Rättsenheten

Datum
2021-06-22

Diarienummer
2021-10066-4

Mottagare
Infrastrukturdepartementet
103 33 Stockholm

Er referens

Europeiska kommissionens förslag till förordning om harmoniserade regler för artificiell intelligens

Säkerhetspolisen har tagit emot förslaget till förordning och lämnar de synpunkter som anges nedan. Utöver det som framförs inom ramen för detta remissvar har myndigheten för avsikt att följa det fortsatta förhandlingsarbetet i EU och lämna ytterligare synpunkter när det efterfrågas och när myndigheten ser ett behov av det.

Övergripande synpunkter

Med hänsyn till att åtgärder för att skydda nationell säkerhet utgör medlemsstaternas exklusiva kompetens undantas Säkerhetspolisens verksamhet förordningens tillämpningsområden. Det är angeläget att det tydligt framgår av förordningen att den inte är tillämplig på AI-system som tas fram eller används för åtgärder som syftar till att skydda nationell säkerhet.

Även om Säkerhetspolisens verksamhet i stort undantas förordningens tillämpningsområden får förordningen konsekvenser för Säkerhetspolisens förmåga på grund av myndighetens nära samverkan med andra brottsbekämpande myndigheter när det gäller utveckling och användning av tekniska system och applikationer.

Syftet med den föreslagna förordningen är att införa ett harmoniserat regelverk för utveckling, försäljning och användning av AI-system inom EU/EES. Förutom vissa uttryckliga undantag är således samma krav tillämpliga för brottsbekämpande myndigheter som för kommersiella aktörer. Med hänsyn till att brottsbekämpande myndigheters behov och syften skiljer sig från kommersiella aktörers bör regleringen i betydligt större utsträckning anpassas för AI-system som används inom brottsbekämpning.

Utifrån den föreslagna definitionen av AI respektive högrisksystem kan en majoritet av brottsbekämpande myndigheters användning av AI komma att klassificeras som hög risk. Säkerhetspolisen vill i detta avseende understryka

Postadress
Box 12312
102 28 Stockholm

Besöksadress
Bolstomtavägen 2
171 69 Solna

Telefon
010-568 70 00
+46-10-568 70 00

Telefax
010-568 70 10
+46-10-568 70 10

E-post/Internet
sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se

att användning av AI-tekniker inom brottsbekämpningen per se inte innebär ökat intrång i den enskildes integritet utan tvärtom kan vara integritetsfrämjande. I det dagliga arbetet hanterar Säkerhetspolisen enorma mängder information och data och mängden ökar i rasande takt i och med den globala digitaliseringsutvecklingen. Att manuellt gå igenom all data är nästintill omöjligt och även om resurserna finns innebär det ett repetitivt arbete, där risken för fel i manuell hantering är ofrånkomlig. Att automatisera sådant arbete med hjälp av AI leder till ett snabbare och mer träffsäkert resultat. AI-system kan göra en initial ytlig granskning av datamängden och flagga upp information som sannolikt relevant för specifika fall. En manuell granskning behöver då endast ske av en mindre mängd information som är av mer direkt intresse, vilket minskar risken för intrång i enskildas integritet. Säkerhetspolisen efterfrågar därför en mer nyanserad bild av brottsbekämpande myndigheters användning av AI i förordningen.

Det är viktigt att regleringen inte negativt påverkar svenska myndigheters förmåga att bedriva effektiv brottsbekämpning med ny och innovativ teknik. För att detta ska kunna uppnås får inte åtgärderna för kontroll och efterlevnad hindra innovation eller utveckling. Krav som inte i tillräcklig utsträckning ställs i proportion till vikten av en effektiv brottsbekämpning kan leda till att brottsbekämpande myndigheter väljer att istället använda teknik som inte omfattas av förordningens krav, vilket på längre sikt bidrar till att myndigheterna hamnar efter tekniskt.

Förordningens krav bör i större utsträckning utformas efter hur AI-system faktiskt utvecklas och används. Då maskininlärningsbaserade AI-system lär sig och anpassas automatiskt från egen data så är gränsdragningen mellan utveckling och användning inte lika självklar som i traditionell mjukvaruutveckling. En för hård reglering av utveckling riskerar att hämma vidareutveckling av AI-system varför regleringen bör vara likvärdig för utveckling och användning.

Alltför högt ställda krav på kommersiella tillhandahållare kan även leda till snedvriden konkurrens och att företag undviker att lansera sina AI-system på den europeiska marknaden.

Artikel 2 – Tillämpningsområde
Säkerhetspolisen anser att det uttryckligen bör framgå av artikel 2 att förordningen inte är tillämplig på AI-system som tas fram eller används för åtgärder som syftar till att skydda nationell säkerhet. Det bör därför införas en liknande skrivning som den föreslagna artikel 2.3, vilken uttryckligen undantar användning av AI-system för militära syften från förordningens tillämpningsområde.

Artikel 3 – Definitioner
Definitionen av AI framgår av artikel 3.1 och med hänvisning Annex I. Eftersom definitionen av AI är avgörande för förordningens tillämpningsområde är det angeläget att förordningens definition av AI inte blir för bred utan enbart träffar de typer av tekniker som förordningen är avsedd att reglera. För att tydliggöra omfattningen föreslås att Annex I ska innehålla beskrivningar av system som träffas av definitionen respektive system som faller utanför tillämpningsområdet.

Artikel 4 – Hur Annex I revideras
I Annex I listas de tekniker som ska anses utgöra AI i förordningens mening. Av artikel 4 framgår att kommissionen genom en delegerad akt får ändra denna lista.

Med hänsyn till vilka långtgående följder en ändring av Annex I har för förordningens tillämpning borde kommissionen ges befogenhet att uppdatera Annex I genom en genomförandeakt. På så sätt ges medlemsstaterna en större möjlighet att påverka en revidering av vilka system och tekniska lösningar som ska anses utgöra AI.

Artikel 7 – Hur Annex III revideras
I Annex III listas de system som är s.k. högrisksystem. Av artikel 7.1 framgår att kommissionen genom en delegerad akt får ändra denna lista.

Säkerhetspolisen anser att kommissionen istället borde ges befogenhet att uppdatera Annex III genom en genomförandeakt. På så sätt ges medlemsstaterna en större möjlighet att påverka vilka AI-system som ska anses vara s.k. högrisksystem.

Remissvaret har beslutats av säkerhetspolischefen Klas Friberg.