Att dela det odelbara

Av Fredrik Sandström, Hanna Bogsjö Österberg, Staffan Malmgren

Fredrik Sandström

Hanna Bogsjö Österberg

Staffan Malmgren

Digitaliseringen innebär att verksamheter i allt högre grad är beroende av sammanlänkade IT-miljöer, gemensamma plattformar och komplexa leveranskedjor. Parallellt har regleringen av IT, cybersäkerhet och digital motståndskraft utvecklats snabbt, inte minst genom nya EU-regelverk såsom DORA[1] och NIS2-direktivet[2], det senare genomfört i svensk rätt genom cybersäkerhetslagen (2025:1506). Därtill kommer nationell lagstiftning, där säkerhetsskyddslagen (2018:585) intar en särställning i ett svenskt perspektiv.

En röd tråd i olika nya regelverk på IT-området under senare tid är tvingande krav på de villkor som IT-avtal måste innehålla. Som en följd förskjuts fokus i avtalsförhandlingar allt mer från traditionella affärsmässiga frågor som omfattning, pris och riskfördelning, till frågor om regelefterlevnad, insyn och kontroll. Detta tar sig konkret uttryck i bl.a. hårdare säkerhetskrav, krav på incidenthantering och rapportering, samt i vissa fall även krav på särskilda uppsägningsgrunder, revisionsrättigheter och krav rörande underleverantörer.

I praktiken är det vanligt att en köpare av IT-tjänster omfattas av flera regelverk samtidigt. I det förberedande arbetet inför upphandling av IT-tjänster är därför en inledande och central fråga vilka regelverk som gäller, vilka rättsliga ramar dessa sätter för leverantörsrelationen och hur de påverkar utformningen av avtalet. Detta är särskilt påtagligt för företag som verkar inom finansiell sektor och andra högreglerade områden.

En utmaning för många köpare av IT-tjänster är de skilda angreppsätt lagstiftaren valt för att definiera tillämpningsområdet för olika relevanta regelverk. Vissa knyter tillämpligheten till verksamhetens art eller aktörens formella klassificering, medan andra tar sikte på vilka funktioner som faktiskt stöds, eller till en verksamhet och dess betydelse ur ett samhälls- eller säkerhetsperspektiv. Skillnader i tillämpningslogik innebär att samma IT-tjänst eller leverantör kan omfattas av olika krav beroende på vilket slags verksamhet kunden bedriver, hur verksamheten är organiserad, och hur tjänsten i fråga används.

Som ett analytiskt grepp kan tre regelverk som är särskilt relevanta vid köp av IT-tjänster ställas mot varandra för att belysa skillnader i tillämpningslogik och räckvidd.

Skillnaderna mellan tillämpningsområdena kan ge intrycket av att det är möjligt att, genom organisatoriska eller tekniska åtgärder, påverka vilka regelverk och krav som är tillämpliga (en form av s.*k. regulatory arbitrage*). Ett exempel som ibland diskuteras är möjligheten till ”paketering” av viss verksamhet i ett separat bolag. Ett annat är åtgärder för att segmentera olika IT-tjänster och IT-miljöer, och på så sätt undanta delar av verksamheten från ett visst regelverks tillämpningsområde.

1 Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011

2 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148

Regelverk	Vad avgör tillämplighet?	Vad träffas?	Vad omfattas?
DORA	Tre samverkande faktorer: (1) vem kunden är (finansiell entitet), (2) vad kunden köper (IKT-tjänster), och (3) hur tjänsterna används (om de stödjer en kritisk eller viktig funktion ställs strängare krav)	Kunden som finansiell entitet (juridisk person)	Digitala-/datatjänster som fortlöpande tillhandahålls genom IKT-system till en eller flera interna eller externa användare ( )
Cyber-säkerhets-lagen	Två samverkande faktorer: (1) vem och hur stor kunden är, och (2) vilka sektorer kunden bedriver verksamhet inom	Kunden som väsentlig eller viktig verksamhetsutövare/-entitet	Avtal som innefattar att behandling av information utkontrakteras till en leverantör
Säkerhets-skyddslagen	Vilken verksamhet kunden bedriver, inklusive vilken information kunden hanterar inom denna verksamhet	Den säkerhetskänsliga delen av kundens verksamhet	Säkerhetskänslig verksamhet, inklusive säkerhetsskydds-klassad information, som leverantören får tillgång till

Under slutet av 2025 uttalade sig t.ex. EIOPA om möjligheten att begränsa DORA:s tillämplighet till endast delar av ett företags verksamhet. Utöver att klargöra att DORA tillämpas på entitetsnivå uttalade EIOPA att det, under vissa snävt avgränsade förutsättningar, kan vara möjligt för en finansiell entitet att undanta icke-reglerade delar av verksamheten från DORA:s krav. En förutsättning för detta är enligt EIOPA att *"IKT-miljöer är fullt separerade, och där risken för påverkan eller smittspridning effektivt kan uteslutas"*.[3]

