RIKSREVISIONEN

Intervju KTH10

Datum: 2023-02-20

Plats: KTH

Deltagande

KTH

Prefekter, institutioner vid Skolan för elektroteknik och datavetenskap

RiR

- Sara, Ludvig

Introduktion av Sara

A: Ska vi börja berätta lite om våra institutioner?

Precis, det är första frågan!

A: KTH är indelat i fem skolor.

B: under avdelningarna finns det även forskargrupper.

A: Så avdelningar är den sista formella organisationen. Ekonomiska huvudansvaret för prefekt är utbildningsbudgeten. Men det är avdelningen som sköter sin egen forskning och forskningsutbildning. Inklusive externfinansierad.

Vilka huvudsakligs arbetsuppgifter som prefekt?

A: vi har en delegation, så en hel del att skriva på avtal, inklusive anställningsavtal. Minns inte exakt siffror, men vi kan firmateckna för statligt finansierad forskning upp till 10 mnkr. Och en del industrisamarbeten. Men inte eu. SFS kan vi. Så det är den delegationen vi har för forskningsfinansiering. Sen kan vi skriva på en hel del anställningskontrakt, men lite begränsat.

På avdelningsnivå, är det ni som skriver på då?

A: ja det är vi.

B: om det är lärare som ska skrivas på så är det skolan.

A: även en nyanställd doktorand måste till skolchefen faktiskt.

Infosäk... hur stöter ni på det i er vardag?

A: många av oss lägger dataförvaring i begreppet. Det är det vi stöter på. Även personligen. Vilka molntjänster kan man använda och inte. Annars när man undertecknar forskningsprojektavtal. Varje projekt har ett avtal. Vissa är väldigt allmänt hållna, typ med VR. Medan dom med företag ofta är mkt mer detaljerade. När beslutet är taget att vi ska ta emot forskningsprojekt och det är finansierat så är det den enskilda projektledaren som ansvarar för det operativa, inklusive datahantering och infosäk. Från min egen institution har vi allt från ren X-forskning till, på min egen avdelning, ett par samarbeten med KI. Vi har t.ex. en doktorand som sitter på KI för att använda deras data. På annan avdelning har de VR-finansierad forskning med människor, etikprövning osv. Dom låser in datan i kassaskåp.

B: många gånger på övergripande prefektnivå har vi ofta uppdrag som är motsatsen till infosäk – att tillgängliggöra data. Och sen kan jag också tycka att den data vi ofta hanterar på institutionen är i huvudsak egengenererade data, från t.ex. experiment. En annan kommentar är att våra verksamheter är väldigt doktorandtunga, så väldigt många doktorandprojekt. Som alltid måste mynna ut i publicerade artiklar osv. sen kan enskilda forskare ha avtal med t.ex. svenska kraftnät.

A: förutom data är det såklart alla våra datorkonton, lösenord osv. det är ju reglerat centralt på KTH. Alla anställda skriver på ett avtal om vad man får och inte får göra. Sen är forskarvärlden väldigt speciell, ett så här stort universitet. Jag är säker på att forskare skickar email som de inte får göra. Traditionen är att man jobbar öppet, man jobbar med forskare i tex. Kina.

Kan man ha överblick över en sån grej?

A: Nej, med så många tusen forskare som KTH har. Enda sättet är ngn slags automatiserad övervakning, identifiera fraser i email t.ex.

B: informationssäkerhet för mig, personligen reflekterar över, är idéer till forskning. Som är mer känsliga, att sprida en idé som man själv har. Måste söka finansiering osv. Helt plötsligt är idén ute i världen. Data – även om du skickar en fil med data måste du koppla den till ngn kontext där man förstår den. Däremot själva grundidéerna bakom, immateriella tillgångar.

Pratar ni om den frågan?

B: inte varje dag, men det kommer ju upp ibland.

A: det är byggt på förtroende mycket. Man litar på att andra forskare inte sprider information som man delat i god tro. Försöker tänka om det skett ngn incident... det är ju många saker vi gör som kan vara känsliga, vi granskar vetenskapliga artiklar, vi granskar forskningsprojekt. Det är en svår fråga. Det är en avvägning mellan tillgängliggörande och skydd av känsliga uppgifter,

Om ni behöver stöd... vart vänder ni er då?

M juristerna om det är ett avtal som inte är ett standardavtal. Med företag speciellt.

