å identifisere en enkeltperson også si noe om helse og etnisk bakgrunn.

Biometriske data kan samles uten at du vet det

Innsamling av biometriske opplysninger kan gjennomføres uten at du er klar over det. Vi legger igjen fingeravtrykk overalt hvor vi ferdes. Det samme gjelder hår og spytt. Disse sporene kan kontrolleres i ettertid uten at du er kjent med det. I andre tilfeller kan biometri behandles i sanntid, eksempelvis ved at ansiktet ditt gjenkjennes i et kameraovervåkingsanlegg, eller at stemmen din gjenkjennes.

Summen av opplysninger du legger igjen, bevisst eller ubevisst, kan tegne en tydelig profil av hvem du er og hvilke preferanser du har. Det faktum at det er opplysninger som er uløselig knyttet til deg, tilsier at den virksomheten som samler inn og bruker opplysningene skal være ekstra varsomt. Hovedregelen bør være at dersom det finnes alternative og tilnærmet likeverdige løsninger, så bør virksomheten velge den løsningen som er minst inngripende for den enkeltes personvern.

Biometrisk informasjon kan lagres i form av en såkalt mal. Dette er en kodebasert representasjon av materialet, i stedet for å lagre en hel måling, for eksempel et fullt bilde av fingeravtrykket, med alle dets detaljer. Det er to grunner til at dette har blitt en måte å håndtere biometriske data på:

1. det oppfattes som mindre inngripende for personvernet
2. det er godt egnet for elektronisk behandling

Lagring av biometriske kjennetegn

Virksomheter som tar i bruk biometriske løsninger for å identifisere enkeltpersoner, bør lagre opplysningene som samles inn på en måte som forhindrer misbruk. Datatilsynet anbefaler følgende metoder:

- Unngå sentral lagring av personopplysninger basert på biometri. Opplysningene bør lagres nærmest mulig den som registreres. Personen kan for eksempel bære opplysningene med seg på et smartkort, eller opplysningene kan lagres i den enkelte avleser, på det enkelte bruksstedet.
- Den lagrede informasjon bør gjøres unik for den enkelte installasjon. At en persons biometriske kjennetegn er registrert i en løsning, bør ikke innebære at opplysningene uten videre kan overføres til et annet system. Virksomheten kan unngå dette ved at templatene krypteres med en unik nøkkel for den enkelte installasjon.

https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/

9. mai 2024