Vad gäller NIS2 har det på EU-nivå inte på ett tydligt sätt klargjorts om samtliga nätverks- och informationssystem inom en verksamhetsutövares verksamhet omfattas, eller bara de som används för att tillhandahålla tjänster/bedriva verksamhet som omfattas av direktivet. Den svenska lagstiftaren har gjort bedömningen att direktivets utformning talar för att hela verksamheten ska omfattas. Även om så inte vore fallet är NIS2 ett s.k. minimidirektiv, vilket innebär att medlemsstaterna får införa mer omfattande bestämmelser. Utifrån bl.a. risken för gränsdragningsproblem har den svenska lagstiftaren gjort bedömningen att varje verksamhetsutövare är odelbar och omfattas i sin helhet.[4] I cybersäkerhetslagen finns därför ingen avgränsning av vilka nätverks- och informationssystem som omfattas, inklusive sådana som omfattas av lagens krav på säkerhet i leveranskedjan.

> Utifrån bl.a. risken för gränsdragnings-problem har den svenska lagstiftaren gjort bedömningen att varje verksamhetsutövare är odelbar och omfattas i sin helhet.

Den svenska säkerhetsskyddslagens tillämpningsområde överlappar med cybersäkerhetslagen. Samma omständigheter som gör att ett företag utgör en viktig eller väsentlig verksamhetsutövare enligt cybersäkerhetslagen, kan medföra att verksamheten även är av betydelse för Sveriges säkerhet. Cybersäkerhetslagen har därför ett undantag från sitt tillämpningsområde för de delar av verksamheten som faller under säkerhetsskyddslagen.[5] Undantaget är utformat så att vissa skyldigheter enligt cybersäkerhetslagen inte gäller för just dessa delar av verksamheten.

Säkerhetsskyddslagen, inklusive de delar som är relevanta vid köp av IT-tjänster, gör skillnad på verksamhet av betydelse för Sveriges säkerhet (säkerhetskänslig verksamhet) och verksamhetsutövaren som sådan. Vissa skyldigheter träffar verksamhetsutövaren som helhet, exempelvis skyldighet att upprätta en säkerhetsskyddsanalys. Däremot gäller krav på att ingå säkerhetsskyddsavtal eller motsvarande med en leverantör av IT-tjänster bara till den del leverantören kan få del av säkerhetsskyddsklassificerade uppgifter eller annan verksamhet av be-

3 *https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora-136-3193_en*

4 Prop. 2025/26:28 s 42 f

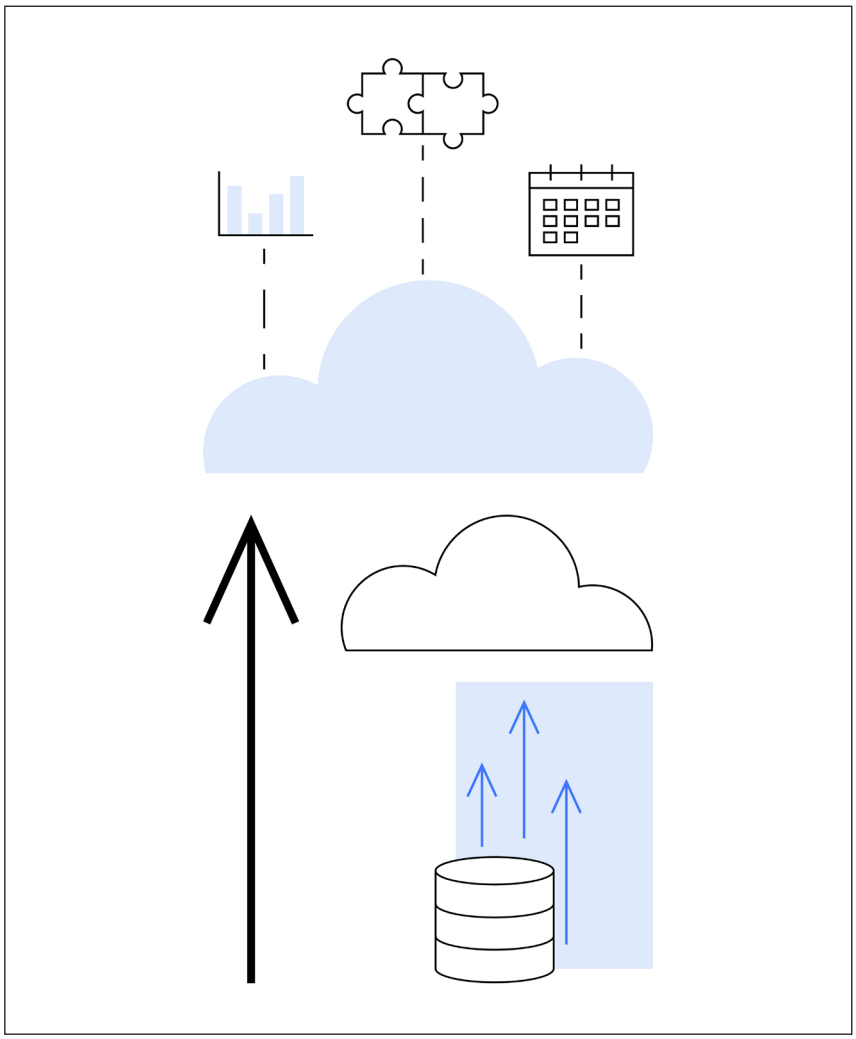
5 1 kap. 12 § 3 st. cybersäkerhetslagen.

