

Hur står det till med den personliga integriteten?

– en kartläggning av Integritetskommittén

Delbetänkande av Integritetskommittén

Stockholm 2016



STATENS OFFENTLIGA
UTREDNINGAR

SOU 2016:41

Innehåll

DEL I, Inledning

Sammanfattning	27
1 Författningsförslag	35
1.1 Förslag till förordning om ändring av förordningen (2007:975) med instruktion för Datainspektionen.....	35
2 Integritetskommitténs uppdrag och arbete	37
2.1 Kommitténs uppdrag.....	37
2.2 Kommitténs arbete.....	38
2.3 Begreppet personlig integritet.....	39
2.4 Kommitténs bedömning av riskerna för den personliga integriteten.....	40
2.5 Motsvarande kartläggningar i andra länder	42
2.5.1 Norge.....	42
2.5.2 Danmark.....	43
2.5.3 Tyskland	43
2.5.4 Storbritannien.....	43
2.6 Betänkandets disposition	44
DEL II, Kommitténs sammantagna bedömning m.m.	
3 Kommitténs sammantagna bedömning	49
3.1 Inledning.....	49
3.2 Den samlade effekten för den enskilde	49

3.3	Generella problem.....	52
3.3.1	Kunskap om hur uppgifterna hanteras.....	53
3.3.2	Möjligheten för den enskilde att påverka	53
3.3.3	Den enskildes egna skyddsåtgärder.....	54
3.3.4	Vad tycker den enskilde?	55
3.3.5	Otillräcklig tillsyn.....	56
3.3.6	Sanktionerna	57
3.3.7	Globaliseringen.....	57
3.3.8	Journalistiska ändamål enligt personuppgiftslagen.....	58
3.3.9	Näthat.....	59
3.3.10	Offentlighetsprincipen.....	60
3.3.11	Personlig integritet ett viktigt värde för hela samhället	61
3.4	Teknikutvecklingen	62
3.5	Kunskapsläget.....	64
3.6	Drivkrafter bakom utvecklingen	65
3.7	Kommitténs bedömning av respektive område	65
3.7.1	Skolan (kapitel 7)	65
3.7.2	Arbetsliv (kapitel 8).....	70
3.7.3	Hälso- och sjukvården och socialtjänsten (kapitel 9)	75
3.7.4	Forskning och statistik (kapitel 10)	77
3.7.5	E-förvaltning (kapitel 11).....	78
3.7.6	Konsumentområdet (kapitel 12).....	86
3.7.7	Sociala medier och e-post (kapitel 13)	89
3.7.8	Försäkringsverksamhet (kapitel 14).....	91
3.7.9	Bank- och kreditmarknaden (kapitel 15)	93
3.7.10	Kronofogdemyndighetens verksamhet, kreditupplysning och inkasso (kapitel 16).....	96
3.7.11	Domstolarnas verksamhet (kapitel 17)	97
3.7.12	De brottsbekämpande myndigheternas verksamhet (kapitel 18)	100
3.7.13	Försvarsunderrättelseverksamhet och militär säkerhetstjänst (kapitel 19)	105
3.7.14	Övervakning med kamera (kapitel 20)	108
3.7.15	Molntjänster (avsnitt 21.1)	110

3.7.16	Big data (avsnitt 21.2)	114
3.7.17	Biometri (avsnitt 21.3)	115
4	Overall assessment	117
4.1	The combined impact on the individual	117
4.2	General problems	120
4.2.1	Knowledge of how data is handled	121
4.2.2	Opportunity for the individual to exert influence	121
4.2.3	The individual's own protective measures	122
4.2.4	What do individuals think?	123
4.2.5	Insufficient supervision.....	123
4.2.6	Sanctions	125
4.2.7	Globalisation	125
4.2.8	Journalistic purposes under the Personal Data Act	126
4.2.9	Internet hate.....	127
4.2.10	Principle of public access to official documents	128
4.2.11	Privacy an important value for the whole of society	129
4.3	The development of technology.....	131
4.4	The knowledge situation.....	132
4.5	Drivers behind development	133
5	Den personliga integriteten	135
5.1	Inledning	135
5.2	Teorier om personlig integritet	136
5.2.1	Inledning.....	136
5.2.2	Rätten att bli lämnad i fred.....	137
5.2.3	Oönskad tillgång till jaget.....	138
5.2.4	Hemlig information.....	138
5.2.5	Kontroll över egna uppgifter och Strömholms kränkningsförteckning	139
5.2.6	Det att vara människa.....	140
5.2.7	Förhållandet mellan människor.....	141

