|  |
| --- |
| Rapport |

Friare övervakningsmetoder - juridiska, etiska och sociala konsekvenser

|  |
| --- |
| *Författare: Imad Tabikh*  *Termin: HT23*  *Kursnamn:* Teknisk kommunikation  *Kurskod:* 1ZT010 |



Sammandrag

Abstrakt

Denna rapport undersöker de komplexa sambanden mellan å ena sidan behovet av nationell säkerhet och brottsbekämpning och å den andra den grundläggande rätten till privatliv och dataskydd. I bakgrunden finns de signifikanta ändringarna av övervakningslagarna efter terrorattackerna den 11 september 2001 i New York, med särskild fokus på “The Patriot Act” och PRISM-programmet. Även EU-kommissionen förslag och europeisk datalagring analyseras.

En genomgång av historiska händelser och aktuell lagstiftning belyser de etiska, juridiska och sammhälleliga konsekvenserna och utmaningarna som uppstår när myndigheter strävar efter att stärka säkerheten, samtidigt som de måste respektera medborgares rätt till privatliv. Rapporten analyserar även USA:s dominanta position inom den globala internetinfrastrukturen, och hur den ger Amerikanska myndigheter en fördel över spionage på data. Rapporten avslutas med en diskussion om de nuvarande och framtida utmaningarna att upprätthålla balansen mellan säkerhet och privatliv. Slutsatsen betonar hur viktigt det är med fortsatt utvärdering av lagar för att skydda medborgare och samtidigt använda sig av digitala verktyg för att bekämpa brott.

Abstract

This report studies the complex coherence between the need of national security, and private integrity. We start with the impact of the changed laws after the September 11 2001 attacks in New York, with heavy focus on “The Patriot Act” and the PRISM-program. The EU-commisions proposal on heavier chat control, and european datastorage is also analysed.

By a walkthrough on historical events and a look at today’s laws, the report shines a light on the consequences of governments work to strengthen national security, while still respecting the citizens right to integrity. The report also analyses USA’s dominant position on the global internet infrastructure, and how it gives American authorities an advantage when it comes to datasurveillance. The report ends with a discussion about future challenges of keeping a balance between the nations security and the citizens right to integrity. The conclusions emphasize the importance of keeping laws updated to protect citizens integrity, while still using digital tools to fight crime.

Nyckelord

Spionage, informationsintegritet, dataskydd, nätverkssäkerhet.

Innehåll

1 Inledning 3

1.1 Syfte och frågeställningar 4

1.2 Metod och material 4

2 Resultat 4

2.1 Hur balanserar samhällen behovet av säkerhet med rätten till privatliv och dataskydd? 4

2.2 Vilken roll spelar teknisk kommunikation i denna balansakt? 5

2.3 Var går gränsen mellan spionage på medborgare och utredning av kriminalitet? 5

3 Diskussion och slutsatser 6

4 Referenser 7

# Inledning

I en värld där de digitala verktygen blir en alltmer central del av våra liv, där information inte bara är makt utan även ett verktyg för övervakning och kontroll, blir frågor om teknisk kommunikation och integritet viktiga. Denna text avser att utforska och analysera de komplexa sambanden vid brottsbekämpning och konsekvenserna av myndigheters rätt att använda internet för att övervaka och spionera på befolkningens data.

Ett av de mest framträdande exemplen på detta är USA:s användning av sin dominerande ställning i den globala internetinfrastrukturen. Genom att koppla upp sig mot undervattenskablar som förbinder kontinenternas internetinfrastruktur har USA skapat en portal där en stor del av världens data passerar, vilket ställer frågor om suveränitet och integritet. Dessa data består inte bara av information från USA:s egna medborgare utan även från individer runtom i världen.

Amerikanska myndigheter använder sig av mjukvara som är designad för att läsa av och analysera data innan de når användaren, vilket ger dem insyn i medborgarnas privatliv Ett exempel på ett sådant program är ”The Planning Tool for Resource Integration, Synchronization and Management”, förkortat PRISM. Programmet används av amerikanska myndigheter för att samla in data från olika internetleverantörer.

Majoriteten av den globala dataströmmen passerar genom USA, inte på grund av att man valt den kortaste vägen utan delvis för att det är den mest kostnadseffektiva vägen, men även för att USA besitter majoriteten av internets infrastruktur. Detta väcker frågor om datatrafikens arkitektur och hur den påverkar andra länders integritet och dataöverföringssäkerhet.

På en nationell nivå ser vi liknande tendenser t.ex. i Sverige, där myndigheterna infört lagstiftning för att möjliggöra dataavlyssning utan misstanke om brott. Detta motiveras av att man vill bekämpa bland annat gängkriminalitet och barnpornografibrott, som ökat markant i Sverige. Detta är en signifikant avvikelse från tidigare praxis där polisen endast hade rätt att avlyssna vid brottsmisstankar.

