Lagar och regler

Mjukvara, applikationer och it-system

På de flesta håll i världen saknas det lagar och regler för hur it-system skall byggas upp rent kvalitetsmässigt. Det finns lagar som vår PUL, Personuppgiftslagen, eller GDPR, General Data Protection Regulation, är två exempel på lagar som reglerar vårt område, men de påverkar inte direkt hur vi arbetar. De talar om hur information om personer och deras aktiviteter får samlas in och lagras, men de talar inte direkt om vad våra it-system får och inte får göra, bara hur de får användas. Jämför med en mobiltelefon, eller för den delen en kniv, båda kan göra många saker, en del olagliga, men det finns inga direkta lagar som säger att det skall finnas direkta funktioner i dessa produkter som förhindrar användarna från att göra duma saker.

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
https://gdpr.eu/what-is-gdpr/
https://sv.wikipedia.org/wiki/Personuppgiftslagen
https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/personuppgiftslag-1998204_sfs-1998-204

Telekommunikationsbranchen tvingas lagra metadata, information vilka ip-adresser som kommunicerat med vilka och när. Men de får inte lagra informationen som överfördes, inte utan brottsmisstanke och godkännande av åklagare. Detta medför att telekom-bolagen måste ha utrustning som kan logga den informationen, precis på samma sätt som det krävs av telefonväxlar och mobilbasstationer att de kan användas för att avlyssna samtal (även det efter beslut från åklagare). I Ryssland loggas all internettrafik sedan början på 00-talet, de är säkert inte ensamma om den saken. Kina gör ju många intressanta saker med sin ökända brandvägg. "The Wall of China".
Men i praktiken påverkar inte den här typen av lagstiftning hur vi utvecklar våra program, det är beställarens ansvar att den utrustning de har kan användas i överensstämmelse med rådande regler.

Det kan säkert dyka upp fall, där någon utvecklat program för någon direkt brottslig verksamhet, spontant tänker jag då på narkotikahandel och ransomware. I fall där någon utvecklat program vars syfte är att användas till någonting som är direkt brottsligt och som gärna dessutom är ett direkt samhällsproblem (som de båda exemplen nyss), så tror jag det är fullt möjligt att dömas för medhjälp till sådana brott. Men även ett sådant exempel visar ju mer på att program och annat it-relaterat kan användas i kriminella syften, snarare än att våra myndigheter skulle vilja begränsa oss i vårt kreativa arbete som programmerare.

Går vi vidare till läkemedelsindustrin, som över lag är den mest reglerade branch vi har, så finns krav på hur läkemedel och medicinsk utrustning skall testas och godkännas. Ännu så länge finns inte några direkta regler för hur utvecklingen skall ske, varken av kemiska preparat eller program kopplad till produktion av dessa eller som komponent i någon medicinsk apparat. Generellt sett brukar lagstiftare (nuförtiden, det finns kuriösa exempel från 1700- och 1800-talen, ja säkert några fram till 1950 ungefär, men i modern tid har vi i Europa och USA mestadels sluppit lagar som direkt reglerar tekniska lösningar. Det mest kända exemplet på undantaget är ju kemikalie- och narkotika-lagstiftningar, där det ju finns tydligt reglerat exakt vilka kemikalier som får, och inte, får användas, i olika syften, dock tror jag inte den säger något om olika produktionsmetoder.

Men det som rent juridiskt begränsar oss inom den medicinska branchen är kraven på hur slutprodukterna testas och godkänns; när det kommer till våra "mjuka" komponenter så betyder det i praktiken att vi får tydliga krav på dokumentation och i praktiken brukar man även vilja följa olika standarder för kvalitet (inte bara för mjukvaran):

För produktion av fysiska produkter har vi ISO-9000 standarderna.

https://www.iso.org/iso-9001-quality-management.html
https://en.wikipedia.org/wiki/ISO_9000