5.3	Behandling av begreppet i tidigare lagstiftningsarbeten	141
5.3.1	Inledning	141
5.3.2	1966 års integritetsskyddskommitté och Yttrandefrihetsutredningen	142
5.3.3	Data- och offentlighetskommittén	143
5.3.4	Skyddet för enskilda personers privatliv – En studie	144
5.3.5	Integritetsutredningen	144
5.3.6	Personuppgiftslagsutredningen	145
5.3.7	Integritetsskyddskommittén	146
5.4	Personlig integritet i detta betänkande	147
5.4.1	Begreppets innebörd	147
5.4.2	Intrång i den personliga integriteten	148
6	Det grundläggande rättsliga skyddet	151
6.1	Inledning	151
6.2	Europakonventionen	151
6.3	EU:s rättighetsstadga	152
6.4	Regeringsformen	153
6.5	Personuppgiftslagen	153
6.5.1	Dataskyddsdirektivet	153
6.5.2	Lagens tillämpningsområde	154
6.5.3	Grundläggande krav för behandlingen	154
6.5.4	Tillåten behandling	156
6.5.5	Information och rättelse	158
6.5.6	Säkerhet vid behandlingen	158
6.5.7	Överföring av personuppgifter till tredje land	159
6.5.8	Kommande lagstiftning	160
6.6	Lagen om elektronisk kommunikation	161
6.7	Tillsyn	163
6.7.1	Inledning	163
6.7.2	Datainspektionen	163
6.7.3	Övriga tillsynsmyndigheter	164
6.7.4	Pågående arbete	165
6.8	Sanktioner	165

6.8.1	Inledning	165
6.8.2	Brott mot personuppgiftslagen.....	165
6.8.3	Straffbestämmelser i bl.a. brottsbalken	166
6.8.4	Skadestånd.....	170
DEL III, Riskbedömning av olika områden och företeelser		
7	Skolan.....	175
7.1	Inledning.....	175
7.1.1	Beskrivning av området.....	175
7.1.2	Regelverk och tillsyn	179
7.2	Digitala lärplattformar och läromedel.....	181
7.2.1	Företeelserna.....	181
7.2.2	Det skyddande regelverket.....	183
7.2.3	Risker för den personliga integriteten.....	184
7.3	Sociala medier i undervisningen.....	185
7.3.1	Företeelsen	185
7.3.2	Det skyddande regelverket.....	186
7.3.3	Risker för den personliga integriteten.....	187
7.4	Elevhälsan	190
7.4.1	Företeelsen	190
7.4.2	Det skyddande regelverket.....	191
7.4.3	Risker för den personliga integriteten.....	192
7.5	Skolfederationen.....	193
7.5.1	Företeelsen	193
7.5.2	Det skyddande regelverket.....	194
7.5.3	Risker för den personliga integriteten.....	194
7.6	Kameraövervakning i skolor.....	195
7.6.1	Företeelsen	195
7.6.2	Det skyddande regelverket.....	195
7.6.3	Risker för den personliga integriteten.....	196
7.7	Kommitténs samlade bedömning av området.....	198
8	Arbetslivet	203
8.1	Inledning.....	203
8.1.1	Beskrivning av området.....	203

8.1.2	Regelverk och tillsyn	204
8.2	Positionering.....	208
8.2.1	Företeelsen	208
8.2.2	Elektroniska körjournaler	208
8.2.3	Fordonskontroll.....	209
8.2.4	Digitala färdskrivare	209
8.2.5	Körstil.....	210
8.2.6	Positionering i annan utrustning	211
8.2.7	Risker för den personliga integriteten.....	213
8.3	Övervakning av aktiviteter och beteenden.....	214
8.3.1	Företeelsen	214
8.3.2	Internet och e-post	215
8.3.3	Personliga konton	216
8.3.4	Ärendehanteringssystem.....	217
8.3.5	In- och utpasseringssystem.....	218
8.3.6	Flödes- och logistiksystem	219
8.3.7	Risker för den personliga integriteten.....	220
8.4	Registerkontroller och medicinska undersökningar	221
8.4.1	Företeelsen	221
8.4.2	Risker för den personliga integriteten.....	222
8.5	Arbetsstagare och sociala medier	223
8.5.1	Företeelsen	223
8.5.2	Risker för den personliga integriteten.....	225
8.6	Kompetensdatabaser	226
8.6.1	Företeelsen	226
8.6.2	Risker för den personliga integriteten.....	227
8.7	Bakgrundskontroller och kandidatdatabaser	228
8.7.1	Företeelserna.....	228
8.7.2	Det skyddande regelverket.....	231
8.7.3	Risker för den personliga integriteten.....	231
8.8	Kameraövervakning	232
8.8.1	Företeelsen	232
8.8.2	Det skyddande regelverket.....	234
8.8.3	Risker för den personliga integriteten.....	235
8.9	Företagshälsovård	237