B: ja, det tar kolossal tid. Finns många forskare som är frustrerade över vissa avtal som är en liten summa pengar men det t.ex. är inblandat ett amerikansk företag, och då blir det krångliga avtal.

Vad är det för synpunkter som kommer från juristerna?

B: svårt att komma på ngt direkt så här. Ofta är forskare i kontakt direkt med juristerna.

A: 80 procent av förhandlingarna handlar om IP-rättigheter. Inte så mkt säkerhetsaspekter. Ericson t.ex. är noga med att man inte får prata med Huawei.

B: Förr i tiden hade vi forskningsprojekt som var mer kopplade till militär. Men inte senaste tiden. Men vi hade industridoktorander som forskade om systemen till JAS Gripen.

Att man sitter på t.ex. KI, är det vanligt om man sysslar med känslig data?

A: min erfarenhet är att det är vanligt med KI. Ericson, där har vi kunnat få över data till oss. Men det är skillnad, där är det känsligt för dom (affärshemligheter), inte personlig integritet. Det jag kan komma på när vi inte för över datan till oss, det är när det är människor.

Vad för skyddsvärden?

B: ganska lågt skulle jag säga. Om man inte kan sätta det i kontext. Klart det finns en del data som skulle kunna ge vissa aktörer en fördel, att ta till sig ny teknik snabbare. Våra verksamheter ser olika ut – finns en grupp som forskar på rymdfenomen, där delas all data. Man samlar in data från experiment på satelliter. Ofta stora projekt med jättemånga aktörer. All den här datan delas mellan alla

aktörer. Vår avdelning som sysslar med X. där kan det finnas det data som kan användas militärt t.ex.

Om man skulle fråga, vem har koll på all data vid era institutioner?

A: då är det väl projektledaren som har det, som är ansvarig. Varje projekt har en ansvarig PI, ofta professor. Den personer ska ha koll.

B: data ligger ju på enskilda forskarna. Det finns inget gemensamt ställe där allt ska laddas upp.

A: det pratas från min avdelning om att vi borde ha ett moln eller system för oss, på KTH eller kanske alla svenska universitet, som är säkert. Just nu finns det bara skräddarsydda lösningar, per projekt.

B: ofta vad man får höra om data som prefekt är det om data har försvunnit, att man inte har backup.

Hur vet PI att dom har det här ansvaret, upplever ni att dom vet?

B: om det är reglerat i avtalet är dom väldigt insatta i det.

A: dom vet det om det är viktigt. Är det ett X-inriktat VR-projekt, då kanske varken jag eller forskaren pratar om den saken. Är infosäk viktigt för projektet så vet dom det. Vad de får informationen ifrån, det kan ju vara genom oss i samband med att avtal ska skrivas på, men annars är det ju deras egen avdelningschef också som ska ha ansvar att informera.

Finns det några riskanalyser som ligger bakom de riskmoment som finns, eller är det t.ex. att forskarna bara vet? Hur vet dom det?

A: Skolan gör ju en riskanalys varje år, men tror inte det står så mkt om infosäk där. I annat fall är det projektplanen. Där kan det ibland finnas en riskanalys. Sen är det kanske lite mjukare bedömningar. T.ex. ska vi jobba med AI? Det är en mjuk bedömning, för vi har inga strikta policyer där. Då blir det upp till den enskilda forskaren, och den som skriver på avtalet. Det blir en mjukare bedömning. I mitt projekt t.ex. är det grundforskning så där ser jag inga risker som helst faktiskt. Senaste tiden har det varit en del om Kina, så vi väntar kanske på en lista över universitet vi inte ska samarbeta med, men det har vi inte än. Det är alltid bedömning från fall till fall.

Kan det vara svåra bedömningar, som är mjuka?

A: har ingen bra erfarenhet.

B: ja... vet inte om det är ett problem. Oavsett på vilket sätt... man måste veta att KTH är väldigt internationellt. En stor del av våra doktorander är kineser. Oavsett om dom sökt doktorandtjänster eller CSC. Och jag har hanterat ett stort utbildningsprogram i massa år, men har inte hört någonting.

När ni väl ska skriva på kontrakt har det redan processats?

A: nej... för egen del läser jag avtalet och ser om jag kan ställa upp på det. Sen efter det ska man anställa till projektet, och då är inte vi i loopen förrän det ligger ett anställningsavtal hos oss. Och då är det skolchefen. Frågan om vi ska ta in en person eller inte hamnar inte hos oss.

B: det hamnar i praktiken hos handledaren.