Grunden för dessa standarder är spårbarhet i alla led, råvarorna i varje levererat exemplar av produkten skall i det idealiska fallet kunna spåras hela vägen tillbaka till där de bröts i gruvor, skördades i skogar och odlades på åkrar. Sedan skall alla led i förädling och sammansättning av produkten kunna spåras och dokumenteras, allt från vilka anställda som gjorde vad, vilka temperaturer som förekom i temperaturkritiska led i produktionen och så vidare. Det skall gå att se vilken maskin, vilka ritningar och instruktioner som användes, för varje producerat exemplar av produkten. Vilka maskiner som användes. Läkemedels och medicinteknikföretagen lägger ned stora resurser på att dokumentera dessa saker. Den här informationen lagras så att om någon misstänker att exempelvis en cancer som uppkommit 30 år senare, skulle kunna ha att göra med en specifik batch av ett läkemedel, så skall det vara möjligt att ta reda på om det skulle kunna vara på det viset. ISO 9000-standarderna räknas av många läkemedelsmyndigheter världen över som ett krav för säker läkemedelsproduktion, men dessa standarder är mycket vanlig inom många former av industriproduktion (inklusive livsmedel). Men skulle något företag (rent teoretiskt) säga att "vi vill inte certifiera oss" så skulle det nog ändå gå att bli godkända, om företaget i stället visar att man gör på liknande sätt, så det är inte ISO-standarderna som är det hårda kravet, det är ordning, reda och dokumentation, myndigheterna önskar och det enklaste sättet att visa att ett företag levererar detta är att företaget visar att de följer sådana här standarder. Det finns alltså ofta en hel grupp standarder under de flesta huvudrubrikerna för ISO-standarder, så ibland kan ett företag tvingas uppfylla en rad olika standarder för att vara fullständigt "ISO 9000" godkända inom sin egen verksamhet.
Det finns ISO-standarder för mjukvarukvalitet, men eftersom medicinteknikföretag sitter hårt fast i de mer hårda standarderna (för produktion av fysiska produkter) så är det inte alltid programdelarna hanteras den vägen. Däremot kan du vara säker på att allting dokumenteras minutiöst och förändringar, fel och liknande dokumenteras och verifieras med en noggrannhet gränsande till byråkratisk överdrift.
En viktig sak att känna till om kvalitet, enligt ISO-standarder är begreppet "avvikelser". En avvikelse är när någonting inte följer dokumentationen. Snubblar någon i en fabrikslokal är det en avvikelse, spiller någon ut en kemikalie är det naturligtvis också det. På samma sätt är det en avvikelse om du tvingas starta om din dator, för att Windows Update kräver det eller för att någonting blivit konstigt. Alla avvikelser skall dokumenteras i en avvikelserapport och sedan skall de arkiveras.

Vi har ISO 14000 standarderna för hantering av miljöpåverkande delar av en produktionskedja, dessa tillämpas på liknande sätt, med revision av verksamheten, med dokumentation och dessa standarder är mycket vanliga inom många industrisektorer. Eftersom läkemedelsbranchen ofta hanterar stora mängder farliga kemikalier, så är även dessa standarder viktiga för läkemedelsbranchen, men just för oss på it-sidan så har de sällan någon betydelse.

https://en.wikipedia.org/wiki/ISO_14000

Vi har även ISO 20000 standarderna för it-service-kvalitet:

https://www.iso.org/publication/PUB100441.html

dessa kan tillämpas både på medicinteknik, supportsystem inom läkemedelsbranchen och naturligtvis inom många andra sektorer.

Skall vi sammanfatta hela det här området med ISO:s standarder för kvalitet i olika former, så är inte kvalitet i dessa sammanhang någonting som liknar begreppet kvalitet i vardagsspråket. I vardagslivet är ju inte heller kvalitet entydigt, en person kan mer än väl tycka att den nyköpta mobilen har hög kvalitet för att alla ytor är blanka och alla skarvar extremt välpassande, samtidigt som samma telefon lätt kan upphöra att fungera om den tappas oförsiktigt på ett hårt underlag. Jämför med en gammal nokia-telefon som kunde tappas och slängas nästan hur som helst, utan några egentliga risker att apparanten skulle gå sönder på riktigt, men bara om det inte fanns vatten i närheten.
I ISO-världen kan man (elakt) säga att en producerad produkt får vara precis hur dålig som helst, bara alla enheter är lika dåliga och likadana, om något exemplar inte är dåligt, skall det finnas dokumentation så att det går att ta reda på varför just det exemplaret inte är dåligt; sådana händelser är ju avvikelser... Naturligtvis är ju normalt syftet att en produkt skall vara bra, eller åtminstone tillräckligt bra för sitt ändamål (vad nu det innebär...). När det kommer till läkemedelsprövning vill ju Läkemedelsverket och andra myndigheter att företaget kan bevisa att preparatet fungerar och att det gör det utan allvarliga biverkningar. Eftersom en del biverkningar inte visar sig annat än efter mycket lång tid, har vi inom EU krav på lagring av all dokumentation i 35 år.

