Blendow Lexnova Expertkommentar - Offentlig rätt, december 2012

Personuppgiftsansvaret när tjänster tillhandahålls via nätverk

Det har under 2012 kommit ett par avgöranden som rör personuppgiftsansvaret enligt personuppgiftslagen (1998:204) när tjänster tillhandahålls via nätverk såsom internet, men en hel del är fortfarande oklart. Med personuppgiftsansvarig avses den som har bestämt ändamålen med och medlen för att behandla personuppgifter. Det är den personuppgiftsansvarige som har att se till att bestämmelserna i lagen följs även när den ansvarige anlitar ett så kallat personuppgiftsbiträde för att för den ansvariges räkning utföra själva behandlingen.

Den 5 juni kom Högsta förvaltningsdomstolen med ett vägledande avgörande (HFD 2012 ref. 21). I målet hade Försäkringskassan av Datainspektionen ålagts att såsom personuppgiftsansvarig göra en risk- och sårbarhetsanalys av självbetjäningstjänster där föräldrar och arbetsgivare via sms respektive dator kan lämna uppgifter till Försäkringskassan. Försäkringskassan överklagade Datainspektionens beslut och menade att kassan inte var personuppgiftsansvarig för någon behandling av personuppgifter innan dessa nått kassan. Högsta förvaltningsdomstolen ansåg att Försäkringskassan hade bestämt både ändamålen med behandlingen – att anmäla olika sjukfall – och medlen för behandlingen – de kommunikationsvägar som hade anvisats för anmälningarna. Enligt domstolen förutsattes det för personuppgiftsansvar att den som bestämt ändamål och medel för behandlingen också vidtar åtgärder som innefattar behandling eller låter sådana åtgärder utföras för sin räkning. Trots att Försäkringskassan inte hade möjlighet att påverka hur uppgifterna hanteras innan de blir tillgängliga för kassan, ansåg domstolen att den serie av åtgärder som vidtas kunde betraktas som led i kassans behandling av uppgifter. Det spelade inte någon roll om någon av åtgärderna var behandling av personuppgifter även hos någon annan, t.ex. den arbetsgivare som gjorde anmälningar. Domstolens slutsats blev att Försäkringskassan kunde åläggas att redovisa säkerheten vid behandlingen.

Rättsfallet får anses ge uttryck för en helhetssyn på personuppgiftsansvaret: Den som inrättar metoder för att för visst syfte behandla personuppgifter får personuppgiftsansvar, åtminstone såvitt avser säkerhetsåtgärder, för hela kedjan av behandlingsåtgärder även om också någon annan skulle ha sådant ansvar för en del av åtgärderna.

År 2002 (dnr 1682-2002) hade Datainspektionen kommit fram till att Saab, som i sålda bilar hade monterat in ett så kallat krockminne för att efter en trafikolycka kunna hämta in personuppgifter från minnet, inte hade personuppgiftsansvar för behandlingen förrän Saab faktiskt hämtar in uppgifterna. Även om Saab hade bestämt ändamålen med och medlen för behandlingen, hade Saab nämligen dessförinnan inte någon rättslig eller faktisk möjlighet att förfoga över uppgifterna. Det avgörandet får anses överspelat genom Högsta förvaltningsdomstolens dom, som klart tyder på att Saab borde ha ansetts ha personuppgiftsansvar till exempel för säkerheten hos krockminnet och vara skyldigt att exempelvis se till att inga obehöriga kunde komma åt personuppgifterna i minnet och att överföringen från minnet till Saab gick till på ett säkert sätt.

Det finns i fråga om personuppgiftsansvaret i Datainspektionens senare praxis också en annan utvecklingslinje som inte verkar bygga på en helhetssyn. Det gäller tjänster som företag tillhandahåller användare via internet. Den som hos Facebook inrättar en sida har av Datainspektionen ansetts ha personuppgiftsansvar för det som han eller hon eller andra användare lägger upp på den sidan, men inspektionen har inte uteslutit att även företaget Facebook kan ha ett

personuppgiftsansvar (beslut 2010-07-02, dnr 685–687-2010). Det sistnämnda ligger i linje med ett beslut som Datainspektionen hade fattat ett halvår tidigare (2010-01-11, dnr 1288-2009). I det fallet ansågs det företag som på internet hade lagt ut en databas över näringsidkare där användare kunde skriva in omdömen om näringsidkarna personuppgiftsansvarig även för det som användarna hade skrivit. Den 18 september 2012 kom emellertid Datainspektionen med ett nytt beslut om ett företag som tillhandahåller tjänster via internet (dnr 913-2012). Den här gången gällde det webbplatsen www.laget.se där idrottsföreningar kan skapa en sida för ett lag med bland annat medlemsförteckning. I detta fall verkade det onekligen som om det var företaget bakom webbplatsen som hade bestämt ändamålen med behandlingen – att administrera och informera om idrottslag – och medlen för behandlingen – de olika funktionerna som tillhandahålls på webbplatsen – och dessutom vilka närmare personuppgifter som skulle kunna föras in, till exempel personnummer i medlemsförteckningen. Men Datainspektionen ansåg ändå att företaget inte hade personuppgiftsansvar utan det hade (bara) de olika idrottsföreningarna. Inspektionen framhöll att den som har tillgång till uppgifterna, men som inte självständigt får ändra, komplettera eller radera personuppgifterna, inte kan anses ha sådan bestämmanderätt över ändamålen med och medlen för behandlingen att han eller hon kan anses som personuppgiftsansvarig. I den situationen att företaget på begäran av en idrottsförening hjälper till med att hantera uppgifter fick företaget anses som personuppgiftsbiträde till föreningen. Det är svårt att förstå hur frågor om säkerheten för personuppgifter som föreningarna registrerar ska hanteras med det synsättet.

Man kan jämföra med hur Datainspektionen har sett på personuppgiftsansvaret vid så kallade molntjänster. I det fallet verkar de företag som tillhandahåller tjänsterna, till exempel lagring och databasprogramvara där användarna kan lagra uppgifter, inte heller ha rättslig behörighet att självständigt ändra, komplettera eller radera personuppgifterna. Men här anser Datainspektionen att företaget alltid är personuppgiftsbiträde åt de personuppgiftsansvariga användarna. På motsvarande sätt får man enligt min mening betrakta relationen mellan webbhotell och deras kunder.

Man kan också jämföra med hur Datainspektionen såg på en hemsida där användare kunde skriva en polisanmälan som sedan sändes med e-post till polisen (beslut 2006-07-10, dnr 706-2006). Företaget som tillhandahöll hemsidan ansågs personuppgiftsansvarigt trots att företaget inte läste, redigerade eller lagrade den information som skrevs in utan bara sände den till polisen. Länsrätten i Stockholms län gjorde efter överklagande samma bedömning (dom 2007-10-24 i mål nr 16617-06).

Det förefaller svårt att hitta någon riktigt klar linje i praxis för när företag som tillhandahåller tjänster via nätet ska anses som personuppgiftsansvarig, personuppgiftsbiträde eller ingetdera. Det är olyckligt med hänsyn till den betydelse sådana tjänster har fått.

Sören Öman

Vice ordförande Arbetsdomstolen, föreståndare för Stockholm Centre for Commercial Law vid Stockholms universitet.