Regeringskansliet
Justitiedepartementet
103 33 Stockholm

Stockholm 2013-07-25

Remissvar Vallagskommitténs slutbetänkande "E-röstning och andra valfrågor" (SOU 2013:24) – diarienummer Ju2013/3126/L6

.SE (Stiftelsen för Internetinfrastruktur) är en oberoende allmännyttig organisation som verkar för positiv utveckling av Internet i Sverige. Vi ansvarar för Internets svenska toppdomän .se, med registrering av domännamn samt administration och teknisk drift av det nationella domännamnsregistret. .SE står för följande värderingar:

Vi tycker om och tror på Internet
Vi värdesätter individens möjligheter med Internet och tror att Internet kan bidra positivt till såväl individers som samhällets utveckling.

Vi vill ha ett stabilt och skalbart Internet
Internets infrastruktur ska vara säker, stabil och skalbar för att på bästa sätt gynna användarna.

Vi vill ha ett Internet för alla
Alla människor i Sverige ska ha samma rätt och möjligheter att utnyttja Internets tjänster. Internet ska vara säkert – användarna ska känna sig trygga och kunna lita på tjänster på Internet.

Inledningsvis, .SE har två medarbetare utnämnda som ledamöter i Digitaliseringskommissionens expertgrupp, och vi ställer oss i allt väsentligt bakom vad som anförs i Digitaliseringskommissionens remissvar:

https://digitaliseringskommissionen.se/remissvar-e-rostning-och-andra-valfragor-sou-201324-slutbetankande-av-2011-ars-vallagskommitte/

.SE (Stiftelsen för Internetinfrastruktur)
Box 7399, 103 91 Stockholm, Tel 08-452 35 00, Fax 08-452 35 02, Org. nr 802405-0190, www.iis.se

Liksom Digitaliseringskommissionen fokuserar .SE på den del av förslagen som rör e-röstning och lämnar utöver det som anförs i Digitaliseringskommissionens remissvar följande synpunkter på remissen.

Vallagskommittén har i SOU 2013:24 föreslagit att Sverige ska införa försök med e-röstning och i första hand förordat försök med e-röstning via Internet i okontrollerade miljöer, men med en utformning så att det även kan tillämpas i vallokaler och röstningslokaler. Enligt utredningen finns det fördelar med e-röstning i okontrollerade miljöer via Internet, den främsta kanske att personer med vissa funktionshinder då kan genomföra sin valhandling på egen hand, utan hjälp med att förbereda valsedeln, och därmed behålla sin valhemlighet. Bekvämligheten för väljarna i stort kan enligt utredningen också anses öka.

Vi befinner oss i ett samhälle där det geografiska avståndet många gånger utgör ett hinder för att avlägga sin röst i de allmänna valen. Det finns dessutom väljare som har svårt att förflytta sig och som naturligtvis bör ha praktiskt tillgängliga möjligheter att närvara i den demokratiska process som allmänna val innebär. För dessa kategorier har också särskilda lösningar inrättats, med möjlighet till utlandsröstning, poströstning och röstning via bud eller ombud.

Vallokalskommittén hävdar att e-röstning kan innebära minskade kostnader och samtidigt öka valdeltagandet. För att minska kostnaderna krävs dock att e-röstning blir så vanligt att man kan stänga fysiska vallokaler vilket i sin tur skulle minska tillgängligheten för andra väljargrupper än de som får ökad tillgänglighet genom e-röstningen.

.SE anser att om kostnadsfrågan ska bli ett argument måste man bortse från tillgänglighetsargumentet, eller åtminstone acceptera att tillgängligheten både ökar och minskar för olika grupper. Det finns ingen entydig forskning som visar att e-röstning generellt ökar valdeltagandet, utan det är mer ett betrakta som ett önsketänkande eller i bästa fall ett antagande från vallagskommitténs sida - som inte har styrkts med fakta - att så skulle bli fallet specifikt i Sverige.