## Syfte och frågeställningar

Rapportens syfte är att presentera frågeställningar om de juridiska, etiska och sociala konsekvenserna av friare övervakningsmetoder. De frågeställningar som ska besvaras och diskuteras i rapporten är.

F1: Hur balanserar samhällen behovet av säkerhet med rätten till privatliv och dataskydd?

F2: Vilken roll spelar teknisk kommunikation i denna balansakt?

F3: Var går gränsen mellan spionage på medborgare och utredning av kriminalitet?

## Metod och material

Frågeställningarna ska besvaras genom en litteraturstudie.

Diverse artiklar och politiska brev används för att samla information nödvändig för att besvara frågeställningarna. Källorna har granskats för dess trovärdighet, objektivitet och relevans för att säkerställa att informationen är pålitlig.

# Resultat

Nedan kommer frågeställningarna besvaras och analyseras utifrån den information som har samlats in från de angivna källorna.

## Hur balanserar samhällen behovet av säkerhet med rätten till privatliv och dataskydd?

Efter terrorattackerna på tvillingtornen i New York (2001) skärpte USA sin säkerhet marginellt, både inrikes och utrikes och ändrade sin policy över hur de övervakar och delar information[1]. 45 dagar efter attackerna ändrades ”The Patriot Act” [2] så att Amerikanska myndigheter mycket enklare kunde övervaka medborgares information och data. Staten kunde bland annat spionera på telefonsamtal, mailkonversationer, banköverföringar, kreditvärdigheter och även följa medborgares aktiviteter på internet. FBI, en polismyndighet i USA som utreder brott som faller utanför vanliga polisiära ärenden[3], skapade så kallade ”National Security Letters” (framöver förkortat NSL), utan några domstolsbeslut. NSL gav FBI tillgång till personliga data [2].

6 år senare gick flera av USAs största bolag, bland annat Microsoft, Yahoo och Facebook med i ett övervakningsprogram kallat PRISM [4]. PRISM är ett övervakningsverktyg som hämtar vanliga medborgares data från de ovannämnda bolagen, med syftet att förebygga brott. Programmet var hemligstämplat, men flera källor läckte dokument, bland annat den efterlyste Edward Snowden[5], en före detta anställd på den amerikanska myndigheten NSA. Efter läckorna blev programmet känt av landets medborgare.

Efter nästan 20 år av Amerikanskt IT-spionage på sina medborgare~~,~~ har det nu tagits fram ett förslag som gör det svårare för Amerikanska myndigheter att beslagta invånares data utan domstolsbeslut [6]. Detta kommer efter flera protester av politiker och invånare som anser att USA behöver värna mer om invånarnas integritet. Republikanen Mike Lee menar att när FBI övervakar medborgare utan några brottsmisstankar eller domstolsbeslut, är det inte bara ett felsteg av FBI utan även en kränkning av medborgarnas integritet [6]. Mike Lee menar att det är viktigt att myndigheter har möjlighet till övervakning, men att det krävs skärpta regelverk över vilken tillgång de ska ha.

## Vilken roll spelar teknisk kommunikation i denna balansakt?

Internetkopplingen mellan kontinenterna är uppbyggd av kablar som är dragna under världshaven. Dessa undervattenskablar sägs vara grunden till 95% av den information som skickas över internet [9]. I oktober 2020 släpptes en rapport som påpekade farorna med bristande säkerhet vid dessa kablar. Resonemanget var att oskyddade kablar kan ge främmande grupper tillgång till konfidentiell information som skickas över atlanten.

Euro-atlantiska rutten för undervattenskablarna är den äldsta och en viktig del av Europas datasäkerhet, då majoriteten av Europas data lagras på servrar i USA.

Att Europas datasäkerhet ligger i USA:s händer väcker många frågor om integritet - efter rapporter om USA:s dataövervakning [2]. Flera kritiker menar att USA har tillgång till privata data från Europas länder och att det finns en fara i att europeiska data ligger i en annan makts händer.

## Var går gränsen mellan spionage på medborgare och utredning av kriminalitet?

Nyligen lade EU-kommissionen fram ett förslag där företag som tillhandahåller tjänster som meddelanden och chattar behöver filtrera användares meddelanden och lämna över dem till polisen i syfte att stoppa spridning av barnpornografi [7]. Detta betyder att företag som använder sig av olika chattsystem måste slopa krypteringsfunktioner, vilket gör att säkerheten hos användarnas data sjunker markant. Niels Paarup-Petersen (C) anser att EU-byråkrater inte ska ta del av varenda nakenbild som skickas mellan tonåringar. Detta skulle vara en inskränkning av deras integritet [7]. Vidare hänvisar Niels Paarup-Petersen (C) till regeringsformen 2 kap. 6 §, som säger att var och en är skyddad mot intrång samt mot undersökning av brev eller annan förtrolig försändelse och hemlig avlyssning av samtal [7].

