



Högsta domstolen  
Box 2066  
103 12 Stockholm

## **LN ./ riksåklagaren ang. dataintrång**

*(Göta hovrätts dom den 21 december 2012 i mål nr B 2215-12)*

Efter att ha meddelat prövningstillstånd i målet har Högsta domstolen förelagt mig att inkomma med svarsskrivelse. Jag vill anföra följande.

### **Min inställning**

Jag bestrider ändring av hovrättens dom.

### **Bakgrund**

#### **Åtalet**

LN åtalades för dataintrång enligt följande gärningsbeskrivning.

LN arbetade bl.a. dagarna den 1 och 8 december 2010 samt den 25 mars 2011 som kommissarie vid polismyndigheten i XXX län med placering i X. Han beredde sig vid dessa tillfällen uppsåtligt och olovligt tillgång till uppgift avsedd för automatiserad behandling genom att via s.k. multifrågor och följdfrågor till dessa använda polisens IT-system för att inhämta uppgifter om vad som fanns antecknat om honom själv i olika register. Slagningarna var inte nödvändiga för att genomföra en viss arbetsuppgift. Gjorda slagningar och utfallet av dessa framgår av bilaga 1.

### **Tingsrättens dom**

LN vidgick de faktiska förhållandena, men förnekade brott.

Tingsrätten dömde LN för dataintrång den 25 mars 2011 till dagsböter. Åtalet avseende dataintrång den 1 december 2010 och den 8 december 2010 ogillades.

Av tingsrättens domskäl framgår bl.a. följande.

LN har ostridigt tagit sig in i polismyndighetens IT-system vid de tillfällen åklagaren påstått. Oaktat vad LN uppgivit om skälen härtill har han inte gjort detta för att genomföra en viss arbetsuppgift. Han har därigenom brutit mot 4 § i RPSFS 2005:8. Denna bestämmelse är inte straffsanktionerad och kan därför inte ensam ligga till grund för att konstatera brott.

Av 4 kap 9 c § brottsbalken framgår att den som olovligt bereder sig tillgång till en uppgift som är avsedd för automatisk databehandling döms för dataintrång.

I målet är inte påstått annat än att de uppgifter som LN erhållit genom att ta sig in i passregistret och fastighetsregistret är uppgifter som varit kända för honom och därför informationen fanns att tillgå på annat sätt. Han kan därför i dessa delar inte anses ha olovligt berett sig tillgång till uppgifterna. Åtalet skall därför ogillas i dessa delar.

Vad gäller uppgifterna från misstankeregistret har dessa i det skede då de inhämtades inte varit tillgängliga för LN. Polisen skall ha möjlighet att utreda brott utan att den misstänkte kan påverka utredningen. Inhämtandet av information från misstankeregistret har därför varit olovligt och LN skall i denna del fällas till ansvar för dataintrång.

### **Hovrättens dom**

LN överklagade tingsrättens dom och yrkade att hovrätten skulle frikänna honom.

Åklagaren överklagade tingsrättens dom och yrkade att hovrätten skulle döma LN för dataintrång även den 1 december och den 8 december 2010 och skärpa bötesstraffet.

Hovrätten ändrade tingsrättens dom på så sätt att hovrätten dömde LN även för dataintrång den 1 december 2010 och den 8 december 2010 samt bestämde påföljden för tre fall av dataintrång till 50 dagsböter om vardera 350 kr.

Hovrätten anförde bl.a. följande i domskälen.

Mot bakgrund av de uppgifter LN har lämnat beträffande skälet till hans åtgärder, är det klarlagt att dessa inte har varit nödvändiga för att han skulle kunna genomföra en viss arbetsuppgift. Att en användning av IT-systemet på det sätt som har skett inte är tillåtet enligt de föreskrifter som har utfärdats av Rikspolisstyrelsen måste ha stått klart för LN, som vid tidpunkten för gärningarna var poliskommissarie i chefsställning. Det är alltså visat att LN med uppsåt olovligen har berett sig tillgång till polisens IT-system vid de aktuella tillfällena.

Eftersom den s.k. multifrågan får till följd att datasystemet lämnar information om och i så fall i vilken utsträckning vederbörande förekommer i de register som Polismyndigheten för, har LN redan genom att ställa en sådan fråga beträffande sig själv berett sig tillgång till uppgifter avsedda för automatiserad behandling. Var och en av de multifrågor han har ställt den 1 december 2010, den 8 december 2010 och den 25 mars 2011 utgör därmed ett brott. De efterföljande slagningar som LN har gjort i registren till följd av de svar systemen har lämnat, får enligt hovrättens bedömning närmast ses som gärningar inom ramen för dessa brott. LN ska därför i denna del dömas för dataintrång i tre fall.