tydelse för Sveriges säkerhet.[6] Säkerhetsskyddslagen gör ingen skillnad på om leverantören skulle ingå i samma koncern som kunden eller har identisk ägarstruktur.

Denna skillnad i tillämpningsområde kan leda till närmast paradoxala slutsatser. Företag som till största delen bedriver helt okänslig verksamhet (utanför såväl cybersäkerhetslagens som säkerhetsskyddslagens tillämpningsområde), men som till en mindre del bedriver högkänslig verksamhet – exempelvis transportverksamhet som både faller under punkt 2 i NIS2-direktivets bilaga 2 och utgör nationellt samhällsviktig verksamhet[7] – kan i sin helhet omfattas av cybersäkerhetslagen. Det innebär att kraven i cybersäkerhetslagen gäller för företagets samtliga IT-tjänster, utom för just de högkänsliga delar av verksamheten som föranledde att cybersäkerhetslagen blev tillämplig från första början (eftersom säkerhetsskyddslagen ska tillämpas på dessa delar i stället). För att minska regelbördan bör alltså ett sådant företag överväga att paketera den högkänsliga verksamheten i ett eget bolag, så att den största delen av verksamheten varken omfattas av cybersäkerhetslagen eller säkerhetsskyddslagen.

Samtidigt framstår sådana resonemang i praktiken ofta som svåra att omsätta. Moderna IT-lösningar är typiskt sett tätt integrerade med övriga system och processer inom verksamheten, exempelvis genom gemensamma plattformar för identitetshantering, drift, datalagring och säkerhet. Därutöver är modern IT-drift i regel centraliserad och utformad för att uppnå stordriftsfördelar, effektiv resursanvändning och enhetlig styrning. Dessa förutsättningar gör det ofta svårt att åstadkomma den grad av teknisk och organisatorisk separation som krävs för att undantagsreglerna ska bli tillämpliga, utan att samtidigt ge avkall på de effektiviserings- och innovationsvinster som utgör själva drivkraften bakom modern IT.

Utifrån dessa förutsättningar är det lätt att förstå att den svenska lagstiftaren valt att betrakta varje företag som en odelbar enhet vid implementeringen av NIS2. Samtidigt är det också lätt att dela den osäkerhet och frustration många större och mer invecklade företagskoncerner känner över att lagstiftningen på IT-området i allt större grad får en strukturell och organisatorisk påverkan. Klart är i vart fall att frågan om hur en köpare av IT-tjänster bör organisera sin verksamhet och bolagsstruktur inte har något självklart svar, vare sig nu eller i den överskådliga framtiden.



Illustrasjon: Colourbox.com

Staffan Malmgren är Legal Technology Officer på Advokatfirman Kahn Pedersen och jobbar särskilt med tekniknära frågor inom bl.a. informationssäkerhetsreglering, it-avtal och dataskydd.

Hanna Bogsjö Österberg är Advokat på Advokatfirman Kahn Pedersen. Hon arbetar inom byråns specialistområde Digital och särskilt med juridiska frågor i samband med digital transformation, IoT och strategiska sourcingprojekt.

Fredrik Sandström, Advokat och Managing Associate på Advokatfirman Kahn Pedersen. Han arbetar främst med juridiska frågor kopplade till IT, digitalisering och teknikintensiva projekt inom bl.a. bank, försäkring, energi och industri.

6 4 kap. 11 § säkerhetsskyddslagen samt 7 kap. 11 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd

7 Jfr Säkerhetspolisen. Vägledning i säkerhetsskydd – Introduktion (2023), s 7