8.9.1	Företeelsen	237
8.9.2	Det skyddande regelverket.....	238
8.9.3	Risker för den personliga integriteten.....	238
8.10	Kommitténs samlade bedömning av området.....	239
9	Hälso- och sjukvård och välfärdsteknik inom socialtjänst ...	245
9.1	Inledning.....	245
9.1.1	Beskrivning av området.....	245
9.1.2	Regelverk och tillsyn	246
9.2	Allmänt om hanteringen av personuppgifter inom hälso- och sjukvården.....	249
9.2.1	Informationshantering i hälso- och sjukvården.....	249
9.2.2	Hur ser informationshanteringen ut i dag?.....	250
9.3	Behörighetsstyrning, åtkomstkontroll och spärrar och annan hantering av personuppgifter inom en vårdgivares verksamhet	254
9.3.1	Företeelsen	254
9.3.2	Det skyddande regelverket.....	256
9.3.3	Iakttagelser från tillsynen	257
9.3.4	Risker för den personliga integriteten.....	258
9.4	Sammanhållen journalföring.....	259
9.4.1	Företeelsen	259
9.4.2	Det skyddande regelverket.....	260
9.4.3	Iakttagelser från tillsynen	260
9.4.4	Risker för den personliga integriteten.....	261
9.5	Kvalitetsregister.....	263
9.5.1	Företeelsen	263
9.5.2	Det skyddande regelverket.....	264
9.5.3	Iakttagelser från tillsyn och myndighetsanalyser...	265
9.5.4	Risker för den personliga integriteten.....	267
9.6	Välfärdsteknik inom socialtjänsten	268
9.6.1	Används välfärdsteknik i dag?	268
9.6.2	Företeelsen	268
9.6.3	Det skyddande regelverket.....	270
9.6.4	Smers rapport om robotar och övervakning i vården av äldre.....	271

9.6.5	Risker för den personliga integriteten.....	272
9.7	Kommitténs samlade bedömning av området.....	273
10	Forskning och statistik.....	277
10.1	Företeelserna	277
10.1.1	Statistik	279
10.1.2	Forskning	281
10.2	Det skyddande regelverket	283
10.3	Risker för den personliga integriteten	284
10.4	Kommitténs samlade bedömning av området.....	288
11	E-förvaltning	291
11.1	Företeelser	291
11.1.1	Avgränsning	291
11.1.2	Ökad insamling, spridning och användning av personuppgifter	292
11.1.3	Betydelsen av att fastställa personuppgiftsansvaret	299
11.1.4	Brister i beställarkompetens	301
11.1.5	Potentiella handlingar och metadata	301
11.1.6	Offentlighetsprincipen.....	303
11.1.7	PSI-lagstiftningen.....	304
11.1.8	Eget utrymme	306
11.1.9	Medborgarprofilering.....	307
11.1.10	Kontroller på nätet.....	310
11.1.11	E-legitimation som avslöjar användaren	312
11.1.12	Myndigheter med uppgifter i molnet	313
11.1.13	Myndigheter i sociala medier och med gilla-knappar på webben.....	313
11.1.14	Informationssäkerhet	315
11.1.15	Regeringens mål i lagmotiv, digital agenda och e-förvaltningsstrategi	317
11.1.16	Samordning och styrning av utvecklingen	318
11.2	Det skyddande regelverket	320
11.3	Kommitténs samlade bedömning av området.....	321

12	Konsumentområdet.....	329
12.1	Inledning	329
12.1.1	Beskrivning av området.....	329
12.1.2	Internetekonomin.....	330
12.1.3	Regelverk och tillsyn	331
12.2	Kartläggning på nätet – IP-adresser, kakor och digitala fingeravtryck.....	333
12.2.1	Företeelserna.....	333
12.2.2	Sökmotorer.....	333
12.2.3	IP-adresser	335
12.2.4	Kakor	336
12.2.5	Digitala fingeravtryck	337
12.2.6	Det skyddande regelverket.....	338
12.2.7	Risker för den personliga integriteten.....	339
12.3	Positionering.....	341
12.3.1	Företeelsen	341
12.3.2	Wifi-tracking.....	341
12.3.3	Bluetooth low energy	343
12.3.4	RFID	345
12.3.5	GPS.....	347
12.3.6	Mobilnät	347
12.3.7	Det skyddande regelverket.....	348
12.3.8	Risker för den personliga integriteten.....	348
12.4	Elektroniska betalningar	349
12.4.1	Företeelsen	349
12.4.2	Det skyddande regelverket.....	350
12.4.3	Risker för den personliga integriteten.....	350
12.5	Sakernas internet (Internet of Things).....	352
12.5.1	Företeelsen	352
12.5.2	Uppkopplade fordon	354
12.5.3	Det skyddande regelverket.....	355
12.5.4	Risker för den personliga integriteten.....	356
12.6	Mediekonsumtion	358
12.6.1	Företeelsen	358
12.6.2	Det skyddande regelverket.....	360
12.6.3	Risker för den personliga integriteten.....	361