.SE konstaterar att det i rapporten inte redovisas fakta som stödjer utredningens många *kan*, *bör*, *antas* och *förväntas* som förekommer för att beskriva de många fördelarna med e-röstning framför allt via Internet. Exempelvis hade påståenden som *"det finns skäl att anta att många väljare väntar sig att de ska kunna använda modern teknik när de röstar"*, att rösträkningen kan ske snabbare eller att risken för fel minimeras (s. 62) tjänat på att underbyggas av fakta från undersökningar och analyser som styrker påståenden av den karaktären, eller åtminstone att skälen bakom antagandena redovisats klart och tydligt. Emellertid är erfarenheterna av e-röstning mycket begränsade även om man tittar internationellt så det finns inte mycket faktaunderlag att bygga på.

Utöver detta finns ett det enligt .SE:s mening ett antal problem med e-röstning i allmänhet och med e-röstning i okontrollerade miljöer via Internet i synnerhet.

För att val ska kunna anses fria och säkra måste ett antal punkter uppfyllas:

- Allmän och lika rösträtt
- Frihet från påtryckningar och möjlighet att ändra sin röst
- Valhemlighet
- Säkerhet och transparens i röstförfarande och rösträkning
- Möjlighet att i efterhand kontrollera resultatet

Samtliga moment måste säkerställas. .SE ställer sig tveksamt till om de kriterier för fria och säkra val som definieras i underlaget över huvud taget kan infrias givet nuvarande grad av säkerhet i kommunikation via och system anslutna till Internet.

Om man vill införa e-röstning måste man förvissa sig om att ett sådant system är lika bra som det existerande, konventionella röstförfarandet och i lika hög grad uppfyller alla krav. Det kräver en systematisk genomgång av:

- Vilka problem vill man lösa?
- Hur vill man lösa problemen?
- Vilka risker finns förknippade med lösningen?
- Hur kan riskerna elimineras eller åtminstone hanteras?
- Vad får det kosta?

Förmågan att värdera tillgängliga lösningar omfattar både människor, processer och teknik.

Säkerhet

.SE har omfattande erfarenhet av arbete med säkerhet i och skydd av komplexa nätverk för kommunikation, framför allt via Internet. Det är för oss tämligen uppenbart att säkerhetsfrågorna är det största hindret för införandet e-röstning från okontrollerade miljöer via Internet. Dessa frågor måste analyseras och hanteras på alla nivåer, hela vägen från bakomliggande infrastruktur och ut till den enskilda användaren.

Det finns en uppenbar risk att val och röstning via Internet utsätts för attacker som syftar till att göra röstningssystemen oåtkomliga från ett visst land, en viss region eller från hela Sverige, framför allt som det är allmänt känt exakt under vilka perioder systemen är öppna för val.

Det är enligt .SE mycket svårt att konstruera helt säkra tekniska system som säkerställer såväl valhemligheten som genomförandet av fria och säkra val. Det handlar bland annat om den tekniska infrastrukturen, om den tekniska systemmiljön hos valmyndigheten, om skydd mot manipulation och åtkomst av information såväl under kommunikation via Internet som vid lagring i valmyndighetens system och slutligen handlar det om väljarnas egen utrustning i form av TV-mottagare, datorer eller mobila enheter som dessa använder för att avlägga sin röst.

Till skillnad från vad utredningen hävdar på s. 75 att ”Säkerhetsproblem vid användningen av internet är väl kända och belysta i ett stort antal rapporter” anser .SE att det finns omfattande osäkerheter som vi ännu inte har sett effekterna av. Angripare avlägsnar sig allt mer från högprofilmetoder som bred spridning av virus och maskar för att i stället jobba mer med riktade attacker i det fördolda med hjälp av trojaner och andra typer av diskret skadlig kod.

Många av dagens attacker genomförs genom utnyttjande av säkerhetsbrister som kan betecknas som så kallade nolldagarsattacker (zeroday exploits), det vill säga att svagheter i program och applikationer används för attacker innan det finns några rättelser (patchar) tillgängliga att skydda dem med. Att tillfälligt stänga av valsystemet under pågående val på grund av att ytterligare en sårbarhet har upptäckts (och eventuellt utnyttjats) är otänkbart. Det borde i praktiken innebära att valet ogiltigförklaras och måste tas om.

Skadlig kod

Det finns en uppenbar risk för att väljarens egen enhet är angripen av skadlig kod, till exempel av virus eller spionprogram som dels kan styra röstningshandlingen och dels röja hur någon röstar. Utredningen definierar detta som individens eget ansvar, vilket förvisso må vara sant, men trots att detta varit en "sanning" i mer än 20 år har vi inte sett någon märkvärd förbättring när det gäller individens förmåga till ansvarstagande i det avseendet. Myndigheterna måste kunna erbjuda ett system som är säkert i sig själv, och även se till att de programvaror som används är uppdaterade och fria från kända sårbarheter både på operativsystemnivå och på applikationsnivå.