En annan aspekt av ökad övervakning av potentiell kriminalitet återfinns i nya förslag om verktyg som ska underlätta övervakning för polisen. Det handlar om fler övervakningskameror, ansiktsigenkänning och drönare som polisen utan brottsmisstanke ska kunna använda mot gängkriminella [8]. Dessa förslag har fått en hel del kritik, då vissa hävdar att sådana metoder banar ny väg mot ett övervakningssamhälle, ett samhälle där myndigheter övervakar och kränker medborgares integritet för att minska brott.

# Diskussion och slutsatser

Denna rapport belyser en central fråga i vår tids digitala samhälle: balansen mellan säkerhet och brottsbekämpning och rätten till privatliv och dataskydd. Efter terrorattackerna i New York 2001 fick USA dramatiska förändringar i sina säkerhets- och övervakningslagar, t.ex. The Patriot Act och PRISM-programmet, vilket medförde en kraftig ökning av statlig övervakning av medborgarnas data. Detta väckte flera debatter och oro för integritetskränkningar av privatlivet och brist på dataskydd.

Den pågående spänningen mellan säkerhet och privatliv är inte enbart aktuell~~t~~ i USA. Även i Europa finns liknande debatter, speciellt med tanke på att en stor del av Europas data lagras på servrar i USA, vilket väcker frågor om integritet och dataskydd. Denna oro förstärks av förslag från EU-kommissionen om att företag ska filtrera användarnas meddelanden för att bekämpa spridningen av barnpornografi, vilket innebär en potentiell inskränkning av den personliga integriteten.

I diskussionen om var gränsen går mellan nödvändig övervakning för brottsbekämpning och vår rätt till privatliv och dataskydd, framstår det tydligt att det inte finns någon enkel lösning. Å ena sidan är det viktigt att myndigheter har verktyg för att effektivt bekämpa brott och upprätthålla säkerhet. Å andra sidan är skyddet av medborgares rättigheter och rätten till privatliv och dataskydd grundläggande principer i demokratiska samhällen.

Slutsatsen som kan dras är att det är viktigt att fortsätta debatten om dessa frågor, då mer och mer teknik integreras i vår vardag. Det är nödvändigt att fortsätta att utvärdera och omvärdera lagar för att hitta en balans som skyddar samhället från brott och terrorism, samtidigt som den värnar om medborgares rättigheter och integritet. Framtida lagförslag måste överväga båda dessa aspekter för att skapa en hållbar och rättvis balans och för att inte gå mot ett övervakningssamhälle.

# Referenser

[1]: J. Garamone, “9/11 drove change in Intelligence Community, NSA chief says,” U.S. Department of Defense, <https://www.defense.gov/News/News-Stories/Article/Article/945544/911-drove-change-in-intelligence-community-nsa-chief-says/> [Hämtad 29-Nov-2023]

[2]: “Surveillance under the Patriot Act,” American Civil Liberties Union, <https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act> [Hämtad: 29-Nov-2023].

[3]: Nationalencyklopedin, "FBI," [Online]. Available: [http://www.ne.se/uppslagsverk/encyklopedi/lång/fbi](http://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/fbi). [Hämtad 29-Nov-2023]

[4]: [T.C. Sottek](https://www.theverge.com/authors/tc-sottek), “Everything You Need To Know About Prism”, The Verge, [Everything you need to know about PRISM - The Verge](https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet), [Hämtad 29-Nov-2023].

[5]: Michael Ray, “Edward Snowden”, Britannica, [Edward Snowden | Education, Biography, Russia, & Facts | Britannica](https://www.britannica.com/biography/Edward-Snowden), [Hämtad 29-Nov-2023]

[6]: Raphael Satter, ”US lawmakers introduce surveillance reforms intented to curb FBI spying”, Reuters, <https://www.reuters.com/world/us/us-lawmakers-introduce-surveillance-reforms-intended-curb-fbi-spying-2023-11-07/>,[Hämtad: 29-Nov-2023].

[7]: Niels Paarup-Petersen, ”Chat Control”, Riksdagen, “[Chat control (Skriftlig fråga 2022/23:526 av Niels Paarup-Petersen (C)) | Sveriges riksdag (riksdagen.se)](https://www.riksdagen.se/sv/dokument-och-lagar/dokument/skriftlig-fraga/chat-control_ha11526/)”, [Hämtad 29-Nov-2023].

[8]: Markus Alexandersson, ”Förslag om mer övervakning sågas: ”Skrämmande”, TT/Aftonbladet, [Förslag om mer övervakning sågas: "Skrämmande" (aftonbladet.se)](https://www.aftonbladet.se/nyheter/a/WR5Gv2/forslag-om-mer-overvakning-sagas-skrammande), [Hämtad 29-Nov-2023].

[9]: Colin Wall, ”Invisible and Vital: Undersea Cables and Transatlantic Security”, CSIS, [Invisible and Vital: Undersea Cables and Transatlantic Security (csis.org)](https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security), [Hämtad: 29-Nov-2023].