12.7	Smarta mätare.....	361
12.7.1	Företeelsen	361
12.7.2	Det skyddande regelverket.....	363
12.7.3	Risker för den personliga integriteten.....	364
12.8	Appar.....	364
12.8.1	Företeelsen	364
12.8.2	Det skyddande regelverket.....	367
12.8.3	Risker för den personliga integriteten.....	367
12.9	Peer-to-peer-plattformar	368
12.9.1	Företeelsen	368
12.9.2	Det skyddande regelverket.....	368
12.9.3	Risker för den personliga integriteten.....	369
12.10	Kommitténs samlade bedömning av området.....	369
13	Sociala medier och e-post	373
13.1	Sociala medier.....	373
13.1.1	Avgränsning	373
13.1.2	Begreppet sociala medier.....	374
13.1.3	Olika kategorier av sociala medier.....	376
13.1.4	Funktioner för klagomålshantering	378
13.1.5	Annonsförsäljning	379
13.1.6	Två typer av information	379
13.1.7	Vilka har intresse för uppgifter om användarna?....	382
13.1.8	Radering av uppgifter i sociala medier	385
13.1.9	Användarvillkor.....	385
13.2	E-post.....	386
13.3	Det skyddande regelverket	390
13.4	Kommitténs samlade bedömning av området.....	394
14	Försäkringsverksamhet	399
14.1	Om försäkring och hantering av personuppgifter	399
14.1.1	Vad är försäkring?	399
14.1.2	Behov av behandling av personuppgifter inom försäkringsföretagen.....	400
14.1.3	Den rättsliga regleringen.....	400

14.1.4	Tillsyn m.m.	401
14.1.5	Branschöverenskommelser.....	401
14.2	Behandling av uppgifter för att bedöma premier m.m.	402
14.2.1	Försäkring och modern teknik.....	402
14.2.2	Ny teknik ger nya bedömningsgrunder.....	403
14.2.3	Insamling av kördata	405
14.2.4	Aktivitetsmätare	405
14.2.5	Data från andra källor	406
14.3	Exempel på risker för intrång i den personliga integriteten.....	408
14.3.1	Dataläckage	408
14.3.2	Dataanvändning.....	409
14.3.3	Risk för diskriminering på försäkringsmarknaden?.....	409
14.3.4	Inhämtning av uppgifter om hälsa.....	410
14.4	Kommitténs samlade bedömning av området.....	412
15	Bank- och kreditmarknad	415
15.1	Allmänt om behandling av personuppgifter inom bank och kreditmarknadsföretag.....	415
15.1.1	Den rättsliga regleringen.....	416
15.1.2	Tillsyn m.m.	417
15.2	Behandling av uppgifter för kreditprovning och rådgivning.....	417
15.2.1	Företeelsen	417
15.2.2	Det skyddande regelverket.....	418
15.2.3	Risker för den personliga integriteten.....	419
15.3	Kreditkort och transaktioner över internet.....	421
15.3.1	Företeelsen	421
15.3.2	Det skyddande regelverket.....	422
15.3.3	Risker för den personliga integriteten.....	423
15.4	Behandling av uppgifter för att uppfylla rapporteringskrav m.m.	428
15.4.1	Företeelsen	428
15.4.2	Det skyddande regelverket.....	431

15.4.3	Risker för den personliga integriteten.....	432
15.5	Kommitténs samlade bedömning av området.....	434
16	Kronofogdemyndighetens verksamhet, kreditupplysning och inkasso.....	437
16.1	Inledning.....	437
16.2	Kronofogdemyndigheten	437
16.2.1	Allmänt om Kronofogdemyndighetens behandling av personuppgifter	437
16.2.2	Det skyddande regelverket.....	439
16.2.3	Tillstånd och tillsyn.....	440
16.2.4	Risker för den personliga integriteten.....	440
16.3	Kreditupplysning	442
16.3.1	Allmänt om kreditupplysning	442
16.3.2	Det skyddande regelverket.....	443
16.3.3	Tillstånd och tillsyn	445
16.3.4	Risker för den personliga integriteten.....	446
16.4	Inkasso.....	450
16.4.1	Allmänt om inkassoverksamhet	450
16.4.2	Det skyddande regelverket.....	451
16.4.3	Tillstånd och tillsyn.....	451
16.4.4	Risker för den personliga integriteten.....	451
16.5	Kommitténs samlade bedömning av området.....	452
17	Domstolarnas verksamhet	455
17.1	Inledning.....	455
17.1.1	Om domstolarna.....	455
17.1.2	Domstolarnas användning av informationsteknik.....	456
17.1.3	Den rättsliga regleringen	457
17.1.4	Tillsyn	459
17.2	Behandling av uppgifter i verksamhetsregister och besöksterminaler	459
17.2.1	Företeelsen	459
17.2.2	Det skyddande regelverket.....	459