Skydd av infrastruktur

På väg från den enskildes utrustning går informationen via väljarens anslutning till Internetoperatören, via Internet till valmyndighetens anslutning till en Internetoperatör och når slutligen valmyndighetens system, som kan vara utkontrakterat till en tredjepartsleverantör.

Utredningen anser att informationsskyddet kan lösas med kryptering. Men utöver det krävs enligt .SE ett fullgott skydd mot hela infrastrukturen för att motverka att hela eller delar av systemet görs otillgängligt via exempelvis överbelastningsattacker mot infrastrukturen som sådan eller mot tjänsten som infrastrukturen förmedlar. Exempelvis behöver de domäner som används vara signerade med DNSSEC för att förhindra att användare via domännamnssystemet omdirigeras till en identisk, men förfalskad sajt, där användaren luras att både identifiera sig och lämna sin röst. I extremfallet kan trafiken spelas in för att sedan föras vidare till det äkta systemet, vilket gör attacken i princip omöjligt att upptäcka. Se exemplet med SMHI på .SE:s sajt:
https://www.iis.se/domaner/teknik/dnssec/kaminskybuggen/

Tillit

De system som stöder den demokratiska processen skall inte bara vara tekniskt pålitliga, de måste även betraktas som pålitliga av svenska folket i allmänhet, i motsvarande grad som det konventionella, manuella systemet för förrättning av allmänna val.

.SE är av meningen att det mycket enkelt kan uppstå misstankar om att allt inte går rätt till om man som väljare "bara" klickar på en skärm för att avlägga sin röst. (För övrigt ett av de starkaste skälen till att Nederländerna slutat med datoriserad röstning och gått tillbaka till ett manuellt system.)

Alla kan förstå förloppet i situationen med ett konventionellt (manuellt) röstningsförfarande. Väljaren tar själv sina valsedlar, lägger sin valsedel i respektive kuvert, identifierar sig och prickas av i röstlängden, bevittnar hur kuvertet läggs i en valurna och kan förstå att den valsedeln sedan kommer att räknas.

Ett fåtal kan däremot mer än diffust begripa hur ett klick på skärmen på en surfplatta eller en mobiltelefon rent faktiskt omvandlas till ett resultat som sammanställs och presenteras i media och som ytterst ligger till grund för exempelvis regeringsbildning för nästa mandatperiod. Den här grundläggande oförståelsen riskerar att ta sig uttryck i en minskad tillit till demokratiprocessen.

Detta är i .SE:s ögon särskilt giltigt i skenet av att vi de senaste 2-3 åren har upplevt massiva problem med:

a) minst ett omfattande haveri hos tredjepartsleverantör till bland annat offentlig förvaltning (Tieto-kraschen),

b) intrång i myndigheters datorsystem (Skatteverket, Polisen med flera),

c) omfattande avlyssning från främmande makt (PRISM med mera) och

d) allvarliga brister i säkerhet hos de företag (certifikatsutfärdare, CA) som utfärdar certifikat som kan tjäna som stöd för identifiering av individer och system (till exempel Diginotar, RSA, Comodo).

Till detta kan vi lägga ett stort antal incidenter med intrång, överbelastningsattacker, bedrägeriförsök, nätfiskeattacker och utbrott av skadlig kod.

Med dessa händelser i färskt minne är det oss helt främmande att kunna hysa fullständig tillit till myndigheternas förmåga att skapa ett system som är säkert mot intrång, robust mot attacker och ger ett fullgott informationsskydd så att den personliga integriteten och valhemligheten bevaras.

Exempelvis kan de långtgående rättigheter som via lagstiftning förlänats Försvarets radioanstalt (FRA) i kombination med dess uttalade samarbete med främmande makt, inte anses vara förenliga med bevarandet av valhemlighet och teknisk säkerhet. Valhemligheten är grundbulten i ett demokratiskt styrelseskick, och så länge exempelvis FRA har ens teoretiska möjligheter att granska medborgarnas elektroniska kommunikation, förefaller allmänna val från okontrollerade miljöer, förmedlade via Internet, vara en risk som inte är värd att ta.