A: jag kan tänka mig att det kanske kommer, pga. Nato bland annat, att vi får en lista på universitet som vi inte ska rekrytera på.

A: vi träffade i Trondheim, deras prefekter. Hos dom är det mkt striktare. Om det beror på Nato eller inte vet jag inte. Har en känsla av att KTH är öppnare är dom flesta.

Är det tydligt vad för ansvar för infosäk formellt enligt riktlinjer?

B: det pågår ju ett arbete med det.. man kan säga så här: det finns ett ökat fokus på det. Det har eskalerat sisa året. Det är väl mkt av Ukraina-kriget som satt saker på sin spets.

A: det är tydligt sett till befogenheter osv, vad som är delegerat. Och hur vi ska vidaredelegera. Det är samtidigt inte alls reglerat i detalj. Läser man våra styrdokument så är dom ganska allmänt hållna. Där finns en viss otydlighet kan man säga. Frågan är hur det kan bli tydligare, det handlar ju om en bedömning till slut, som ska göras av forskarna.

B: det är svårt i en sån här miljö att ha en generell policy. Det blir case to case. Allt som är viktigt och bra vill man ju publicera, och gärna så snart som möjligt. Publicering är prio ett och där gäller det att vara rädd om data i den aspekten.

Vad finns det för möjligheter idag efter ett avslutat projekt? Vad händer med forskningsdatan?

A: praktiska implementeringsfrågan är ju att alla har konton... det är molnlagring via Microsoft som är godkänd, om inte avtal säger annorlunda. Och där ligger väl... när man slutar på KTH försvinner ju email och användare. Men data ligger ju kvar.

B: jag har förhört mig om det där, och det är väldigt svårt att få ut data. Det händer ibland att folk vill ha ut det. Finns en risk för att det finns för många backup och datan ligger för spridd.

A: samtidigt finns det projekt där data är öppna, särskilt inom AI. Många av våra forskare som laddar upp det, för man vill stötta öppen och reproducerbar forskning. Finns en önskan om att lägga ut data.

På era respektive institutioner, har ni några utpekade... om man har en specifik fråga kring infosäk, har ni personer på institutionerna man kan vända sig till?

A: Nej, men skolan ska ha det. Vi är i processen att utse det på skolan. Vår IT-support är centraliserat, så dit kan man alltid vända sig. Skolan har en säkerhetsansvarig också, allmän säkerhet. Så det är väl jag som är ansvarig.

B: i praktiken... om det är nån som vill skaffa sig data på vår institution, då måste man ha kontexten också. Bara data är inte användbart.

A: Ofta måste man ha källkoden också, om det är dataprogram.

B: vi är på väg in i ett forskningssamarbete,

De kommer att sätta upp sitt första experiment i KTH:s lokaler. Där diskuterar vi hur samarbete ska gå till, där behöver man hantera infosäk. I första hand är det immaterialrättsliga aspekter.

Det här företaget, är det någon sån här spinoff, ett gäng forskare från början?
B: nej, inte spinoff, men de är KTH-alumner, så det är väl därför man vänder sig till KTH.

Har ni, RSO... har ni kontakt med dom direkt, eller mer att man rekommenderar forskare?
A: Inte som prefekt, men som forskare, och speciellt EU-projekt. Tyngre byråkrati.

B: har vi kontakt med dom så är det att forskarna inte är nöjda med deras support, att det kanske går för långsamt.

Riskanalyser, gör ni ngt motsvarande på institutionsnivå, några verksamhetsrisker

A: skolan ska ha en riskanalys, och den har vi bidragit till. Det vi gjort på institutionsnivå, vi gör research assessment exercise, där vi blir utvärderade utifrån. Det arbetet vi gjorde 2021, där vi gick en ganska omfattande riskbedömning. Men där undrade man mer frågor av typen hur man behåller konkurrenskraft osv. Var inget specifikt om infosäk.

Var det en gemensam assessment?

B: Ja, hela KTH.

A: indelat i ämnesområden.

Görs inga riskanalyser specifikt om forskningsdata?