17.2.3	Risker för den personliga integriteten	460
17.3	Behandling av uppgifter i ljud- och bildupptagning	461
17.3.1	Företeelsen	461
17.3.2	Det skyddande regelverket.....	462
17.3.3	Risker för den personliga integriteten.....	463
17.4	Informationsutbyte mellan domstolar och andra myndigheter	464
17.4.1	Företeelsen	464
17.4.2	Det skyddande regelverket.....	464
17.4.3	Risker för den personliga integriteten.....	465
17.5	Utlämnande av uppgifter på medium för automatiserad behandling.....	466
17.5.1	Företeelsen	466
17.5.2	Det skyddande regelverket.....	466
17.5.3	Risker för den personliga integriteten	467
17.6	Kommitténs samlade bedömning av området	469
18	De brottsbekämpande myndigheternas verksamhet	473
18.1	Inledning.....	473
18.1.1	De brottsbekämpande myndigheternas användning av informationsteknik.....	473
18.1.2	Allmänt om den rättsliga regleringen.....	474
18.1.3	Tillsyn.....	476
18.2	Hemlig rumsavlyssning och annan ljudupptagning som inte avser elektronisk kommunikation	477
18.2.1	Företeelsen	477
18.2.2	Det skyddande regelverket.....	477
18.2.3	Risker för den personliga integriteten.....	479
18.3	Hemlig kameraövervakning och annan bildupptagning....	480
18.3.1	Företeelsen	480
18.3.2	Det skyddande regelverket.....	480
18.3.3	Risker för den personliga integriteten	482
18.4	Hemlig avlyssning av elektronisk kommunikation	483
18.4.1	Företeelsen	483
18.4.2	Det skyddande regelverket.....	483

18.4.3	Risker för den personliga integriteten	486
18.5	Hemlig övervakning av elektronisk kommunikation.....	487
18.5.1	Företeelsen	487
18.5.2	Det skyddande regelverket.....	487
18.5.3	Risker för den personliga integriteten.....	492
18.6	Genomsökning och kopiering av mobiltelefoner och datorer.....	496
18.6.1	Företeelsen	496
18.6.2	Det skyddande regelverket.....	496
18.6.3	Risker för den personliga integriteten	498
18.7	Polismyndighetens informationsinhämtning på internet m.m.	499
18.7.1	Företeelsen	499
18.7.2	Det skyddande regelverket.....	499
18.7.3	Risker för den personliga integriteten	500
18.8	Tillgång till uppgifter i flygbolagens databaser (Passenger Name Record, PNR) och i EU:s informationssystem för viseringar (VIS)	501
18.8.1	Företeelsen	501
18.8.2	Det skyddande regelverket.....	501
18.8.3	Risker för den personliga integriteten.....	502
18.9	Polisens behandling av personuppgifter i register och databaser.....	503
18.9.1	Företeelsen	503
18.9.2	Det skyddande regelverket.....	503
18.9.3	Risker för den personliga integriteten.....	507
18.10	Internationellt informationsutbyte.....	512
18.10.1	Företeelsen	512
18.10.2	Det skyddande regelverket.....	513
18.10.3	Risker för den personliga integriteten.....	515
18.11	Kommitténs samlade bedömning av området	516
19	Försvarsunderrättelseverksamhet och militär säkerhetstjänst	523
19.1	Inledning.....	523

19.1.1	Allmänt om verksamheten.....	523
19.1.2	Den rättsliga regleringen	524
19.1.3	Tillsyn m.m.	525
19.2	Försvarets radioanstalts behandling av uppgifter i försvarsunderrättelseverksamhet (signalspaning)	526
19.2.1	Företeelsen	526
19.2.2	Det skyddande regelverket.....	527
19.2.3	Risker för den personliga integriteten.....	529
19.3	Försvarsmaktens informationshantering i försvarsunderrättelseverksamhet- och militär säkerhetstjänst.....	534
19.3.1	Företeelsen	534
19.3.2	Det skyddande regelverket.....	534
19.3.3	Risker för den personliga integriteten	536
19.4	Kommittén samlade bedömning av området	537
20	Övervakning med kamera	541
20.1	Inledning.....	541
20.1.1	Allmänt om kameraövervakning m.m.	541
20.1.2	Den rättsliga regleringen.....	542
20.1.3	Tillsyn	547
20.2	Användningen av övervakningskameror och därmed jämförbar utrustning.....	547
20.2.1	Företeelsen	547
20.2.2	Risker för den personliga integriteten.....	549
20.3	Lagring och automatisk bildanalys	552
20.3.1	Företeelsen	552
20.3.2	Risker för den personliga integriteten.....	556
20.4	Kommitténs samlade bedömning av området.....	557
21	Några särskilda företeelser	561
21.1	Molntjänster	561
21.1.1	Företeelsen	561
21.1.2	Det skyddande regelverket.....	566
21.1.3	Kommitténs samlade bedömning av området	571