Val via elektroniska förfaranden i okontrollerade miljöer via Internet lider av att det finns en motsättning mellan att säkert identifiera en individ som väljare med rösträtt i det aktuella valet, och samtidigt hålla vad denne de facto väljer hemligt, med bibehållen koppling mellan väljare och transaktion och med möjlighet att i efterhand kontrollera att det blev rätt.

Utredningen skriver att *"Det måste vidare vara möjligt att verifiera och kontrollera resultatet i efterhand"*. .SE ser det som omöjligt att göra detta och samtidigt kunna garantera att valhemligheten förblir intakt, åtminstone med rimliga investeringar.

Givetvis har det även inom det konventionella systemet existerat problem i form av valfusk i enstaka vallokaler, för enstaka väljare och med misstag begångna av enstaka individer i förtroendeställning som bud eller ombud. Vi kan aldrig utesluta den mänskliga faktorn. Skillnaden mellan konventionell röstning och e-röstning är att ett enstaka fel i det senare fallet kan få så oändligt mycket större konsekvenser och eventuellt också påverka valutgången.

Om vi ska införa ett elektroniskt röstningsförfarande och samtidigt behålla ett visst mått av verifierbarhet, behöver vi skapa en lösning där väljaren kan få en bekräftelse i form av ett kvitto eller likande, som bara väljaren kan komma åt och ingen annan.

Transparens och öppenhet

Ett e-röstningssystem av det slag som utredningen beskriver kräver en hög grad av transparens och öppenhet. Innebörden i transparensen är enligt .SE att systemet måste uppfylla tre grundläggande krav:

- Bygga på öppna standarder.
- Bygga på öppen källkod.
- Utsättas för oberoende granskning.

Öppna standarder är mycket centrala inom hela IT-området. Utan standarder för exempelvis dataformat eller nätverkskommunikation skulle information inte kunna utbytas effektivt mellan olika användares utrustningar via Internet. Enkelt uttryckt kännetecknas en öppen standard av att den är *öppet och fritt tillgänglig och kan implementeras fritt utan restriktioner*. EU har antagit en formell definition av vad som utgör en öppen standard. Åtminstone följande kriterier måste vara uppfyllda:

- Standarden skall sponsras och underhållas av en icke vinstdrivande organisation, och dess fortsatta utveckling skall ske i en öppen beslutsprocess som är tillgänglig för alla och som ger alla intressenter möjligheter till påverkan.
- Standarden skall ha publicerats, och standarddokumentet skall vara tillgängligt antingen gratis eller till ett symboliskt pris. Det måste vara tillåtet för var och en att kopiera, distribuera och använda dokumentet antingen utan avgift eller mot en symbolisk avgift.
- All den "intellektuella egendom" - vilket i detta sammanhang innebär patent - som kan omfattas av (delar av) standarden skall ha gjorts oåterkalleligt tillgängliga utan royalties eller andra licensavgifter.
- Det får inte finnas några restriktioner rörande återanvändning av standarden.

Öppen källkod (engelska open source) avser oftast programvara där källkoden är tillgänglig att använda, läsa, modifiera och vidaredistribuera för den som vill. Detta gör att användaren kan försäkra sig om att programmet gör vad det ska, eller anpassa det till sina behov. Källkoden ska kunna användas, studeras och modifieras helt utan eller med minimala restriktioner enbart för att säkerställa att ytterligare mottagare också kan få dessa möjligheter. I praktiken, för att programvaran ska kunna distribueras måste den mänskligt läsbara formen, alltså källkoden, finnas tillgänglig tillsammans med en anteckning eller instruktion som ger dessa friheter, det vill säga någon form av licens.

Oberoende granskning kan innebära formell certifiering av systemets ingående delar mot befintliga standarder, med stöd av exempelvis årlig granskningsplan, genomförande av granskningarna och återrapportering till ansvarig myndighet.

Oberoende granskning kan också innebära en granskning från engagerade och intresserade samhällsmedborgare som kan göra det lättare att verifiera funktionalitet och säkerhet i den programvara som används, något som har belagts av de många projekt med öppen eller fri programvara som har funnits och finns, inte minst i Internetsamfundet.