### **Överklagandet**

LN har överklagat hovrättens dom och yrkat att Högsta domstolen ska ogilla åtalet.

LN har till grund för sitt överklagande anført bl.a. följande. I 4 § RPSFS 2005:8 (FAP 170-1) föreskrivs inget förbud mot att söka uppgift om sig själv, bara att sökningen ska vara tjänsteanknuten. De uppgifter som han sökt i fastighets- och folkbokföringsregistret är allmänt tillgängliga. Så är inte fallet med uppgifterna i misstankeregistret. Skälet till sökningen i det registret var att

han skulle kunna hantera en situation som uppstått under en utbildning av eftersöksjägare, vilken han som länsansvarig polis ledde. Enligt hans bedömning hade sökningen därför en i 4 § FAP 170-1 föreskriven tjänsteanknytning. Besöket i misstankeregistret skedde dessutom efter det att LN hörts i ärendet (som sedermera avskrevs), varför ingen utredning har kunnat skadas.

Hovrätten har påpekat att det via multifråga går att nå Polisens allmänna spaningsregister. Det är riktigt men i förevarande fall ointressant eftersom LN inte förekommit i det registret och inte heller sökt uppgift där.

I ett fall som detta, där sökningarna avsett dels ett register som är allmänt tillgängligt (fastighets- och folkbokföringsregistret), dels ett register som i och för sig är sekret (misstankeregistret), men där sökningen – i vart fall med den extensiva tolkning som ska tillämpas i ett straffrättsligt sammanhang – varit tjänsteanknuten och – i vart fall – inte kunnat skada någon pågående utredning, bör sökningarna bedömas som tillåtna och åtalet ogillas.

## **Grunderna för min inställning**

### **Bestämmelsen om dataintrång**

Enligt 4 kap. 9 c § brottsbalken döms den som, i annat fall än som sägs i 8 och 9 §§, olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad databehandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift för dataintrång till böter eller fängelse i högst två år.

Försök och förberedelse till dataintrång som om det fullbordats inte skulle ha varit att anse som ringa är straffbart enligt 4 kap. 10 § brottsbalken.

Bestämmelsen om dataintrång infördes i brottsbalken 1998 i samband med att den tidigare datalagen (1973:289) ersattes med personuppgiftslagen (1998:204) (prop. 1997/98:44). Datalagens bestämmelse om dataintrång (21 §) överfördes då till brottsbalken utan ändring i sak. Bestämmelsen om dataintrång fick sin nuvarande utformning genom en lagändring 2007 som i huvudsak syftade till att genomföra EU:s rambeslut 2005/222/RIF om angrepp mot informationssystem (prop. 2006/07:66).

Bestämmelsen om dataintrång skyddar helt allmänt datalagrat material mot obehöriga åtgärder, oavsett om åtgärderna medför ett otillbörligt integritetsintrång eller inte (prop. 1973:33 s. 105).

Uttrycket ”uppgift som är avsedd för automatiserad behandling” infördes i samband med lagändringen 2007 och ersatte det tidigare använda begreppet ”upptagning för automatisk databehandling”. Avsikten med begreppet är att

fånga in alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en automatiserad behandling anpassad och läsbar form. Även program av olika slag ska omfattas av begreppet. Det är för tillämpningen av begreppet utan betydelse var någonstans de nämnda uppgifterna finns eller förvaras i systemet (prop. 2006/07:66 s. 40 f. och 49).

Ansvar förutsätter att gärningen är olovlig. Samtycke från den som är behörig att förfoga över uppgiften eller som sker i överensstämmelse med gällande rätt utesluter således brott (a. prop. s. 17).

Beträffande uttrycket ”olovligen bereder sig tillgång till” finns det inte i lagrummet angivet någon begränsning med avseende på syftet med åtgärden. Intrånget behöver således inte ha skett i något särskilt syfte, t.ex. för att hämta information eller för att åstadkomma skada eller någon annan följd. Inte heller krävs att någon säkerhetsåtgärd kringgås. Vad som beläggs med straff är själva intrånget (Holmqvist m.fl. Brottsbalken En kommentar Kap. 1-12 s. 4:9 c s. 5).