21.2	Big data.....	575
21.2.1	Företeelsen	575
21.2.2	Det skyddande regelverket.....	579
21.2.3	Kommitténs samlade bedömning av området	581
21.3	Biometri	583
21.3.1	Företeelsen	583
21.3.2	Det skyddande regelverket.....	587
21.3.3	Kommitténs samlade bedömning av området	588

DEL IV, Övrigt

22	Informationssäkerhet och integritet	593
22.1	Inledning.....	593
22.2	Informationssäkerhet som område.....	594
22.3	Det skyddande regelverket	595
22.4	Lägesbild över informationssäkerheten i Sverige.....	597
22.5	Informationssäkerhet och integritet.....	599
22.5.1	Relationen mellan informationssäkerhet och integritet.....	599
22.5.2	Risker för integriteten ur ett informationssäkerhetsperspektiv	601
22.5.3	Ett europeiskt perspektiv på informationssäkerhet och integritet.....	606
22.5.4	Inriktning för informationssäkerheten i Sverige ur ett integritetsperspektiv.....	607
22.6	Tillsyn och informationssäkerhet.....	610
22.7	Kommitténs samlade bedömning av området.....	611
23	Vilket skydd erbjuder samhället den enskilde?.....	613
23.1	Inledning.....	613
23.2	Tillsyn	616
23.2.1	På vilket sätt kan tillsyn ge ett skydd?	616
23.2.2	Fungerar tillsynen?.....	618
23.3	Ekonomisk ersättning.....	622

23.3.1	På vilket sätt kan ekonomisk ersättning vara ett skydd?.....	622
23.3.2	Möjligheten för den enskilde att begära ersättning.....	625
23.3.3	Ersättningsbeloppen vid rätt till skadestånd med stöd av personuppgiftslagen	627
23.3.4	Fungerar ersättningssystemet i dag?	629
23.4	Straffrättsliga sanktioner	631
23.4.1	På vilket sätt kan straffrättsliga åtgärder vara ett skydd?.....	631
23.4.2	Fungerar straffrättssystemet i dag?	634
23.5	Kommitténs samlade bedömning	635

DEL V, Kommitténs förslag

24	Förslag om ökad information till regering och riksdag	641
24.1	Integritetskommitténs uppdrag	641
24.2	Integritetsskyddskommitténs överväganden	642
24.3	En snabb utveckling	643
24.4	I Norge och Tyskland	645
24.5	Kommitténs överväganden och förslag	646
24.5.1	Behovet av ett nytt organ för säkrare avvägning i lagstiftningen	646
24.5.2	Behovet av överblick och rapportering om utvecklingen	647
24.5.3	Rapport till regeringen	648
24.5.4	Skrivelse till riksdagen	649
24.5.5	Uppdraget att redovisa utvecklingen	650
24.5.6	Inget rådgivande organ vid Datainspektionen	652
24.5.7	Kostnader	654
25	Konsekvenser av våra förslag	657
25.1	Inledning.....	657
25.2	Ekonomiska konsekvenser	657
25.3	Andra konsekvenser.....	658

DEL VI**Ett dygn med familjen Svenssons elektroniska spår 659****DEL VII****Reservation 691****Bilagor**

Bilaga 1 Kommittédirektiv 2014:65 695

Bilaga 2 Kommittédirektiv 2016:12..... 707

Bilaga 3 Integritetsskyddande teknik..... 709

Bilaga 4 Digitalisering och personlig integritet 743

Sammanfattning

Inledning

För att kunna ta del av många fördelar med modern informationsteknik delar vi med oss av våra personuppgifter. Ibland betalar vi som vanligt, men ofta får vi betala för olika tjänster genom att dela med oss av uppgifter om oss själva och ibland också om våra vänner. Det är svårt för oss att förstå och ha en överblick över på vilket sätt våra personuppgifter samlas in, sprids och vidareanvänds. Det är i dag möjligt att behandla stora mängder uppgifter om oss på ett sätt som blir mycket närgånget. Sådana behandlingar görs inte bara av kommersiella företag utan också av myndigheter.

På vilket sätt påverkar användningen av modern teknik vår möjlighet att bestämma över vilka uppgifter om oss som andra ska få ta del av? Finns det någon möjlighet att upprätthålla en fredad sfär, som inte myndigheter, företag eller andra enskilda kan komma åt? Hur står det till med den personliga integriteten i det moderna informationssamhället?

Integritetskommitténs uppdrag är att utifrån ett individperspektiv kartlägga och analysera risker för intrång i den personliga integriteten som kan uppkomma i samband med användning av informationsteknik. I detta delbetänkande presenterar vi en översiktlig beskrivning av faktiska och potentiella integritetsrisker som var och en av oss utsätts för.