Ett tydligt exempel på it-fokus inom medicintekniken är alla de larm som kommit på senare år, om medicinska apparaters bristande it-säkerhet. Ta pacemakers som enkelt kan stoppas av en förbipasserande på gatan:

https://www.mnemonic.io/resources/blog/uncovering-vulnerabilities-in-pacemakers/
https://www.venafi.com/blog/researchers-discovered-vulnerabilities-allow-attackers-control-pacemakers-remotely
https://www.wired.com/story/pacemaker-hack-malware-black-hat/

det finns liknande händelser med respiratorer och annan utrustning med. Men myndigheterna runt om i världen verkar vakna för att vi naturligtvis måste ha apparater som måste vara säkra även mot "cyberhot". Själv skulle jag inte bli förvånad om någon ond hacker skulle manipulera en röntgenapparat, eller en apparat för strålbehandling av cancerpatienter, så att maskinen börjar zappa personalen och andra förbipasserande med farlig strålning. Har vi tur hinner it-säkerhets-medvetandet höjas innan detta händer.

(ISO föresten betyder International Organisation for Standardization, https://en.wikipedia.org/wiki/International_Organization_for_Standardization)

Men om vi sammanfattar det finns det sällan direkta lagar och regler som säger hur vi skall agera när vi producerar it-system för uppfylla lagkrav. Lagarna handlar nästan alltid om andra delar, som inom medicinen där vi noga dokumenterar hur vi arbetat och hur vi testat våra produkter. Våra rutiner för hur arbetet dokumenteras och verifieras (ja och dokumentationen av verifikationen, det räcker inte att vi testar ett program noga, vi måste dokumentera hur vi testat det).

Går vi vidare till exempelvis energi (olja, kärnkraft, vindkraft och vattenkraft; energidistribution) eller transport (flyg, järnväg, sjöfart och vägtransporter) så finns jättemånga regler för olika saker, främst säkerhet och miljö. I praktiken innebär det även där att man följer ISO-standarder inom produktionen av fordon och utrustning. Det medför att man dokumenterar allt nästan till gränsen av besatthet. Men det är inte alltid självklart att vi måste följa specifika standarder för kvalitet, inom IT. Detta gör förmodligen ingen skillnad eftersom all mjukvaruutveckling ändå måste