A: det är väl på skolnivå i så fall...men inte på institution. Jag tycker att varje forskare ska utvärdera sitt arbete och risker individuellt, kontinuerligt

B: Det görs ju riskanalys generellt, framförallt när det gäller fysiskt skydd, skalskydd, inbrottsskydd. Vi är utsatta för det också, datorer kan stjälas med viktig information. Den typen av riskanalyser görs ju. Och vilka konsekvenser det kan få. Då är det ofta frågan om en dator som inte uppbackas Dator, framförallt på doktorandnivå. Sen riskerna att materialet sprids, den risken finns ju också, men det är ofta egengenererade experimentella data. Oftast är det inte jättekänsligt. Sen kan det finnas dom som jobbar med känsliga saker, typ cybersäkerhet. Kan ju finnas forskning med uttalat samarbete med militära... det håller på att utbilda cybersoldater för framtiden. Där måste finnas en avvägning mellan Försvarsmakten och lärosätet, vad de kan ställa till förfogande. Så det inte blir torrsim av allting.

A: MSB är väl med och finansierar det, det ingår väl i deras roll. Att formulera risk... dom borde ha koll.

Har ni ngt, när skolans riskanalys görs, är det skriftligt eller sitter ni gemensamt då?

A: lite olika, men brukar var havdagsworkshopar, när vi ska utveckla verksamhetsplanen t.ex. då har vi ledningsworkshop, prefekter och skolchef. Sen spelar vi efter det in skriftligt.

Det gör ni en gång per år?

A: Ja.

Följer ni också upp då, årligen?

A: vår nya verksamhetsplan är treårig, men den ska ändå följas upp årligen.

B: oftast blir ju de skarpa uppföljningarna om ngt faktiskt händer. Nu var det en sprängning i Kista för några månader sen, där man sprängde en del av bland annat KTB:s lokaler.

Apropå incidenter, vet ni vad ni ska göra?

A: det har vi fått ganska nyligen, ett incidenthanteringssystem. Vi hade inbrott ganska nyligen på min institution, så då fick jag veta det nyligen. Då är även skyddsombudet.

B: det finns kopplingar till obehörigas tillträdde. På ett sånt här ställe som är ett universitet dyker det upp massa personer som vill ha hjälp med det ena eller det andra. De lyckas ta sig in, står utanför kontor och knacka på. Skulle lika gärna kunna vara en spion. Den typen av incidenter finns. Då hade man kunnat stjäla data, om man vet var det finns.

Upplever ni att ni och era kollegor är medvetna om det här?

A: Ja, nu tror jag, eftersom det händer regelbundet, att nån blir av med en dator på dagtid. Så lätt att missta personer för en student som letar efter nåt.

Finns utbildningsinsatser för infosäk?

A: ja, digital.

Förväntas man gå dom?

A: Ja det förväntas, men har inte varit så bra på att påminna om det.

B: hot och tvång funkar väldigt bra om man ska få igenom sånt. T.ex. om man inte går pedagogikkurs får man inte längre vara examinator.

A: de har iaf gjort det tillgängligt. Att det är webbaserat.

Kan du lite på dina forskare att dom vet vad som ska göra när det kommer till infosäk?

A: jag litar på mina avdelningschefer att dom vet.

B: jo, det stämmer nog rätt bra. Vår personal har en väldigt hög digital kompetens.

Alla lagar man måste förhålla sig till som forskare, exportkontroll, OSL osv

B: Ja, det där ha ju kommit upp mer och mer de senaste åren, exportkontroll.

Krävs ju nästan en juridisk kompetens, hålla koll på massa regelverk utöver att forska?

A: ja jag tror KTH håller på att vakna upp, att vi behöver bättre processer. Vi har ju en vicerektor för internationalisering t.ex. med honom har jag senast förra veckan pratat med om de kinesiska sju universiteten. Vi håller på att formulera processer kring de här frågorna.

B: exportkontrollen är något som kommit upp, hört mkt mer om det de senaste åren. Men jag erkänner villigt att jag är ingen expert på de kraven. Det beror väl på att det inte dykt upp ngt kritiskt fall än så länge där jag behövt ta ställning

A: Vi håller på med mkt grundforskning. De flesta av oss. Vet inte om vi är blåögda när vi säger att "här finns inget känsligt". Men jag tror inte vi är det. Den mesta forskningen kommer ju bli officiell eftersom vi publicerar allt.

B: den typen av information betraktar jag kanske mer som ett resultat, inte bara själva datan. Då har t.ex. företag, i vissa projekt får dom rätt att t.ex. patentera resultaten innan vi publicerar. Den rättigheten får vi ibland skriva ifrån oss.

A: tillgång till arbetsmaterial, det som inte publiceras. Det kan man få på ett sätt om man nästlat sig in här. Men är frågande hur känslig den informationen är i de flesta fall. jag skulle vilja säga att om det är känsligt så vet vi det. Då finns det ett avtal. eller om det är ett industrisamarbete.