Kommitténs riskbedömning

För att göra det möjligt att jämföra de risker för den personliga integriteten som är förknippade med olika företeelser i samhället har kommittén valt att beskriva riskerna utifrån tre nivåer; viss risk, påtaglig risk eller allvarlig risk för den personliga integriteten. En riskbedömning utgår dels från sannolikheten för att ett intrång inträffar, dels från effekterna eller konsekvenserna av intrånget. Mer om hur vi har arbetat med riskbedömningen redovisas i kapitel 2.

Företeelser som är förknippade med viss risk för den personliga integriteten

När det gäller företeelser som är förknippade med den lägsta graden av risk för den personliga integriteten handlar det ibland om företeelser som sannolikt inte så många av oss blir föremål för. Det kan också vara så att det inte är så många uppgifter som behandlas eller att det inte är så känsliga eller närgångna uppgifter. Det kan också vara så att det finns en bra och tydlig lagstiftning och att det inte har uppmärksammats särskilt stora tillämpningsproblem. Men dessa företeelser är ändå förknippade med risker för den personliga integriteten.

De företeelser som kommittén bedömt som förknippade med vissa risker för den personliga integriteten är:

- Hanteringen av personuppgifter inom elevhälsan (skolan)
- Skolfederation (skolan)
- Arbetsgivares granskningar av vad arbetstagare skriver på sociala medier (arbetsliv)
- Kompetensdatabaser och bakgrundskontroller inom arbetslivet
- När vårdgivare tillhandahåller både hälso- och sjukvård och personaladministrativa tjänster (arbetsliv)
- Statlig statistikverksamhet (forskning och statistik)
- Myndigheters användning av sociala medier (e-förvaltning)
- Kronofogdemyndighetens verksamhet

- Inkassobolagens verksamhet
- Personuppgiftsbehandling i domstolarnas verksamhetsregister, i samband med ljud- och bildupptagningar och i samband med informationsutbyte med andra myndigheter
- Tvångsmedel med stöd av 27 kap. rättegångsbalken (brottsbekämpning)¹
- Polisens spaningsverksamhet på internet och utåtriktade verksamhet i sociala medier (brottsbekämpning)
- Polisens hantering av personuppgifter som överförs av flygbolag och polisens deltagande i internationellt samarbete (brottsbekämpning)
- Behandling av personuppgifter i den militära underrättelsetjänstens it-system²

Företeelser som är förknippade med påtaglig risk för den personliga integriteten

När det gäller företeelser som är förknippade med den högre graden av risk för den personliga integriteten handlar det ofta om företeelser som innefattar behandling av fler uppgifter om enskilda och om behandlingar som omfattar många av oss. De uppgifter som behandlas kan vara känsliga eller närgångna. Sådana företeelser är ofta reglerade, men har ibland brister i regelverket eller i tillämpningen av dessa. Kommittén har bedömt riskerna efter en sammanvägning av dessa faktorer.

- Kameraövervakning (i allmänhet och särskilt beträffande övervakning inomhus i skolan)
- Informationsdelning inom och mellan myndigheter (e-förvaltning)

¹ För de enskilda personer som blir föremål för åtgärden är intrånget i den personliga integriteten tveklöst mycket närgånget. Men ur ett riskperspektiv ska även sannolikheten för att någon blir föremål för åtgärden beaktas, liksom andra relevanta faktorer som ett fungerande regelverk och risken för oönskad spridning m.m. Kommittén bedömer därför att åtgärden utgör en viss risk för den personliga integriteten, det vill säga den lägre riskgraden.

² Se fotnot 1.

- Informationsutbyte med enskilda (e-förvaltning)
- Vidareanvändning av offentlig information enligt PSI-lagstiftningen (e-förvaltning)
- Oskyddad e-post
- Försäkringsföretagens verksamhet
- Kreditprövning och rådgivning samt rapporteringskrav (bank- och kreditmarknad)
- Domstolarnas utlämnande av uppgifter på medium för automatiserad behandling
- Spaningsmetoder som enbart regleras av polislagen (brottsbekämpning)
- Polisens behandling av personuppgifter i register (brottsbekämpning)
- Signalspaning (försvarsunderrättelseverksamhet och militär säkerhetstjänst)³
- Tekniker som involverar många och detaljerade biometriska uppgifter (biometri)

Företeelser som är förknippade med allvarlig risk för den personliga integriteten

När det gäller företeelser som är förknippade med den högsta graden av risk för den personliga integriteten handlar det ofta om företeelser som innefattar behandling av många uppgifter om enskilda och om behandlingar som omfattar stora delar av befolkningen. Det handlar också ofta om behandling av mycket känsliga eller närgångna personuppgifter. Sådana företeelser kan sakna reglering eller ha stora brister i regelverket eller i tillämpningen av dessa. Kommittén har bedömt riskerna efter en sammanvägning av dessa faktorer.

³ För de enskilda personer som faktiskt blir föremål för granskning är intrånget i den personliga integriteten tveklöst mycket närgånget. Men ur ett riskperspektiv ska även sannolikheten för att någon blir föremål för åtgärden beaktas, liksom andra relevanta faktorer som ett fungerande regelverk och risken för oönskad spridning m.m. Kommittén bedömer därför att åtgärden utgör en påtaglig risk för den personliga integriteten, det vill säga den något högre riskgraden.