dockumenteras i detalj, för att de standarder man följer inom de mer "hårdare" delarna av produktionskedjan kräver att vi också skärper oss och dokumenterar alla steg, alla förändringar, alla buggar; och naturligtvis exakt vad och hur vi testat.
En annan viktig faktor inom den här sektorn är skadeståndsregler. Där går ju USA i spetsen, ett fordon som förväntas användas i USA måste vara såpass säkra att producenten inte behöver oroa sig för att drabbas av fantasifullt höga skadestånd. Detta är ju en hotbild som i högsta grad även gäller för kärnkraftsbranchen, där en katastrof kan leda till stora och extremt långsiktiga konsekvenser runt om i världen, inte bara i kraftverkets direkta närområde, och där de inblandade lätt kan bli måltavla för stora skadestånds-processer. Detta är trots allt den viktigaste orsaken till varför det byggts så lite ny kärnkraft på den här planeten, de senaste 30-40 åren.
Tittar vi på transportsektorn brukar producenter av flygplan, fartyg och tåg alla köra med tredubbla styrsystem, i de fall man använder program som administrerar viktiga styrrörelser. På tåg är det väl mest fråga om bromssystem, men tredubbla styrdatorer ändå. Fartyg styrs i två dimensioner och flygplan i tre, oavsett så kör de med trippla system i autopiloter och liknande (exempelvis i det datoriserade system för att göra att JAS 39 Gripen kan flygas, över huvud taget. Precis som många andra moderna stridsflygplan är ju detta egentligen väldigt instabilt, för att kunna ändra kurs extremt snabbt, men för att det inte skall vingla runt som ett löv i en höststorm, så finns ett digitalt stabiliseringssystem, som ser till att flygplanet går rakt när piloten vill det; där är det tre oberoende datorer som tillsammans röstar om hur rodren skall ställas in, för att uppnå detta. Minst två måste vara överens om ett roderutslag för att rodren skall läggas om). Anledningen till varför dessa system tredubblas är inte att det finns lagar som kräver det, men att tillverkarna vill vara säker på att det inte sker några obehagliga olyckor på grund av konstruktionsfel. Både skadestånd och prestigeförlust skulle kunna vara betydande.
I många sådana här styrsystem så är de olika datorerna av helt olika modell och med helt olika program. Detta för att förhindra att samma fel uppstår samtidigt på alla tre datorerna eller i alla tre programmen.
Att bilbranchen oftast valt att gå en annan väg, med sina försök till självkörande robotbilar, beror inte på att vägtrafikmyndigheterna är mindre intresserade av trafiksäkerhet, än vad exempelvis sjöfartsmyndigheterna skulle vara. Robotbilar utvecklas ofta av företag som Google, Uber, Tesla för att nämna de tre största. De två första är it-företag och det tredje är grundat av och drivs av människor från it-branchen. Jag vill inte säga att vi inom it saknar fokus på kvalitet, men vi är så vana med buggar att vi nästan förväntar oss sådana i alla program och vi har i stället vant oss med att patcha och uppdatera saker regelbundet, för att de skall fungera långsiktigt. När traditionella bilföretag bygger robotbilar är de över lag betydligt konservativare, även fast de ofta kör med enkel styrdator de med; bilföretagen har ju alltid haft ett hårt fokus på att pressa kostnader och "varför skulle just vi ha tre datorer i vår bil när alla andra klarar sig med en?" är nog den frågan som fått även dessa att säga att vi skall ha en styrdator.

När vi är inne på det här området så har vi ett annat problem som är relevant för oss att reflektera över, oftast ser vi den inbäddade mjukvaran i fordon som en produkt i sig som testas och utvecklas helt separat från det fordon där den skall köra(s). Naturligtvis läggs det stora resurser på systemtest, där styrprogrammet testas i praktiken i ett fordon, men det torrsimmas också väldigt mycket innan man kommit såpass långt. Ett program som rätt identifierar en förskoleklass på ett övergångsställe, måste ju göra det tidigt nog, för att inte köra över barnen. Om det senare kravet är uppfyllt eller ej, testas oftast separat i ett senare skede.

Jag läste om ett intressant statligt initiativ i England, där hemtjänstpersonal i London försågs med var sin Land-Rover av någon lyxigare modell, som redan hade alla sensorer som ansågs behövas för en robotbil. Sedan kompletterade man med kameror för att dokumentera både omgivning och förarens arbete och därefter var planen att spela in hur dessa bilar kördes i tät stadstrafik, under några år. Meningen var inte att hemtjänstbilarna skulle köra själv, men att samla in data för att utveckla program för självkörande bilar, utan att utsätta någon för risken med bilar styrda av

buggiga program i tät stadstrafik. Den övergripande planen var att inte Storbritannien skulle komma efter USA inom det här området. Tyvärr har jag inte hittat några referenser nu, till det här projektet, det här är ju enligt min mening ett mycket mer ansvarsfullt sätt att utveckla självkörande bilar på, än det som är vanligt i USA.

På de många håll där det testas självkörande bilar så saknas direkta lagar för att reglera självkörande bilar. I praktiken är det nog till och med såpass illa, att det nog på väldigt många håll i världen helt enkelt bara är att ta ut sin robotbil på gatan och "se hur det går". Problemet är naturligtvis att det finns många intressanta lagar som kan tillämpas när det går fel, här hemma har vi exempelvis "allmänfarlig vårdslöshet", "vårdslöshet i trafik", "vållande till annans död" och kanske till och med dråp. Inför en sådan lista väljer nog de flesta seriösa företag, att skaffa ordentliga tillstånd först.