B: just industrisamarbete så har industrin alltid varit väldig skickliga på att hantera vad som är känsligt.

A: så funkar det också, att dom jobbar med oss men vi får inte... ibland kan man bli lite sur på Ericson att de inte berättar vad dom håller på med. Det skulle vara bra med ömsesidigt utbyte – vi berättar för dom vad vi gör men dom berättar inte för oss vad dom gör. Dom vill inte att vissa saker ska sprida.

B: vissa områden har varit med tabubelagda än andra. Inom mitt område... ABB känner ni kanske till,

Dom stödjer inte den forskningen eftersom dom inte vill ha någon allmän forskning på området.

För att det just är så konkurrensutsatt?

B: Ja precis. Är man världsledare och man har ett stort försprång vill man inte släppa det.

Händer det ibland att ni säger nej till externa företag? När ni granskar avtal? Att ni inte kan skriva på?

A: ja det har hänt, men har varit andra frågor då. Ett fall som ofta kommer upp med våra stora systemföretag som Ericson och ABB är att dom vill ha fri tillgång till resultat från projekten. Då tycker jag och våra jurister att vi inte kan ge dom fri

tillgång hur som helst. Pga. otillbörlig konkurrensfördel för dom. Då har vi sagt nej till dom. Eller snarare att det finns fall där vi inte kommit fram till avtal.

Det är något annat, att dom ska kunna använda, men ni vill också i forskarsammanhang kunna använda?

A: det är ju också så att våra jurister hjälper ju oss att komma fram till ramavtal för ett stort projekt eller centrumbildning, men sen måste ändå varje enskild forskare skriva ett avtal och ge bort sina rättigheter, pga. lärarundantaget. Men då pratar vi IP. De avtal där vi inte kommit i mål har det handlat om IP snarare än data. Har inte sagt nej till avtal pga. säkerhet.

B: inte jag heller. Sen kan det bero på att man är okunnig på ngt sätt. Att man inte ser risken. Men tror det snarare handlar om IP-rättigheter då. Men kan ju vara militära saker, ibland kanske man är naiv, det vet jag inte.

A: pga. offentlighetsprincipen... det ligger ju ngt i att du säger att vissa saker aldrig ens kommer till oss, för att dom tar det säkra före det osäkra.

Väldigt stor andel externfinansierat på KTH?

B: ja helt klart, 70 procent.

Bedrivs forskning på basanslaget?

A: går typiskt till forskning på olika sätt. Ett sätt är att betala sista tiden för en doktorand, för att tiden tagit slut. Det betalas typiskt en del av våra egna löner, professorers löner. Och i viss mån till forskning. Och allmän merfinansieraring av projekt. T.ex. Wallenberg betalar 25 procent av OH-kostnader. Så det mesta av fakultetsmedlen går till forskning.

Men finns inte helt projekt som finansieras av basanslaget?
B: nej väldigt ovanligt, man fyller i hål med de pengarna. Mkt av den handläggartid man lägger... mkt forskning kopplat till doktorander. Även om det finns en forskare som har en forskaranställning så finns det ju också i det sammanhanget en koppling till gruppens verksamhet. Det är ju avdelningar som själva förfogar över medlen. Forskningspengarna går direkt till avdelningen.

Ser ni några utmaningar själva när det kommer till informationssäkerhet och datahantering inom era områden och institutioner?

A: få ett samlat grepp, för att det är så väldigt spritt det vi gör, både geografiskt och ämne och tid, cyber. Få ett samlat grepp på frågan. Kanske inte ens går. Men det

är ju bra att... det är ju bra för oss med den här granskningen, får oss att tänka på frågorna.

B: många olika aspekter... innan förfrågan kom från er, jag har gått i flera år och tänkt att framtiden ligger i att tillhandahålla data, att allt som skapats ska offentliggöras. Snarare åt det hållet har jag tänkt.

Finns det ngt KTH centralt kan göra för att stötta er?
A: det är implementeringen då. Speciellt molnlagringstjänst som alla tycker är bra och litar på. Nu har vi Microsoft och det finns nackdelar med det.

B: om man då ska sjösätta en riktig plattform där man kan ladda upp sina data, tillhandahåll.

A: Dela på ett sätt man litar på, det finns inte idag.

B: och som inte heller går att missförstå. Det är en annan risk att någon använder datan på fel sätt.

Har vi sagt ngt känsligt här idag?

Nej.