Dataintrång är ett uppsåtligt brott. Alla uppsåtsformer är tillämpliga, även likgiltighetsuppsåt (a. prop. s. 50 och Holmqvist m.fl. Brottsbalken En kommentar Kap. 1-12 s. 4:9 c s. 6).

## **Min bedömning**

### *Skuldfrågan*

LN har ostridigt, vid tre tillfällen, berett sig tillträde till Polisens IT-system genom att via s.k. multifrågor söka på sitt eget personnummer. Polisen har ett system som benämns PMFWEB, vilket närmast kan beskrivas som en sökmotor i Polisens IT-system. Vid användandet av detta system kan användare ställa en s.k. multifråga (PMF). En slagning på personnummer eller ett registreringsnummer genom en multifråga innebär en sökning i ett antal databaser där PMF sammanställer informationen enligt de val som användaren kan göra i applikationen. De val som avses är främst om svaret ska sammanställas som ett begränsat eller som ett utvidgat svar. En del databaser som är knutna till PMF kan också nås via direktlänkar.

PMF redovisar inte all information i de databaser i vilka sökbegreppet ger en träff. I PMF framgår om en person förekommer eller inte i respektive databas. Beträffande misstankeregistret och brottsregistret redovisas också i förekommande fall hur många avsnitt som finns för den aktuella personen. Vid behov kan den som söker i PMF klicka sig vidare via länkar i PMF till respektive databas för att ta del av den ytterligare information som finns lagrad där.

De av LN ställda multifrågorna resulterade i sökningar i alla de databaser som var kopplade till frågan, däribland Polisens person- och adressregister (PPA),

misstankeregistret (MR), brottsregistret (BR), allmänna spaningsregistret (ASP) och DNA/utredningsregistret (DNA). Multifrågan gav LN svar på i vilka av de genomsökta databaserna han förekom och i vilka databaser han inte förekom. Resultatet av sökningen redovisades i säkerhetsloggen för respektive genomsökt databas med siffran 0 om det inte blev någon träff i registret och 1 om det blev en träff i registret.

Vid vart och ett av de tre tillfällena har LN därefter gått vidare och gjort fördjupade slagningar i vissa databaser. Den 1 december 2010 gjorde han fördjupade slagningar i fastighets- och folkbokföringsregistret via Polisens person- och adressregister. Den 8 december 2010 gjorde han också fördjupade slagningar i fastighets- och folkbokföringsregistret via Polisens person- och adressregister. Slutligen gjorde han den 25 mars 2011 fördjupade slagningar i misstankeregistret.

Som ovan anförts leder en s.k. multifråga till att IT-systemet PMFWEB lämnar information om huruvida den eftersökte förekommer i samtliga de databaser som är knutna till multifrågan. LN har därför redan genom att ställa en s.k. multifråga berett sig tillgång till en uppgift som är avsedd för automatiserad behandling. Han har fått information om huruvida han förekommer i exempelvis misstankeregistret respektive allmänna spaningsregistret. Att LN endast har haft för avsikt att göra fördjupade sökningar i vissa register saknar betydelse för frågan om rekvisiten ”bereder sig tillgång till en uppgift som är avsedd för automatiserad databehandling” ska anses uppfyllda. För att LN ska kunna dömas för dataintrång erfordras emellertid också att hans handlande skett olovligen.

Av betydelse för om hans handlande skett olovligen är i vilken utsträckning den som är behörig att förfoga över uppgifterna, dvs. Polisen själv, har gett tillstånd till att deras IT-system får användas. Åtkomst till samtliga databaser som är knutna till PMFWEB förutsätter särskild behörighet. LN har av Polisen givits behörighet att göra slagningar i Polisens IT-system. I detta fall har Rikspolisstyrelsen, som systemägare, genom bestämmelser i 4 § RPSFS 2005:8 gjort den begränsningen att IT-system<sup>1</sup> som är tillgängliga inom Polisen endast får användas när det är nödvändigt för att genomföra en viss arbetsuppgift. Det ska vidare vara sannolikt att användandet i det enskilda fallet är till nytta för arbetets genomförande. I 5 § RPSFS 2005:8 anges vissa undantag för användningen av system för e-post, internetåtkomst, telefoni och öppna delar av Polisens intranät<sup>2</sup>. Dessa undantag omfattar inte den användning som förekommit i detta ärende.