- Digitala lärplattformar och digitala läromedel (skolan)
- Vissa sociala medier (i allmänhet och särskilt beträffande användningen av sociala medier i skolans undervisning)
- Arbetsgivares positionering och annan övervakning och kontroll av arbetstagarnas aktiviteter och beteenden på arbetet
- Kameraövervakning på arbetsplatser
- Hälsa- och sjukvård och välfärdstjänster inom socialtjänsten
- Viss forskning
- Myndigheter med kunddata i molnet (e-förvaltning)
- Medborgarprofilering och kontroller på internet (e-förvaltning)
- Brister i myndigheters informationssäkerhet (e-förvaltning)
- Konsumentområdet
- Försäkringsföretagens framtida verksamhet
- Användningen av kreditkort och andra digitala transaktioner (bank- och kreditmarknad)
- Kreditupplysningsföretagens verksamhet
- Lagring och vidarebearbetning av uppgifter som har samlats in med hjälp av kamerövervakning
- Publika molntjänster
- Big data

Informationssäkerhet och integritet

Vi har som enskilda personer ofta små möjligheter att påverka hur uppgifter om oss hanteras. Därför är det nödvändigt att de som hanterar våra personuppgifter tar sitt ansvar för säkerheten. Kommittén anser att det finns starka indikationer på allvarliga brister i informationssäkerheten i offentliga verksamheter. När det gäller den privata sektorn har kommittén inte tillräckligt underlag för att göra en generell bedömning. I kapitel 22 skriver vi mer om detta viktiga ämne.

Övervägande om behovet av ett integritetsskyddsråd

Vi bedömer att det saknas behov av ett nytt integritetsskyddsorgan som, på det sätt som Integritetsskyddskommittén ansåg kunde övervägas, skulle ha till huvuduppgift att verka för en säkrare avvägning av motstående intressen i lagstiftningen.

Förslag om ökad information till regering och riksdag

Kommittén lämnar förslag om att Datainspektionens uppdrag att följa och beskriva utvecklingen på it-området när det gäller frågor som rör personlig integritet och ny teknik, ska utvidgas till att även omfatta de legala förutsättningarna för integritetsskyddet och att myndigheten årligen ska lämna en redovisning om utvecklingen inom området till regeringen (kap. 24).

Vi föreslår även att regeringen i en årlig skrivelse till riksdagen ska informera om utvecklingen och det aktuella tillståndet när det gäller frågor som rör personlig integritet, informationsteknik och de legala förutsättningarna för integritetsskyddet.

Ett dygn med familjen Svenssons elektroniska spår

I del VI finns en vardaglig beskrivning av några integritetsrisker som en vanlig familj kan drabbas av under ett dygn. Syftet är att på ett lättillgängligt sätt redovisa hur modern teknik påverkar den personliga integriteten.

Sammanfattningsvis

I detta betänkande redogör kommittén för behandlingen av personuppgifter inom ett antal områden som en enskild person kommer i kontakt med i olika livsskeden och gör en riskbedömning av dessa. Vi beskriver därtill några vanliga generella företeelser, som har inverkan på den personliga integriteten. Vi drar också vissa slutsatser

beträffande den samlade effekten för en enskild person av all den insamling och lagring av personuppgifter, kartläggning och övervakning som han eller hon deltar i eller blir föremål för.

Den digitala utvecklingen innebär en genomgripande förändring av samhället och enskildas livsvillkor. Personuppgifter i digital form genereras och används i allt högre grad inom alla samhällsområden. Antalet aktörer ökar, användningsområdena ökar, lagringstiderna ökar, spridningen och utbytet mellan aktörerna ökar, vidareanvändningen hos respektive aktör ökar liksom spridningen över nationsgränserna. Vi ser också att vissa stora aktörer, som en följd av utvecklingen i stort och deras egna affärsstrategier, får tillgång till en allt större mängd personuppgifter och därmed har möjlighet att teckna en alltmer komplett bild av en enskild person. Ur den enskildes perspektiv innebär utvecklingen att kunskapen om hur uppgifterna hanteras, liksom möjligheten att påverka detta, hela tiden krymper i förhållande till den ökande hanteringen av personuppgifter i samhället.

I motsvarande mån begränsas även den enskildes möjlighet att genom ett verkligt fritt val bestämma hur uppgifter om honom eller henne ska hanteras. Integritetskommitténs generella slutsats är därför att den enskilde – parallellt med den digitala utvecklingen – utsätts för stegvisa försämringar av den personliga integriteten.

Självfallet innehåller den digitala utvecklingen en enorm nyttopotential, men i det här delbetänkandet har vi fokuserat på faktiska och potentiella risker.