Det är viktigt att kostnaderna för det centrala ansvaret för att hantera förslag till förbättringar och uppdateringar tas av ansvarig myndighet. Det som är avgörande för att nå framgång är hur myndigheten väljer att ta in förändringar och hur bidrag från communityt tas emot.

Påverkan

Förutom .SE:s starka invändningar mot möjligheten att skapa en skalbar, säker och robust teknisk miljö är risken för påverkan på väljaren vid röstning i okontrollerade miljöer via Internet en viktig aspekt. E-röstning från datorn hemma eller på jobbet, från mobilen på

bussen eller surfplattan i baren, riskerar att undanröja valhemligheten och göra individer i olika former av beroendeställning mer utsatta för påtryckningar som det kan vara mycket svårt att värja sig mot. Bara det faktum att möjligheten finns att avlägga sin röst under stark påverkan av alkohol eller droger är avskräckande – något som inte är lika enkelt i den konventionella miljön med fysiskt deltagande.

Periodicitet

Med riksdags-, landstingskommunala och kommunala val vart fjärde år i Sverige och sporadiskt förekommande beslutande folkomröstningar kan vi förvänta oss att det förflyter relativt lång tid mellan de gånger ett e-röstningssystem kommer att användas i skarpt läge. För att hålla en hög kvalitets- och säkerhetsnivå kräver systemen löpande underhåll och omfattande testning under perioderna mellan valen för att säkerställa att systemet fungerar som det ska, med uppdaterade programvaror, något som kommer att driva kostnaderna och därmed sannolikt göra e-röstningssystemet dyrare än konventionell röstning där kostnaden i huvudsak enbart uppkommer vid valtillfällena.

Trots att utredningen uttrycker en förhoppning om att kostnaderna har förutsättningar att minska på sikt kan .SE inte finna någonting i rapporten som styrker en sådan förhoppning.

.SE:s slutsatser

Utan att gå så långt som till att genomföra allmänna val från okontrollerade miljöer via Internet finns det en rad andra möjligheter att fördjupa demokratin med stöd av elektronisk kommunikation. På .SE anser vi att det finns anledning att närmare se över dessa möjligheter.

Som påpekas i utredningen är e-röstning ett instrument för det övergripande målet att fördjupa det demokratiska inflytandet för medborgare i Sverige, var de än befinner sig och i princip oavsett deras förutsättningar för övrigt, digitalt utanförskap, hemlöshet, funktionshinder eller missbruk.

Valet är den yttersta tilldelningen av den politiska makten genom personer som ombud. Demokratiskt inflytande kan emellertid också utövas genom andra metoder, som exempelvis offentliga opinionsundersökningar (enkäter) och lokala eller nationella folkomröstningar. Enkäter eller opinionsomröstningar är inte bindande för institutionerna (till exempel kommunfullmäktige, landstingsfullmäktige eller riksdagen). I sådana situationer skulle elektronisk kommunikation via Internet i större utsträckning och med högre frekvens än idag användas för fördjupade och förankrade beslutsunderlag.

En annan rimlig åtgärd är att förenkla processen i vallokalen eller röstlokalen genom att förse valbåsen med terminaler som på begäran skriver ut valsedlar för det eller de partier väljaren valt, eventuellt även med den kandidat förkryssad som väljaren eventuellt personröstar på.

Därigenom skulle alla registrerade partier behandlas lika, och det skulle underlätta för nya partier som skulle slippa den gigantiska uppgiften att på egen hand distribuera valsedlar till alla vallokaler. Dessutom skulle vi förmodligen slippa krångel med felaktiga och ogiltiga valsedlar. Rösterna kan fortfarande räknas på det gamla vanliga – öppna och transparenta – sättet.

.SE anser alltså inte att e-röstning i okontrollerade miljöer uppfyller grundläggande demokratiska krav på frihet från påtryckningar, säkerhet, bibehållen valhemlighet,

verifierbarhet och transparens. Vi anser därför att Sverige inte bör genomföra försök med e-röstning i okontrollerade miljöer via Internet i valet 2018. Vi anser dock att riksdag och regering ska fortsätta att utreda och utveckla området, samt följa och stödja förekommande forskning om e-röstning för att få ett bättre underlag kring vilka digitala komponenter som faktiskt kan införlivas i den svenska demokratiska processen.

Danny Aerts, Vd