<sup>1</sup> Med ”IT-system” avses enligt 3 § RPSFS 2005:8 ett informationsbehandlingssystem som baseras på informationsteknik, såsom radio-, telefoni-, datorkommunikations- eller datorsystem.

<sup>2</sup> Med ”öppna delar av Polisens intranät” avses enligt 3 § RPSFS 2005:8 del delar av Polisens intranät som är åtkomliga utan att särskild behörighet krävs, t.ex. kontorsinformationsprogram.

Enligt min bedömning är genom Rikspolisstyrelsens föreskrifter på ett tydligt sätt klarlagt att all användning av Polisens IT-system som inte är nödvändig för att genomföra en viss arbetsuppgift är otillåten. Sådan användning måste alltså betraktas som olovlig.

LN har invänt att det inte är förbjudet att, som i detta fall, göra slagningar på sig själv, så länge slagningen är tjänsteanknuten. Enligt LN har hans slagningar varit nödvändiga för att genomföra en viss arbetsuppgift, nämligen för att med bibehållen auktoritet kunna undervisa s.k. eftersöksjägare inom Nationella viltolycksrådet i Kronobergs län.

Det är enligt min bedömning uppenbart att inte någon av de aktuella sökningarna i databaserna kan anses ha varit nödvändig för att LN skulle kunna fortsätta att undervisa eftersöksjägare. Olovlighetsrekvisitet är därmed uppfyllt.

LN har således olovligen vid tre tillfällen berett sig tillgång till Polisens IT-system redan genom att ställa en s.k. multifråga. Som hovrätten också funnit bör de efterföljande slagningar som LN har gjort i registren till följd av de svar systemet har lämnat, närmast ses som gärningar inom ramen för respektive dataintrång.

Vad gäller samtliga slagningar är det utan betydelse i straffbarhetshänseende om de databaser som Polisens system söker igenom ger besked som bara innehåller uppgifter som kan erhållas på annat sätt eller som den som utför slagningen kan förväntas ha kunskap om. Det som är straffbelagt är själva intrånget, dvs. att olovligen bereda sig tillgång till viss information. Detta sålunda oberoende av att LN dessutom vid samtliga multifrågor fått besked om förekomst i det skyddsvärda misstankeregistret.

Att LN hade kännedom om att det fanns en misstanke beträffande honom registrerad i misstankeregistret saknar således betydelse för hans rätt att söka i registret. Som angivits ovan var sökningen inte heller nödvändig för att genomföra en viss arbetsuppgift. Dessutom hade det kunnat förekomma att andra misstankar registrerats i misstankeregistret, vilka han ännu inte fått vetskap om.

Någon invändning om att LN, som var poliskommissarie i chefsställning, vid den här tiden inte kände till regleringen i RPSFS 2005:8 har inte framförts. LN måste också ha förstått att sådana slagningar som han gjorde inte var nödvändiga för att genomföra en arbetsuppgift och att de därmed skett utan Polisens samtycke, dvs. olovligen.

LN har sålunda med uppsåt olovligen berett sig tillgång till Polisens IT-system vid de tre aktuella tillfällena.

LN ska sammanfattningsvis dömas för tre fall av dataintrång.

*Påföljdsfrågan*

Vid straffvärdebedömningen bör bl.a. beaktas vilken typ av IT-system intrånget sker i. I detta fall är den fördjupade sökningen i misstankeregistret mest straffvärd. Det faktum att LN delgivits misstanke om tjänstefel vid tiden för sökningen innebär inte att det går att se mindre allvarligt på hans handlande. Han kunde t.ex. inte veta om misstanken kvarstår som den delgavs eller om det uppkommit andra misstankar som han inte delgivits.

Vid straffvärdebedömningen bör därför, vilket hovrätten också gjort, i skärpande riktning beaktas att LN gjort en fördjupad sökning i misstankeregistret. Den utdöma påföljden, som avser tre fall av dataintrång, framstår som väl avvägd.

Hovrättens dom bör mot denna bakgrund stå fast.

**Bevisuppgift m.m.**

Som bevisning återopas förhör med LN. Förhöret kan förebringas genom uppspelning av tingsrättens ljud- och bildupptagning. Vidare återopas loggutdrag, förundersökningsprotokollet, tab 5, s. 4-7. Jag anser att målet bör kunna avgöras utan huvudförhandling.

Anders Perklev

Hedvig Trost

Kopia till:

Utvecklingscentrum Stockholm  
Utvecklingscentrum Malmö  
Riksenheten för polismål (AM-97099-11)