Sveriges advokatsamfund

Stockholm den 22 februari 2022

R-2021/2718

Till Justitiedepartementet
Ju2021/04080

Sveriges advokatsamfund har genom remiss den 21 december 2021 beretts tillfälle att avge yttrande över Domstolsverkets promemoria De allmänna domstolarnas rapportering inom brottmålsförfarandet.

Bakgrund

Författningsförslagen är en del av strävandena att utveckla det digitala informationsutbytet i brottmålshanteringen och rättsväsendets informationsförsörjning (RIF). I detta ingår att hanteringen av ärenden som sker mellan myndigheterna i brottmålsprocessen ska övergå från pappersform till digital hantering direkt mellan myndigheternas ärendehanteringssystem.

Advokatsamfundets uppgift är främst att ta ställning till om författningsförslagen påverkar den enskildes rätt till integritet och privatliv samt om inskränkningen av denna rätt som förslagen innebär står i rimlig proportion till samhällets intresse av att kunna behandla personuppgifter för de aktuella ändamålen.

Sammanfattning

Advokatsamfundet anser att förslagen i promemorian i flera delar är rimliga i sig, men att det samtidigt finns vissa förhållanden som bör föranleda ytterligare överväganden och bedömningar i enlighet med vad som påtalas nedan.

Laboratoriegatan 4, Box 27321, 102 54 Stockholm
Tfn 08-459 03 00, advokatsamfundet.se, info@advokatsamfundet.se

Advokatsamfundet kan därför inte ställa sig bakom författningsförslagen i deras nuvarande utformning.

Synpunkter

Allmänna synpunkter på förslaget

Av promemorian framgår att de ifrågavarande uppgifterna behandlas för specifika, tydliga och i förväg definierade ändamål samt att det finns rättslig och laglig grund för behandlingen i de olika författningar som gäller för berörda myndigheters verksamhet.[1] Advokatsamfundet konstaterar även att förslagen inte innebär att de olika myndigheterna ska få direktåtkomst till varandras uppgifter, utan att det endast är fråga om lösningar för elektroniskt utlämnande.[2] Det finns dessutom en rättssäkerhetsvinst i att reglerna så långt som möjligt samlas i färre författningar där uppgifterna inte behandlas hos onödigt många aktörer.[3] I dessa avseenden framstår promemorians förslag som väl genomtänkta och förankrade.

Dock har Domstolsverket i promemorian enligt Advokatsamfundets bedömning inte i tillräcklig omfattning beaktat de särskilda risker som föreligger för den personliga integriteten när det är fråga om behandling av personuppgifter som angår brott och lagföring. Advokatsamfundet konstaterar att man i promemorian i och för sig resonerat kring det särskilda skyddsbehov som en sådan behandling innefattar och kan instämma i promemorians slutsatser, men anser att frågeställningen inte behandlats tillräckligt uttömmande. När ny lagstiftning och andra föreskrifter tas fram bör lagstiftaren analysera konsekvenserna för den personliga integriteten vid personuppgiftsbehandling, vidta en så kallad integritetsanalys. Integritetsskyddsmyndigheten (före detta Datainspektionen) har tagit fram en checklista för denna analys som vänder sig till lagstiftaren.[4]

Säkerheten vid behandling av informationen och personuppgifterna

Advokatsamfundet konstaterar att det i brottmålsprocessen hanteras sådan information om enskilda som utgör personuppgifter. Därtill är personuppgifterna av

[1] Promemorian, s. 28 ff.
[2] Promemorian, s. 35 f.
[3] Promemorian, s. 24.
[4] Vägledning för integritetsanalys, 2016. En vägledning från Datainspektionen för att bedöma integritetsriskerna med ny eller ändrad lagstiftning.

särskilt integritetskänslig art, eftersom det rör sig om uppgifter om brott och lagföring av brott. Därför ställs särskilt höga krav på säkerheten i samband med behandling av denna slags personuppgifter.[5]

Om det är fråga om behandling av särskilt skyddsvärda uppgifter ställer detta särskilt höga krav på att uppgifterna inte blir felaktiga, förvanskade eller förloras. Det ställs också särskilt höga krav på att tillgången till uppgifterna begränsas till så få som möjligt och endast till sådan personal som behöver ha tillgång till uppgifterna i sitt arbete. Detta medför att det måste ställas krav på särskilt hög nivå på de olika säkerhetsåtgärder som ska gälla för berörda informationssystem och kommunikationen mellan dem. I detta ingår att krav måste ställas på kryptering, loggning av systemens användning och att olika lösningar finns för att övervaka systemen. Det måste även finnas rutiner och lösningar för att kunna rätta, korrigera eller komplettera sådan information som av olika skäl blivit missvisande eller felaktig.[6]

Det kan därtill tänkas att myndigheterna väljer olika slags informationstekniska lösningar för behandlingen av den aktuella informationen och personuppgifterna. Detta kan rentav innebära att en utomstående får i uppdrag att sköta informationshanteringen, till exempel genom upphandling av molntjänster eller annan outsourcing. I så fall blir det svårt att se att en sådan lösning skulle kunna genomföras utan att de aktuella personuppgifterna kommer att anses utlämnade till leverantörerna.[7] Det betyder att uppgifterna rentav kan bli tillgängliga för en av myndigheterna anlitad extern leverantör, som dessutom kan finnas utomlands. Detta innebär en risk för minskade möjligheter att utöva kontroll över hur leverantören hanterar informationen, men även för att leverantören i enlighet med det egna landets nationella regelverk överför, utlämnar eller på annat sätt tillgängliggör uppgifter för myndigheter eller andra organisationer på ett sätt som inte skulle vara tillåtet eller lämpligt enligt svensk lagstiftning.

Mot bakgrund av de aktuella personuppgifternas känslighet borde promemorian ha ägnat större uppmärksamhet kring frågor om behörighetsbegränsning och behörighetskontroll avseende den personal hos myndigheterna som ska ha tillgång till

[5] Jfr. t.ex. art. 10 och 32 GDPR.
[6] Se t.ex. HFD 5118-21.
[7] SOU 2018:25 s. 348 ff. och SOU 2021:1 s. 271 f.

personuppgifterna. Detsamma gäller beträffande loggning avseende de åtgärder som personalen vidtar med personuppgifterna.

En ytterligare fråga som under en tid kommit att bli mer och mer aktuell utgörs av det ökande hotet från olika slags IT- eller cyberattacker.[8] Ett antal incidenter har inträffat som drabbat svenska kommuner, myndigheter, företag och andra aktörer och som väckt stor uppmärksamhet. Frågeställningen borde därför ha uppmärksammats betydligt utförligare i promemorian och borde ha föranlett ett resonemang kring behovet av samordning mellan myndigheterna för att möta hoten från IT- och cyberattackerna. Om de olika system som författningsförslagen omfattar exponeras för sådana slags attacker utan att det finns några alternativa och redundanta system som kan tas i drift kan konsekvenserna bli förödande.

Det hade därför varit önskvärt om promemorian hade framhållit behovet av framtagande av säkerhetsföreskrifter för informationshantering och betydelsen i att sådana föreskrifter uppmärksammas och efterlevs.

Advokatsamfundet kan, med hänsyn till vad som nu anförts, inte ställa sig bakom promemorians förslag.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander

[8] Se t.ex. Försvarets radioanstalts, Försvarsmaktens, Myndigheten för samhällsskydd och beredskaps, Polismyndighetens och Säkerhetspolisens gemensamma Rapport 2020 – Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden.