Lee A. Bygrave (red.)

YULEX 2002

Institutt for rettsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:

Institutt for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 82-7226-066-2
ISSN 0806-1912

unipubskriftserier

Utgitt i samarbeid med Unipub AS
Denne boken går inn i universitets- og høyskolerådets skriftserie
Trykk: GCSM AS
Omslagsdesign Kitty Ensby

FORORD

Denne boken er den andre i Yulex-serien. Siktemålet med serien er å tilby venner av Institutt for rettsinformatikk smakebiter fra ulike problemstillinger som har opptatt instituttets medarbeidere gjennom året. Den første utgivelsen i serien ble svært godt mottatt, og alt tyder på at det også vil være tilfellet med *Yulex 2002*.

God jul og fornøyelig lesing inn i det nye året!

Lee A. Bygrave

PREFACE

This book is the second in the Yulex series. The aim with the series is to offer friends of the Norwegian Research Centre for Computers and Law a "Christmas smorgasbord" of the various themes upon which Centre staff have worked over the past year. The first edition of the series was very well received; all indications are that *Yulex 2002* will be too.

Merry Christmas and happy reading into the New Year!

Lee A. Bygrave

INNHOLD

SELVREGULERING

OLAV TORVUND

Selvregulering har blitt et slags credo for mange som arbeider med handel og annen aktivitet på internett. Men om man forsøker å finne ut hva disse egentlig tror på, kommer man ikke særlig langt. Hvis selvregulering, slik dette ordet brukes, har et konkret innhold, så er det i alle fall ikke lett å få øye på. I denne artikkelen tar jeg for meg noen former for selvregulering, slik at man kan ha et noe bedre grunnlag for å vurdere om dette er en egnet strategi for nettet.

En begrunnelse for å velge selvregulering som strategi, er at man mener at lovgiver bør være tilbakeholden med å regulere en fremtidig virkelighet som ingen riktig vet hvordan kommer til å bli. Man vil at spillereglene utvikles av aktørene i markedet. Og disse reglene kan gjerne utvikles gradvis, etter hvert som problemene oppstår.

I en del internett-miljøer kan man finne en ganske ekstrem motstand mot regulering. Det er en ideologi om at alt skal være fritt og uten innblanding. Jungelens lov er en mer treffende betegnelse på en slik tilstand enn selvregulering. Nettets rovdyr, hyener og gribber ønsker ikke at andre skal hindre dem i deres virksomhet.

Debatten om *selvdømme* er også ganske gammel. Her er spørsmålet om en lukket krets kan regulere en avgrenset virksomhet innenfor kretsen, uten at denne kan overprøves av domstolene. Begrunnelsen er at dette i liten grad berører noen utenfor kretsen, og det aksepteres at man ikke har noe rettskrav på å være medlem i et balalaikaorkester hvor man ikke er ønsket. En gang i internettets barndom var man kanskje en liten og lukket krets som drev med en virksomhet som var uinteressant og uvesentlig for verden utenfor. Men det er ikke lenger tilfellet, slik at dette ikke kan begrunne at man kan melde seg ut av rettssamfunnet.

En klassisk form for selvregulering er avtaler. En fullstendig avtalefrihet gir fullt rom for selvregulering. Bruk av standardkontrakter gir partene store muligheter for å regulere sin virksomhet selv. Men det betyr også at den som er sterk nok kan presse andre til å måtte goda sin egen, ikke særlig balanserte regulering. De senere års erkjennelse av at man trenger et forbrukervern – som riktig nok har gått for langt – viser at en slik modell for selvregulering ikke uten videre kan aksepteres.

Utviklingen av preseptorisk lovgivning på en rekke kontraktsområder, ved siden av den generelle hjemmelen for å sette til side urimelige avtaler i avtaleloven § 36, illustrerer at en fullstendig selvregulering vil være en illusjon. Man vil ha et større eller mindre spillerom for selvregulering innenfor rammen av en mer eller mindre spesifikk lovgivning.

Om vi holder oss til avtaler, så illustrerer dette også en av de fundamentale svakhetene i en selvregulering: Avtaler binder bare de som er part i avtalene. Hvis man ønsker at et marked skal reguleres gjennom en selvregulering, bl a for å hindre uakseptabel opptreden fra de som opererer i markedet, så må denne reguleringen på en eller annen måte kunne håndheves. Hvis de som ikke ønsker å følge spillereglene bare kan la være å akseptere dem, vil man ikke ha oppnådd så mye – i alle fall hvis målet er å hindre en markedsadferd som de fleste finner uakseptabel.

Med utgangspunkt i avtaleregulering kan man også sette et spørsmålstegn ved hvorvidt en selvregulering hvor mye er opp til partene selv, egentlig er en rasjonell strategi for regulering. De som måtte være interessert i fotball kan ha mange meninger om regler for offside. Men det ville bli ganske kjedelig om hver fotballkamp startet med lange forhandlinger om hvilken offsideregel som skal gjelde for akkurat denne kampen. Og rasjonelt er det ikke. Det kan være en fordel at man har fastsatte spilleregler, selv om man gjerne hadde sett at enkelte av reglene ble endret. Det er neppe tids- og ressursbesparende at alle selgere i et marked har et kobbel av advokater som forfatter avtalevilkår som er så lange at de fleste ikke orker å lese dem, og så vanskelige at de som forsøker ikke forstår dem. Vi er mange som vet at vi ikke burde gjøre slik, men som likevel klikker «I accept» på all verdens avtalevilkår som vi ikke gidder å lese. En slik form for selvregulering er ikke noe som myndighetene bør stimulere til.

Dersom vi ønsker at en regulering skal gjelde for flere enn de som direkte har inngått en avtale, så er den tradisjonelle avtalemodellen ikke egnet. Man trenger en felles regulering, og ikke en individuell regulering for hver enkelt transaksjon. Samtidig ønsker vi ikke at den sterkeste parten skal kunne diktere hvilke vilkår som skal gjelde, og vi vil ikke at de useriøse skal kunne slippe unna. Utfordringen blir hvordan man utvikler en selvregulering som ivaretar disse ganske motstridende hensynene, herunder hvem som utvikler reguleringen. Endelig er det et spørsmål om hvordan slike regler håndheves.

Bruk av «agreed documents» kan myke opp og avdempe noen av ulempene med en avtaleregulering. Der hvor man har få og/eller velorganiserte aktører i et marked, kan det være grunnlag for å fremforhandle slike avtaler, som i rimelig grad balanserer de ulike aktørenes interesser. Men når i alle fall den ene av aktørene er svak og/eller uorganisert, er det ikke grunnlag for å etable-

re slike avtaler. Man mangler simpelthen noen som kan forhandle og bli enige om vilkår på vegne av den ene parten.

En velkjent, og kanskje noe spesiell form for «agreed document» er tariffavtalen. Den er muliggjort gjennom organisering – i første rekke på arbeidstakersiden. Det kan innvendes at dette er avtaler som inngås på vegne av medlemmene, og ikke standardavtaler som partene kan velge å benytte seg av. Men dels er det ikke helt ukjent fra andre områder at partene forplikter seg til å benytte en bestemt avtale, dels fungerer tariffavtaler også i en viss grad som mønster for arbeidsavtaler mellom parter som ikke er organisert og som avtalen ikke direkte gjelder for. Og uansett er disse avtalene interessante som eksempel på avtaler mellom organiserte parter som har funnet fram til en noenlunde fungerende modell for selvregulering.

Når det er myndighetene som opptrer som motpart i forhandlinger, kan det diskuteres i hvor stor grad det er en reell selvregulering. Forbrukerombudet har etter markedsføringsloven § 13 annet ledd bl a mandat til å føre forhandlinger med næringsdrivende og deres organisasjoner for å bidra til at urimelige avtalevilkår ikke benyttes. Myndighetene har her gått inn i rollen som representant for en temmelig uorganisert gruppe av forbrukere.

En form for selvregulering er ulike former for klubbregler. Hvis man vil være med i det gode selskap, så må man akseptere reglene. Den som vil delta i konkurranseidrett må akseptere idrettsorganisasjonenes spilleregler og deres håndhevelse av disse. Man kan gjerne drive idrett uten å akseptere disse reglene, men da er man satt utenfor – uansett om man måtte mene at det er det gode eller det dårlige selskap man er utestengt fra.

Hvorvidt klubbreglene er effektive, avhenger av hvor sterkt klubben står og hvor viktig det er å være innenfor. Om et meglerhus skulle miste sitt børsmedlemskap, så er man stengt ute fra det markedet man lever av. Den som kan fastsette reglene for et slikt marked, har en sterk posisjon. Om jeg derimot skulle bli kastet ut av en snobbete vinklubb fordi jeg synes det er sløsing å spytte den gode vinen ut igjen, så er vel det noe som er til å leve med.

Det er ikke uvanlig at retten til å utøve et yrke eller å drive en virksomhet er knyttet til medlemskap i en forening. Fra gammelt av kjenner vi laugsvesenet, som gjorde at man ikke kunne utøve et håndverk uten å være medlem av lauget. Dette er avskaffet, og det er ikke lenger så lett å finne denne form for kobling mellom medlemskap og yrkesutøvelse i Norge. Men i andre land er dette velkjent. Man skal ikke lenger enn til Sverige for å finne et eksempel på at advokatbevillingen er knyttet til medlemskap i Advokatsamfunnet. Det er heller ikke så vanskelig å finne eksempler på at f eks retten til å drive bankvirksomhet er knyttet til medlemskap i bankforeningen. Hvis utelukkelse fra

en forening også innebærer yrkesforbud og/eller forbud mot utøvelse av en næring, har man et meget effektivt middel til å håndheve klubbens regler.

Hvis medlemskap i klubben får for stor betydning, trer igjen noen av svakhetene ved selvregulering fram. Utviklingen har vært særlig tydelig gjennom profesjonaliseringen og kommersialiseringen av idretten. Når ens yrke er å drive idrett, blir konsekvensene av en utestengelse stor. Om en fotballspiller mister sin spillelisens, så mister han ikke bare muligheten til å drive sin hobby innenfor organiserte rammer. Han mister jobben og får i praksis yrkesforbud. Da kan man ikke lenger leve på siden av de regler som gjelder arbeidsforhold ellers i samfunnet. Det er da også de alminnelige domstoler som har tvunget fotballen til å avvikle livegenskapen – noen hundre år etter resten av samfunnet, og som gjør at klubber ikke i samme grad som før kan basere sine inntekter på salg av gladiatorer i et internasjonalt marked. Det var også frykten for søksmål ved de alminnelige domstoler som førte til den heller ynkelige reaksjonen fra Den Internasjonale Olympiske Komite etter dopingskandalene under vinter-OL i Salt Lake City, og det er dette som hevdes å være grunnen til at friidrettsforbundet i USA angivelig skal ha latt være å rapportere flere tilfeller hvor amerikanske utøvere har avgitt positiv prøve i dopingkontroll.

En annen side ved klubbregler er at man ikke (lenger) ønsker konkransebegrensende karteller. Hvis medlemskap i en klubb er så viktig at man i praksis stenges ute fra et marked om man ikke er med, og denne klubben bestemmer vilkårene for hvordan medlemmene kan drive sin virksomhet, skjermes man mot konkurranse. Man ønsker derfor ikke at en selvregulering gjennom slike klubber skal bli for effektiv. Å finne en balanse her kan være en betydelig utfordring.

Sterke klubber kan få den samme virkning som monopoler. Få medlemmer sammen med strenge og lite gjennomsiktige kriterier for å komme inn trekker en sterk klubb i retning monopol. Bankene er en gruppe som har fått søkelyset rettet mot seg på dette grunnlaget. Motsatt vil en lav terskel for medlemskap og gjennomsiktige kriterier kunne bidra til å åpne for konkurranse innenfor rammene av klubben.

Et marked med få og store aktører og hvor store kapitalkrav eller andre strenge krav gjør det vanskelig for nye å etablere seg, kan ligne på et marked med en streng klubb. Luftfart er et eksempel på en slik virksomhet. Men så lenge de ikke samarbeider om en regulering, og de etablerte i alle fall ikke formelt kan bestemme hvem som skal slippes inn i det gode(?) selskap, så mangler det sentrale elementet for å opptre som klubb i en selvreguleringssammenheng.

Vender vi tilbake til utgangspunktet, som er handel og annen virksomhet på internett, så har problemet i betydelig grad vært at mekanismene for selv-

regulering er for svake. Bildet er ikke entydig. Noen sterke aktører, med Microsoft i spissen, setter viktige spilleregler gjennom sin kontroll over deler av teknologien. Videre er de maktstrukturer og reguleringsmekanismer som gjelder for sentrale elementer i infrastrukturen særdeles lite gjennomsiktige. NORID, organisasjonen som tildeler og administrerer domenenavn under <.no> domenet, skriver om seg selv at deres registreringstjeneste «er delegert til UNINETT av IANA (Internet Assigned Numbers Authority), og drives i forståelse med det norske Post- og teletilsynet.» Det er vanskelig å få klarhet i hvordan denne «delegeringen» fungerer, og det som skjer høyere opp i dette hierarkiet er særdeles lite gjennomsiktig.

Beveger vi oss opp fra infrastrukturen og til de som driver en virksomhet basert på denne strukturen, kommer vi inn i det området som de fleste tenker på når de ønsker selvregulering. Markedet for nettbaserte tjenester er sammensatt, og monopolister deltar også her. Men vårt hjemlige marked for e-handel har, i alle fall til nå, vært lite organisert og ikke preget av noen få dominerende aktører. Så langt har ikke problemet med selvregulering vært at noen aktører blir for sterke og kan diktere spillereglene, men tvert i mot at ingen er sterke nok til at reguleringen bli effektiv.

Visse former for selvregulering er knyttet til merkeordninger. Man må forplikte seg i forhold til visse regler for å kunne benytte merket på sine nettsider. Et eksempel er *Nsafe*, som er etablert i samarbeid mellom Forbrukerrådet og eForum.[1] Dette er også en klubbløsning, og det er den antatte markedsføringsverdien av å kunne benytte et merke som indikerer seriøsitet som skal lokke markedsaktørene inn i ordningen.

Et typisk element i norske selvreguleringsinitiativer – i alle fall de som gjelder aktører som henvender seg til forbrukere – er klagenemnder av ulike slag. Vanligvis vil en slik nemnd være opprettet gjennom en avtale mellom en bransjeorganisasjon på den ene siden, og Forbrukerrådet på den annen. Klagenemnder som kun er forankret i et reguleringsinitiativ fra partene, vil vanligvis bare avgi uttalelser. De treffer ikke vedtak som er bindende for partene. Et velkjent eksempel på en slik nemnd er Pressens Faglige Utvalg (PFU), som avgir uttalelser om hvorvidt et presseorgan har opptrådt i strid med «god presseskikk». Nettnemnda er en klagenemnd som skal håndheve *Etiske regler for internett*.[2] Den er opprettet av IKT-Norge og Internettforum. Nettnemnda har mange likhetstrekk med PFU.

Hvorvidt uttalelser fra klagenemnder blir fulgt av aktører som får en avgjørelse mot seg, avhenger av nemndas autoritet og prestisje, og dermed hvor

---

1 Se <http://www.nsafe.no/>.

2 Se <http://www.nettnemnda.no/>.

hardt kritikken faktisk rammer. Men man må kunne gå ut fra at de som har vært med på å etablere eller har sluttet seg til en slik klagenemnd, i alle fall i utgangspunktet har til hensikt å rette seg etter nemnden. Gjør man ikke det, ville det ikke hatt noen mening å ha noen slik nemnd.

Noen nemnder har sanksjoner av ulik styrke som kan iverksettes mot den som ikke retter seg etter nemndens uttalelser. *Nsafe* kan beslutte å frata en aktør retten til å bruke merket. Langt mer brutale sanksjoner møter en ved klager over tildeling av domenenavn. Her vil man kunne overføre et domenenavn til klager. Dette er i praksis en tvangsfullbyrdelse av nemndsvedtak. Når sanksjonene blir så sterke som i disse tilfellene, kan man reise spørsmål om rettssikkerheten for den som et vedtak retter seg mot. Men de spørsmålene lar jeg ligge i denne sammenhengen.

Et problem med selvregulering som man ikke tvinges inn i, eller hvor ulempene med å stå utenfor er så store at de aller fleste velger å være innenfor, er at de «snille» velger å stå innenfor, mens de «slemme» står på utsiden. Når målet med reguleringsinitiativet ofte er å disiplinere de «slemme», så blir en slik regel lite effektiv.

Et utbredt sett av regler som er akseptert av de fleste aktørene i et marked kan imidlertid få virkning også i forhold til de som står utenfor. Hvordan myndighetene kan medvirke, kommer jeg tilbake til nedenfor. Men også uten deres medvirkning kan reglene få betydning. Hvis man har sanksjonerte lovregler med kriterier som «god skikk», «(u)rimelighet» osv, så vil nok etablerte standarder i markedet få betydning, også i forhold til aktører som ikke har sluttet seg til de regler som setter standarden.

Også i forhold til erstatning etter den alminnelige uaktsomhetsstandarden, må man regne med at utbredte regler vil kunne få betydning for den standard som legges til grunn i culpavurderingen. Myndighetene kan på ulike måter medvirke til å gjøre en selvregulering effektiv. Man kan velge å gjøre «klubbens» regelverk bindende for alle, gjennom å ta det inn i lov eller forskrift. Et eksempel på det siste er advokatforskriften.[3] Her har man tatt Den Norske Advokatforenings regler for god advokatskikk inn som forskriften kapittel 12, og dermed gjort dem til en del av forskriften. Men det er nok ikke så vanlig at man velger denne løsningen.

Går vi tilbake til avtaleregulering, er Forbrukerombudets kompetanse til å forhandle om avtaler et eksempel på at myndigheter går inn i en selvreguleringsprosess. Rett til å forhandle er i seg selv ikke så mye. Men Forbrukerombudets maktmiddel er at en sak kan bringes inn for Markedsrådet med krav om at de forbyr bruk av visse avtalevilkår, dersom man ikke kommer til

[3] Forskrift til domstolloven kapittel 11, 1996-12-20, nr 1161.

enighet gjennom forhandlinger. Markedsrådet er uavhengig, og det er ikke alltid Forbrukerombudet får medhold hvis en sak bringes inn for dette organet. Men i de fleste tilfeller vil man være interessert i at en sak ikke bringes inn for rådet, og dermed kan forhandlingsordningen bli effektiv.

Man finner også andre former for inngripen fra myndigheter dersom partene ikke selv komme fram til en akseptabel løsning. Det er ikke lett å finne eksempler i Norge på at myndighetene har gitt partene en frist til å komme fram til en løsning, med en trussel om at man kommer til å gripe inn med lov dersom partene ikke kommer til enighet. Men et eksempel som også har virkning for Norge, er direktivet 97/5/EF om *cross-border credit transfers*. Her hadde EU-kommisjonen tidligere gjennomført en studie av bankpraksis, og de var lite fornøyd med tingenes tilstand. De pekte på flere forhold som det måtte ryddes opp i, f eks krevde man at også bankene skulle være bundet av sine egne avtaler og at man ikke skulle ta betalt to ganger for samme tjeneste. Det ble satt en frist, med beskjed om at man ville gripe inn med et direktiv dersom bankene ikke selv klarte å komme fram til en løsning som EU-kommisjonen ville si seg fornøyd med. Da bankene ikke selv klarte å bedre sin praksis på egenhånd, kom så direktivet. Og når man så hvor håpløst resultatet ble på enkelte punkter, har nok mange banker angret på at de ikke gjorde mer for å løse dette selv.

I realiteten har vi også i Norge en slik trussel om å gripe inn ved ethvert tariffoppgjør. Hvis noen går til streik, så vet alle at staten før eller siden kommer til å gripe inn med tvungen lønnsnemnd, selv om de alltid bedyrer at de ikke har noen planer om å gjøre det. Og det kan heller ikke være tvil om at partene selv spekulerer i og noen ganger prøver å fremprovosere lønnsnemnd og dermed overlate til myndighetene å avslutte en konflikt som de ikke klarer å komme ut av på egen hånd.

En interessesant modell for selvregulering er den nordiske avtalelisensordningen innenfor opphavsretten. Etter åndsverkloven § 36 første ledd og 38a kan en organisasjon som representerer en vesentlig del av norske opphavsmenn på vedkommende område, og som er godkjent av vedkommende departement, inngå visse avtaler som også får virkning for opphavsmenn som *ikke* er medlem i vedkommende organisasjon. Gjennom lovgivning utvides dermed disse avtalene til å omfatte alle opphavsmenn innenfor avtalens saklige virkeområde.

Noen av de klagenemnder som er opprettet har også fått en lovgivningsmessig støtte, som innebærer at nemndsbehandling kan få rettsvirkninger som den ellers ikke kunne ha hatt. Et eksempel på dette finner vi i finansavtaleloven § 4. Hvis en klagenemnds vedtekter er godkjent av Kongen, får kunden en lovbestemt rett til å kreve nemndsbehandling i saker hvor nemnden er kompetent. Det har også visse prosessuelle virkninger i forhold til et eventuelt

etterfølgende søksmål dersom en sak bringes inn for en slik nemnd – i praksis Bankklagenemnda.

Denne korte oversikten løser ikke på noen måte utfordringene med selvregulering i de fremvoksende markeder for elektroniske tjenester mm. Men det bør være tilstrekkelig til å påvise at selvregulering ikke er noe entydig begrep. Hvis selvregulering er et mål uten at det er nærmere presisert, blir det i beste fall et særdeles uklart mål.

DETERMINING APPLICABLE LAW AND JURISDICTION IN CONTRACTUAL DISPUTES REGARDING VIRTUAL ENTERPRISES[1]

EMILY M. WEITZENBÖCK

Abstract

This paper discusses the need for choice of law and jurisdiction clauses in the contract entered into between virtual enterprise members and also in the contracts between the virtual enterprise and external parties such as customers or suppliers. There is first an examination of what happens where there is no express jurisdiction clause, followed by an analysis of the situation where there is no express choice of law clause. It is shown that where there is no such express clauses, it may be very difficult for the parties to have a measure of legal certainty the moment a dispute arises as regards where to sue and which law will apply to resolve their dispute. The discussion focuses on the legal situation in Western Europe – ie, in EU and EFTA countries.

1 Introduction

The use of information and communications technology ("ICT") enables small, specialised firms – regardless of their geographical location – to communicate effectively, pool together their resources and core competencies by

---

[1] This paper was originally prepared for the 8th International Conference on Concurrent Enterprising, Rome, June 2002, and is reproduced in the proceedings of the conference: see KS Pawar, F Weber & K-D Thoben (eds), *Proceedings of the 8th International Conference on Concurrent Enterprising: 'Ubiquitous Engineering in the Collaborative Economy'* (Nottingham: Centre for Concurrent Enterprising, University of Nottingham, 2002; ISBN 0 85358 113 4), pp 27–34. Work on this paper has been partly funded by the European Commission through IST Project *ALIVE (workgroup on Advanced Legal Issues in Virtual Enterprise)* (IST-2000-25459). This paper is the sole responsibility of the author and does not represent the opinion of the European Community. The Community is not responsible for any use that might be made of the content of the paper.

creating a virtual enterprise ("VE") between them, thereby providing one face to the customer, wherever that customer is located. There is, therefore, very often a strong international element present in the operation of a VE, from which a number of private international law issues may arise, particularly where there was no prior agreement on choice of law or jurisdiction in the event of disputes.

When a dispute arises between parties located in different countries, the first question that the party wanting to sue asks is where to sue, that is, which country's court is authorised to hear the case. Once the competent court to hear the dispute has been identified, the next question that arises will be to determine which country's law is applicable to resolve the dispute.

Traditional private international law has looked to geography when determining jurisdiction and selecting the applicable law. One would therefore look at where the defendant is domiciled or where it has its place of establishment. However, on the Internet, "place" matters less and less and it is often difficult, in the absence of an express choice of law by the parties, to determine which is the applicable law to govern a particular contractual relationship.

2 Research Approach and Sources

This paper discusses the need for choice of law and jurisdiction clauses in the contracts between the VE and its customer, as well as in the agreement which is entered into between the members of the VE themselves (hereinafter referred to as the "VE Interchange Agreement"). This analysis is carried out by examining what the position is where there is no express choice of law or jurisdiction by the contractual parties; ie, what happens where the parties have not expressly chosen the law in terms of which the contract is to be construed and interpreted, or the place where disputes are to be lodged. Focus is directed at the current situation in Western Europe.

More specifically, as regards jurisdiction, reference is made to Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (hereinafter referred to as the "Jurisdiction Regulation") which entered into force on 1st March 2002. As a regulation, this legal instrument is binding and directly applicable with respect to all European Union (EU) Member States except Denmark which has chosen not to adopt it. Accordingly, the Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters will continue to be used for jurisdiction rules where a party is domiciled in Denmark. However, Denmark has expressed an interest

in the conclusion of an agreement with the European Commission to allow it to apply the rules laid down in the Jurisdiction Regulation. Another important source is the Lugano Convention which has similar provisions to the Brussels Convention and which applies to Member States of the European Free Trade Association (EFTA), ie, Norway, Iceland, Liechtenstein and Switzerland. Work has been undertaken for the revision of the Lugano Convention on lines similar to the Jurisdiction Regulation. In this paper, reference is made to articles in the Jurisdiction Regulation but, where the provision mentioned varies from the position under the Brussels and Lugano Convention, the difference is pointed out.

As regards the issue of applicable law, reference is made to the 1980 Rome Convention on the law applicable to contractual obligations. This Convention applies to all EU Member States and, as part of the *acquis communautaire* of the Community, should be acceded to by any country which joins the EU in the future. It is not open for signature by non-Members of the EU. Reference is also made to the 1980 United Nations Convention on Contracts for the International Sale of Goods, and to the 1955 Hague Convention on the Law applicable to International Sale of Goods.

3 Importance of Choice of Law and Jurisdiction Clauses

Writers on Internet law believe that the most effective way to resolve Internet private international law problems is to use choice of law and choice of jurisdiction clauses in electronic contracts as a means of agreeing to a common choice of law, rather than leaving it to the uncertainties of geographically-oriented choice of law regimes [Burnstein, 1998]. Free choice of governing law is a basic principle of the 1980 Rome Convention (Article 3). Similarly, free choice of jurisdiction is a basic principle of the Brussels & Lugano Conventions (Article 17) and the new Jurisdiction Regulation (Article 23).

In the context of virtual enterprise networks, it is recommended that both the VE Interchange Agreement between the members of the VE, as well as the contract that the VE enters into with its customers and with external suppliers, should have express choice of law and exclusive jurisdiction clauses. In the absence of such clauses, a court seised of a dispute relating to a VE will have to first determine whether it has jurisdiction to hear the matter before it, and, in the affirmative, what the proper law to resolve the dispute is [Weitzenböck, 2001].

4 Determining Jurisdiction in the Absence of Choice

4.1 Problems with the Application of the Criterion of Domicile to Virtual Enterprises

As mentioned above, the first question that needs to be asked upon deciding to sue is *where* to sue. The general rule in the Jurisdiction Regulation (Article 2) is that a person shall be sued in the courts of the place where such person is domiciled. Article 2 uses the term "person" and the question that therefore arises when the claim is against a VE is how one is to apply this rule to a VE which, very often, does not have a separate legal identity from its members [Van Schoubroeck *et al*, 2001]. The question of *where* to sue becomes linked with that of *whom* to sue. Perhaps the answer lies in Article 60 of the Regulation which clarifies the notion of domicile in respect of a company, other legal person or "association of natural or legal persons", by providing that domicile is the place either where it has (a) its statutory seat or (b) central administration or (c) principal place of business. It is submitted that a VE might be considered to fall within the term "association of natural or legal persons" since its members are either natural persons and/or legal persons. In such a case, its domicile could be either where it has its central administration or its principal place of business. However, it may still be difficult to identify where a VE with members from different countries has its central administration or principal place of business. Should one here focus on the key internal actors of the VE such as the VE broker who is responsible for the marketing of the VE and functions as the contact between the VE and its customer(s), or should one look at where other actors such as project managers, competence managers, etc. are based? What if these actors are based in different jurisdictions?

It should be mentioned at this point that although the Brussels and Lugano Conventions have the same concept of the domicile of a natural person as the Jurisdiction Regulation, the domicile of a company or other legal person or association of natural or legal persons is considered to be its seat. To determine that seat, the court has to apply its rules of private international law (Article 53) with the resultant risk that this concept of seat could vary from one country to another.

The problem of where to sue the VE exists where the plaintiff is one of the members of the VE and is magnified where the plaintiff is a supplier or customer (i.e. not a member) of the VE. The latter, not being privy to the internal set-up and organisation of the VE, is likely to find it harder to identify its central administration or central place of business. Should one therefore sue

some or all of the individual members of the VE? Both the Brussels and Lugano Conventions and the Jurisdiction Regulation (in their respective Article 6) permit a defendant, where such person is one of a number of defendants, to be sued in the courts for the place where any one of such defendants are domiciled, qualified with the proviso in the Jurisdiction Regulation that the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings. One should here remember that, to be able to sue all the partners in contract, the customer or supplier should have entered into a contract either directly with all of them or with their legally authorised representative.

Where the VE has an online presence and conducts business through a website by, eg, selling goods or providing services online, the VE would be considered to be an information society services provider falling within the EC Electronic Commerce Directive [Directive on electronic commerce, 2000]. The VE, as a service provider, is obliged under Article 5(1) of the Directive to provide easy, direct and permanent access to recipients of its services and competent authorities of, *inter alia*, its name and the geographic address at which it is established. Therefore, where the VE is an information society service provider in terms of the Electronic Commerce Directive, the aforementioned information that must be provided to its customers will assist such customers to identify at least one possible place where to sue – ie, the country where it states that it is established.

4.2 Matters Relating to Contract

Another alternative place where a claimant may sue the virtual enterprise in matters relating to contract is in the courts for the place of performance of the obligation in question. This arises from a special rule relating to contracts in both the Brussels and Lugano Conventions (Article 5(1)) and the Jurisdiction Regulation (Article 5(1)(a)).

The first question that arises is what is meant by "matters related to a contract". One could envisage disputes arising either between the VE members in terms of the VE Interchange Agreement, or between the VE and an external party (ie, not a VE member) who had contracted with it (eg, a customer or a supplier). The phrase "matters related to a contract" has been interpreted by the European Court of Justice (ECJ) which declared that the word "contract" here should be given an independent meaning in the sense that it should be interpreted independently of the national law of one state [*SPRL Arcado v SA Haviland*, 1988].

Disputes relating to the existence of the agreement over which the claim is based are considered to fall within Article 5(1) [*Effer v Kantner*, 1982]. Such

would be disputes regarding the existence of the VE Interchange Agreement or the contract with its supplier or customer, and on which the claim is based. As Cheshire and North [1999] observe,

> "[c]ourts would be too easily deprived of jurisdiction if an allegation by the defendant that no contract existed was sufficient to prevent the dispute falling within Article 5(1). The court seised of the matter may end up deciding that no contract exists but this is neither here nor there. All that matters is that this court is satisfied that the requirements of Article 5(1) are satisfied, including that it is a matter relating to a contract."

Another issue that arises is where is "the place of performance of the obligation" in the case of contracts involving VEs. The Jurisdiction Regulation clarifies the meaning of place of performance by distinguishing between contracts for the sale of goods and contracts for the provision of services in subparagraph (b) of Article 5(1). In the case of sale of goods, the place of performance of the obligation is the place where, under the contract, the goods were delivered or should have been delivered. In the case of services, it is the place where, under the contract, the services were provided or should have been provided. Article 5(1)(c) states further that if subparagraph (b) is not applicable, then subparagraph (a) would be.

Though the distinction between goods and services in Article 5(1) is welcome, the Regulation contains no definition of either "goods" or "services" and thus one may question under which category digitised products would fall. One should here examine what rights accompany the transfer of the digital product. Where the user is only given the right to download the work onto a physical medium (eg, a CD or DVD) but has no right to make further copies of the work, this contract has the characteristic of a licence contract and not sale [Østergaard, 2000]. Thus, where the contract is for the provision of a digital product via the Internet, the place of performance is presumably where the product is downloaded ("provided").

It should be noted that the Brussels and Lugano Conventions do not have the above-mentioned clarification of the place of performance as regards the sale of goods or the provision of services. These Conventions merely provide that in matters relating to contract, a person may be sued in the courts for the place of performance of the obligation in question. One would therefore have to determine what "the obligation in question" is. In *De Bloos v Bouyer* [1976], the ECJ held that Article 5(1) refers not to any obligation under the contract but to the contractual obligation forming the basis of the legal proceedings, the one which the contract imposes on the defendant, the non-performance of which is relied upon by the claimant. However, in the case of

a VE Interchange Agreement, it may not always be easy to determine what "the obligation in question is" as there might be a number of different obligations in the contract which may be due to be performed in different states. Thus, eg, a VE may be contacted to design and set up a website and to promote, maintain and upgrade it for a certain period. Each of these services may be performed in a different country. Which is the obligation in question here? The ECJ in *Shenavai v Kreischer* [1987] held that the judge dealing with the case should identify the principal obligation on which the claimant's action is based and jurisdiction is then to be determined in accordance with this. However, a problem may arise when it is not possible to identify the principal obligation, in which case different obligations could end up being subject to the jurisdiction of different Member States.

As mentioned above, the amendments to Article 5(1) of the Regulation have now somewhat clarified the place of performance with regard to sale of goods and the provision of services.

4.3 B2C Contracts

It is presumed that, in practice, most of the customers of a VE will be businesses (B2B contracts). However, one cannot absolutely exclude the possibility of a VE entering also into some business-to-consumer (B2C) contracts, and so the special rules regarding these types of contracts will also be briefly examined in this paper.

Special grounds of jurisdiction apply to B2C contracts under the Brussels and Lugano Conventions, and these rules have been updated in the Jurisdiction Regulation. The main rule in both instruments (Article 16 of the Regulation, Article 14 of the Conventions) is that consumers can only be sued in their own jurisdiction. However, consumers have the option of suing either in their own jurisdiction, in the other party's jurisdiction, or in another jurisdiction by agreement in terms of Article 17 of the Regulation or Article 14 of the Brussels and Lugano Conventions. At the same time, as discussed above, although difficulties related to the question of "domicile" of a VE may be avoided by the fact that the consumer may sue in the state of his or her domicile, problems may still arise for the consumer in trying to identify *whom* to sue.

The new Article 15(1)(c) of the Jurisdiction Regulation makes it clear that the main rule in Article 16 applies to consumer contracts concluded over the Internet. This provides that jurisdiction will be established if "by any means" a business directs its commercial or professional activities to the Member State of the consumer's domicile or to several Member States including that Member State. Though this rule applies to businesses such as VEs which use the Internet to promote and provide their goods and services to consumers in

Europe, it is not unique to virtual enterprises. Suffice it here to say that like other online businesses, VEs should be aware that they are open to being sued by customers in those countries where the VE has actively directed its activities [Lubitz 2001].

5 Determining Applicable Law in the Absence of Choice

Once the competent forum has been determined, if the parties have not selected the law applicable to the contract, then the court seised of the matter must determine the proper law.

Where a dispute is tried in one of the fifteen EU member states, the Rome Convention may be applicable. This Convention applies to all contractual obligations involving a choice between the laws of different countries, except for the matters specified in Article 1 of the Convention such as succession, insurance, matrimonial and family matters. Both B2B and B2C matters may fall within the Convention, as may contracts relating to goods and/or services.

Where the contract is one of sale of goods, the 1980 United Nations Convention on Contracts for the International Sale of Goods (CISG) might have relevance. The CISG, though not a choice of law convention with conflict rules, might be applicable as substantive law to sales contracts between parties with places of business in different contracting states. Where only one of the parties has a place of business in a contracting state, the CISG will still be applicable if the private international law rules lead to the application of the law of a CISG-contracting state [CISG, Article 1]. This Convention applies only to B2B sales contracts and is entered into by most of the EU and EFTA states (except for Great Britain, Ireland, Portugal and Liechtenstein). It has substantive rules such as on the formation of a sales contract, duties and obligations of the seller and buyer, passing of risk and breach of contract.

If the CISG is not applicable and the matter relates to international sales of goods, the 1955 Hague Convention on the Law applicable to International Sale of Goods might be applicable where the parties are from the contracting states of this Convention. Western European contracting states are Belgium, Denmark, Finland, France, Italy, Norway, Spain and Sweden. All the aforementioned states apply the Hague Convention only to B2B sales, except for Norway where it is also applicable to B2C sales.

A court seised of a matter which has an international element would thus have to determine which of the aforementioned international conventions is applicable, depending on the nature of the dispute and the parties involved.

As regards virtual enterprise networks, where the dispute is between the VE members and is based on the VE Interchange Agreement, it is likely that only the Rome Convention would be applicable, where the matter is tried in one of the EU member states. The Interchange Agreement is the backbone agreement underlying the existence, operation and duration of the VE between the members, and it defines their rights and duties. It is rather similar to a joint venture agreement and is therefore not a contract of sale between the VE members.

Where the dispute is between the VE and a party external to the VE, such as a customer or a supplier, the CISG might also be applicable where the contract is B2B and relates to contracts of sale of goods between the parties in a CISG-contracting state as explained above. A contract to deliver goods to be manufactured or produced by one party is considered a sales contract, unless the party who orders the goods undertakes to supply a substantial part of the materials necessary for their manufacture or production. However, the CISG states clearly that where the contract is one in which the preponderant part of the obligation of the party who furnishes the goods consists in the supply of labour or other services, it will not apply.

If the CISG is not applicable but the 1955 Hague Convention is applicable, the main rule is that in default of an express choice of law, a sale is governed by the domestic law of the country where the vendor has his habitual residence at the time when he receives the order.

Because of the limited sphere of application of the CISG and Hague Conventions (to B2B sales contracts in signatory states), and since very often contracts between the VE and its customer are contracts for the provision of some sort of service rather than a sales contract, the applicable law is frequently the Rome Convention when the matter is tried in an EU member state.

5.1 Article 4 of the Rome Convention

Where the parties have not previously agreed on the governing law of the contract, then, according to Article 4(1) of the Rome Convention, the contract is governed by the law of the country with which it is most closely connected. This general rule of "closest connection" echoes the trend prevalent in Europe prior to the ratification of the Rome Convention (eg, in England) and also in some other European countries which are not signatories of the Rome Convention (eg, Norway). As the notion of closest connection might be rather vague, Article 4 contains some presumptions to help give the concept more precision and objectivity (Cordero Moss, 2000; Giuliano and Lagarde, 1980). The most relevant one is set out in Article 4(2), which provides that the contract is most closely connected with the country where the party

who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporate, its central administration. If the contract is entered into in the course of that party's trade or profession, that country shall be the country in which the principal place of business is situated or the place of business specified in the contract.

According to the Giuliano-Lagarde Report [1980], the concept of characteristic performance essentially links the contract to the social and economic environment of which it will form a part. This is usually the performance for which the payment is due, such as, depending on the type of contract, the delivery of goods, the granting of the right to make use of an item of property, the provision of a service. The obligation to pay for such performance, on the other hand, should not be deemed to be the characteristic performance of the contract.

Imagine a virtual enterprise made up a group of talented creative freelancers which was contracted by a French firm to design and produce a promotional brochure. The characteristic performance is the design and production of the brochure by the VE. The proper law, according to Article 4(2), is the principal place of business of the VE. If, as is often the case in practice, the VE has not been set up as a separate legal person, but its members are based in the same country – say, Italy – Italian law would be the applicable law. However, if the VE members are situated in different countries (eg, Italy and Austria) and the different stages of the design and production are being carried out in these countries, then, although the characteristic performance of the contract is identifiable, it points to two different countries. Such a situation makes the application of Article 4(2) difficult, if not impossible. One would here try to see whether the contract is severable and whether part of it has a closer connection with another country (see *infra* regarding Article 4(5)).

Other situations may arise where it is complex and perhaps impossible to determine the characteristic performance. In the example mentioned in section 4.2 *infra*, suppose that a VE is contracted to design and set up a website, and to advertise, promote, maintain and upgrade it for a certain period. The customer is not satisfied with the maintenance and upgrading of the website and wants to sue the VE. Suppose that the VE does not have a distinct legal personality but is made up of members established in different countries. What is the characteristic performance in this case and which is the applicable law? When this cannot be identified, the presumption in Article 4(2) cannot be applied, and one must then try to identify to which country the contract is most closely connected (Article 4(5)). The judge is thus left with a margin of discretion to identify the predominant "pointers" or connecting

factors which show that the contract is closely connected to a specific country. It is submitted that one should look at the particular circumstances of the case, how the VE is set up and where it appears to the customer to be operating from. For example, if the contractual negotiations for the VE were carried out by one particular VE member who also runs and takes care of the operation of that particular VE project (such member is usually referred to as the VE broker), perhaps the contract has the closest connection to the country where the VE broker's business is situated.

In the above example, the judge may also decide to sever the contract and deem the maintenance and upgrading of the website to be an independent and separable part of the whole agreement. Article 4(1) of the Rome Convention provides that "a separable part of the contract which has a closer connection with another country may by way of exception be governed by the law of that other country". The Giuliano-Lagarde Report on the Convention [1980] held that severance should be allowed "by way of exception, for a part of the contract which is independent and separable, in terms of the contract and not of the dispute, where that part has a closer connection with another country". It gives the example of contracts for joint ventures and complex contracts. The above could be said to be such a complex contract.

5.2 Choice of Law, B2C Contracts and Mandatory Rules

Special rules apply to contracts with consumers also as regards the choice of law. A consumer is defined in the Rome Convention (and also in the Brussels & Lugano Conventions and the Jurisdiction Regulation) as a person who enters into a contract outside his trade or profession. Of particular note for VE networks are the first two indents of Article 5(2) which provide that even where an express choice of law was made in the consumer contract, this is not allowed to have the result of depriving the consumer of the protection afforded to him by the mandatory rules of the country in which he has his habitual residence:

- if in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all the steps necessary on his part for the conclusion of the contract, or
- if the other party or his agent received the consumer's order in that country.

Mandatory rules are defined in Article 3(3) as rules "which cannot be derogated from by contract". In order to determine whether rules of a particular country are mandatory, reference must be made to the law of that country

[Cheshire and North, 1999]. Thus, if an English court is concerned to ascertain whether a French domestic rule is mandatory, it has to ask whether under French law that particular rule cannot be derogated from by contract.

If no express choice of law has been made, then, in the above cases, the contract shall be governed by the law of the country in which the consumer has his habitual residence (Article 5(3)).

6 Conclusion

This paper argues that both the VE Interchange Agreement and the contracts which the VE has with its customers should have an express (exclusive) jurisdiction clause and a choice of law clause. Provided the choice is in line with the international legal instruments discussed above, it is most likely to be enforced by a court of law in Western Europe. However, one should bear in mind that the Internet facilitates global and not just regional (ie, European) e-commerce. Thus, other international and national laws should be considered to ensure that the choice would also be recognised in these jurisdictions and not struck down on the basis of, eg, overriding mandatory laws or public policy.

References

Burnstein, M: "A Global Network in a Compartmentalised Legal Environment", in K Boele-Woelki & C Kessedjian (eds), *Internet: Which Court Decides? Which Law Applies? Quel tribunal décide? Quel droit s'applique?* (The Hague: Kluwer Law International, 1998), pp 23–34.

North, P & Fawcett, JJ: *Cheshire and North's Private International Law* (London: Butterworths, 1999, 13th ed).

Cordero Moss, G: "Jurisdiksjon og lovvalg for europeiske kontrakter – Noen spørsmål om Lugano- og Brussel- og Romakonvensjonene" (2000) *Lov og Rett*, pp 131–147.

Giuliano, M & Lagarde, P: "Report on the Convention on the law applicable to contractual obligations" ("Giuliano-Lagarde Report"), OJ C 282, 31.10.1980, pp 1–50.

Lubitz, M: "Jurisdiction and Choice of Law for Electronic Contracts: an English Perspective" (2001) *Computer und Recht International*, Issue 2, pp 39–45.

Van Schoubroeck, C; Cousy, H; Windey, B & Droshout, D: "A Legal Taxonomy on Virtual Enterprises", in Thoben, K-D; Weber, F & Pawar KS (eds), *Proceedings of the 7th International Conference on Concurrent Enterprising* (Nottingham: Centre for Concurrent Enterprising, University of Nottingham, 2001), pp 357–364.

Weitzenböck, E: *Legal Issues of Maritime Virtual Organisations*, CompLex 4/01 (Oslo: Unipub, 2001).

Østergaard, K: "Den virtuelle forhandler – "Nye" internationale privatretlige problemstillinger?", in *Julebog 2000* (Copenhagen: Jurist-og Økonomforbundets Forlag, 2000), pp 123–149.

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 012, 16.01.2001, pp 1–23.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), OJ L 178, 17.2.2000, pp 1–16.

EC Convention on the Law Applicable to Contractual Obligations ("1980 Rome Convention"), OJ C 027, 26.01.1998, pp 34–46.

EC Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, Brussels 1968 ("Brussels Convention"), OJ L 299, 31.12.1972, pp 32–42.

1955 Hague Convention on the Law applicable to International Sale of Goods, available at <http://www.jus.uio.no/lm/hcpil.applicable.law.sog.convention.1955/> (accessed 11.04.2002).

1988 Lugano Convention on Jurisdiction and the Enforcement of judgments in Civil and Commercial Matters ("Lugano Convention"), OJ L 319, 25.11.1988, pp 9–33.

1980 United Nations Convention on Contracts for the International Sale of Goods, available at <http://www.jus.uio.no /lm/un.contracts.international.sale.of.goods.convention.1980/index.html> (accessed 11.04.2002).

De Bloos v Bouyer, Case 14/76 [1976] ECR 1497.

Effer SpA v Kantner, Case 38/81 [1982] ECR 825.

SPRL Arcado v Haviland, Case 9/87 [1988] ECR 1539.

Shenavai v Kreischer, Case 266/85 [1987] ECR 239.

ONLINE DISPUTE RESOLUTION – WHAT IT MEANS FOR CONSUMERS[1]

LEE A. BYGRAVE

1 Introduction

Much enthusiasm exists for the increased use of extra-judicial mechanisms for resolving disputes, particularly with respect to e-commerce.[2] The popularity of such mechanisms (hereinafter termed "alternative dispute resolution" or "ADR") hinges mainly upon their apparent speed, flexibility and affordability relative to traditional litigation in the courts, plus their ability to alleviate pressure on an already overloaded court system.

Some of this quick-fix enthusiasm is bubbling over to embrace the *online* facilitation of ADR (hereinafter termed "online (alternative) dispute resolution" or "ODR"). By "ODR" is meant, broadly speaking, a process whereby disputes are substantially handled (through negotiation, mediation, conciliation, arbitration or a combination of such) via electronic networks such as the Internet.[3] Enthusiasm for ODR rests on the view that it will significantly enhance the advantageous features of ADR relative to court litigation. This view is far from far-fetched. There can be little doubt that ODR is potentially able to provide parties to a dispute the opportunity of having the dispute

---

1 This paper is based on a speech given at a conference entitled "Domain Names and Internet Governance" organised by the Baker & McKenzie Cyberspace Law and Policy Centre in Sydney, 7 May 2002. A slightly different version of the paper has been published in *Internet Law Bulletin*, 2002, vol 4, no 8, pp 81–88.

2 See, eg, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market (hereinafter termed "E-Commerce Directive"), Article 17(1) of which requires that EU Member States not "hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means".

3 Arguably, the term "electronic dispute resolution" or "EDR" would be equally as appropriate a nomenclature for this process. Indeed, "EDR" is perhaps less misleading than "ODR" since the adjective "online" connotes an immediacy with the process which does not necessarily exist. Nevertheless, use of "online" seems to have become ingrained in discourse in the field.

resolved quickly and efficiently without the parties ever needing to physically meet in person or at a particular forum.

While the application of ODR need not be limited to disputes arising out of online transactions, it is often presumed that such disputes are best resolved online.[4] This presumption pertains especially to disputes over transactions that are of the "high-volume, low-cost" type. Indeed, because online transactions between businesses and consumers (hereinafter termed "B2C" transactions) are often of this sort, ODR has been trumpeted as a preferred avenue for consumers who seek redress from businesses with which they have dealt. Recourse to ODR (and other forms of ADR) is also seen as a convenient way of side-stepping the complex jurisdictional issues that can muddy court litigation over e-commerce disputes, particularly those revolving around cross-border B2C transactions.[5]

Nevertheless, it would be foolish to view ODR (or ADR generally) as a panacea for consumer (or business) difficulties. While recourse to such processes will tend to simplify the issue as to which forum should hear a dispute, it will usually not solve of itself the frequently troublesome issue as to which set of laws should be applied to settle the substantive part of the dispute. In theory at least, ODR/ADR schemes could bypass the latter issue by creating their own set of rules for resolving the substantive part of a dispute. In practice, though, it is difficult to escape the issue entirely.

Exemplifying this difficulty is the Uniform Domain-Name Dispute-Resolution Policy (UDRP) developed by the Internet Corporation for Assigned Names and Numbers (ICANN) to resolve disputes over domain names.[6] While the UDRP is aimed at providing a set of rules that can be applied across and relatively independent of national jurisdictions, its application still tends to involve (and arguably necessitate) the arbitrator(s) making a choice as to which national legal standards (usually in the field of trademark protection) shall constitute the primary point of reference for determining, say, whether a domain name has been registered in "bad faith". Especially problematic is that, despite this tendency, the UDRP provides little guidance

---

4 The presumption arguably underlies Article 17 of the E-Commerce Directive, *op cit*. See, eg, the preamble to the Directive, recital 52. Cf the general observations in National Alternative Dispute Resolution Advisory Council (NADRAC), *On-line ADR*, Background paper of January 2001, paragraphs 13 *et seq.*, <http://law.gov.au/aghome/advisory/nadrac/ADR.html> (last accessed 23.11.2002).

5 Further on these jurisdictional difficulties, see, eg, M Foss & LA Bygrave, "International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law" (2000) 8 *International Journal of Law and Information Technology*, pp 99–138.

6 See <http://www.icann.org/udrp/>.

on how such choices should be made. Of course, an ODR/ADR scheme could always bypass the issue of applicable (national) law by preemptively stipulating that the laws of a particular jurisdiction shall apply, but this measure would greatly undercut the flexibility and fairness of the scheme.

Further, the widespread use of ODR in relation to B2C transactions faces major hurdles. Some of these hurdles are primarily legal in nature. For example, many jurisdictions prevent the application of ODR (or ADR generally) if the scheme seeks to cut recourse to the court system by consumers *before* a dispute has arisen.[7] Other hurdles are more a function of psychological, cultural and social factors, such as a lack of "Internet literacy" and/or an abundance of "Internet wariness" on the part of many consumers.[8] The situation is not helped by increasing evidence that many, if not most, ODR schemes currently fall woefully short of meeting consumer needs.[9] While some sets of standards have been drafted in an attempt to remedy this shortfall,[10] they are unlikely to be sufficient without further measures.

The current meaning of ODR for consumers can be teased out in summary fashion by drawing an analogy with much of the "fast food" on offer at roadside kiosks and milkbars: at first glance, ODR looks finger-licking good but its nourishment value needs improving. At the same time, the "fast food" of ODR tends currently to be offered through a new and relatively unknown chain of roadside kiosks; there is, as yet, no ODR McDonalds. Thus, many consumers travelling on the information highway drive past these kiosks without sampling the fare.

2 Consumer concerns and business dilemmas

A reasonably representative list of what consumers desire of ODR can be derived from several sets of recommendations put together by consumer groups.[11] In summary form, the list embraces:

---

7 See further, *inter alia*, the analysis with respect to barriers under European law in C Kuner, "Legal Obstacles to ADR in European Business-to-Consumer Electronic Commerce", available via <http://www.kuner.com/> (last accessed 23.11.2002).

8 See further the analysis in NADRAC, *op cit*, paragraphs 30 *et seq.*

9 See section 3 *infra*.

10 See section 4 *infra*.

11 I refer here especially to the recommendations by Consumers International and the Trans Atlantic Consumer Dialogue: see sections 3 and 4 *infra*.

- **Transparency** – ODR schemes should provide readily accessible information about all aspects of their services;
- **Independence** – ODR schemes should operate independently of vested business interests;
- **Impartiality** – ODR schemes should operate without bias favouring business interests;
- **Effectiveness** – there should be mechanisms to ensure business compliance with ODR outcomes;
- **Fairness/integrity** – ODR schemes should observe due-process standards ensuring, *inter alia*, that each party to a dispute has equal opportunity to express their point of view;
- **Accessibility** – ODR schemes should facilitate their easy use by consumers;
- **Flexibility** – ODR schemes should permit adaptation of their procedures to suit the circumstances of the particular dispute at hand; recourse to courts by consumers should not be precluded unless by prior and equitable agreement;
- **Affordability** – ODR schemes should be affordable for consumers, particularly in light of the amount of compensation being sought.
- **Speed** – ODR schemes should be run quickly and efficiently.

These listed points of concern should not be taken as hard and fast categories. There is considerable overlap between them – eg, the concern for affordability overlaps with the concern for accessibility; the concern for fairness and integrity overlaps with the concern for impartiality. Further, the concerns relate not just to ODR but ADR schemes generally. At the same time, they are also concerns that businesses tend to share.

The most important point to be drawn from a consideration of the concerns is that, to a large extent, consumers (and many businesses) want the benefits of rule-of-law without the costs of rule-of-law. I use the notion "rule-of-law" here not so much to denote the concern that processes be subject to legal regulation but rather the concern for ensuring that decision making complies with principles of due process; ie, that decision making is non-arbitrary, non-capricious, predictable and transparent and, concomitantly, that hearings leading up to decisions are based on principles of natural justice.

In wanting the benefits of rule-of-law without the costs of rule-of-law, might not consumers (and many businesses) be validly charged with wanting to have their cake and eat it too? (Or, in keeping with the "fast food" analogy used earlier, is this not a situation of consumers wanting to have their roadside donut and eat it too?).

Undoubtedly, some of the above-listed concerns are in tension, if not at odds, with each other – at least if one considers the practicalities of running ODR schemes. Take, for instance, the issue of affordability: the consumer wants low-cost schemes but the ODR-provider ordinarily needs to cover its costs and deter the mounting of frivolous complaints. Who will pay arbitrators or mediators in cases involving consumer small claims? Potentially heightening this dilemma is the fact that, generally, the greater the skill and competence of arbitrators or mediators, the greater is the amount they charge for their services. A consumer is unlikely to be able or willing to foot their bill or even a substantial part of it. Thus, resolution of disputes about small claims might well end up being routed around the high-skilled end of the dispute-resolution market which might, in turn, detrimentally affect the fairness/integrity of the procedures.

Of course, there are ways to ameliorate the problem. For example, numerous small claims of the same kind could be merged into one relatively large claim for treatment by the ODR-provider. However, some ameliorative strategies will raise further problems. For instance, were an ODR-provider to meet its costs through substantial sponsorship from business, its ability to act independently and impartially – and/or, just as importantly, its ability to be *seen* as acting independently and impartially – might well be compromised.

Another instance of tension occurs with respect to the concern for transparency. Prospective parties to B2C transactions will tend to want information from ODR-providers on how previous disputes have been handled, including the outcomes and reasoning applied. Transparency at this level will help meet the general need for prescriptive guidance. Yet *actual* parties to disputes will frequently want the nature and outcomes of the dispute resolution proceedings kept confidential – this being usually to encourage transparency between each of the parties and thereby buttress the integrity of the proceedings.

Moreover, certain aspects of ODR raise dilemmas that "offline" ADR either does not raise at all or does not raise as prominently. These dilemmas pertain to the relative difficulty with ODR of ensuring the requisite integrity and security of proceedings. Guaranteeing that electronic communications between the parties are free from unauthorised access and/or alteration is especially difficult when using open networks, such as the Internet. Authentication difficulties also arise when parties are unfamiliar with each other and only deal at a distance. Additionally, the parties – particularly in conciliation and mediation processes – will tend to be robbed of many useful cues that they would otherwise have in face-to-face meetings. While all of these problems can be mitigated significantly through technological measures (eg, use of

encryption mechanisms, video-conferencing facilities, new types of software),[12] it is doubtful that they can be eliminated.

All of the above suggests that ODR is unlikely to produce a "win-win" result for consumers (or, indeed, businesses). Rather, use of ODR will tend to be a case of "win some" (eg, in terms of speed and convenience) and "lose some" (eg, in terms of fairness and integrity).

3 Existing practices and problems

The most up-to-date, comprehensive empirical research on ODR schemes for B2C transactions is (to my knowledge) that carried out by Consumers International, which has conducted two analyses of relevant schemes: the first in August 2000; the second in August 2001.[13] The latter study canvasses just under thirty ODR services which (at least as of 31.8.2001) are potentially available to consumers in cross-jurisdictional disputes with businesses. Most of the services are based in North America.

The study results are troubling from a consumer viewpoint. Overall, the study suggests that the ODR market is largely geared towards catering for business needs, with businesses concomitantly enjoying a greater range of ODR options than consumers enjoy. Indeed, ODR for B2C disputes appear often to be an add-on to services catering primarily for B2B disputes. Hence, the ODR services canvassed in the study tend to be geared towards handling high-value claims – only thirteen of them can cover the typical B2C dispute involving a relatively low-value claim. Further, none of the services meet fully the points of concern listed in the previous section.

More specifically, major problems with the services relate to, *inter alia*,

- their non-transparency – there is often a paucity of detail provided about their governing structures (eg, lines of ownership; officers' credentials), plus a paucity of readily available case-history information (eg, how many cases handled; how resolved; what reasoning applied);

---

[12] See further E Katsh, J Rifkin & A Gaitenby, "E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of 'eBay Law'" (2000) 15 *Ohio State Journal on Dispute Resolution*, pp 705, 718 *et seq*.

[13] The findings of the most recent analysis are set out in Consumers International, *Disputes in Cyberspace 2001* (November 2001), <http://cinternational.eval.poptel.org.uk/document_store/Doc35.pdf> (last accessed 23.11.2002).

- their expensiveness – only twelve are affordable for consumers pursuing low-value claims;
- their limited language options – most allow only for the use of English;
- their limited ability to assist consumers in obtaining redress from recalcitrant businesses – only seven services are able to provide any assistance in this respect (primarily through operation of trustmark schemes);
- their frequent failure to provide adequate assurance of their independence and impartiality *vis-à-vis* businesses – most of the services are private, for-profit enterprises that rely, at least in part, on business sponsorship; at the same time, few services seem to include consumer representatives in their governing bodies.

4 Developing rules

There is, as yet, no legally binding international instrument setting out standards that deal specifically with ODR; neither is there a similar instrument dealing with ADR more generally. However, numerous sets of standards in the form of "soft rules" (guidelines, recommendations and the like) are emerging internationally with relevance for both ODR and ADR schemes. Particularly noteworthy is that all of the various sets of proposed standards are basically in harmony with each other. In other words, there is broad agreement – at least *prima facie* – in terms of ideals.

The set of standards with the hitherto most global reach are contained in the OECD's Guidelines for Consumer Protection in the Context of Electronic Commerce, adopted in December 1999.[14] Within the European Union, several instruments have emerged which attempt to elaborate basic principles for the operation of ADR and ODR schemes in the context of B2C transactions. The first and perhaps most important is the *Commission Recommendation 98/257/EC of 30.3.1998 on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes*. This recommendation contains principles for ADR schemes that engage in arbitration (as opposed to mere mediation, conciliation, etc). The principles are in terms of independence, transparency, adversary procedure, effectiveness, legality, liberty and representation. A more recent Commission Rec-

[14] The relevant standards are reproduced further below.

ommendation lays down broadly similar principles for mediation and other ADR processes offered by third parties.[15]

Both Recommendations are underpinned by Article 17 of the E-Commerce Directive which, *inter alia*, directs EU Member States to "encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned". Member States are further directed (in Article 17(3)) to "encourage bodies responsible for out-of-court settlement to inform the Commission [of the European Communities] of the significant decisions they take regarding Information Society services and to transmit any other information on the practices, usages or customs relating to electronic commerce". Indeed, at the international level, this is probably the closest one gets to *legally mandated* standards for ADR/ODR. At the same time, it is perhaps arguable that state-sponsored ODR/ADR schemes are legally bound to comply with standards enunciated pursuant to "fair trial" provisions in human rights treaties,[16] at least when the schemes are used to determine civil rights and obligations.

Apart from the OECD and EU instruments described above, there exist quite a number of relevant policy instruments issued by international consumer groups and international business groups. The most significant of these are:

- Trans Atlantic Consumer Dialogue (TACD), "ADR in Context of E-Commerce" (February 2000);[17]
- Global Business Dialogue on Electronic Commerce (GBDe), "Consumer Confidence: Alternative Dispute Resolution" (September 2001).[18]

Broadly similar standards to those expressed at the international level are to be found in the national instruments of some countries. In Australia, for example, relevant standards are set out in the Federal Government's *Benchmarks for*

---

15 See Commission Recommendation 2001/310/EC of 4.4.2001 on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes.

16 An example of such a clause is Article 6(1) of the 1950 *European Convention on Human Rights and Fundamental Freedoms* which states, "in the determination of his civil rights and obligations … everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law".

17 Available at <http://www.tacd.org/db_files/files/files-82-filetag.pdf> (last accessed 24.11.2002).

18 Also known as the "Tokyo recommendations on ADR": see <http://consumerconfidence.gbde.org/adrtokyo2001.pdf> (last accessed 23.11.2002).

Industry-Based Customer Dispute Resolution Schemes (1997),[19] along with its "Best Practice Model for Business" (2000).[20] More recently, the National Alternative Dispute Resolution Advisory Council (NADRAC) has elaborated a framework for developing more detailed standards for ADR generally,[21] and is in the process of working out principles for ODR specifically.[22]

5 Some outstanding issues

In the following, I attempt to give a brief rundown on some of the major outstanding issues. The first issue pertains to the standards and principles described in section 4 above. As already noted, there appears to be broad consensus about the core ideals which ODR/ADR schemes should strive to meet. Does this mean, then, that the principles are sufficient?

In my view, while the basic thrust of the principles is fine, they suffer from several weaknesses. One weakness is their frequently high level of generality. At the same time, this characteristic probably goes a long way to explaining the apparent consensus about them. Amongst the most diffuse sets of principles are those contained in the OECD Guidelines. The provisions directly concerning ADR/ODR are contained in Part IV(B), which recommends:

> "Consumers should be provided meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden.
>
> Businesses, consumer representatives and governments should work together to continue to use and develop fair, effective and transparent self-regulatory and other policies and procedures, including alternative dispute resolution mechanisms, to address consumer complaints and to resolve

---

19 Available at <http://www.selfregulation.gov.au/publications/BenchmarksForIndustry-BasedCustomerDisputeResolutionSchemes/BMARK1.pdf> (last accessed 23.11.2002).

20 See Federal Minister for Financial Services and Regulation, *Building Consumer Sovereignty in Electronic Commerce* (May 2000), available at <http://www.ecommerce.treasury.gov.au/publications/BuildingConsumerSovereigntyInElectronicCommerce-ABestPracticeModelForBusiness/context.htm> (last accessed 23.11.2002).

21 See NADRAC, *A Framework for ADR Standards* (April 2001), <http://www.law.gov.au/aghome/advisory/nadrac/frameworkreport/html/introducing.htm> (last accessed 23.11.2002).

22 See NADRAC, *Dispute Resolution and Information Technology: Principles for Good Practice*, draft of March 2002, <http://www.law.gov.au/aghome/advisory/nadrac/Technology_ADR2.htm> (last accessed 23.11.2002).

consumer disputes arising from business-to-consumer electronic commerce, with special attention to cross-border transactions.

Businesses and consumer representatives should continue to establish fair, effective and transparent internal mechanisms to address and respond to consumer complaints and difficulties in a fair and timely manner and without undue cost or burden to the consumer. Consumers should be encouraged to take advantage of such mechanisms.

Businesses and consumer representatives should continue to establish co-operative self-regulatory programs to address consumer complaints and to assist consumers in resolving disputes arising from business-to-consumer electronic commerce.

Businesses, consumer representatives and governments should work together to continue to provide consumers with the option of alternative dispute resolution mechanisms that provide effective resolution of the dispute in a fair and timely manner and without undue cost or burden to the consumer.

In implementing the above, businesses, consumer representatives and governments should employ information technologies innovatively and use them to enhance consumer awareness and freedom of choice.

In addition, further study is required to meet the objectives of Section VI at an international level."

With respect, the above recommendations are little more than "feel-good" formulations which most people find difficult to reject but which fail to provide sufficient prescriptive guidance.

At the same time, those instruments that provide a greater degree of prescriptive guidance – such as the EC Commission Recommendation of 1998 – sometimes fall short in terms of their practicability. For example, the independence principle (Principle I) set down by that Commission Recommendation states that if an arbitrator "is appointed or remunerated by a professional association or an enterprise, he must not, during the three years prior to assuming his present function, have worked for this professional association or for one of its members or for the enterprise concerned." The three-year exclusion period is arguably too long relative to the goal being sought, particularly in a time when there would seem to be a shortage of arbitrators who are specialists in B2C transaction disputes.[23] Another pertinent example is the legality principle (Principle V), which reads:

[23] See also Kuner, *op cit.*

> "The decision taken by the body [arbitrator] may not result in the consumer being deprived of the protection afforded by the mandatory provisions of the law of the State in whose territory the body is established. In the case of cross-border disputes, the decision taken by the body may not result in the consumer being deprived of the protection afforded by the mandatory provisions applying under the law of the Member State in which he is normally resident in the instances provided for under Article 5 of the Rome Convention of 19 June 1980 on the law applicable to contractual obligations."

This seems effectively to require the application of mandatory rules of law of both the place where the arbitrator is established and of the country where the consumer resides – a requirement that is rightly criticised for being "both overly complicated and unnecessary".[24]

Also problematic is that none of the existing sets of standards specifically address the unique characteristics of ODR (as opposed to "offline" ADR). Concomitantly, they fail to take express account of the problems (mentioned in section 2 *supra*) that these characteristics can entail. Given their newness and the vulnerability of their media, ODR schemes will only work if underpinned by technological-organisational mechanisms promoting certainty and trust. Thus, it is vital that existing sets of ADR standards be supplemented by principles specifically providing for the use of such mechanisms and elaborating on ways in which they can be implemented.

Last but certainly not least, I incline to the view that the existing sets of standards fail to take sufficient account of marketplace pressures facing ODR schemes. There is considerable potential for businesses to put pressure on ODR-providers to arrive at business-friendly outcomes. The pressure could result from a threat by a business to withdraw from a particular ODR-scheme. Obviously, this threat will have more bite the greater the ODR-provider is economically dependant on the business concerned.

We gain some idea of the potential for such pressure from an incident relating to the handling by two competing ODR-providers, TrustE and BBBOnline, of a privacy-related complaint about eBay in 2000.[25] The complaint in question was filed by a customer of eBay with TrustE and BBBOnline (eBay being a member of both the TrustE and BBBOnline privacy seal programs, each of which offer dispute resolution for privacy-related complaints by online consumers). BBBOnline and TrustE initially decided the

---

[24] *Id.*

[25] The incident is described in R Gellman, "Online privacy dispute resolution: BBBOnline" (2000) 7 *Privacy Law & Policy Reporter*, p 145.

complaint differently from each other, with the decision by TrustE being more favourable to eBay. The latter then allegedly threatened to withdraw from the BBBOnline program if BBBOnline did not change its initial decision. BBBOnline apparently succumbed to the threat and substituted a new decision for its first decision (using the same docket number as the initial decision: 2000-03). The new decision evidently reads that the complaint has been resolved but provides no further details.[26] And the first decision has evidently been withdrawn from public view on the Internet.

The eBay case indicates that business membership of two (or more) competing seal programs with separate dispute resolution schemes may be inappropriate, though (as Gellman points out) we cannot judge whether the result of the eBay case was fair as we do not know the exact nature of the decision reached by TrustE in that case. It could be that, objectively, the TrustE decision was the better one, such that BBBOnline's vacation of its original decision was proper. Yet the case illustrates the potential for businesses with considerable commercial clout to encourage what are for them sympathetic arbitration outcomes by threatening withdrawal from an arbitration scheme.

How, then, could we go about countering the potential for businesses to pressure ODR-providers into facilitating business-friendly outcomes? The existing sets of standards provide little guidance apart from the obvious "feel-good" admonitions that ADR schemes operate independently, impartially etc. The most direct solution is to cut back the operation of marketplace dynamics in the provision of B2C ODR. That means minimising the extent to which B2C ODR schemes are set up and run essentially as business ventures with a profit-taking concern. Concomitantly, it means minimising the financial dependency of B2C ODR-providers on funding from a small number of businesses that have large economic clout. It might also mean providing more public/government sponsorship of dispute resolution schemes. Alternatively, it could mean providing greater business sponsorship but on an industry-wide basis, wherein members of an industry association establish and fund one dispute resolution scheme for the industry concerned. The latter option remains vulnerable to the potential for business bias, yet arguably the experience with some industry-sponsored ombudsman schemes (eg, for the banking or telecommunications sectors within a particular country) shows that broad-based business funding does not necessarily compromise the impartiality of complaints resolution.

---

[26] I have been unable to find the decision on the BBBOnline website and am relying on Gellman's report (*op cit*) of the facts.

More generally, we need to encourage the establishment of national and international "Clearing Houses" that can assist consumers in assessing and accessing ODR schemes. Some such initiatives are already underway, particularly in Europe.[27] Such initiatives need to involve or be supplemented by systems for assessing the extent to which ODR-providers comply with "best-practice" principles as laid down in, eg, the EC Commission Recommendations or the Australian Benchmarks for Industry-Based Customer Dispute Resolution Schemes. The systems must also facilitate public disclosure of these compliance checks. To a large extent, Consumers International is carrying out this sort of function already – which is most welcome from a consumer perspective. Yet there is probably a need for the participation of another body that is not aimed at one-sidedly promoting the consumer (or business) agenda.

More ambitiously, we ought to consider the desirability of a system of public accreditation of ODR-providers somewhat similar to the Gatekeeper scheme operating in Australia with respect to Public Key Infrastructure. An accreditation system could manifest itself in a seal/trustmark program whereby accredited ODR-providers would be entitled to bear a stamp or seal of approval.

So far, few accreditation schemes seem to exist for ODR-providers.[28] Indeed, establishment of *mandatory* accreditation schemes in this context will probably fly in the face of the self-regulatory principles for e-commerce which major international business groups propound.[29] Another potential problem with accreditation systems – mandatory or not – will be finding

---

[27] See especially Council Resolution of 25.5.2000 on a Community-wide network of national bodies for the extra-judicial settlement of consumer disputes, encouraging the creation of the "European Extra-Judicial Network" ("EEJ-Net"). The latter is intended to provide a network of national contact points ("Clearing Houses") in EU Member States which can assist consumers wishing to file a complaint with an ADR scheme. Supplementing the EEJ-Net is a similar scheme recently launched for complaints in relation to financial services – the "Financial Services Complaints Network" ("FIN-NET"): see <http://europa.eu.int/comm/internal_market/en/finances/consumer/adr.htm> (last accessed 23.11.2002).

[28] In the UK, a national accreditation scheme is run by TrustUK (a government-endorsed, non-profit body) for ODR-providers that operate within the framework of a trustmark program: see further <http://www.trustuk.org.uk> (last accessed 24.11.2002). Otherwise, there seems to be a paucity of formalised oversight schemes. See further Consumers International, *op cit*, 13.

[29] See, eg, International Chamber of Commerce *et al*, "A Global Action Plan for Electronic Commerce" (October 1999, 2nd ed), <http://www.iccwbo.org/home/electronic_commerce/word_documents/SJAPFIN.doc> (last accessed 24.11.2002).

appropriate bodies to implement them. These problems notwithstanding, accreditation is likely to go a considerable way towards engendering consumer trust in ODR.

THE WORLD TRADE ORGANISATION AND LEGAL REGULATION OF E-COMMERCE

SUSAN SCHIAVETTA

1 Introduction

The development of information and communications technology (ICT) has produced an abundance of ways for the world to communicate. One of the most important outcomes of this development is the Internet, which has provided the platform for a new arena for trade and commerce. While the emergence of this new trading arena is advantageous in respect of economic growth, it has also created various challenges for governments. One challenge of particular importance concerns how best to co-ordinate the various regulatory responses of national governments to e-commerce. International organisations have the potential to play a significant role in co-ordinating national responses but the efficacy of some of them, such as the Organisation for Economic Co-operation and Development (OECD), is hampered by the fact that they are to a large extent merely support mechanisms lacking authority to issue legally binding decisions. The World Trade Organisation (WTO), on the other hand, is not hampered in this way. It thus stands forth as the one international organisation that can play a decisive role in shaping the legal regulation of e-commerce. In particular, the WTO is arguably the only international organisation with requisite knowledge and authority to resolve the major trading issue as to how e-products should be classified for the purpose of collecting customs duties.

2 GATT

Trading internationally is a particularly profitable way of doing business, but originally many believed that it had an adverse affect on national economies. As a result, restrictions were employed to prevent, or at the very least control, exports. Such restrictions can transpire through various obstacles; eg, enforcing quantitative restrictions which limit the amount of goods that can be

imported into a country, or by imposing excessive tariff duties on goods when they enter a country. Both examples indirectly curb market penetration, and ultimately result in discrimination between domestic and foreign products. The General Agreement on Tariffs and Trade (GATT) came into being in 1947, and outlined rules governing international trade. By regulating tariff and non-tariff barriers placed on goods traded on an international scale, it sought to produce a level playing field between its signatory states, thereby stimulating free trade.

In due course, GATT formed a *de facto* organisation that was also, albeit unofficially, branded as "GATT".[1] This organisation administered GATT, and contributed immensely to its growth. In response to economic and political demands, several rounds of negotiations have taken place over the years which have amended and extended the original international trading rules. In particular, the Uruguay Round (Geneva 1986–1994) broadened the regime to cover services and intellectual property, via the adoption of the General Agreement for Trade in Services (GATS) and the Agreement on Trade Related Aspects of Intellectual Property (TRIPS).[2] On the whole, these documents provide the legal ground rules for international commerce which work on a contractual basis. The governments of the countries involved are bound by these rules and must therefore shape their trade policies within the boundaries of these "contracts".[3] One of the most important adjustments to this trading system was the crystallisation of the *de facto* administrative body into a distinct international organisation, the WTO.

2.1 The WTO

The WTO came into being in 1995 via the framework of GATT, and thereby "[placed] the international trading system on a firm constitutional footing".[4] The salient duty of the WTO is to act as a medium for trade negotiations.[5] Taking up this role, it acts in the same way as a lawyer advising clients as to their contractual rights and obligations, adding further support when the

---

1 See further WTO, *Trading into the future* (Geneva: WTO, 2001, 2nd ed), p 4, available at <http://www.wto.org/english/res_e/doload_e/tif.pdf> (accessed 08.10.2002).

2 Final Act Embodying the Results of the Uruguay Round (Geneva: GATT, 1993) [KZ5185 1987 A3 1993]. The Final Act is like a covering note; all the other agreements are attached to this. Principally, the Agreement establishing the WTO acts as an umbrella agreement to GATT, GATS and TRIPS.

3 *Supra* n 1.

4 AH Qureshi, *The World Trade Organisation: Implementing International Trade Norms* (Manchester: Manchester University Press, 1996), p 3.

5 *Supra* n 1.

contract needs revision. In a nutshell, the main role of the WTO is to guarantee that trade runs as smoothly, predictably and freely as possible. The WTO must realise its duties while respecting the environment, optimising the world's resources and contributing to the enhancement of underdeveloped countries.[6] Providing the institutional framework for development and administration of its substantive laws, the WTO is made up of a range of bodies so as to ensure accurate representation and efficient management. At the top of the organisational structure is the Ministerial Conference, which assembles every two years to report on the WTO's progress. Meeting on a more regular basis is the General Council, which is subordinated by three auxiliary councils: the Council for Trade in Goods, the Council for Trade in Services and the Council for Trade-Related Aspects of Intellectual Property Rights.

2.2 The Agreements

Each of the Agreements include a Most Favoured Nation (MFN) provision and a National Treatment (NT) provision. The MFN provision states that each Member State must treat every other Member State as their "most favoured" trading partner. Any benefits given to one Member State must thus be given to the others. Running along similar lines, the NT condition stipulates that all products should be treated equally, regardless of whether they have a local or imported origin.[7] Over and above these fundamental clauses, the Agreements address issues that are specific to their own area, although GATT and GATS have more or less the same format. The main difference between these two Agreements is their profundity and stability. In respect of services, while the basic framework is in place with GATS, this system is still in its infancy stages, and so remains incomplete. As for TRIPS, although it endorses the basic concepts of MFN and NT, it takes quite a different approach to that of GATT and GATS. Reflecting that ideas and knowledge are increasingly the focus of trade, TRIPS seeks to ensure that intellectual property rights are not abused during the trading process. As a result, it looks specifically at the different forms of intellectual property rights and the standards with which they interact.

2.3 Prominent Powers

Generally, any regulation that comes from international organisations is of a non-binding nature, and thus signatories agree voluntarily to abide by its

---

6 Qureshi, *supra* n 4.

7 At this stage, the NT clause only extends to the services covered in the annexes to GATS.

content. In respect of the accompanying enforcement measures, these tend to be weak, and consequently international organisations habitually fail to bring dissenting Member States back into line. In contrast, the WTO is an organisation with teeth; the process of juridification of trade makes the WTO particularly powerful. Hence, the WTO is arguably in the best position to influence national governments, especially regarding legal regulation of e-commerce. The contractual characteristic of the WTO Agreements means that their provisions can be enforced against Member States. In the event that a Member State fails to abide by the WTO "code", two methods of redress may come into play: the Dispute Settlement Mechanism (DSM) and the Trade Policy Review Mechanism (TPRM).

Similar to the measures in Article 226 of the Treaty establishing the European Communities (EC Treaty), the DSM allows a Member State to complain if it feels that another has violated any of the WTO rules. When this procedure is activated, the parties must agree to adhere to the judgments of the arbitrating panel. After a decision has been made, the "disobedient" Member State must move quickly to rectify its position, otherwise it can be subject to compensatory measures, sizeable penalties and destructive trade sanctions.[8] While the DSM is a conflict resolution procedure, the TRPM is more of a surveillance system, which involves examining the individual trade policies of the Member States.[9] Again, this system can be compared to the review processes of the European Commission, which analyses the implementation of legislation by Member States with a view to eliminating non-compliance.

2.4 The Legal Regulation of E-commerce

E-commerce is basically an activity covering all forms of the purchase and sale of goods and services using electronic means, such as the Internet. Within this lie two main forms of e-commerce: business to business and business to consumer. Undoubtedly, this electronic method of trading has added a new dimension to the trading arena, stimulating opportunities as well as challenges. Regarding the latter, tools such as the Internet produce new ways for old crimes to be committed, and so legal regulation must ensure that issues like fraud are also covered in cyberspace. Further, since the Internet has no regard for national boundaries and facilitates extensive cross-border transacting, conflicts of law are bound to arise under domestic legislation. Hence, international co-ordination of regulatory policy is necessary. While rules

---

8 See further Qureshi, *supra* n 4, chapt 5.

9 *Ibid*, chapt 6.

produced at this level tend to take a very generalised stance, they can go a long way towards resolving possible conflicts.

Various international organisations have already prepared such global guidelines. For example, the OECD has issued guidelines on the acceptance of digital signatures and the taxation of e-commerce. Yet while such initiatives are beneficial, they only demand voluntary compliance. By contrast, the WTO administers a regime requiring much more from its Member States. The WTO is more like the institutions of the European Community (EC) than the other international organisations since it drafts and manages legally binding instruments which are somewhat reminiscent of the EC Treaty. Moreover, WTO rules are supported by an efficient and effective compliance system. As the notorious "banana case" demonstrates, the WTO can be particularly influential.[10] Accordingly, the WTO is the international organisation best equipped to realise a stable, coherent and predictable legislative framework for e-commerce to thrive.

3 The WTO's role with respect to e-commerce

Since the Uruguay Round, e-commerce has emerged as the most promising international business development and stands to deliver many benefits if it remains barrier free. Consequently, the WTO Ministerial Conference urged the General Council to investigate all trade-related aspects of e-commerce, taking into account the economic, financial and development needs of developing countries.[11] During the resulting "Work Programme",[12] the subsidiary Councils and the Member States have been actively involved, making many recommendations. Moreover, Member States have agreed to activate a "standstill" process whereby they refrain from introducing custom duties on electronic transmissions until the WTO's position has been clarified.

---

10 Case WT/DS31, reported in J Mander & D Barker, "The World Trade Organisation: Process and Rulings", available via <http://www.ifg.org/aboutwto.html> (accessed 10.10.2002). In this case, after being subjected to the threat of trade sanctions and hefty fines, the EU had to readjust its trading regime to ensure that it did not conflict with rules laid down in GATT.

11 See further the WTO's *Declaration on Global Electronic Comm*erce, available via <http://www.corpwatch.org/trac/corner/worldnews/other/other164.html> (accessed 08.10.2002).

12 Work Programme on Electronic Commerce, WT/GC/16, 12 February 1999.

3.1 Main Quandary

One of the focal parts of the WTO work concerns the classification of e-products. Examples of e-products are the electronic delivery of books and the ability to download computer software straight on to a computer's hard drive. Member States have identified three possible transactions that involve the Internet: transactions which are completed entirely on the Internet, right from selection to delivery; transactions involving "distribution services" in which a product, whether good or service, is selected and purchased online but delivered by conventional means; and transactions involving the telecommunication transport function, including the provision of Internet services.[13]

Obviously, goods that are purchased over the Internet but delivered via traditional methods, fall within the GATT rules, as they can cross a physical border. However, when products are delivered in a digitised form, determining which regime they come under becomes more complicated. Whilst the vast majority of these products are undoubtedly services and thus subject to the rules set down in GATS, there exist a number of e-products that are difficult to categorise. This causes confusion for Member States and their economic operators.

As many e-products have a "goods" alternative, it has been suggested that they should be classed according to their physical equivalent; thus, a book downloaded in digital format should be classified as a good, notwithstanding that it is of the virtual variety. The argument here is that the Internet has merely produced new means to deliver the product, it has not changed the underlying concept of the product and so it should continue to come within the scope of GATT. Conversely, it has been suggested that while this is logical it is not very accurate, as the carrier medium for the product is the dutiable merchandise, not the information contained within it. For example, the delivery of software has always been subject to the GATT rules, but only because of its carrier medium – ie, the floppy disc. Now that the information is delivered via electronic means, the carrier medium is no longer required. Therefore, it is argued, the software product delivered using digital means should really fall under the rules contained in GATS.[14]

---

[13] See further Microsoft White Paper, *WTO and Electronic Commerce: Issues for World Trade*, 8.9.1999, at <http://www.microsoft.com/issues/essays/11-15wto-b.asp> (accessed 9.10.2002).

[14] See further, eg, *Questions and Answers Regarding Ambassadors Hayes' Statement on Duty Free Treatment for Electronic Transmissions*, United States, 19th February 1998, <http://www.ecommerce.gov/question.htm> (accessed 3.12.2001). Cf M Foss & LA Bygrave, "International Consumer Purchases through the Internet: Jurisdictional Issues Pur-

3.2 Consequences of classification

A decision as to whether cross-sectoral e-products are considered to be a good or a service can have far reaching consequences in respect of the treatment that such products get. For instance, if the WTO decides to classify e-products as goods, they can be subject to custom duties. In such a situation, a country would be free to place customs duties on e-products if they believed that they originated from another country. The problem with taxing such imports is that it can be very difficult to track an electronic transaction and rule unequivocally that it has "crossed a border". Getting an administration system set up would be very complicated and costly, and may result in conflicts in respect of jurisdiction. Yet, the consequential revenue can help underdeveloped Member States build up their electronic infrastructure. At the same time, though, account should be taken of the fact that the start-up costs might be too burdensome at the outset, and that such a right to tax is likely to be extremely hard to implement.

Undoubtedly, questions will arise as to who should collect the revenue and why they have jurisdiction. Whilst these are valid concerns, it would appear that the real question is whether or not collecting customs duties is really worthwhile. A study undertaken by the WTO's Economic Research and Analysis Division in 1999 found that, on average, if countries placed tariffs on e-products, the revenue collected would account for less than 1 per cent of their total tariff revenue and 0.03 per cent of their total fiscal revenue.[15] The report also suggests that even if all forms of digitised products were treated as goods and thus subject to custom duties, "[t]he revenue loss would be minimal except for China and Hungary".[16] As a counter-argument, it has been claimed that even as little as this revenue may be, it is badly needed nonetheless.[17]

If e-products are classed as services then they will not fall subject to custom duties, and thus such problems are overridden entirely. However, this is

---

suant to European Law" (2000) 8 *International Journal of Law and Information Technology*, No 2, pp 99, 109ff.

15 See further L Schnuknecht & R Péraz-Esteve, *A Qualitative Assessment of Electronic Commerce*, WTO's Economic Research and Analysis Division, Staff Working Paper ERAD-99-01.

16 *Ibid*, p 7.

17 CE McClure Jr, "Achieving Neutrality between Electronic and Non-Electronic Commerce", Presentation to the Advisory Commission on electronic Commerce, Williamsburg, Virginia, 22.6.1999, <http://www.ecommercecommission.org/williams/presenta/1mclure.doc> (accessed 9.10.2002).

not to say that upon classifying them as services, other issues will not transpire. For instance, classifying "like" products as different things when supplied via different means leads to a discriminatory system, as those buying products on-line could be subject to cheaper prices. Similarly, applying different regimes to products that are essentially the same also overturns the idea of technological neutrality. Additionally, since the GATS agreement is still incomplete – issues like safeguards, subsidies and government procurement of services have yet to be settled – it is questionable whether GATS can securely accommodate e-products at present. Indeed, if GATS were to be applied then this could lead to a destabilisation of applicable trade disciplines since, eg, the NA principle only applies to the scheduled services. As a result, Member States will be able to revive barriers eliminated under GATT and the Information Technology Agreement in certain areas.[18] However this particular issue is only an interim problem, as coming WTO Rounds will serve to strengthen the GATS regime.

Taken as a whole, because insignificant benefits arise for the majority when e-products are treated as goods, and that considerable controversy surfaces as a consequence, such a decision seems unjustified. Moreover, most WTO Member States appear to recognise that a duty-free cyberspace in respect of customs duties "[e]ncourages vigorous competition, innovation, and entrepreneurship on the Internet and avoids the trade distorting effects of customs duties".[19] The fact that the EC Value Added Tax (VAT) regime[20] already classifies all e-products as services further supports this argument, on the basis that classifying the same product in two ways to accommodate different systems, and possibly during the same transaction, stimulates unnecessary divergence. By and large, it would appear that classifying e-products as services as opposed to goods would be more advantageous.

3.2.1 The TRIPS Technique

In a white paper by Microsoft, it is proposed that classifying e-products as goods or services is not the answer at all; rather, the TRIPS regime should probably be applied as all e-products involve intellectual property rights in

---

[18] In particular, due to the fact that software has traditionally been classed as a "good", GATS does not deal with it in its schedules. As for the Information Technology Agreement, this prevents its signatory states from placing customs duties on IT products. See further Microsoft White Paper, *supra* n 13.

[19] D Marantis, "The Internet and Customs Duties", <http://usinfo.state.gov/journals/ites/0500/ijee/factsheet2.htm> (accessed 8.10.2002).

[20] See further 6th VAT Council Directive 77/388/EC; Council Directive 2002/38/EC; and Council Regulation (EC) No 792/2002.

some form.[21] Here Microsoft recognises that the information is the most important part of the contract, mainly because the carrier medium is no longer an integral part. Such a system has the advantage of countermanding the problems associated with custom duties. However, using TRIPS as the governing agreement would appear to suggest that property rights lie in information. Such a stance does not sit well with legal doctrine in some jurisdictions which hold that information itself is not property.[22] Consequently, while uniformity may be achieved in respect of classifying e-products, it threatens deep-rooted principles in other areas of law.

3.2.2 General Agreement on Trade in E-commerce

Taking the TRIPS idea on board, the real question is: should more confusion be engendered? If neither GATT, GATS or TRIPS is the appropriate regime, it may be more plausible to establish a whole new system that would deal specifically with e-commerce, rather than try to fit it in to yet another pre-established regime. Microsoft's white paper also covers this theme, advocating that it might be wise to establish a completely new agreement. In this way, the classification of e-products would not be considered as a stand-alone issue but rather in light of other e-commerce topics. If such an idea were to be endorsed then a General Agreement on Trade in E-commerce (GATE) would be the likely result.

GATE would not only include the MFN clause and the NT article but also outline minimum standards in respect of e-commerce, in particular the conclusion of contracts online. Thus, it may include articles on digital signatures, data protection and computer-related fraud. Such a system would not prevent the WTO from classifying e-products as either goods or services, which would allow them to identify certain e-products as falling subject to either GATT or GATs where appropriate, thereby achieving consistency between the offline and online world. In truth, this might be a good thing, as some products do not fit neatly into one category. However, problems associated with collecting customs duties would re-emerge. Moreover, the EC institutions may have to reorganise their system of classifying all e-products as services for VAT purposes, so as to eradicate any divergence and possible confusion.

---

21 Microsoft White Paper, *supra* n 13.

22 For England, see *Oxford v Moss* [1979] Crim LR 11. For Scotland, see *Grant v Allan* [1988] SLT 11. See also the UK Theft Act of 1968.

3.3 The Doha Round

The Declaration of the WTO's Fourth Ministerial Conference held in November 2001 approved the launch of a new round of negotiations, the Doha Round. A range of topics are to be discussed, but most importantly the observations hitherto on e-commerce will be analysed with a view to establishing the WTO's position.[23] The work done by the WTO to date has laid sound foundations which will serve the negotiators well. Unfortunately, the length of time that the negotiations normally take will slow down the process of regulation considerably. The standstill position of Member States regarding imposition of customs duties on e-products is due to remain in place until the Fifth Ministerial Conference in Mexico in 2003, and it is expected that this arrangement will merely be extended. In reality, since the Doha Round is not due to be completed until January 2005, and it is unlikely that the WTO's e-commerce position will be fully elucidated by then, no major changes are likely to take place in the short term.

3.4 Knock-on effects of WTO action

In addition to the WTO producing legal certainty for the trading arena, this clarity will also affect other areas indirectly, such as liability matters. Specifically, the rights and obligations of both the vendor and the buyer vary according to whether the product involved is a good or a service. For instance, default rules in statutory laws provide for implied terms and warranties as to the quality of goods. In respect of services, the vendor has a duty to carry out services with reasonable skill and care, but there are no implied terms or warranties as to the result of the subject matter supplied.[24] Classification will not matter if it is the express duties that are breached, and in some cases the judge may decide that even in the absence of express terms, implied duties will be applicable in contracts for supply of services.[25] However, this will vary from country to country, and on a case-by-case basis. As a result, it will be a lot clearer if the classification issue is settled, as this will allow judges to concentrate on settling the case rather than having to first decide what the case involves.

---

[23] See further <http://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_e.htm> (accessed 8.10.2002).

[24] See further N Kawawa, "Contract Law relating to Liability for Injury Caused by Information in Electronic Form: Classification of Contracts – A comparative Study, England and the US" (2000) *Journal of Information, Law and Technology*, <http://elj.warwick.ac.uk/jilt/00-1/kawawa.html> (accessed 9.10.2002).

[25] See further *St Albans City and District Council v International Computers Ltd* [1996] 4 All ER 481.

3.5 Cultural Aspects

While recognising that the main issues here pertain to commercial matters, there is also a cultural aspect to the discussion. Trade in cultural products has grown immensely in recent years, the US, Japan, China, Germany and the UK being the biggest exporters.[26] Unfortunately, at the same time as this boom, globalisation also threatens the survival of culture. Consequently, Member States have previously been particularly vociferous on this subject. During the Uruguay Round, for example, France advocated it would not sign up to GATS if the audiovisual sector was an integral part of the Agreement. France believed that if it had to offer market access and apply the NT clause to foreign audiovisual products then this would threaten its market.[27] Other countries have made similar attempts to protect their cultural assets in other sectors.[28] Thus, cultural issues will also have to be considered during the negotiation process, as many e-products have cultural elements and therefore may require different treatment.

4 Conclusion

It appears that the WTO is particularly well-suited to shape the evolution of the legal regulation of e-commerce. It is a very influential international organisation as far as producing and supervising regulation goes, and, of course, it is in a good position to comment on trade-related aspects of e-commerce. Not only will it go on to clarify many of the issues that other international organisations are not equipped to deal with, but its actions will also affect the way in which governments deal with other important issues. In respect of the classification issue, the GATE system is a good idea for the sake of offline and online consistency; however, implementing the system would be a bold move. Member States are unlikely to feel comfortable with signing a new contract that brings with it more legally binding obligations, and hence such a system is not likely to develop in the foreseeable future.

---

[26] See further United Nations Educational, Scientific and Cultural Organization, "Culture, Trade and Globalisation", <http://www.unesco.org/culture/industries/trade/html_eng/question3.shtml> (accessed 11.10.2002).

[27] A similar argument was advanced in case 60-61/84, *Cinetheque v. FNCF* [1985] ECR 2605.

[28] For instance, Canada gave favourable postage rates to Canadian periodicals and introduced a tax which led to Canadian advertisers placing advertisements with domestic, instead of foreign, magazines: see further Mander & Barker, *supra* n 10.

Moreover, the GATE approach does not really solve the underlying problems associated with classification and may only serve to disrupt other pre-established regimes. In a similar vein, both GATT and TRIPS also generate a number of dilemmas. Consequently, for the sake of uniformity, simplicity and e-commerce developmental purposes, it is recommended that e-products be classified as services.

WHAT SHOULD ACCESS LEGISLATION BE LIKE IN THE FUTURE? – POSSIBLE STRUCTURES FOR ACCESS LEGISLATION

DAG WIESE SCHARTUM

1 Introduction and approach

The Internet is creating new possibilities and capabilities to introduce "open government" and improved access to government-held information. In this article, I discuss the information held by government – ie, information either produced or received by a public organ.[1] In particular, I discuss the development of national legislation in connection with such information. First, I comment on the considerations which could be viewed as the very backbone of legislation that gives access to government-held information (section 2). I then explain some of the basic structures and properties of contemporary Norwegian access legislation, assuming that most of these characteristics are relevant in the majority of European jurisdictions (section 3). Thereafter, in section 4, I draw attention to what I believe represents a clear shift in factual information access policy which is the result of creative use of Internet technology. In section 5, I combine elements from the previous sections in an attempt to propose possible structures and elements for a future, amended, access legislation. By so doing, I question the fruitfulness of pursuing the traditional approach.

This article mainly contains a legal-political approach to the discussion of "open government". It is both "legal" and "political" in the sense that the discussions relating to preferred political solutions are founded on basic legal arguments, supporting open government and access rights. Further, it is partly based on a categorisation and discussion of existing legislation within the field. The article is not political in a general sense, since non-legal arguments in favour of a certain understanding or solution are not part of my arguments. In my view, lawyers are needed in order to develop new concepts

[1] This could be seen as different to "public sector information", which can be used to designate (the narrower) information concerning the public (government) sector.

of openness, creating "handles" and room for manoeuvre for politicians. This is a first and fumbling attempt to make such a contribution.

2 Why access to government-held information, and at what level?

Before I discuss access rights in more detail, it is necessary to remind the reader of the main reasons for government being open with information. In this context, I present the ideals of democracy and rule of law as two main components. The democracy perspective contains the main collective arguments in favour of access to government-held information. In this perspective, access to such information is, first and foremost, a prerequisite for democracy because it gives individuals and collective entities (companies, associations, etc) the ability to control the exercise of political power. Through this, and articulated by a free press, government may be made politically accountable for its malfunctions. Irrespective of this control function, however, access to government-held information can be seen as having an educational function, and may therefore be seen as a possible method for enlightening the population, thus making citizens more capable of participating in democratic decision-making processes and discussion.

While I choose to view democracy as primarily an expression of collective interests, I choose to regard the rule of law ("Rechtsicherkeit" / "rettsikkerhet") as primarily representing individual interests in obtaining legally correct results in individual cases (cases before courts, or administrative cases). Here, access rights have significance because they constitute a basis for citizens' control (with or without assistance) over the authority exercised in individual cases. Moreover, they imply a possibility for individuals to plan their lives and actions in accordance with the best opportunities embedded in the legal or political regime.

Access to government-held information can be regarded, in other words, as a necessity for controlling the exercise of public authority (political, judicial) at collective and individual levels. Furthermore, it may be seen as an important contribution to the education of individuals, and, thus, a prerequisite for an active population that may advocate the interests of social communities as well as purely private interests.

On the basis of these simple observations, we may ask if every increase in people's access to government-held information should be viewed as improving democracy and legal protection. Does the sheer fact that, for instance, the

Internet exists and new government information services are thereby introduced imply that people's ability to control and learn about government business improves? In one sense, obviously, the more files governments open and make accessible on the Internet (or in other ways), the more "open government" we will get. As a basis for the discussions in this article, I argue, however, that "open government" in this simple sense should not be regarded as the objective of government information policy and information access legislation. Rather, I will argue that the aim should be an openness which could represent a *relatively* unchanged or (preferably) improved "informational proportionality" between individuals and governments.

When we regard access rights to government-held information in the above-mentioned control perspective, it becomes apparent that such access rights may be seen to be related to power and the disparity between (typically) powerful government organisations and (typically) less powerful individuals and private organisations. Thus, citizens' ability to control power should – as a starting point – always be evaluated in the light of government agencies' ability to exercise power. The more efficient the exercise of government power, the more citizens' access rights are needed to retain the proportionality between the two positions. If government's ability to process information increases, citizens' rights to access and ability to process information should be equally improved, in order to avoid changes in the power relationship.

Viewed in this way, amending statutory access rights can be seen partly as an "information race", where significant ICT gains on the governmental side should be balanced by similar gains on the other side. Technology which allows governments to access new types of information, to search for information in more effective ways, to analyse and manipulate information etc, may thus be seen as problematic in a control and power-relationship perspective, unless citizens' information processing abilities are increased in similar ways. Therefore, even dramatically increased access for citizens to files consisting of traditional documents may not offset the fact that government is developing huge, but publicly inaccessible, databases. Even if government databases are generally open to everybody, this may not necessarily generate sufficient progress in the "information race" if, at the same time, for example, government alone possesses powerful analytical tools. The measure is not change in access to government-held information alone, but changes in the proportionality between the government's and citizens' respective abilities to access and process information.

3 The statutory puzzle of access rights to government-held information

Norwegian legislation regulating access to information has developed into a rather complex body of rules. Here, I do not intend to encumber the reader with details but instead select structural questions concerning access to government-held information.[2] Within the field of information access, there are three main sets of rules covering public administration in general. In addition, there are several pieces of special legislation giving access rights in specific fields – eg, rights in relation to information in the Population Register and the Central Co-ordinating Register for Legal Entities. Here, I limit the discussion to the pieces of general legislation.

The table below shows three groups of people entitled to gain access to government-held information. The most important group from a democratic perspective is universal access, ie (in principal) without regard to age, nationality or other personal characteristics. The Freedom of Information Act of 1970 (FOIA) constitutes the most important body of regulation in this field. The Act gives everybody the right of access to government case documents in specific cases. Certain categories may be exempted, such as "internal documents". Access to other pieces of information is prohibited due to professional secrecy. In addition, the Personal Data Act of 2000 (PDA) gives universal access rights (with some exceptions) to certain information describing data processing, where data concerning individuals are included. The Administrative Procedure Act of 1967 (APA) establishes access rights for the parties to individual cases handled by government bodies, ie, for persons who may be directly affected by the decision in question. Professional secrecy only partly limits the rights of such parties. Thirdly, the PDA gives access rights to persons about whom government bodies process information. These persons have the right both to access information about themselves, and detailed general information within areas where everybody has access rights according to the PDA – cf, above.

---

[2] Among the most important examples of legislation enabling access to *privately*-held information is the Personal Data Act of 2000, which applies to both private and public sectors (see further below in this section). Additionally, access rights exist with regard to, eg, shareholder registers, certain account statements in limited companies etc.

Legislation	Entitled persons	Accessible material
FOIA PDA	Everybody	Meta-information and case-relevant info.
APA	Parties to cases	Case relevant info.
PDA	Registered persons	Meta-information and personal data

The FOIA and PDA explicitly give access to two types of material, which may be classified as 1) meta-information and 2) target information, while the APA only regulates access to documents and pieces of information ("target information"). It is hard to make strict distinctions between the two categories of information. By "meta-information", I mean information people often access to approach "target information". Meta-information will typically have functions such as navigation and identification, and will, for example, allow the individual to decide what specific in-depth ("target") information to access. Central meta-information is found in different kinds of registers/journals/logs, and contains information about types of cases, document titles in the case files, officers in charge, dates, names of sender and receiver etc. The definition of meta-information in the FOIA (journals and other registers) means that the Government Archives Act (GAA) regulates a large proportion of such information. According to the FOIA, everybody may have access to such registers.[3] The GAA imposes a duty on government agencies to establish such registers, with certain types of information and in specific ways. The PDA, on the other hand, explicitly states the types of meta-information that everybody may access, but does not explicitly require that such information be established in advance.

According to the FOIA and APA, the object of information access is a "case", while the object according to the PDA, is "processing" (of personal data). Both objects may be hard to define: that which has been defined as a "case" in records is not necessarily that which should be regarded as a case when somebody makes an access request. Moreover, that which should be viewed as "processing" may be difficult to determine in cases where several information systems co-function in an intimate collaboration between several data controllers.

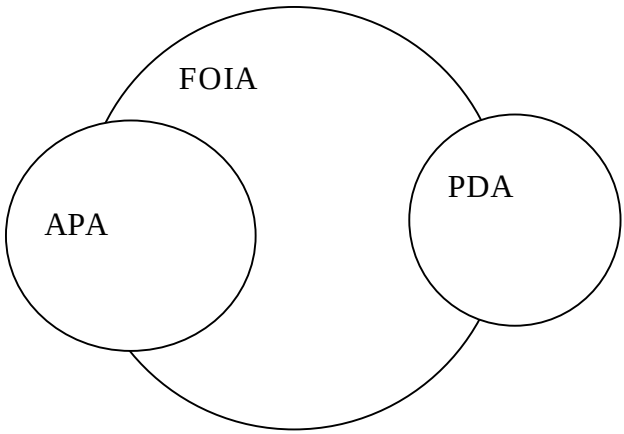
[3] Generally, though, internet logs and the like are regarded as falling outside this statutory right of access.

Knowledge about the objects (cases, processing) is obtained through access to certain "documents" and/or "pieces of information" (target information). Documents are bearers of information, typically containing modestly structured and formalised information, for example, a paragraph of text, video or audio recording etc. The concept of "document" is defined independently of the type of medium used; thus, it also covers "electronic documents". In common with the concept of "case", delimiting what should be regarded as a "document" can be problematic, particularly when the document is "electronic". Pieces of information are typically structured and formalised, linked to specific definitions, restrictions, selections etc. Access rights are thus described as linked to documents and/or widely defined pieces of information, except certain (more narrowly defined) pieces of information.

What I try to account for above are three different sets of general legislation which establish access rights for people in different:

- positions (everybody, party, registered), which are related to different
- objects (case, processing), giving access to different
- information levels (meta-information, target information), realised by means of different
- units of information (document, piece of information).

Often, two or three sets of legislation will be of equal interest to persons wishing to access information. The category "everybody" is all-embracing; many people will additionally be "registered" (ie, data subjects), and sometimes even "party" to a case. Moreover, people being party to a case will (almost) always be "registered". Each body of statutory regulation gives access to information that only partially overlaps.



Viewed from the citizen's perspective, this is not a satisfactory situation. Each of the Acts is complicated enough in itself to dispirit most people. The three Acts have not been drafted in context, and when combined, they represent a body of text which (at best) can be described as rather impervious.

When the PDA was prepared, the Ministry of Justice realised that the total picture of access legislation was complex, something that would involve a great need for assistance and guidance. Thus, every controller of personal data has an obligation, according to section 6(2) of the PDA, to give guidance to data subjects with regard to alternative statutory access rights. Such advice shall be given by the controller, unprompted, and should clarify whether other statutory rights of access to information than those in the PDA, would give access to more information. This obligation applies to all controllers, both in the public and private sectors. With regard to situations where people seek information from a government agency, it implies that the agency (being the "controller"), is required to have knowledge about access rights according to the three major pieces of legislation, and, in addition, any other relevant pieces of access legislation. The obligation to give advice may, to a certain degree, ease the problems created by statutory complexity. On the other hand, expectations should not be too high with respect to government agencies' ability to guide people in such matters. Sometimes, the questions to be answered are far from trivial, and general access legislation is outside the specialised field of government agencies. In section 5 of this article, I return to the question of amending general access legislation as an alternative solution. However, before entering into discussions regarding amendment, other developments linked to governmental information services should be brought to the readers' attention, and considered as arguments in favour of a renewed approach.

4 Government-held information: From access request to publication

In Norway, rights to access information have traditionally been based first and foremost on statutes giving citizens the right to *claim* access to documents in specific cases. The process of gaining access to information is in other words, initiated by the individual citizen. Government agencies have not themselves been expected to take the first step, although they may know that certain groups of citizens or the media would show great interest in a case/document. Obviously, this division of initiative has been based on a number of well-founded practical reasons. More importantly, however, is the

fact that citizen-initiated access to information implies that the "agenda" is defined by the citizen and not by government. This is quite a reasonable arrangement because, in order to exercise effective control, the citizen must be able to choose what cases to control, select relevant documents in each case etc. In order to enable individuals, and in particular the media, to exercise an independent role as controllers, our legislation has not only established access rights to government documents, but, in addition, access rights to meta-information, ie "information about the information".

The traditional approach outlined is, in many ways, sympathetic, since it is the citizen as controller who takes action and decides the issues at stake. Nevertheless, the approach is rather time-consuming for the individual, and thus creates thresholds which may be hard to cross. By and large, only the very well informed and very angry citizen is likely to use their legal right of access to relevant information. In this way, access rights may primarily have value in cases of significant political or private interest, where the media or influential people take action on behalf of the public. On the other hand, such practical barriers may be viewed as sufficient, as lower thresholds would only annoy government agencies with citizens' many "nitty-gritty" problems, and prevent government from doing its "real job". Clear legal rights to access information, in combination with appropriate practical thresholds, may thus be viewed as representing an appropriate balance. However, judged from the perspective that access to information is intended to have a popular-educational effect, every threshold will be regarded as undesirable.

Presumptions of conflict are embedded in the FOIA. The Act is intended to define clear boundaries between information to which citizens have a clear-cut right, cases where government may give discretionary access to information, and cases where access to information is prohibited. Long-winded definitions of "internal documents" for instance, seem to anticipate discussions between insistent citizens and reluctant government officials. The legislation may, in other words, be regarded as a compromise between conflicting interests.

An antagonistic relationship between government and citizens fits well with the mood of the 1950s and 1960s, when this legislation was prepared, and when legislation, to a large extent, came into existence to protect individuals from an ever stronger government. Forty years on, other aspects of government receive much more attention. Today, government is regarded more as being at the service of its citizens. Citizens are not merely the subjects of power but increasingly playing the role of customers and users of government services. Where such service-orientation has met the Internet, new advantageous information services directed at the general public have

popped up in more than 90 percent of Norwegian central government agencies and more than 70 percent of local government agencies.

The web-based information services offered by Norwegian government agencies range from average to excellent in quality. In my view, what is particularly interesting in this context is that the best services are provided by local governments. The reason for this is partly that local government is responsible for a wide spectrum of services for its citizens. Thus, local government web-based information services cover a broad field, meaning that these services take a much more holistic approach than that of most specialised central government agencies. Moreover, the best local government services supply citizens with everything from general information about budgets, plans, services for citizens etc, to detailed information regarding which political representatives were present at which meetings, and scanned text of every document in every case not subject to professional secrecy.

There are many aspects to these web-based information services that deserve a closer presentation and discussion. Nevertheless, I limit myself here to a discussion regarding the publishing of case documents which constitutes an important element in most such information services. The essential point is that all those case documents, which anybody may access through their local government web-service, were previously (ie, a couple of years ago) only accessible on request pursuant to the FOIA or APA. Certainly, chances are that selected, embarrassing documents are withheld and not displayed on the Internet. Thus, the point is not that no document is left at the back of desk drawers, so that citizens need to formally request access. Rather, compared to the traditional situation of most documents being locked in the offices of secretive bureaucrats, today's user-oriented "publish-as-much-as-you-can" services seem to make the traditional rights to access on request an issue of reduced importance.

Access to government-held information at this stage of internet development and in these times of service-orientation by governments, is not really about the kind of techniques that our traditional legislation is built upon; ie, it is not about access on request. It is rather about supplying citizens with information on the bases of their measured or assumed interests, and on the basis that maximum openness is a democratic ideal. In other words, the main recent development in openness of government has occurred in the field of access by publication rather than access on request. Compared to the latter, the publication of government case documents etc is much less regulated by law. Apart from the general framework of rules concerning protection of personal data and professional secrecy, no rules explicitly concern such publication. On the other hand, however, rather complicated statutes regulate

information access on request. Thus, the creative constructions of local governments' web-based information services have largely been possible without the constraints of legislation.

One might ask whether we should have statutory regulations regarding how government publishes case documents etc. In my view, such a need clearly exists, and the reason is twofold. There are good reasons to ask whether or not the factual publication practices of local and central government agencies are an argument in favour of establishing new minimum standards in the field of making case documents publicly available. The issue is not whether to establish a common standard that reflects the most excellent information services, but whether or not a minimum standard should be defined and established by law. One sub-question is, for instance, whether or not statutes should mandate every local government at municipality and county level to have web-services directed towards their own populations.[4] With regard to the various branches of central government administration, similar decisions may be made in statute law, regulations or instructions. A year ago, when the number of government web-sites was considerably lower than at present, such measures would have been rather dramatic and may not necessarily have been feasible. However, with the high and still rising number of web-sites during 2001–2002, a duty to establish certain government information services for citizens will, first of all, function as a corrective for latecomers among government agencies. Furthermore, it will signal the transition from the experimental stage of the previous century, to a phase where such services are institutionalised as part of government's basic communication repertoire vis-à-vis citizens.

A possible legal regulation of web-based government information services should obviously go beyond merely mandating the existence of such services. It should additionally define some of the types of material that should always be available. Here, I refrain from going into detail with regard to the various materials that should be considered, but only mention some examples. For instance, it should be considered whether all meeting agendas of elected bodies and the decisions in each case should be published, provided this does not conflict with statutory duties of confidentiality. In Norway, quite a few cases at local and central government level, including draft legislation, are distributed to a list of parties, which are expected to have an interest in the issue at stake. A possible requirement would be that all such written hearings in government cases be published on the government's web-pages. Another field to

[4] That is, separate to services directed towards tourism, industrial and commercial development etc.

consider is documents about financial aspects of government activities, and to what extent accounts, budgets and related activity plans should be published and thereby made universally accessible.

I end my example-dropping here and at the same time emphasise that these are examples of the necessity for a political and administrative debate before such proposed decisions may become of actual interest. Moreover, it should be remembered that mandatory publication of several of the document types mentioned would not necessarily imply a revolution, since several government bodies already have such publication practices. Thus, my examples would partly open up closed windows, partly keep open windows open, and partly create new windows where the need for insight is recognised but insufficiently realised. The objective should thus be to reaffirm, consolidate and change.

Legal regulation should not only comprise the question of what to publish, but even (on a general and technology-neutral level) include answers to questions regarding how such information services should be organised and run. Here, I point to some of the relevant organisational/operational issues that should be addressed. When a government agency selects case documents for publication, the choice of documents is taken at the agency's own discretion. This may result in an incomplete and sometimes biased selection. A lack of fixed criteria for defining the content of an information service, can allow a political determination regarding which case documents should be released to the public. For example, the selection of internal reports from a ministry may be controlled by political choices. It may be a problem if the administration has unfettered discretion to withhold certain reports and documents, particularly if these files contradict the selected and accessible material.

The risk that the machinery of government will be able to use the Internet in a manner that gives government a dominate position in the public debate concerning its own role and actions, can be minimised through "declarations of content". I mention above the possibility of establishing a publishing duty, linked to certain types or series of documents. As an adjunct to such duties, the formulation and publication of pre-decided criteria for the selection of documents should be considered. This implies that "rules" describing the contents of government information service should always be formulated and published. In addition, a deadline for the publication of documents should be established, and, in a similar way, possible "out-dating routines" – ie, routines for removal or deletion of documents. In this way, it would be difficult to control publication practice through subjective, political and tactical deliberations.

Looking back on development within the field of government web-based information services during the last five years, it is rather astonishing to see how positive and innovative many actors within the machinery of govern-

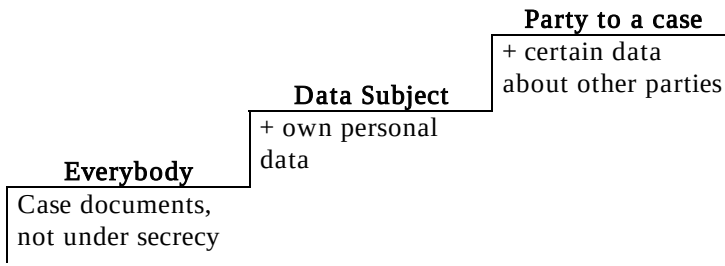
ment have been, and what great results many agencies have achieved – particularly if we compare this to the rather reluctant (or at least prudent) attitudes demonstrated by important parts of bureaucracy in relation to the traditional right to make requests for information access. However, the two approaches to openness obviously produce different effects for civil servants. Here, I mention just one aspect of these effects.

One plausible effect is the result that web-services produce joint benefits, not least for officials. A service to citizens is obviously also a service to members of government agencies. Considerable proportions of the information that has been made accessible on the Internet has not been generally, or easily, accessible to the officers in the relevant government agencies, and (even more so) hardly available to officers in co-operating government agencies. Thus, government internet-based information services have not only eased an information deficit among the general population, but also an internal government problem of access to information.

5 Amending information access legislation: approaching a new conceptual view?

So far, I have explained and discussed a statutory information access regime which suffers from a lack of coherence and holistic view of open government. Furthermore, I have pointed to a factual development of advanced government information services employing Internet technology which have developed alongside the existing access legislation, inspired by user-orientation. In this section, I try to bring together and shape these points into proposals for basic elements in a renewal of access legislation for the government sector. My aim is to illustrate how current legislation may be co-ordinated and restructured into one body of access rights.

Entitled groups: Entitlement to access information is linked to certain roles – eg, as citizen ("everybody"), data subject ("registered") or a party to a case. Often, the same persons may choose several roles, and thus several legal bases for information access. If we consider all general access rights within the government sector as a whole, we find a picture of a cumulative approach relating to each of the three roles. On this "access ladder", certain rights to access a wide range of general information are given to everybody, while data subjects may access information about themselves. In addition, as a party to a case, you have the right to access case-relevant information about other parties. The higher up on the access ladder, the more sensitive the information may be.



The access ladder

My simple point is that analysis of existing access legislation seems to show that it contains a certain coherent logic. This coherence is only partly a result of direct, overall analysis. I am thus not claiming that inconsistencies do not occur if existing access rights, linked to the various roles, are analysed as a whole. However, regardless of the system dynamics of various pieces of access legislation, an "internal logic" between them must exist if the possibility of applying all rights at the same time is to be more than a supposition. Whether we retain the current access legislation divided into three laws, or we establish an overall access law for government sector, a comprehensive analysis will be necessary. However, the results of a holistic analysis will be easiest for people to comprehend if it results in one body of general legislation.

Initiative: Traditional access legislation places the right to take initiative at the level of the individual. Nevertheless, innovative development and use of government web-sites have created a situation where it is the government rather than individuals taking this initiative. Even if this new situation may seem contradictory with regard to some of the considerations underlying access legislation, and which emphasise the public's ability to decide what to investigate and control, it has created a positive change with a marked increase in openness concerning government affairs. Thus, revised access legislation should acknowledge access to published documents and access on request as complementary statutory elements.

To a large extent, however, the publication of case documents by the government should be controlled by citizens and/or made part of a systematic and declared practise. Firstly, every grant to access information on request should lead to automatic publication of the document in question on the web-pages of the government agency in question. In this way, individuals will partly decide which documents are to be published by government. Secondly,

every government web-page should publish case documents etc according to certain fixed criteria, which they establish and announce. Apart from possible demands for minimum information services (cf, section 3), the agencies themselves should decide the concrete content of their information services. Such selection criteria should state the types of information they will publish, when they will publish, and when they will delete or archive the various types of information. An approach where access on request and by publication is combined with a user and systematic approach would give, in my view, the general public acceptable control over government publication practises.

Objects of access: As previously explained, current access rights are linked either to a specific "case" or a specific "processing" of personal data; ie, it is documents or pieces of information connected to such cases or processings that may be accessed. A "case" may easily be associated with an object or objects and occurrences as a whole. "Processing" has a more dynamic content, with an emphasis on events and performed operations. Both concepts have their strengths and describe somewhat different aspects of the same phenomenon of "processing cases". Moreover, both concepts may be used in both a general and an individual sense. "Processing" may designate the procedures etc that are followed in a certain type of process (decision making, information access etc) or the process followed in an individual case. In the same way, "case" may refer to a type of decision/action or to a specific incident.

If we see the possible connections between the approaches of "case" and "processing", it might be fruitful to make a joint model where both concepts are specified as a combination of certain "objects" and "aspects":

Processing of cases

Aspect / Object	**Processing of data** (factual basis of decisions)	**Processing of operations** (logic of decisions)
Type of case (general)	Meta-information Target info.	Meta-information Target info.
Individual cases	Target info. (documents, single info.)	Target info. (documents, single info.)

The figure above illustrates a possible coherence between "objects" (type of case and individual cases) and certain "aspects" of these objects (processing of data and operations). It contains four possible "addresses" to which meta- and target information may belong, eg, documents concerning processing of operations in a specific case, and documents concerning the processing of data in a specific type of case. In many cases, though, it will not be possible or fruitful to ask for specific objects or aspects, and the person who claims access will instead request information on a general basis.

Levels of information: Current access rights are linked to 1) meta-information, 2) documents, and 3) pieces of information, the last two categories being "target information". Meta-information is selected information, defined and selected with the aim to decide which target information to access. As explained in section 3, the Norwegian APA contains no explicit right to access meta-information about relevant case documents.[5] Such meta-information should, however, always be defined in relation to each statutory access right. Moreover, the current fragmented approach to meta-information – ie, where such information is described separately, without any reference to other similar rights – is an obstacle to realising the full potential of access rights. When someone contacts a government agency, they should always have the right to access all meta-information linked to processing of cases. For instance, a party to a case should have an automatic right to access meta-information, regardless of status as an entitled person, ie, also have the right to access meta-information about the processing of personal data and sets of public case documents. Obviously, a government agency will have its own specific view regarding what should be considered part of a specific case to which a person is a party. Quite another matter is what a person, being party, views to be relevant and useful in future situations. The likelihood is high that meta-materials that may be accessed independently of status as party, may be regarded as interesting even in the context of a specific case.

If access legislation is amended in line with these arguments – ie, if accessible meta-information is defined as one entity – another task would be to control and consider to what extent the meta-information, currently produced in accordance with archiving legislation etc, is sufficient and adequate. For instance, it may be feasible to have access rights to files of precedent cases of relevant government bodies in situations where parties wish to question the decision in a specific case.

---

[5] However, this does not mean that, in practice, parties to cases are denied access to correspondence logs etc if they ask.

Documents and pieces of information are typically the bearers of target information, ie, the information that is of primary interest to the person claiming access.[6] A problem may be what to regard as a document or piece of information, separate to other documents and pieces of information. In my view, however, this is a limited problem. One argument is that, no matter how we divide data into documents or other units, they will in many cases be closely related to other documents. This is, to an extreme degree, the case with email. Each message may be viewed as a document, but each such document may have little information value until a series of messages has been completed. Similarly (but less extreme), connections exist between a report, its background material, relevant attachments, decisions based on the report etc. Irrespective of what we regarded as a "document", the main thing is that every part of the information content has an "address", and that all such addresses (names and reference numbers of documents etc) are linked to other addresses (of documents) that are part of the same decision-making or information exchange process. The division of units that are bearers of information is, in other words, not decisive. More important is that all individual information units and the relationship between such units are unambiguously defined. Hence, whether or not each email in a series of messages is defined as one document, or one chooses to define the entire series as one document, is not the main issue as long as each message and its relationships to other messages is defined.

Particular pieces of information constitute the lowest level of target information. As opposed to information in documents, this is (typically) highly structured and formalised information, ie, linked to meta-information and specific definitions and constraints. Pieces of information are traditionally linked to documents as exceptions; for example, access is given to a document, except for information about "health" (according to a definition of this concept). With contemporary database technology, it is hard to maintain "document" as the main concept, if even information entered in databases is to be covered by access legislation. More and more of the information about our society exists as compilations of pieces of information in databases. Thus, future access legislation must contain rights that specifically include databases, implying that not only single pieces of information, but even *patterns* of such information be available. Persons should have, in other words, the right to determine which relationship between pieces of information they

[6] This is not to say that meta-information could not be regarded as target information in specific cases – eg, if one wishes to examine the contact pattern between various parties to a case, and records are used to map this information.

wish to examine. A person who wants to find out how many people under the age of 18 in a certain district are receiving child support, should be able to do so, provided that such data is available in a searchable government database.[7]

Documents and pieces of information may be seen as constituting a representation and description of certain actions/functions that must be executed in order to reach a specific result. This is particularly true with regard to rules (legal and others). From this perspective, it may be appropriate to ask whether or not access rights should also comprise the execution of *functions*, ie, access to computer systems that execute the functions described in a certain text. Such rights are probably not realistic, unless such routines already exist and are available from the relevant government agency. Joint needs for access to such computerised routines for both government and the general public may, however, increase the likelihood that such services will come to exist in the future.

6 Conclusion and a further question

In this article, I present some perspectives and proposals concerning both current and possible future access legislation. Most of the discussions above have been of a rather tentative and preliminary nature. My general point, of which I am quite certain, is that future discussions about access legislation should not be rooted in the single access traditions, but, as much as possible, integrate various ways to achieve a more open government administration. In one sense, this view is inspired by advanced government web-pages where access to information may be obtained by publication, on request in single cases, on request in series of cases (cf, subscription), as access to automatic functions for simulating operations on data sets etc. Such web-services are so complex with regard to the achievement of open government, that they seem to challenge traditional legislation.

There are certainly many questions relating to the issues discussed in this article upon which I have not touched. The most obvious (and difficult) question is the link between access rights in the private and those in the public sector. The EU Data Protection Directive (95/46/EC) establishes a joint data protection regime for the two sectors, meaning that even access rights are similar for each – at least within the data protection context. One obvious

[7] For practical purposes, however, such rights should probably only be established if they may be linked to a published database and made generally available on the Internet.

idea is to investigate whether or not it is possible, and desirable, to make joint access legislation that applies without regard to the question of access to "processing of personal data" or a "case". My view is that this is both possible and desirable. At the same time, putting forward such thoughts may be said to demonstrate my lack of realism with regard to political and legislative processes. Indeed, the entire set of arguments in favour of amending access legislation which I formulate in this article, are probably not feasible unless special circumstances occur. My guess, though, is that factual innovation and application of web-based information access technology, are about to create such circumstances.

KUNSTIG INTELLIGENS – DE VENNLIGE MASKINENE[1]

JON BING

Lady Lovelaces argument

Datamaskinen ble nesten funnet opp på 1830-tallet. Den eksentriske, britiske matematikeren Charles Babbage (1791-1871) hadde arbeidet med avanserte, mekaniske regnemaskiner, bl a med støtte fra det offentlige. Han generaliserte utformingen og la planer for en «analytisk maskin» hvor søyler av tannhjul skulle lagre data som ble bearbeidet ved mekaniske beregninger styrt av hullkort – den samme typen hullkort som ble brukt i Jaquards vevemaskiner – og som skulle drives av en dampmaskin. Babbages maskin ble aldri fullført, rett og slett fordi den krevde en presisjon ved produksjon av delene som datidens verktøymakere ikke kunne møte. Men da de første elektroniske datamaskinene ble konstruert like etter annen verdenskrig, oppdaget man til sin overraskelse at prinsippene var foregrepet i Babbages analytiske maskin.

I sitt arbeid ble Charles Babbage bistått av en bemerkelsesverdig kvinne, Ada Augusta, Lady of Lovelace (1815-1852). Hun var datter av den britiske poeten Lord Byron, og hadde arvet et talent for matematikk fra sin mor. Hun omtales ofte som verdens første programmerer, og har fått et kjent programmeringsspråk (ADA) oppkalt etter seg.

Babbages arbeid med den analytiske maskinen vakte internasjonal interesse i hans samtid, og en av de som ble nysgjerrig, var en italiensk militæringeniør, kaptein Luigi Menabrea (som etter hvert skulle bli Italias statsminister). Han skrev en artikkel om maskinen på fransk i 1842. Denne ble oversatt til engelsk av Ada, i oversettelsen korrigerte hun samtidig Menabreas misforståelser – og etter oppfordring fra Babbage kompletterte hun artikkelen med sine egne noter. Disse er i dag den mest verdifulle kilden til forståelse av Babbages teorier.

---

[1] Først offentliggjort som brosjyre utdelt ved norske flyplasser som *Kunstig intelligens – de vennlige maskinene*, Kreab, Oslo (7 sider). Også tilgjengelig på <www.ITpro.no> fra 14-24. april 2002.

Lady Lovelace innså at en generell datamaskin kunne løse mange slags oppgaver. Hun stilte seg også spørsmålet om det fantes grenser for hva en analytisk maskin ville kunne gjøre – om den faktisk ville kunne anses for å være «intelligent». Dette avviser hun med det som er blitt kjent som Lady Lovelaces argument: «Den analytiske maskinen har ingen pretensjoner i det hele tatt om å *skape* noe. Den kan gjøre *hva som helst,* men bare det *som vi instruere den om.*» Lady Lovelace tok altså utgangspunkt i programmene, og understreket at hvis maskinen skulle utføre en oppgave, måtte den programmeres for dette. Maskinen var ikke kreativ, den var deterministisk og derfor – i motsetning til mennesker – ikke i stand til å få nye ideer, til å finne opp nye nytt.

Turings test

Omtrent hundre år senere stillte man seg det samme spørsmålet på ny. Under den annen verdenskrig hadde tyskerne tatt i bruk en maskin for å kode radiomeldinger, f eks de kortbølgemeldingene som ble brukt for å koordinere tyske ubåters jakt på de livsviktige konvoiene som brakte utstyr og mat fra Amerika over Nord-Atlanteren til England. Kodesystemet bygget på det som kalles polyalfabetisk substitusjon, der 17576 substitusjonsfunksjoner ble brukt etter tur. Med de variasjonsmulighetene som et pluggebord ga, kunne inngangs- og utgangssymbolene permuteres på omtrent $4x10^{26}$ ganger, det var så mange muligheter at tyskerne stolte på at de allierte ikke kunne dekryptere meldingene selv om de ble oppfanget.

På et herresete nord for London, Bletchley Park, ble det dannet en gruppe av matematikere og andre kryptoanalytikere. Blant disse var Alan Turing (1912-1954). I en artikkel fra 1936 – «On computable Numbers» – hadde Turing løst et berømt, matematisk problem («Entscheidungsproblem») ved et tankeeksperiment som bygget på en logisk maskin som arbeidet etter visse spesifiserte prinsipper, og som ved å følge disse prinsippene, demonstrerte løsningen på problemet. Denne tenkte maskinen omtales senere som en «turingmaskin», og er i prinsippet en generell datamaskin. Ved Bletchley Park ble ideene brukt for å forsere Enigma-koden. Dette klarte de, og suksessen med å lese de krypterte meldingene ble en av krigens best bevarte hemmeligheter.

I løpet av krigen ble flere maskiner bygget ved Bletchley Park. I 1943 tok man i bruk en elektronisk maskin med 1800 radiorør som ble kalt Colossus. Det kan argumenteres for at dette var den første elektroniske datamaskin i verden selv om den var spesialbygget for å knekke koder – men på grunn av at beretningen om Bletchley Park ble hemmeligholdt til langt utpå 1980-

tallet, er den blitt overskygget av den mye større amerikanske ENIAC, som ble ferdig i 1946.

Det er i seg selv et tankevekkende bilde av krigen å se for seg sammenhengen mellom akademikerne i provisoriske skur i haven rundt Bletchley Park, og sjømenn – blant dem mange norske – som sto på mørklagte skip og stirret utover svart hav etter den grønne skumstripen som viste at en torpedo var på vei.

Etter krigen fortsatte Turing arbeidet med datamaskiner. Og han var uenig i Lady Lovelaces argument, for datamaskiner kunne programmeres slik at de kunne *lære* av sine egne erfaringer. Han mente at argumentet kunne sammenlignes med at en elevs oppdagelser skulle anses som gjort av læreren, og lot fantasien løpe av med seg i tanken på en datamaskin med fjernsynskamera, mikrofoner, høyttalere, hjul og servo-mekanikk som kunne rulle over landskapet og slik «få en sjanse til å lære ting på egen hånd». Påstandene hans om intelligente maskiner vakte oppsikt og debatt. Blant annet var det ikke uten videre klart hva «intelligens» egentlig var. Turing foreslo en test som i dag bærer hans navn: Tenk deg at du har to teletype-terminaler. Den ene terminalen går til et avlukke hvor det sitter et menneske, den andre til et avlukke hvor den knyttes til en maskin. Så får du adgang til å stille de spørsmål du vil ved å skrive dem på terminalen, og svarene skrives ut på terminalene. Du skal forsøke å bestemme i hvilket avlukke det står en maskin ved å lese svarene. Er du ikke i stand til dette, må man anse maskinen som «intelligent».

Turing fikk ikke leve lenge nok til å forfølge ideene sine til en naturlig konklusjon. Han var homoseksuell, og ble funnet skyldig i å ha praktisert sin legning. Han ble dømt til å gjennomgå en hormonbehandling som skulle «kurere» ham. Behandlingen gjorde ham syk. Sterkt deprimert tok han sitt eget liv ved å spise et eple dyppet i blåsyre – en symbolmettet slutt på livet til en av de som var med på å legge selve grunnlaget for det vi kaller «informasjonssamfunnet».

Kunstig intelligens

Arbeidet med å konstruere maskiner eller utvikle programmer som er «intelligente», er altså slett ikke av ny dato. Forskningsfeltet omtales ofte som «kunstig intelligens» («artificial intelligence» eller bare «AI»), selv om mange finner at det ligger en slags programerklæring i denne betegnelsen, og foretrekker det mer nøytrale uttrykket «kunnskapsbaserte systemer» (KBS).

Dette kan være noe mer enn en diskusjon om terminologi. Det er de som i arbeidet med intelligente systemer ser det som en oppgave å lage en maskin som i prinsippet fungerer på samme måte som den menneskelige hjerne. And-

re anser dette for å være av underordnet betydning, det sentrale er at man utvikler systemer som løser kompliserte oppgaver. Man kan si at de første er opptatt av kognitive prosesser, mens de andre er mer opptatt av systemets atferd, og finner det unødvendig å ta stilling til hvorvidt prosessene ligner menneskers tankeprosesser.

Ett av Turings yndlingseksempler var en sjakkspillende datamaskin. Sjakk er et spill med helt faste regler, man skulle tro det var enkelt for et datamaskinprogram å kalkulere de beste trekkene og slik vinne et spill. Men mulighetene er så mange, at dette i praksis ikke lar seg gjøre. Det systemet som i dag er best kjent, er Deep Blue, en spesialbygget IBM-maskin som tapte mot Garri Kasparov i 1996. Men maskinen ble oppgradert, og i 1997 oppga Kasparov spillet etter 19 trekk og erklærte Deep Blue for vinner. Likevel kunne ikke maskinen «se» mer enn seks trekk fremover i spillet.

Sjakk er et spill med helt faste regler. Man kan ta som utgangspunkt at en regel har tre elementer: (1) en viss omstendighet som er relevant for beslutningen, (2) det resultat som tilstedeværelsen av omstendigheten favoriserer (verdi) og (3) den relative vekt som tilstedeværelsen av omstendigheten teller med. I faste regler kan alle disse elementene fastlegges på forhånd. Man kan bygge komplekse og uoverblikkbare regelstrukturer, men avgjørelser vil alltid være forutberegnlige (forutsatt at man er enige om hvilke omstendigheter som foreligger – det er man ikke alltid, jurister vil da gjerne si det foreligger strid om faktum som avgjøres ved bevisføring). Et sjakktrekk er et eksempel på en avgjørelse som styres av faste regler, men hvor sammenhengen mellom reglene er så kompleks at mennesker mister oversikten, og en datamaskin altså bare kan etablere den for et lite antall trekk fremover i spillet.

Men mange avgjørelser bygger på *skjønn.* Dette kan også beskrives som regelstyrte avgjørelser, men to forhold skiller de skjønnsmessige fra de faste avgjørelsene:

- Man kan aldri på forhånd bestemme hvilke omstendigheter som kan anses for å være relevante for en ny avgjørelse.
- Man kan aldri på forhånd bestemme med hvilken relativ vekt en omstendighet vil kunne telle med i en ny avgjørelse.

Hvis dette er en riktig teori, har man i og for seg angitt en grense for muligheten for automatisering. Men dette er bare en prinsipiell grense. Vi kan tenke oss at et program analyserer et meget stort antall skjønnsmessige avgjørelser som er truffet, flere hundre eller tusen. Da vil programmet ut av dette materialet kunne danne et komplekst sett med regler, som i og for seg er faste, men som vil avgjøre nye spørsmål «på samme måte» som de tidligere avgjørelsene. I praksis vil man da oppleve dette som at det fortsatt treffes skjønnsmessige

avgjørelser, selv om det i prinsippet er uriktig – den skjønnsmessige beslutningen er modellert ved et stort antall faste regler. Og hvis programmet kan hente erfaring fra en uavhengig kilde – vi kan tenke oss at det liksom «kikker over skulderen» til en menneskelig beslutningsfatter – så vil det også kunne oppdatere og raffinere sine egne regler.

Nevrale nett betegner en type programmer som kan bygge opp regler ved hjelp av eksempler på denne måten. Programmet «lærer» av eksemplene, og danner selv reglene som kan bli et så komplekst system at et menneske ikke verken kan overblikke dem eller treffe avgjørelser ved hjelp av dem. Turing ville gjenkjenne sin lærende datamaskin. Og kanskje han ville hevde det også var «intelligent» ettersom man ikke ville se forskjell på avgjørelser truffet av programmet eller et menneske.

Ekspertsystemer

Ofte gjengis regler som en «hvis [en omstendighet foreligger] så følger [et bestemt resultat, verdi]». Dette er en forenklet form for den som er gjengitt ovenfor, hvor den *vekt* som tilordnes forekomsten av omstendigheten, ikke er angitt eksplisitt. Vi er vant med å bruke slike regler – i sin enkleste form kan et eksempel være «*hvis* en person hoster *og* har rennende nese, *så* er vedkommende forkjølet». Helt sikkert er det ikke, for årsaken kan jo for eksempel være at vedkommende er plaget av allergi – denne usikkerheten kan vi uttrykke for eksempel ved å angi en sannsynlighet for resultatet – «*så* er vedkommende forkjølet *med 80 % sannsynlighet*». Og vi kan legge til tilleggsmomenter, hvis det f eks er vinter, øker vi sannsynligheten for forkjølelse, hvis det er i pollensesongen, reduserer vi det ytterligere.

Det har fremstått som en mulighet å utvikle systemer som bygger på slik kunnskap. Man kunne ta kunnskapen til f eks en spesialist i øre-, nese- og halssykdommer. Vedkommende angir alle de omstendighetene han eller hun bygger på når vedkommende stiller en diagnose. Hvis dette gjøres nøyaktig nok, og er fullstendig nok, ville programmet kunne stilles til disposisjon for en allmennpraktiker, som så kunne få hjelp til vurderinger som ellers ville måtte gjøres av eksperten. Slike systemer kalles derfor *ekspertsystemer.*

Et tidlig eksempel med en viss suksess var Ed Shortliffes program MYCIN, som var konstruert for å diagnostisere årsaken til blodinfeksjoner. Programmet stilte brukeren en serie med spørsmål om pasientens symptomer, og på dette grunnlaget anga det så sannsynlig årsak. Årsakene kunne være mange, for eksempel en bakterie som pasienten var blitt smittet av på reise i utlandet, og som brukeren (den behandlende lege) ikke hadde erfaring med

fra før. Derfor ville han eller hun heller ikke lete etter symptomer som kunne vise at det nettopp var denne bakterien som var årsaken.

På 1980-tallet ga slike eksempler forskere en voldsom optimisme i hvor langt man kunne komme med ekspertsystemer. Det var kanskje i dette tiåret at entusiasmen rundt «kunstig intelligens» var høyest. Man så ingen prinsipielle grenser for ekspertsystemene, det hele ble lett sett på som et spørsmål om å samle inn fullstendig kunnskap fra ekspertene innen et område («knowledge acquisition»). Men om det bare var praktiske problemer, så viste de seg å være så store at ekspertsystemer ikke vokste til den industrien man trodde de ville bli. For problemene med å samle fullstendig kunnskap innen et domene er faktisk betydelige. Et mye brukt eksempel er å beskrive det rommet man oppholder seg i. Dette lyder enkelt, men det viser seg at man ofte glemmer å angi faktiske omstendigheter som fremstår som så selvfølgelige at de ikke trengs å nevnes; det folk oftest glemmer å angi, er at rommet har et gulv. Uten gulv vil et datamaskinprogram, som har regler om tyngdekraft, trekke helt uriktige slutninger om hva som skjer når en person trer inn gjennom døren.

Det betyr på ingen måte at ekspertsystemene ikke er med oss i dag. Tvert imot så er de «smarte» egenskapene til mange programmer nettopp eksempler på bruk av de samme prinsippene. For eksempel skriver jeg dette essayet ved hjelp av tekstbehandlingsprogrammet MS Word. Nederst til venstre på skjermen sitter det en blid, liten katt – en «office assistant» – rett som det er dukker det opp en lampe over kattens hode for å vise at den har et forslag. Dette er et lite «ekspertsystem» som overvåker min tekstbehandling, og på grunnlag av de opplysningene som slik samles, kommer med forslag. Spesielt intelligent er den ikke – men hva kan man egentlig vente seg av en katt?

Datamaskinassistert forvaltning

Norge har – sammen med de andre nordiske land og enkelte andre land, som f eks Nederland – en høy automatiseringsgrad i offentlig forvaltning. Ett av de systemer som har vært gjenstand for nokså detaljert analyse, var det systemet for bostøtte som ble utviklet av Statens husbank tidlig på 1970-tallet. Bostøtteordningen var basert på et plenarvedtak i Stortinget, og skulle dekke differanse mellom «virkelige» og «rimelige» boutgifter for husstander som kom inn under ordningen.

Søknaden behøvde bare inneholde én opplysning: Søkerens fødselsnummer. Systemet brukte dette til å hente inn fra Det sentrale personregister opplysninger om hvem som bodde på samme adresse: Disse ble én husstand i forhold til søknaden. Systemet hentet inntektsopplysninger fra skatteadmi-

nistrasjonen, trygdestatus fra trygdeadministrasjonens – og «faktisk» og «rimelige» boutgifter ble beregnet på grunnlag av bankens egne opplysninger om boligens type, alder mv. Som resultat ble det enten skrevet ut et standard brev som forklarte hvorfor man ikke fikk støtte, eller en postanvisning. Slik ble ca 100 000 vedtak truffet to ganger i året. Denne forkortede forklaringen yter selvsagt ikke systemet rettferdighet, men antyder at man her hadde en ordning som traff beslutninger som fikk betydning for enkeltmenneskers velferd helt automatisk – uberørt av menneskehånd eller -ånd.

Nå skal man være forsiktig med å kvalifisere et slikt system som «kunnskapsbasert» – bostøttesystemet var programmert på en tradisjonell måte ved bruk av det noe trauste programmeringsspråket COBOL. Men det illustrerer at det i moderne masseforvaltning brukes datamaskinsystemer til å støtte beslutninger – deler av prosessen er gjerne automatisert. Uten slike systemer ville forvaltningen innen trygd, skatt, arbeidsformidling, lånekasse, bank, forsikring mv ikke kunnet fungere slik vi har vent oss til det.

Muligheten for at det treffes avgjørelser i privat eller offentlig forvaltning som fullt ut er automatisert, har begrunnet en bestemmelse om innsyn i personopplysningsloven § 22. I slike tilfeller vil det kunne være vanskelig for den enkelte å forstå grunnlaget for beslutningen, og utskrift av programmet vil ikke hjelpe de fleste av oss – derfor kan man kreve at det redegjøres for «regelinnholdet i datamaskinprogrammene som ligger til grunn for avgjørelsen».

Maskinintelligens – et stykke frem

Datamaskinbaserte systemer blir stadig «smartere» – de lærer gjennom bruk, og støtter brukerens behov stadig bedre. Som skissert ovenfor kan det argumenteres for at det i prinsippet ikke er noen begrensning for hvor «intelligente» datamaskinprogrammer kan bli, selv om de praktiske hindringene er store. Professor Margaret Boden (University of Sussex) er en av de fremtredene filosofene som har arbeidet med spørsmål rundt kunstig intelligens, og hun har noen trøstens ord til de som frykter å bli innhentet av intelligente maskiner: Det finnes minst to ting som ethvert barn kan, som vi ennå ikke har klart å løse med datamaskinprogrammer. Det ene er å forme en uttalelse i naturlig språk om et vilkårlig emne. Det andre er å styre en hånd så den griper et tomt glass som er plassert et tilfeldig sted på et bord.

Men allerede i den nære fremtid vil vi møte maskiner med et billedlig talt mer menneskelig ansikt enn vi kjenner i dag – maskiner som lar seg styre med talte kommandoer og svarer oss, en bil som selv ringer Viking eller Falken hvis den får problemer (og oppgir nøyaktig posisjon), stereoanlegg som re-

gistrerer vårt ansiktsuttrykk og velger musikk etter humøret vårt, intelligente hus som regulerer strømforbruk etter værmeldingen, overvåker elektrisitetsanlegg og sikkerhet – en nesten uendelig rekke med påfunn. Noen vil være nyttige, andre vil vi vel helst se på som unødvendige og kanskje fort gå lei av.

Det er ikke sikkert at vi vil kalle slike systemer «intelligente». Men at de blir vennlige, og at mange av dem blir nyttige deler av våre egne hverdagslige omgivelser, kan vi trygt regne med.

DEN LEVENDE FRANKENSTEIN[1]

JON BING

En av filmene høsten 2001 var *AI* av Steven Spielberg. Omtalen av filmen har bl a dvelt ved at Spielberg overtok dette prosjektet fra Stanley Kubrick, som selv ikke rakk å realisere det. Forholdet mellom to så sentrale regissører er selvsagt interessant. Men det må være tillatt å besvære seg litt over at få synes å ha lagt vekt på at filmfortellingen er skrevet av den sentrale amerikanske science fiction-forfatteren Ian Watson, og at man heller ikke har interessert seg nevneverdig for at bak fortellingen som ligger til grunn for prosjektet – «Supertoys last all Summer Long» – finner man en av de mest særpregede, britiske science fiction forfatterne, Brian W Aldiss (jf <http://brianwaldiss.com>). Jeg tror man da ville ha funnet en nøkkel til det sentrale temaet i filmen.

Brian W Aldiss (født 1925) er ikke ukjent for norske lesere. Han slo gjennom med romanen *Non-Stop* i 1958, oversatt til norsk med samme tittel (1973). Som en eksponent for seriøs, fantastisk litteratur forsvarte han science fiction, blant annet med slagordet: «Science fiction is no more written for scientists than ghost stories are written for ghosts.»

Men det var Aldiss arbeid som litteraturkritiker – bl a ti år som kulturredaktør i *Oxford Mail* – som tiltrakk seg interessen til daværende kringkastingssjef Torolf Elster. Elster var selv en ikke ubetydelig science fiction-forfatter, noe som blant annet demonstreres i den lekelystne novellesamlingen *Sjørøvere* (Tiden 1959). På et tidspunkt da science fiction ble ansett for å være kiosklitteratur fulgte Elster opp sin overbevisning, og bestilte fem originale kåserier av Brian Aldiss, som ble sendt som opplesninger i radioen 1958. Disse kåseriene ble senere til kjernen i det som er den første ambisiøse fremstilling av den fantastiske litteraturs historie, *Million Year Spree* (1973 – senere revidert og utvidet i samarbeid med David Wingrove som *Trillion Year Spree,* 1986).

Aldiss trekker frem én roman som betegner begynnelsen for tematikken i moderne science fiction, Mary Shelleys *Frankenstein, or the moderen Prometheus* (1817). Romanen er trivialisert i utallige filmatiske beretninger om

[1] Først trykt i *Dagens næringsliv*, 3-4. november 2001.

det monsteret som vitenskapsmannen Victor Frankenstein lappet sammen av kirkegårdsfunn, og ga liv – modellert etter forsøkene til Luigi Galvani ved Universitetet i Bologna, som i 1786 hadde fått musklene i en froskelår til å trekke seg sammen ved hjelp av elektrisitet, selv om frosken selv var død. Romanens tema er på en måte todelt: Frankensteins etiske ansvar overfor Gud idet han skaper kunstig liv, og hans ansvar overfor det han har skapt – en skapning som følte lojalitet overfor ham, men som han selv svikter. Temaet om forskeres ansvar har stått sentralt i det århundre som nettopp er avsluttet, stikkord som atombombe og genteknologi er tilstrekkelige antydninger.

Romanen ble til under ekstraordinære omstendigheter. Mary Shelley var bare nitten år da den ble skrevet i 1816. Sammen med poeten Percy Bysshe Shelley var hun kommet til Gèneve-sjøen, og tatt inn i en nabovilla til Lord Byron. Det var dårlig vær den sommeren, og Lord Byron foreslo en selskapslek, de skulle skrive hver sin fantastiske fortelling. *Frankenstein* er Marys seirende bidrag til denne makabre, litterære leken.

Så fascinert av sommeren ved bredden av Gèneve-sjøen var Brian Aldiss at han brukte den som bakgrunn for romanen – *Frankenstein Unbound* (1973), oversatt til norsk som *Den levende Frankenstein* (1977). Filmkritikere burde kanskje ha oppdaget at denne romanen ligger til grunn for Roger Cormans film (med samme navn) fra 1990.

På denne bakgrunnen blir det sentrale tema i Spielbergs film *AI* tydeligere. Filmens hovedperson er en robot skapt i bildet til en liten gutt, som programmeres til «ekte» følelser overfor den kvinnen som får ham til erstatning for sin egen sønn. Det er en Frankenstein-beretning gjenfortalt om kunstig intelligens, et av de etiske temaer som har vært et bakteppe for utviklingen av moderne informasjonsteknologi, aktualisert av f eks Stephen Hawkings advarsel fra i sommer om at menneskeheten vil kunne bli erstattet av intelligente maskiner.

Jeg tviler imidlertid på at Aldiss er udelt begeistret for alle referansene til Pinocchio-motivet som er lagt inn i filmen. Naturligvis bygger også Mary Shelleys *Frankenstein* på enda eldre parabler. Den våte sommeren 1816 leste det merkelige selskapet ved bredden av Genève-sjøen blant annet en samling med jødiske eventyr, hvor bl a beretningen om det vesen Rabbi Judah Löw formet av leire og ga liv for å forsvare gettoen i Praha på slutten av 1500-tallet.

Men selv om leirmannen skal ha blitt til støv i tårnkammet i Altneusynagogen – som fremdeles står i Prahas getto – så lever altså dilemmaet videre, nå sist gjenfortalt med effekter lånt fra moderne informasjonsteknologi av Steven Spielberg på grunnlag av Aldiss novelle om forholdet mellom en kvinne og en robot som forveksles med forholdet mellom mor og barn.

SPEILBILDER AV SPEILBILDENE[1]

JON BING

Igjen fyller en av Steven Spielbergs fantastiske filmer bredlerretene på norske kinoer med Tom Cruise i hovedrollen. *Minority Report* tar som utgangspunkt at det er mulig å forutse når et drap blir begått, og at politiet kan varsles så tidlig at det kan forhindre forbrytelsen. Drapet blir altså *ikke* begått, men den potensielle gjerningsmannen straffet.

Dette er ikke noen anmeldelse av filmen, som har mange svakheter, ikke minst en unødvendig sentimentalitet. Heller ikke skal jeg falle for fristelsen til å diskutere det tvilsomme kriminalpolitiske premiss som er antydet.

La meg i stedet invitere til den tankelek som utgangspunktet innbyr til. Altså at man kan gripe inn og endre fremtiden. Men hva var da fremtiden? Mordet dramatiserer valget: Drapsmannen står med pistolen hevet, men skuddet er ennå ikke falt. Fra valget springer det ut to mulige verdener, én hvor offeret blir drept, én hvor morderen besinner seg. Slik vokser mulige virkeligheter frem av våre valg i et komplisert mønster som Jorge Luis Borges har kalt «Haven med de forgrente stier».

Denne tankeleken om forholdet mellom valg og virkeligheter er et grunnleggende tema i filmen. Filmen bygger på en novelle av Philip K Dick fra 1956. Dick er en av de store, amerikanske forfatterne av fantastisk litteratur, en merkelig mann som skrev som rasende på 1960-tallet, men han ble tiltrukket av Californias narkotikabaserte subkultur og gikk etter hvert litt i stå. I det siste året av sitt liv opplevde han at Ridley Scott laget en film på grunnlag av romanen med den utrolige tittelen *Do Androids Dream of Electric Sheep?* (på norsk fattigslig oversatt som *Livstyvene*). Han fikk sett nok av filmen til at han, kanskje litt motstrebende, godtok den (kanskje til og med likte den) før han døde i 1982, bare 54 år gammel.

Scotts science fiction-film er en av de mest kjente som er laget: *Bladerunner* med Harrison Ford i hovedrollen. Den sammensatte fortellingen kretser rundt menneskelike androider. Ja, de er faktisk så menneskelike at det er vanskelig å se forskjell på androider og mennesker. Og dermed klarer Dick gjennom sin fabel igjen å få stilt et grunnleggende spørsmål, nemlig hva et

---

[1] Først trykt i *Dagens næringsliv*, 14-15. september 2002.

menneske egentlig er. Det er ikke nettopp blitt mindre aktuelt etter hvert som forskning rundt kunstig intelligens reduserer forskjellen mellom hva et menneske og en maskin egentlig kan utrette.

Det finnes også en tredje film basert på en fortelling av Dick, *Total Recall* (1990) med Paul Verhoeven som regissør og Arnold Schwarzenegger i en hovedrolle han faktisk får gjort noe utav. Her tilbys en form for submersiv virtuell virkelighet. Akkurat som i en drøm oppleves den som virkelige for drømmeren, og slik kan man kjøpe eventyrlige opplevelser på boks. Men hovedpersonen oppdager at hans drøm (kanskje) er virkelig.

Originaltittelen på novellen som ligger til grunn for *Total Recall,* er «We can remember it for you wholesale». Dick er en forfatter som mestrer den vanskelige kunst å lage titler som kan stå alene, nærmest som en gåtefull strofe lyrikk – min personlige favoritt er *The Man Whose Teeth Were All Exactly Alike.*

Eksemplene som filmene representerer, illustrerer for så vidt Dicks livslange litterære prosjekt. Som forfatter og menneske var han opptatt av å forstå hva virkelighet egentlig er, hvor grensen går mellom illusjon og virkelighet, når speilbildet blir et speilbilde av seg selv. Fortellingene bruker oppfinnsomme utgangspunkt som gir spørsmålet en ny omdreining, en ny innfallsvinkel. Selv har han karakterisert seg som en skjønnlitterær filosof, ikke forfatter. Men han skrev sine arbeider for et høyst kommersielt marked, derfor er fortellingene samtidig spennende, av og til redusert av tidspress til rene røverromaner. Vil man ha et eksempel på de siste, kan man forsøke seg på den norske versjonen av *Our Friends from Frolix 8,* som på norsk er kommet til å hete *Hjelp fra rommet,* utgitt som kiosklitteratur og frarøvet litterære kvaliteter i oversettelsen. Heldigvis er altså andre av romanene hans oversatt på en mer skånsom måte.

Etter sin død har Dicks anerkjennelse vært jevnt stigende. Det grunnleggende tema han har tatt opp, og de innfallsvinklene han har gitt til dette, er nettopp sentrale for det samfunnet vi selv er i ferd med å skape ved hjelp av datamaskinbaserte systemer, hvor Internettets kybernetiske landskap er like virkelig som granskog og svaberg. En amerikansk tenåring svarte i et fjernsynsintervju: «For meg er virkeligheten bare ett av flere grensesnitt, og det er ikke det jeg foretrekker.» Nettopp i et samfunn hvor folk kjenner personene på Hotell Cæsar bedre enn sine naboer, og hvor barn søker spenning i interaktive spill på skjerm, blir Dicks litteratur relevant. Det er en risikofri spådom at flere av fortellingene hans vil finne veien nettopp inn i nye filmer og de andre media som nettopp skaper denne relevansen.

ROOMS FOR THOUGHT[1]

JON BING

The German photographer, Candida Höfer, has become world famous for her photographs. Many of these are interiors from museums, galleries and other examples of public "inner space". Some of her most pertinent works are studies from libraries, such as the national library of Paris, libraries in Cologne, Los Angeles and Oslo.

Confronted with these images, one realises that they reveal, in a sense, the architecture of thoughts. For the reading rooms of libraries must be amongst the few rooms constructed to serve silence. The people in the rooms read, and reflect on what is read. They add new understanding to what already has been understood. The rooms are constructed for communication, not for connecting people but connecting books and people.

There may be other rooms with similar functions, like the reading room at a university, which – we like to think – has been constructed for students to teach themselves. But in such a room, the students are joined together by shared interests, two neighbours at the table usually are working with the same subject, their whispered conversation concerns the same topic, the conversation in the break has a background in the same lectures.

In a library, though, it is different. Side by side are persons with the most different interests. They constitute, in a sense, parallel universes.

The rooms are often monumental; the roofs are vaults and arches, the books lining the walls form orderly patterns of authority. But studying the images of Höfer, the attention is drawn to the reading light, the desk, the open book. One can nearly see the outline of the invisible reality created by the relation between the reader and the book – the vault is necessary to give place to the power of the mind, to the fascination of learning something new – or, perhaps, the boredom of having to read something demanded by someone else: A teacher or an employer.

---

[1] First published in Ulf Grønvold (ed), *The New Bibliotheca Alexandrina* (Oslo: The Norwegian Museum of Architecture, 2002), pp 69–78. Parallel texts published in French ("Espaces de réflexion") and Arabic.

It is fascinating to see how the photographs reveal something of the architecture of imagined worlds. Studying the images, I see – side by side – the lawyer attempting to understand the concept of a "copyrighted work" and the professor in astrophysics struggling with the theory of black holes. Seated side by side, one can hear the other turn a leaf in his or her book. But both are immersed in separate worlds of concepts and ideas – as far away from each other as two heads can be, but even so framed within the same architecture, working in the same room.

This is the wonder revealed by the photograph. The photographs are images of the inner space of buildings.

I grew up with an intense interest in the exploration of space. I used to look towards the black sky of northern Norway, in which the stars glittered in many colours, teaching myself their fabulous names … Aldebaran, Beatrix, Betelgeuse, Rigel, Spica … I despaired when learning that the theory of relativity did not allow a space vessel to reach even the closest star – Proxima Alpha Centauri – in a lifetime. And I was waiting impatiently for the first real launch of a man towards the moon. It seemed to me that this first, tiny step of man towards outer space was long overdue. And it did take sufficiently long time for me having grown up when Neil Armstrong placed his boot onto the dusty lunar surface; I actually published a book celebrating not only the first moonwalk, but also the moon in literature, mythology and the history of science.

Neil Armstrong took his "giant leap for mankind" on 20th July 1969. Less than two weeks later, on 1st September 1969, the first Interface Message Processor was installed at the University of California Los Angeles by the Advanced Research Program Agency (ARPA), a civil research branch of the US Department of Defense. The IMPs made it possible to interconnect the mainframes at universities and research institutions at that time, and to send data or programs between the institutions. If one needs a date for the birth of the Internet, 1st September 1969 is as good as any.

To me this is more than a coincidence; it is a significant indication for the time when dreams started to change. The dream of outer space dwindled, the practical problems of logistics, costs and politics made my juvenile visions of man blasting off to far planets naïve and unrealistic. But at the same time as this dream faded, a new dream was in the making – the dream of "inner space". It also seemed as unrealistic at first when Professor JCR Licklider, who headed the program of information technology at ARPA, suggested that one should construct a global network of computers and users. The idea was sufficiently grand to gain the nick-name "The Intergalactic Computer Network". This nick-name actually reveals the relation to the dream of conquering outer space.

Here, we will not trace the development of the network: how ARPA split the network into a military and a civil part around 1980, leaving the administration of the civil network, now re-named Internet, to the National Science Foundation; how the NSF stopped to fund the network around 1990, and how Tim Berners-Lee at the same time gained support from the Organisation Européene pour la Recherche Nucléaire – still known by the abbreviation CERN – for his project World-Wide Web. Or how a young American, Marc Andreessen, launched the first web browser, Mosaic, in 1993 – a program that is the common ancestor to both Netscape and Microsoft Internet Explorer. But step-by-step a situation was emerging in which a wealth of information was created – a maze, a chaos of web sites and pages.

It is, however, rather daunting to reflect that at the end of 1993, only 50 servers were set up to browse the Internet. In a very brief time, in less than ten years, this new inner space of information has become a universe for exploration and discovery. Amazing things can be learned, the most whimsical facts can be studied.

I still remember the first time a guest lecturer from the UK had come over by one of the new, cheap air companies to Norway, and told that one of his friends had instructed him to collect the bag for air sickness, as a bag from this company was missing in his collection. We thought this was a rather weird hobby until we discovered that there were at least two home pages on the Internet devoted to such bags, reproducing them and commenting upon their value for collectors. Or when one of my students, writing a thesis, had taken his first expeditions into inner space, and become fascinated by the possibilities. He had an aquarium with salt-water sea horses, and one of them had behaved in a disturbing manner. Using his new skills, he had found a lot of information on sea horses on the Net, including a home page with a small expert system offering a diagnosis of the symptoms of ailing creatures. He had described the behavior of his sea horse according to the prompts, and the Internet service had returned with the suggested conclusion that the sea horse was terminally ill, and probably would be dead by the next morning. His enthusiasm in finding that the service actually proved to be right far exceeded his grief in losing a sea horse.

Probably all of us have anecdotes like this, illustrating our experiences from the first experimental flights in the inner space of the Internet. And this environment was re-named *cyberspace* by the Canadian author, William Gibson, in his novel *Neuromancer* (1984):

> "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathemati-

> cal concepts … A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding …"

Yet this inner space already existed prior to the time we embarked on the voyage in cyberspace. For a conventional library is itself such an inner space. Many of us re-discover in the Internet available at our own desk the joys of our childhood, when we realized that the library was a multi-universe of possibilities. We agree that there are vast differences between the traditional technology of libraries stacked with books, and the hyperlinked cyberspace of Internet. Yet these obvious differences should not make us blind to the even more important similarities: They are both a space of knowledge and entertainment, presenting experiences from around the world to our own laptop, whether a screen of liquid crystals or the pages of a printed book is resting on our knees. And in both cases, also, the vessel for travelling is our own marvelous imagination, which creates images from text or graphics vivid and personal. In a sense, we are also traveling within our own mind, the innermost and private space in which the most important events of our life take place.

In a modest way, I have myself tried to express this relation between the outer space of starships and the inner space of libraries. Having accepted that the laws of nature, as we know them, prohibit travel faster than light, I asked myself what would be sufficiently valuable to ship between inhabited worlds in a possible future of a space-faring humankind, where the starships would spend generations in transit between inhabited worlds. The answer was obvious: Knowledge. From this emerged a series of juvenile novels of the voyages of the starship *Alexandria* (the choice of name was obvious), staffed by librarians, bringing the huge data banks of knowledge collected from many worlds to a new planet. In the novels, the world at which the starship arrived would always have a problem or conflict. But rather than solving this by flashguns or novel weaponry, the librarians would search their files, and come up with a piece of information that provided a solution. This reveals, of course, my obvious motive for the adventures – the novels do not pretend to prophesy a possible future, but rather indicate a strategy for the solution of the conflicts in our own time and societies. Perhaps naively, they plead that libraries have a role in our present affairs, and that the knowledge, experiences and insights contained in the inner space of the library vaults also may provide solutions in our multi-cultural societies: The distance measured in politics or attitudes between the nations of this world often seems more difficult to bridge than the distance between solar systems.

There are many strategies for travelling the inner space of library shelves. One of my French friends has developed a certain principle which he calls "the importance of the book next door". In searching for a certain book, walking along the shelves, reading the book spines, he often had come to experience that it was the book next to the one he was searching for, that really proved to be interesting. When you have decided that you need information from a certain book, you do in a sense already know its content. Yet next to it may be a book you did not know – but due to the classification system determining its position on the shelves, this book is to some extent related to the book you are looking for. And in this relation there may be a creative tension, revealing an aspect of your interest of which you yourself had not been made conscious. Therefore, the book next door may be what you really need, though you did not know so in advance.

Hence, within the vaulted space of libraries, set out on your own voyages for new knowledge or enjoyment – it may be as exciting as exploring new worlds. And in contrast to the worlds you are likely to find in outer space, the worlds of the inner space of libraries will most certainly be inhabited by amazing creatures and wonderful people.

THE SCHENGEN INFORMATION SYSTEM IN AUSTRIA: AN ESSENTIAL TOOL IN DAY-TO-DAY POLICING AND BORDER CONTROL WORK?[1]

STEPHEN K. KARANJA

Abstract

This article discusses the Schengen Information System (SIS) in Austria. SIS is a joint information technology and communication system for exchange of information concerning wanted persons and objects. Its purpose is to allow checks on persons to be made quickly and efficiently at border controls in order to detect criminals and illegal immigrants moving into and from one Schengen country to another. The article is based largely on interviews with key persons responsible for SIS in Austria, supplemented with background material from written literature and legal sources. The purpose of the interviews was to gather information on the functioning of SIS and the implementation of control mechanisms. The general conclusions are that SIS is functioning well and has become an essential tool in day-to-day police and border control work. The control safeguards are also working well. However, there are a number of concerns that still need to be addressed, while others are already being addressed. These concerns are discussed in detail as an evaluation of the effectiveness of SIS' internal and external control and safeguards.

1 Methodology

The interviews were carried out in Vienna between 26 February and 8 March 2001.[2] The persons interviewed were from the Austrian Data Protection Commission (DPC) and the Ministry of the Interior. From the DPC,

---

[1] This is a slightly modified version of a paper published in the *Journal of Information, Law and Technology*, 2002, <http://elj.warwick.ac.uk/jilt/02-1/karanja.html>.

[2] I would like to thank those interviewed for availing their time, and Professor Erich Schweighofer, University of Vienna for making these interviews possible.

the deputy data protection commissioner was interviewed, and from the Federal Ministry of Interior, five persons were interviewed in total: the first was head of the National Schengen Information System (NSIS) and Data Processing Unit, plus the technical representative to the Schengen Council; the second person was a senior officer in the Department of Immigrations; the third person was the director of the Austrian SIRENE (Supplementary Information Request at the National Entries); the fourth person was the co-ordinator for data protection, law and order; the final interviewee was the person responsible for legal, organisational and financial questions in the Data Processing Unit and a national legal representative to the Schengen Council.

The interviews were informal and semi-structured. The interviewees were sent a similar list of general questions in advance, with which they could prepare and orient themselves before the interviews. As it was not possible to substantiate the information collected through independent sources, given the sensitive nature of the system itself, a standard list of questions was used for cross-checking and verification purposes. Consequently, it was easier to substantiate information received during an earlier interview with that of a later one. Another advantage of using general questions was that it encouraged interaction with the interviewees. The objective was to give them leeway to express themselves freely and in-depth. During the interviews, the general questions were supplemented with more specific oral questions posed by the interviewer. These questions were aimed at eliciting further information, in particular information relevant to the role of the specific department being interviewed. The general questions covered a range of issues such as Schengen legislation and documentation, functioning of SIS and SIRENE, data quality and security, data modelling, role of SIS in the Schengen co-operation, the relationship between SIS and other cross-border systems.

Following each interview session, the interviewer documented the interview as a written report, from notes taken during the interview. Later, the written reports were sent to the interviewees for verification and comment. In some cases, additional verification questions accompanied the reports. Out of a total of five reports sent, response was received for three documents with clarification and additional comments. In general, the interviewees were informative, open and candid in their responses.

2 Background Information

Austria joined the Schengen co-operation in 1995 but did not begin to implement the Schengen Convention[3] until 2 December 1997. The two-year delay may seem long, especially as Austria already had data protection legislation dating from 1988.[4] However, other legislative, technical and border control conditions needed to be fulfilled before implementation could commence. The Schengen Convention had to be incorporated into the national legal system, the Schengen Information System established, and external border controls improved.

The issue of external border control was especially thorny for Germany. Austria's Schengen external border with the Czech Republic, Slovakia, Hungary, Slovenia, Switzerland and Liechtenstein is 1,200 km long. Germany was concerned that Austria might not be able to fulfil the conditions for external border control, and insisted that Austria effectively control its external borders before beginning to implement the Convention.

In the interview with a representative of the immigration authorities, it transpired that Austria had used ATS 3 billion to enhance control along its external borders. Over 6,500 new personnel had been deployed along the external border, new technical equipment bought, and SIS IT infrastructure laid down in an effort to comply with Schengen external border control conditions.

3 Schengen Information System

3.1 General

The SIS consists of two main components: the national systems referred to as the national SIS (NSIS), located within the territories of each of the Schengen Contracting Parties, and a central technical support system known as the

---

[3] Convention of 19 June 1990 implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders.

[4] Article 126 of the Schengen Convention stipulates that, at the time of the Convention's entry into force, the level of protection of personal data should be at least equal to the level resulting from the principles laid down in the Council of Europe Convention on data protection of 28 January 1981 (ETS 108), and the data must not be transmitted unless this level of protection actually exists in the territory of the Contracting Parties involved in the transmission.

Central SIS (CSIS), situated in Strasbourg, France (Schengen Convention, Article 92). The NSIS enables designated national authorities to carry out searches in SIS. The CSIS ensures that data files of the national sections are updated and kept identical at all times by online transmission of information.

The SIS is the most important technological compensatory measure in the removal of internal borders in the Schengen co-operation. It is a fundamental requirement for implementation of the Schengen Convention. No country may commence implementation of the Convention before SIS has been established. The persons I interviewed at the Ministry of the Interior were of the opinion that SIS plays an important role in crime and border control.[5] Hence, it has become a very important tool in day-to-day police work. To illustrate this, one interviewee referred to the first case to be solved through SIS in Norway.[6] He emphasised that, had it not been for the Schengen co-operation and SIS, such a quick arrest could not have been possible. My experience in crossing the Schengen external border between Austria and her two non-Schengen neighbours – Hungary and Slovakia – confirms that SIS has indeed become an important tool in border control work.[7]

3.2 Establishment of the System and Data Modelling

As the responsibility for establishing the national part of SIS – NSIS – is left to individual Contracting Parties (Article 92), countries have come up with different technical and data-modelling solutions. The question regarding the establishment and data modelling was aimed at finding the path the Austrian authorities had followed and whether it had been influenced by other Contracting Parties' solutions.

The findings reveal that, in Austria, the Ministry of the Interior has responsibility for the operation of SIS and, therefore, undertook the task of establishing the system. However, the establishment efforts involved other government ministries, namely the Ministry of International Affairs, the Min-

---

5 See section 5 – The Role of SIS in Interstate Co-operation.

6 The case was reported in *VG* and *Dagsavisen* on 26 January 2001. It involved the arrest of an Iranian man who had been charged in a German court for organised human smuggling. As a result of a search in SIS, he was arrested in Bergen, Norway, where he had sought asylum. He had been registered, under many aliases, as a wanted person by a court in Leipzig in the former East Germany. One of the names was identical to the name he used in Norway. According to *Dagsavisen*, if it were not for SIS, the man would have lived unnoticed in Norway. The person had resided for many months in Bergen and had established himself with his own apartment.

7 See my article, "Crossing the Schengen External Border", in LA Bygrave (ed), *Yulex 2001* (Oslo: Institutt for rettsinformatikk, 2001), pp 93–102.

istry of Justice and the Ministry of Finance. The DPC, though not directly involved, was often consulted, especially regarding data protection matters. As for the technical aspects, the establishment of NSIS was the result of the work of the Ministry of the Interior's Electronic Data Processing (EDP)-Centre, in co-operation with IBM. It was emphasised that the Austrian solution had been a success and has been exported to the Nordic countries, particularly Norway.

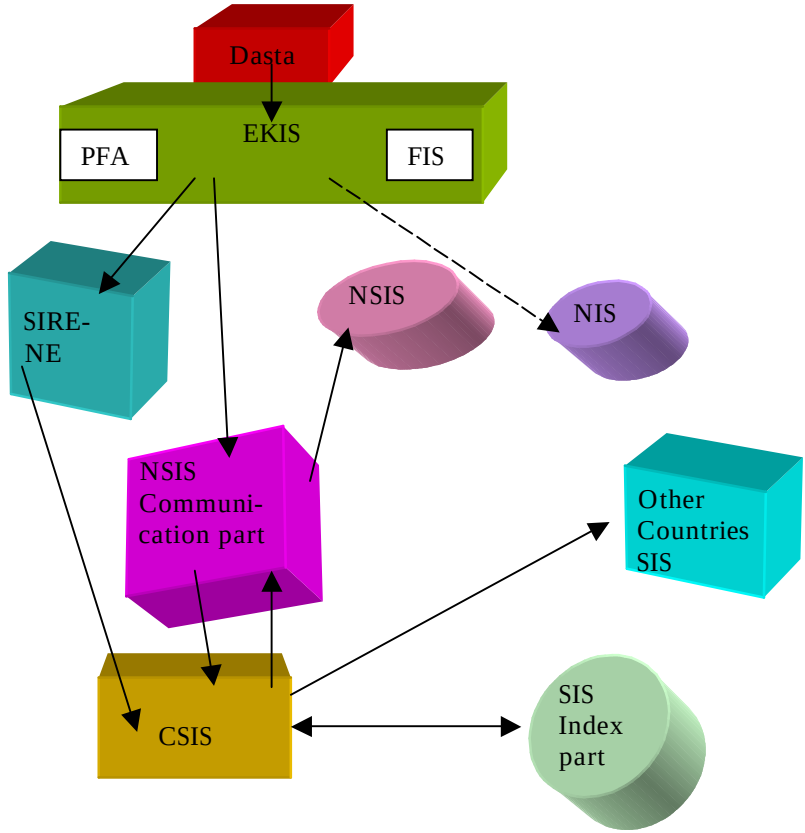
It was also emphasised that the Austrian NSIS is based on pre-existing national infrastructure. However, it was not developed in isolation. The team involved with implementation studied other countries' solutions, in particular those belonging to Spain, Portugal, the Netherlands and Germany, most of whom operate different systems.

As regards data modelling, the Austrian team did not need to create a new data model and design as this was already stipulated in the Schengen Convention. Their task was to follow the Schengen provisions, indicating which data is to be registered and the reasons for registration. In addition, a dictionary for storage which directs how data is to be stored already existed. Therefore, it was not necessary to develop a separate SIS data map, as most of the data that can be registered under the Convention had already been stored in the national information system (NIS). As SIS is largely an index system and database that stores basic data for purposes of search only, data is not stored in relation to categories. For details of data stored in SIS, one has to consult the supplementary data system – SIRENE.

3.3 The Functioning of the SIS

The question regarding the functioning of SIS was necessary in order to elicit information on the process which data follows: from the decision to register, through to when the data is ready for search, and how long this process takes. The aim was also to find out about the technical and organisational relationship between SIS, NIS and SIRENE. The relationship between SIS and SIRENE has been contentious, with some commentators claiming that the systems are one and the same, and others that the systems are separate, both technically and organisationally. The confusion arises because SIRENE is not included in the description of the components of SIS in Article 92 of the Schengen Convention. In addition, the Convention does not refer explicitly to SIRENE.

Figure 1: Austria: The technical aspects and functioning of the NIS and SIS



PFA – Criminal Register
FIS – Foreigner Register
→ Flow of information

The diagram above (Figure 1) was used during the interviews to answer the question and clarify the confusion. It represents the flow of data and the technical and organisational aspects of SIS in Austria.

The police, immigration authorities, customs services and courts may enter information into SIS. The process of entering data into SIS starts at the police stations. Here, police officers at the first level of criminal police au-

thority prepare an EKIS (national system for criminal investigation) document for entry into the national criminal system. The document is then transmitted to a data station (DASTA), which is a second level security authority (*Sicherheitsdirektion*). At the DASTA, the data is entered online by the staff into EKIS. If the EKIS document contains a special indicator for SIS-relevant data, special software filters the data set from the EKIS file and communicates it to a specific file of NSIS, which is then communicated by special software to CSIS. Where the SIS data set is relevant to Article 95 (extradition) or Article 99 (discreet surveillance), it is first communicated to SIRENE and from there onto CSIS. CSIS, after indexing the data, distributes it to NSIS in all Schengen countries, including the NSIS in the reporting country. Once distributed, the data is searchable. The whole process takes only 3 minutes to complete, which means, therefore, that SIS is very up to date. The same search query is sent both to SIS and the national system in Austria. This is because a national search is not only a SIS search, it also involves a search in the national system. The explanation given was that if this were not the case, persons not registered in SIS might escape detection because a negative hit in SIS does not necessarily mean that a person is 'clean'. Searching the national system may reveal other information, as a person may be registered in the national system but not in SIS.

As shown in the diagram, NSIS, SIRENE and NIS are all different technical and organisational units (see 5.2 below). Personnel working with these systems are different and the systems are located in different buildings. I had to travel to different locations and buildings to interview representatives of the different systems. As regards data protection and data security, keeping the systems separate is desirable so that any data protection problem affecting one system may not necessarily spill over to the other systems.

3.4 Access to Data in the System

Access to data in SIS has also been a contentious issue. The Schengen Convention does not set limits to the number of persons with access authority, instead leaving access regulation to the national laws of the Contracting Parties. Consequently, the list of persons with access differs considerably among the Contracting Parties. The question relating to access to data in SIS was therefore aimed at establishing a clear picture of who has access, how many persons have access and how access is controlled in Austria.

According to the Schengen Convention, data in SIS can be searched and accessed by authorities designated by the Contracting Parties for the purposes of border checks and controls, and other police and customs checks, when carried out inside the country in accordance with national law (Articles 92 &

101). Data entered pursuant to Article 96, relating to foreign nationals, may be searched by the authorities responsible for issuing visas, examining visa applications, issuing residence permits and the administration of aliens, within the framework of the application of the provisions on the movement of persons under the Convention (Article 101(2)).

In Austria, over 30,000 persons are allowed access to the data in SIS using 16,000 stationary terminals throughout the country.[8] This number is not restricted and can be increased as the need arises. In addition, officers on patrol and at external land-border crossing points are issued with laptop computers for access to information in SIS. The laptops are equipped with only the most important data, updated on a daily basis. Consequently, the officers cannot access all the data in NSIS. In case of a positive hit, they have to verify the information by radio to the main terminal, as data may have changed since their laptops were last updated. The practice is in line with the recommendation of the Schengen Joint Supervisory Authority (JSA) regarding copying alerts in SIS.[9]

Foreign missions abroad do not have online access to the SIS. They are issued with a CD containing information necessary to determine whether a person applying for visa should be accepted or not. The result of the query is either a red or a green light. The green light indicates that a visa can be issued if the applicant satisfies all other conditions. The red light, on the other hand, indicates that an objection exists to issuing a visa. In such cases, the officer should verify this and get details from headquarters at home. There are plans for mission offices abroad to submit queries online to SIS in the future. The CD is replaced fortnightly.[10]

3.5 Authorities with Control Responsibilities

Each Contracting Party is responsible for designating which national authorities have control responsibilities (Article 92 & 101). In practice, this means that each Contracting Party appoints the authorities in charge of NSIS. As the Convention does not specify which authorities these should be, the Member States have wide discretionary powers, and one must look at the national scene and legislation to identify the authorities. In Austria, the Ministry of the Interior is responsible for NSIS. It is also the top security organ in Aus-

---

8 In the Netherlands, the number of persons with access for the purpose of searching the SIS register is 7,000. Five hundred persons are authorised to change data. A few thousand can access data by telephone. This opens significant possibilities for leakage of information.

9 See JSA Opinion 97/1 of 22 May 1997.

10 *Ibid.*

tria. The Ministry has 9 police divisions with 100 police districts below them. Responsibility for control and security follows this hierarchy. Other authorities with control responsibility are Customs and Immigration. The DPC also has a role to play as a data control organ and appeal body for decisions made by the Ministry of the Interior.

4 SIRENE

4.1 Legal Basis

The issue of the legal basis of the SIRENE is still debated. Two opposing views seem to exist. The persons I interviewed were also divided on the issue, their views reflecting the two positions. The first position, which is held by the Schengen Member States and was reflected by the Ministry of the Interior, purports that SIRENE has a clear legal basis in Article 108 of the Schengen Convention. Earlier, in a decision of 1994, the Schengen Executive Committee supported this view by stating that the SIRENE manual contains the legal basis of SIRENE.[11] The second position, which was reflected in the interview with the DPC representative and held by the Central Data Supervisory Authority of Schengen (CDSA), claims that SIRENE has no clear legal basis either in national law or the Schengen Convention.[12] While these two views continue to exist, the issue of the legal basis remains unresolved. However, expectations are that when the second generation of SIS is implemented, rules will be developed to provide SIRENE with a clear legal basis.

4.2 Technical Aspects

The creation of SIRENE was meant to give SIS a human interface through which supplementary information on a positive hit in SIS could be exchanged. All relevant case information is exchanged and could include fingerprints and photographs in cases where identification is vital. DNA data are not yet exchanged. For security reasons, SIRENE consists of electronic files only and no

---

[11] See also the Schengen Executive Committee decision SCH/M (92) 24 rev. that the legal basis is to be found in the SIRENE manual.

[12] See JSA Opinion of 22 February 1995 on the legal basis of the SIRENE Bureaux. The JSA recommended that, as the Schengen Convention does not explicitly provide for the SIRENE Bureaux, they ought to be given a legal basis, either by amending the Convention or by amending national legislation in a harmonised fashion. However, on 27 June 1996, the Central Group concluded that an adequate legal basis existed. The issue is not yet conclusively resolved.

manual files. From an organisational point of view, SIRENE is a separate communication system to SIS. In Austria, NSIS and SIRENE belong to different organisations within the Ministry of the Interior. 22 SIRENE officers from the criminal police are working at the Austrian SIRENE office.

4.3 The Process of Exchange of Information

As stated above, SIRENE comes into the picture usually when there is a positive hit in SIS and where supplementary information regarding the hit is required. In such circumstances, a request for information is made to SIRENE. In principle, the request is made to the SIRENE office and not to a particular person. Since the SIRENE office operates 24 hours a day, it is the officers on duty who act when a request is made.

Figure 2: A hit in Austria

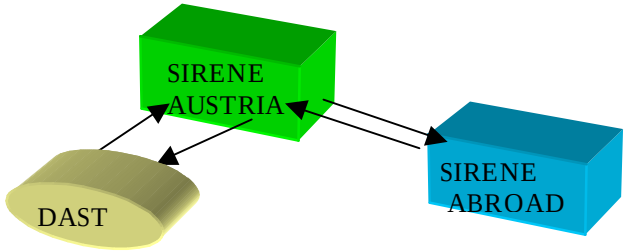
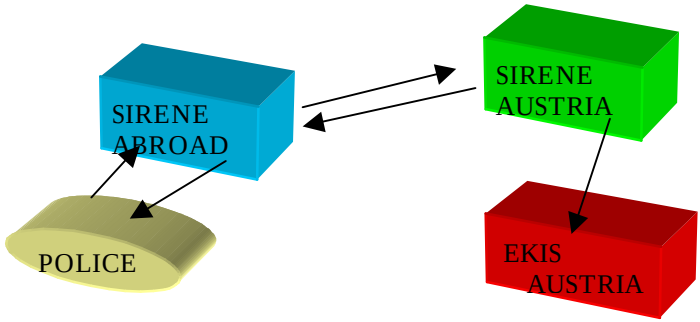


Figure 3: A hit abroad



Information is exchanged electronically through standardised forms. For example, a *G – Form* is for a hit and a *Q – Form* for data on usurped identity (a new form for cases where a perpetrator uses the name of a stolen passport as an alias), and so on. There are standardised forms for every purpose, eg, for arrest (see Article 95 of the Schengen Convention), for refusal of entry for foreign nationals (see Article 96), and so on. Where further clarification of electronically transmitted information is required, this may be requested by telephone or additional electronic messages. Supplementary information is supplied on request when there is a hit and further information is required. If a hit occurs in Austria itself, and the authorities require more information, then the request is sen to the Austrian SIRENE, which forwards the request to the SIRENE of the Contracting Party concerned. The supplementary information is then supplied to the Austrian SIRENE and forwarded to the requesting authority (see Figure 2 above). If the hit occurs abroad, the request is made to that country's SIRENE, and then forwarded to the Austrian SIRENE, who retrieves the relevant information and relays it back to the requesting SIRENE to forward to the source of the request (see Figure 3 above). This procedure is applied in all cases, except in cases concerning Article 95. In Austria, supplementary information under Article 95 is prepared at the time of entering a report in SIS. At this time, the necessary information is also prepared and distributed to all foreign SIRENEs. The response time to a request depends on the case. In some cases, it can take as little as 15 minutes.

5 Schengen Legislation and Documentation

During the negotiation and signing of the Schengen Convention, a number of documents were designated confidential, making them inaccessible to the public. Even institutions such as national parliaments found it difficult to access documents during the ratification process. The aim of the question relating to Schengen legislation and documentation was to find out which new documents were generated in the process of ratification and incorporation of the Schengen Convention into the Austrian legal system, and the extent to which these documents are accessible. It was also necessary to find out about the influence of the Schengen Convention on data protection legislation, especially in the Austrian police sector.[13]

[13] In countries that did not have data protection legislation, the Schengen Convention was seen to play a significant role for data protection in general and particularly in the police sector. Even in countries that had data protection legislation prior to the Schengen Conven-

The Schengen Convention is an intergovernmental treaty that requires incorporation into the national legal systems of the Contracting Parties. What emerged during the interviews was that there was no need to enact a new Schengen law, as the Schengen Convention has direct application and legislation status in the Austrian legal system. Austria belongs to the monism tradition. However, some statutes were amended to reflect changes incorporated by the Schengen Convention, for example the Police Co-operation Act. As explained previously, the Schengen data protection provisions did not have a specific impact on data protection regulation in the police sector. Austria has had a long-standing tradition of regulating data processing in police matters. The earlier Austrian Data Protection Act of 1988 applied to police information systems. This has been reflected in the new Data Protection Act of 2000.[14] Consequently, both the Data Protection Act of 2000 and the Schengen Convention apply to data protection in SIS. The Data Protection Act applies only where the Schengen Convention is silent. This is in line with the general rule in Article 104(2) of the Schengen Convention which states: 'where the Convention contains no specific provision, the relevant national law of the Contracting Parties applies'.[15]

The long tradition of data protection in police matters is also reflected in regulations. There are no regulations applying to the Schengen specifically. However, data protection regulations and guidelines have been issued that apply to data protection in general. The guidelines are general manuals for input of data into the national information systems, which also would apply to SIS. Apart from these documents, no other publications have been issued. For example, no annual reports pertaining to SIS and no information directed at educating the public on the Schengen Convention has been issued. The only public information on the Schengen Convention was issued in the period preceding the implementation of the Schengen Convention in 1997.

As regards the accessibility of Schengen documents, those interviewed at the Ministry of the Interior were of the opinion that the documents are accessible. They emphasised that, with the incorporation of the Schengen Acquis into the legal framework of the EU, EU rules on transparency and access to information

---

tion, for example Norway, the Convention has improved data protection in the police sector, especially with regard to data subjects' rights.

[14] See also W Kotschy, "Data protection in Schengen and Europol: Existing rules on data protection in the police sector in Austria", paper presented at the Council of Europe Regional Seminar on Data Protection in the Police Sector, Strasbourg, 13-14 December 1999: ADACS/DG (2000) 3 Sem Strasbourg, 27 April 2000.

[15] Schengen JSA, *Fourth Annual Activities Report*, March 1999 – February 2000, p 48.

apply to Schengen documents as well.[16] Nevertheless, Schengen technical documents remain confidential in order to protect the security and integrity of the systems from interference by criminal elements such as hackers.

6 The Role of SIS on Interstate Co-operation

When asked their opinion on the role of SIS on interstate co-operation, the interviewees were unanimous in viewing SIS as a positive contribution to interstate co-operation. They pointed out that it has been a very important measure in the realisation of free movement. At first, only few countries were involved in the co-operation, which was outside the EU framework. Currently, 15 countries are members (Great Britain is not a full member and participates in SIS only), of which 13 are EU Member States. It was claimed that this is proof that free movement does work, but it could not work without the security measures undertaken. SIS has been a very important measure in maintaining the internal security of member states and the control of illegal immigration. Searches in SIS have been efficient and have resulted in many positive hits, which have enhanced security and controlled crime and illegal immigration in the Schengen area.[17] The number of hits, both within the country and in the rest of the Schengen countries has increased with time. SIS has played a positive role in these areas.

However, some problems were pointed out which, if solved, could improve the working of SIS. It was said that in Austria, the prosecution and judicial authorities are not making good use of the capability of the system as regards entering data under Article 95. Only about 10% of the system is in use. The national Schengen authorities have initiated dialogue with judicial authorities to try to increase awareness of the system among them.

Another problem relates to the Schengen Convention, which is claimed to be very restrictive regarding the data to be entered in SIS. It was pointed out that this reduces the ability of the police to deal with crimes that could easily have been dealt with if such information had been allowed. For example, information on stolen car registration plates cannot be registered, although information on stolen cars is permitted. Registration plates are stolen and

---

[16] However, accessibility may still be impeded due to the cumbersome EU accessibility procedure.

[17] Since its launch in Norway on 25 March 2001, SIS has contributed to the arrest of 14 persons suspected of committing serious crimes in Norway: *Aftenposten* (morning edition) 3 September 2001.

used on stolen cars to commit robbery or other crimes. If they could be registered, it would be easier to track down stolen cars. This would involve expanding the list of information entered into SIS, and could only be carried out by amending the Convention.

7 Control and Safeguards

7.1 Introduction

Data protection in the Schengen Convention is ensured through a series of rules and control systems. Although rules are important in the protection of data and individual rights, it is the practising of the rules that determines the effectiveness of protection. Control of the application of the rules is what determines the overall effectiveness of the practice. In order to determine how the rules of data protection in Austria are applied, I analyse in the following the control systems that are in use, applying the evidence collected from the interviews. As Cameron (2000) has noted: "systems have blends of internal and external controls and remedies".[18] Below, I focus on this categorisation of internal and external control.

7.2 Internal Control

Internal control refers to safeguards built into the system to ensure the quality and security of the data, as required under Article 118 of the Schengen Convention. They are a combination of technical, personnel and organisational controls. *Technical* controls take various forms and are undertaken to ensure that the system complies with data protection rules concerning collection, quality and security of data. The Schengen Information System is an open-loop online system. According to Gregory and Horn, an open-loop online system utilises people for gathering data or carrying out the control instructions, unlike a closed-loop system, which is fully automated at all stages, from data origination through processing back to the implementation of control.[19] People are therefore an important part of internal controls in SIS, especially at the origination of data (collection, conversion and verification) and entry stages. *Organisational* controls refer to the management structures

---

[18] I Cameron, National Security and the European Convention on Human Rights (Uppsala: Iustus Förlag, (2000).

[19] RH Gregory & RLV Horn, *Automatic Data-Processing Systems – Principles and Procedures* (London: Chatto and Windus, 1963), p16.

and the responsibilities of both management and staff. For convenience and clarity, I discuss below internal controls through different stages of data processing, starting with the origination of data, entry of data and access to data. Technical controls and personnel involved in control will be discussed for each stage in data processing. Organisational control will be discussed at the end of this section, as it runs throughout all the data-processing phases.

7.2.1 Origination of Data

Origination of data refers to three activities: collection, conversion and verification. According to the findings from interviews, police criminal officers of first level collect data for entry into SIS in Austria. They prepare the records for entry into EKIS and flag the data for entry into SIS. Prosecutors and courts collect and prepare data on extradition (Article 95 of the Schengen Convention) for entry into EKIS. Similarly, the immigration authorities collect and prepare data under Article 96, refusal of aliens to enter, for entry into EKIS. The collecting officers are responsible for checking that the data for inclusion in SIS comply with collection-of-data rules, especially the purpose principle, as stipulated in Articles 95–100 of the Convention. Once the data records are ready, the officers send them to a DASTA. At the origination stage, only human control is performed.

7.2.2 Entry of Data

Both human and technical controls are carried out at the data entry stage for SIS data records. Entry of data into SIS is the responsibility of second-level criminal officers at the DASTAs. However, before the data is entered, the officers at the DASTA are required to carry out data verification. Data verification includes checks to determine that the records are in the approved format, convey the correct meaning to the reader, and will lead to the appropriate action.[20] The officers at the DASTA visually control the data record to confirm that it complies with registration rules and, if necessary, correct it. In Austria, this is referred to as the 'four-eyes –entry' principle, where two officers visually control the record. When the officers are satisfied that the data record conforms to the stipulated conditions, they enter the record online into EKIS. In EKIS, special software filters data records marked for SIS and communicates them to a special file in NSIS. Special software in NSIS further controls and communicates the data record to CSIS. However, data records under Articles 95 and 99 of the Convention are first sent by the special software program in EKIS to SIRENE, and SIRENE later communicates the re-

[20] *Ibid,* p 6.

cords to CSIS. After the data records have been indexed at CSIS, they are redistributed to all Schengen Contracting Parties' NSISs, ready for search.

7.2.3 Access to Data

Access to data is required for various reasons: search, updating, correction, deletion, and individual access request (this will be discussed later as part of the external control). The objective of SIS is to offer online searchable access facilities for criminal and immigration authorities. Hence, search is the most common form of access to SIS. In data protection, the rule of thumb for access is necessity. The person who accesses the data must have a legitimate reason, such as fulfilling a public duty required of him/her. According to the findings from the interviews, access for purposes of search seems to be available to practically all officers responsible for border, crime, and immigration control in Austria. The number is not restricted and may increase as the need arises. The large number of people with access authority opens up the possibility for leakage of information.

Access for purposes of updating, correction and deletion of information is restricted and open only to DASTA officers who have the authority to enter data into SIS. Every six years, a control is made to ensure that the data are current. In normal cases, deletion of data happens automatically after the duration stipulated for storage expires (Article 112). The central system checks regularly for expiration dates. A month before deletion, a notice is automatically issued to the Contracting Party concerned and, unless they request retention, the data is automatically deleted.

In order to control access in general, a log audit is kept for all access to SIS. A log is created for every access. In the log audit, the user's identity or name, password, time, and reason for access are recorded. The Schengen Convention requires that every tenth query be recorded (Article 103). However, the practice in Austria is to log every query and the result. The log audits are stored at the EDP centre at the Ministry of the Interior and are deleted after six months, as required under the Convention.

To ensure data security, control of log audits is routinely performed. Currently, the control is done by use of a random generator sent via emails to police divisions, requesting the reasons for access. Every week, 5 police divisions are controlled, involving a total of 20 persons. A project for control through online networks is on trial, and this will radically improve the number of controls. Where a violation of access rights is discovered, the officer concerned is reported to the criminal investigator, who may prosecute. So far, no reports on violations concerning SIS have been filed to the investigator. However, numerous violation reports have been filed concerning the national

information system. As a result of a recent scandal concerning the national system[21], the Ministry of the Interior is considering to enhance access control and security by use of biometrics options. Similar log-audit procedures apply for access to SIRENE. The SIS and SIRENE have separate networks for communicating information, encrypted to ensure security.

Although the access audits serve a useful role in monitoring use of the system, the DPC views the lack of manpower or capacity to control the log audits as critical. The data protection officer from the Ministry confirmed this. Currently, only about 20 persons in five police divisions are controlled every week. This is a very low number for a system that can be accessed by over 30,000 persons at any given time. As many protocols as possible should be controlled for the procedure to be effective.

In addition, the systems are most vulnerable to threats originating from within the system. Those authorised to access the system pose the biggest threat to the security of the system, as the recent scandal in Austria and earlier scandal in Belgium[22] confirm. Although the Austrian incident did not involve SIS, it did, however, indicate that those who are entrusted with administering the system are its weakest link. Adequate control of log audits is important in order to forestall such scandals. Other measures, such as use of biometrics, would go a long way towards mitigating the problem. It is encouraging that the Ministry of the Interior is considering these possibilities as pointed out by the interviewees.

7.2.4 Organisational Controls

Organisational controls of a system involve personnel and procedures. As noted previously, SIS is an open-loop system, utilising people for its control function. Personnel are therefore a very important component of the internal control system. As discussed above, first-level criminal officers are responsible for collection of data, and second-level criminal officers for verifying and enter-

---

[21] According to *Toward Freedom Magazine*, the incident is "Europe's Watergate". In a book by the former leader of Austria's police union, it is claimed that the extreme-right Freedom Party had made widespread and systematic use of paid police informants to obtain confidential information from the police computer system, EKIS. At a 1997 press conference, a party politician, without revealing the names of his contacts, had openly presented EKIS printouts. See further <http://www.towardfreedom.com/jan01/notebook.htm> (last visited 26.11.2002).

[22] Data printouts from SIS were found lying about at a railway station. See further Schengen JSA, *Third Annual Activity Report*, March 1998 – February 1999, SCH/Aut-cont (99) 8 rev, pp8-9. See also <http://www.cnpdpi.pt/schengen/Eng/relato_sir_eng.htm> (last visited 26.11.2002).

ing data into SIS. In addition, the Ministry of the Interior has appointed a person responsible for data protection and security in the national system. This person is also responsible for data protection and security in SIS. Furthermore, the responsibility for data protection in the police systems has been decentralised to each of the 9 police districts, each of which has a person responsible for data protection and security. The Ministry of the Interior has also appointed a person responsible for security and data protection for SIRENE. This person is answerable to the overall data protection officer at the Ministry. Procedures are regulations and technical control systems such as rules and procedures for deletion, updating, correction and access logs, as discussed above. However, a very important procedure not yet discussed is reporting. Reporting entails the making of documentation such as annual reports, educational material and other statistical material. This seemed completely absent in the Austrian SIS control systems. Such documentation is important for external control and transparency in the system (as discussed below).

7.3 External Control

External control refers to some form of institution or mechanism, independent of the system, such as supervision, audit and parliamentary and judicial bodies. The importance of external control is not to replace internal control, which by all means is the most effective safeguard if it works properly, but to ensure that internal controls are working effectively.[23] The Schengen Convention provides for supervision (see Articles 114 & 115) as a form of external control, and judicial control was included by the Amsterdam Treaty during the incorporation of Schengen into the EU legal framework.[24] A third form of external control that may be added is the individual right of access to data (Article 109). I regard the right of access as a form of external control, since it is not exercisable without the initiative of a data subject who is external to the system. I now discuss these controls in relation to the findings from the interviews.

7.3.1 Supervision

The Schengen Convention provides for supervision at two levels: national (Article 114) and joint (Article 115). As regards *national supervision,* the Schengen Convention requires that each Contracting Party appoints a national authority to perform the task of supervising the national section of SIS, independently and in accordance with national law. In Austria, the DPC is

---

[23] Gregory & Horn, *supra* n 19.

[24] Title IV, Article 68(2) of the EC Treaty and Title VI, Article 35(5)-(6) of the EU Treaty.

such a body. It is independent and carries out controls and investigations on the national data systems and handles complaints from data subjects. According to findings from the interviews, the DPC has had occasion to carry out security controls on the national information system (NIS) and SIRENE but not NSIS. In 1998, it carried out a surprise control on SIRENE. The controls were targeted at persons with access authority and aimed at ensuring that they had the necessary knowledge and qualifications. Control has also been directed at technical security measures, such as logging audits to ensure that they are properly executed and controlled. However, as mentioned above, lack of personnel to control the log audits is a serious drawback.

As an appeal body for decisions made by the Ministry of the Interior, the DPC has not been very active because very few appeals relating to SIS have been made. So far, as far as I am aware, only one case has been appealed to the DPC and the decision of the Ministry was upheld. However, there have been many appeals relating to NIS.

Joint supervision of CSIS is allocated to the Joint Supervisory Authority (JSA). JSA must perform its tasks in accordance with the Schengen Convention, the 1981 Council of Europe Convention on data protection,[25] the 1987 Council of Europe Recommendation on use of personal data by the police,[26] and French national law. However, the JSA lacks the necessary powers to make legally binding decisions and carry out investigations. Although it issues annual reports, it does not have the power to implement the recommendations made therein.[27] Furthermore, despite the new arrangement with the European Council, providing the authority free access to carry out its work independently, the Council maintains control over the authority's budget. This may interfere with its independence. As presently constituted, the JSA may not be an effective external control.

---

[25] ETS 108.

[26] Recommendation No R (87) 15 Regulating the Use of Personal Data in the Police Sector (adopted 17.9.1987).

[27] Although the JSA has made several recommendations in its opinions published in the annual reports from 1996,1997, 1998, 1999 & 2000, very few of these suggestions have been implemented. The ability of the JSA to carry out investigations and controls on CSIS has also been hindered on occasion by the French authorities. However, the JSA was able to carry out inspection of CSIS in October 1996. In 1998, 10 states, already applying the Convention under the request of the JSA, carried out inspections of their respective SIRENE Bureaux.

7.3.2 Judicial Control

Judicial control, especially international or joint judicial control, was never a strong point in the Schengen co-operation. The Schengen Convention totally circumvented the idea of joint judicial control. However, the incorporation of the Schengen Agreement into the EU legal structure has acknowledged that the European Court of Justice has limited jurisdiction here. This may salvage the situation. Despite shortcomings in joint judicial control, the national judicial systems of Contracting Parties remain the most viable judicial control organs regarding Schengen issues. In Austria, courts exercise judicial control as the appeal organs for decisions originating from the DPC. The DPC is the first-level appeal organ concerning decisions of the Ministry of the Interior. It sits as a tribunal and reviews decisions made by the Ministry of the Interior. However, it has been rarely called upon to exercise its judicial review power. So far, it has done so only once. There have been practically no appeals against the decisions of the Ministry of the Interior.

It is difficult to tell whether this is an indication of the efficiency of the Ministry of the Interior in its internal control of SIS or in its decisions (as those from the Ministry were inclined to point out), or an indication of a lack of information on the part of data subjects on their rights, or due to the short time SIS has been operational. A combination of all these factors could be the explanation.

In other jurisdictions, such as France, Germany and the Benelux states, where SIS has been in operation for some time now, a significant number of cases are finding their way to the courts.[28]

In principle, an individual has a right of appeal, especially where one exercises the right of access, to the administrative Supreme Court, if not satisfied with the decision of the DPC. In addition, if the matter raises a constitutional question, a reference can be made to the Constitutional Court. Unlike the DPC, the courts have not yet had occasion to review a Schengen appeal case.

Although joint judicial control was lacking in the earlier Schengen legal system, by extension of national judicial control, the European Court of Human Rights (ECtHR) has joint control over appeals originating from Schengen Contracting Parties' courts. However, the ECtHR has not yet addressed such appeals. It takes a long time before individual applications meander through and exhaust national remedies. This could explain the present lack

---

[28] See E Guild, "Adjudicating Schengen: National Judicial Control in France" (1999) 1 *European Journal of Migration and Law*, pp 419–439; A Hurwitz, "The 'Schengen' Practice and Case-Law in Belgium" (2000) 2 *European Journal of Migration and Law*, pp 37–48; H Staples, "Adjudicating the Schengen Agreements in the Netherlands" (2000) 2 *European Journal of Migration and Law*, pp 49–83.

of such appeals to the ECtHR. However, it is only a matter of time before appeals emerge, especially from the original Schengen Contracting Parties.

Judicial control is important especially in addressing wider questions of human rights and the interpretation of the Schengen Convention. Some national judicial decisions have pointed to the lack of clear registration and search criteria in the Schengen system, as practised by the Contracting Parties. In France, in the case of a Romanian national, Mrs Forabosco, the court criticised the registration practice in Germany, where the authorities register information about persons whose asylum application has been rejected. The French court asserted that such practice contradicts Article 96 of the Schengen Convention.[29] In another French court case, *Tribunal Administratif de paris v. Saïd* (1996),[30] the court condemned French local authorities' search practices. A person from Algeria, with a valid residential permit in France, was issued a deportation order after reporting a change of residential address to the local authorities. The authorities searched SIS and found that the person had been registered as an unwanted person, to be refused entry under Article 96 of Schengen Convention by Belgian authorities, for an offence committed in Belgium while on a visit there. In its decision, the court held that the local authorities had no right of access to search SIS on the basis of a report concerning change of residential address. These decisions also point to a need for joint judicial control in order to give a uniform interpretation of the provisions of the Convention, a responsibility the European Court of Justice should now have, despite its limited jurisdiction.

7.3.3 Individual Control

Under the Schengen Convention, where registration of data is required by law, and the individual has no right of consent or notification (where the data is recorded without the knowledge of the individual), exercise of individual control is dependent on the right of access. In theory, an individual has the power of control through exercising the right of access (Article 109(1)), associated rights of correction or deletion (Article 110), and request of verification of data through national data protection authorities (Article 114). Obviously, the most important of these rights is the right of access. Without this, the exercise of the other rights may be rendered academic.

Unfortunately, the right of access under the Schengen Convention is severely restricted. For example, where access requests fall under any of the ex-

---

[29] See Guild, *ibid*, and Justice, *The Schengen Information System: a human rights audit* (London: Justice, 2000), p 28.

[30] *Ibid.*

ceptions (Article 109(2)), the practice in Austria is to inform the data subject that no data concerning her/him that can be communicated is registered. In Norway, a similar procedure has been adopted. Such ambiguity is found necessary in order not to reveal to the data subject that data concerning him/her is registered but cannot be revealed. In my opinion, however, this is unfortunate as the data subject is left in a state of limbo, not knowing whether any data about himself/herself is registered. This is especially the case where the data registered relates to ongoing criminal investigations or discrete surveillance. In such cases, an individual cannot exercise any control. In principle, if the individual is not satisfied with the reply, he/she may request the national data supervisory authority to check whether any data concerning himself/herself is registered. However, if the data falls under the above mentioned exceptions, the supervisory authority may not be allowed to reply to the data subject (Article 109(2)). In such circumstances, individual control may only be practical in cases where registered data does not fall under the exceptions and, given the nature of SIS, these may be very few indeed.

According to the findings of the interviews, the right of access is barely used in Austria. Although no long-term, concrete statistics were available, during the four months immediately prior to March 2001, there had been about 1,200 requests concerning registration in SIS. According to my source of information, this is a high number of requests for such a short period. The upsurge of requests was attributed to a data registration scandal that had been publicised in the newspapers at the time, concerning the NIS, but not involving the SIS. The experience, as I was informed, was that whenever there was such a scandal, the rate of requests tended to increase and then fall and stabilise again. For example, during the nine-month period prior to the scandal, the number of requests received was about 600. For most of these requests, there is no data registered in SIS. Requests for access are received from inside Austria, as well as from outside Austria and outside the Schengen area.

The right to have data corrected and deleted is practised in a similar manner as the right of access. If there is a need to correct or delete data, the request is normally complied with in cases where Austria is the reporting country. Where another Contracting Party has entered the data, the Ministry notifies the Contracting Party as soon as possible. The same procedure applies to updating data in SIS.

The exercise of individual control is also dependent on the information and knowledge available to the public in general about SIS. Unfortunately, the public seems to be poorly informed. This could partly explain the general public's apparent lack of enthusiasm for exercising their rights of access. Lack of public awareness can pose a serious threat to privacy and transpar-

ency interests, as it compromises the individual's control powers. In Austria, except for the limited information given to the public during the launch of SIS in 1997, no other public information campaign has been carried out. As it transpired from the interviews, the Ministry of the Interior does not issue annual reports or any other documentation that could be of use to the public. The problem could be traced to the Schengen Convention, which imposes no requirement to inform the public. Even where such a requirement may be available under national law, it is unfortunately left to individuals to take the initiative. This is the case in Norway.[31] The JSA has attempted to fill the informational gaps by placing brochures explaining individuals' rights at airport terminals and other authorised crossing points at the external borders of the Schengen area. It has also published alert statistics. However, they are not adequately informative, as they fail to specify the number of persons registered under each Article of the Schengen Convention.

8 Conclusion

In a system such as SIS, where individuals have restricted or no access to their personal information, only internal and external control mechanisms can ensure adequate individual protection. It is imperative, therefore, that those responsible for the system ensure proper internal control mechanisms. On the other hand, efficient external control should complement internal control in order to enhance overall individual protection. Both SIS internal control and external control mechanisms require fine tuning to ensure that innocent individuals do not become victims of the very system that is supposed to protect them. Areas of focus should be the collection and entry of data, control of access, public information and education, and both national and joint supervision. A requirement for a comprehensive data audit of all Schengen systems may be a viable solution for better and more comprehensive individual protection.

---

[31] DW Schartum, "Access to Government-Held Information: Challenges and Possibilities" (1998) 1 *The Journal of Information, Law and Technology*, <http://elj.warwick.ac.uk/jilt/infosoc/98_1scha/>.

PRISEN FOR POLITIINFORMANTENES LIV

JENS PETTER BERG

Justisdepartementet fremmet den 6.12.2002 et lovforslag som vil nekte de mistenkte og deres forsvarere rett til innsyn i opplysninger når politiet ikke vil påberope disse som bevis i alvorlige straffesaker. Justisminister Dørum ønsker med dette forslaget å bedre sikkerheten til politiets kilder, angivelig uten at man av den grunn gir slipp på viktige rettssikkerhetsgarantier. For innsynsnektelse skal bare kunne besluttes av retten dersom det er strengt nødvendig, og ikke dersom nektelse «medfører vesentlige betenkeligheter» av hensyn til den mistenktes forsvar. Den mistenkte sjøl og hans forsvarer får imidlertid ikke være med på rettens behandling av påtalemyndighetens begjæring om innsynsnektelse.

Statsadvokaten i Oslo frafalt 6. desember 2002 tiltalen mot, og løslot to utlendinger som var blitt pågrepet på kureroppdrag i Osloområdet med ca 35 kg heroin. Beslutningen var en reaksjon på Høyesteretts kjæremålsutvalgs avgjørelse dagen i forveien om at disse to hadde krav på fullt innsyn i opplysninger om bl a bruken av politiinformanter i saken.

Høyesterett var ved sin avgjørelse bundet av Borgarting lagmannsretts bevisvurdering, dvs av denne domstolens avgjørelse om «at opplysningene i de tilbakeholdte dokumentene kan være relevante for avgjørelsen av straffesaken». Tap for påtalemyndigheten også i rikets øverste domstol var dermed påregnelig – med mindre påtalemyndigheten hadde klart å få dommerne med på at det var legitimt å foreta en sterkt utvidende tolkning av bevisavskjæringsregelen i straffeprosessloven § 292 andre avsnitt. Alternativet var å overlate en slik avveining mellom hensynet til politiinformanters sikkerhet og hensynet til tiltaltes forsvar til Stortingets avgjørelse – gjennom en lovendring.

Påtalemyndigheten hadde opplyst under rettsforhandlingene at man av hensyn til politiinformanters liv heller ville frafalle saken enn å bøye seg for en avgjørelse om innsynsrett for de tiltalte, men høyesterettsdommerne valgte likevel å overlate verdiprioriteringene til Stortinget som lovgiver. Dermed ble lagmannsrettens avgjørelse om innsynsrett for de tiltalte stående. Bak dommernes knappe begrunnelse lå åpenbart en bekymring for at en slik begrensning av en mistenkts rett til innsyn i opplysninger som kunne være av betydning for saken, måtte regnes som et uakseptabelt innhogg i vår straffeprosessordnings

grunnleggende prinsipp om likeberettigelse (våpenjevnbyrdighet) mellom påtalemyndighet og mistenkte.

Det problemet som melder seg når man av hensyn til politiinformanters sikkerhet vil begrense en mistenkts innsynsrett i opplysninger hos politiet, er at disse opplysningene kan være av betydning for straffesaken mot ham, da særlig for spørsmålet om han er skyldig eller for hvor streng straff som skal idømmes. Jo sterkere indikasjonene er på at opplysningene kan ha en slik betydning, desto mer nærliggende er det at det vil oppstå nettopp slike «vesentlige betenkeligheter» av hensyn til den mistenktes forsvar, som også etter Justisdepartementets lovutkast innebærer at innsynsretten ikke skal kunne beskjæres. I merknadene til den nye bestemmelsen i straffeprosessloven § 242 a nevner departementet som eksempel at det er stilt spørsmål om det er brukt «provokasjon» mot den mistenkte, altså at en politiinfiltratør har lokket mistenkte til å foreta en straffbar handling som ellers ikke ville ha blitt utført.

Høyesterett har i en dom fra 1984, trykt i Rt 1984 s 1076, risset opp grensene for politiet i saker om bruk av de «utradisjonelle» kriminaletterretningsmetodene. I kampen mot narkotikaondet må man, fordi tradisjonell etterforskning ikke duger, akseptere bruk av informanter (tystere) og politiinfiltratører. Politiinfiltratørene må også få lov til å opptre helt på kanten av hva som må regnes som provokasjon – med såkalt «provokasjonstilsnitt» – overfor de mistenkte, slik at de enten avslører straffbare handlinger *som de allerede har utført*, eller utfører en ny straffbar handling *som de likevel ville ha utført* med visse endringer i tid, sted eller utførelse. Men, understreket en samlet rett, vi

> «finner det klart at det ikke kan aksepteres at politiet fremkaller en straffbar handling som ellers ikke ville ha blitt begått ... I utgangspunktet er [derfor] etterforskning med provokasjonstilsnitt bare berettiget når politiet måtte legge til grunn at den straffbare handling ville ha blitt begått også uavhengig av dets rolle i begivenhetsforløpet.»[1]

Det mest skumle med Justisdepartementets forslag til nye lovbestemmelser er at lovavdelingens dyktige jurister nå har lært seg «menneskerettighetsleksen», og tilsynelatende presenterer en velbalansert drøftelse av de kryssende hensyn som gjør seg gjeldende. Som allerede påpekt skal f.eks. den nye bestemmelsen ikke anvendes dersom faktum ligger slik an som i heroinsaken fra september – altså at det er en ikke fjerntliggende mulighet for at politiet har brukt ulovlig provokasjon. Dersom man skreller bort den departementale garnityren, er det imid-

[1] Rt 1984 s 1076 på s 1080.

lertid umulig å lukke øynene for at departementet ved å nekte mistenkte og hans forsvarer noen informert rolle i forbindelse med rettens forhandlinger om å nekte dem innsyn i opplysninger som påtalemyndigheten ikke vil påberope seg som bevis i saken, har satt dem *sjakkmatt* allerede i åpningstrekket. Kunstgrepet med å oppnevne en særskilt advokat (lovforslaget § 100 a) som på vegne av mistenkte og hans forsvarer, men uten å gi disse innsyn i de aktuelle opplysningene, skal imøtegå påtalemyndighetens argumentasjon i saker om innsynsnektelse, kan vanskelig hevdes å reparere en slik tilsidesettelse av våpenjevnbyrdighetsprinsippet. Denne innvendingen har ikke overraskende allerede vært påpekt med styrke av en rekke forsvarere under høringsbehandlingen – men dessverre uten at det fikk justisminister Dørum til å skifte mening.

Dersom Stortinget gir sin tilslutning til forslaget i Ot prp nr 24 (2002–2003), vil Riksadvokaten ha lyktes i bestrebelsene på å forhindre lovregulering av den proaktive kriminaletterretning – det politiarbeidet som starter allerede mens de antatte lovbryterne ikke har gjort mer enn å foreta forberedelseshandlinger som de ikke kan straffes for. Riksadvokaten uttalte i sin høringsmerknad av 31.10.2002 at det «har vært påtalemyndighetens standpunkt i anslagsvis de siste 15 år at straffesaken som sådan *begynner* med ransaking eller pågripelse, og at den informasjon som foranlediget at politiet kunne «slå til» ikke vedrørte saken». Bak denne retorikken ligger et gjennomtenkt strategivalg, hvor målsettingen er å utvirke mindre offentlig innsyn i og svekket domstolskontroll med bruken av kontroversielle politimetoder.

Så lenge Justisdepartementet vil frata den mistenkte og hans forsvarer enhver informert rolle under avgjørelsen av spørsmålet om å nekte innsyn i saksopplysninger, og Riksadvokaten insisterer på at embetets rundskriv om skrankene for bruk av «utradisjonelle» politimetoder må unntas offentlighet av effektivitetshensyn, framstår det som «orwellsk nytale» når disse justisbastioner sammenfallende hevder at de foreslåtte nye lovbestemmelser vil åpne for mer domstolskontroll med politiets metodebruk enn hittil.

Riksadvokatens og justisminister Dørums reaksjon på høyesterettskjennelsen i heroinsaken viser nok uansett at det trengs enda tydeligere tale fra rikets øverste domstol ved neste korsvei: Tida har løpt fra den tilvante oppfatningen i norsk straffeprosess om at det ikke er behov for lovregulering av «utradisjonelle» etterforskningsmetoder, og da særlig bruken av politiinfiltratører for å avsløre straffbare handlinger.

FORFATTEROPPLYSNINGER

Jens Petter Berg (<j.p.berg@jus.uio.no>; født 1952) er cand. jur (Universitetet i Oslo 1980). Han har bl a vært saksbehandler i Finansdepartementet og ved Oslo likningskontor, og underdirektør og rådgiver sistnevnte sted. Han har vært tilknyttet Institutt for rettsinformatikk som forsker siden 1992, og er nå i avslutningsfasen av sitt doktorgradsprosjekt «Skattlegging for hvilken pris? Rettslige skranker for ligningsmyndighetenes håndtering av opplysninger om skattyterne : Med særlig vekt på grunnrettslige, menneskerettslige og personopplysningsvernrettslige skranker».

Jon Bing (<jon.bing@jus.uio.no>) er professor og tidligere bestyrer ved Institutt for rettsinformatikk. Han er dr. juris (Universitetet i Oslo 1982), dr. juris hon. causae (Stockholms universitet 1997), dr. juris hon. causae (Københavns universitet 1998), Visiting Professor ved King's College i London og leder for Personvernnemda i Norge. Han arbeider særlig med personvernrett, immaterialrett og interlegal rett.

Lee A. Bygrave (<lee.bygrave@jus.uio.no>; <http://folk.uio.no/lee/>) er dr. juris (Universitetet i Oslo 2000). I tillegg har han B.A.(Hon.s) og LL.B.(Hon.s) fra Australian National University i Canberra. Han er postdoktorstipendiat ved Institutt for rettsinformatikk, hvor han i hovedsak arbeider med forbrukervern- og personvernspørsmål knyttet til e-handel.

Stephen K. Karanja (<s.k.karanja@jus.uio.no>; <http://folk.uio.no/stephenk/>) er doktorgradsstipendiat. Han har LL.B.(Hon.s) fra University of Nairobi, Kenya og M.A. (ESST) fra Universitetet i Oslo. Han arbeider hovedsakelig med problemstillinger om grensekontroll, overvåkning, informasjonutveksling og personvern innen Schengen-samarbeidet.

Dag Wiese Schartum (<d.w.schartum@jus.uio.no>; <http://folk.uio.no/dags/>) er knyttet til Avdeling for forvaltningsinformatikk (<http://www.afin.uio.no/>). Han er dr. juris (1993) og professor (1997) og har ledet Avdeling for forvaltningsinformatikk siden starten i 1994. Schartum arbeider særlig med personvern, automatisering av rettslige beslutninger, IKT og åpenhet, samt spørsmål vedrørende regelverksutvikling og -administrasjon.

Susan Schiavetta (<susan.schiavetta@jus.uio.no>) er doktorgradsstipendiat. Hun har B.A.(Hon.s) i European Business Law fra University of Abertay Dundee, Scotland og LL.M. (med «distinction») i Information Technology and Telecommunications Law fra University of Strathclyde, Glasgow. Hennes doktorgradsprosjekt handler om online tvisteløsningsmekanismer.

Olav Torvund (<olav.torvund@jus.uio.no>;<http://www.torvund.net/>) er professor og bestyrer ved Institutt for rettsinformatikk. Han er også styreleder ved InterMedia (<http://www.intermedia.uio.no/>). Han er dr. juris fra Universitetet i Oslo (1993). Han arbeider særlig med elektroniske transaksjoner, immaterialrett og kontrakter.

Emily M. Weitzenböck (<emily.weitzenboeck@jus.uio.no>; <http://folk.uio.no/emilyw/>) er forsker. Hun har LL.M. fra Universitetet i Southampton, England og LL.D. fra Universitetet i Malta. Hun arbeider primært med selskaps- og kontraktsrettslige spørsmål knyttet til virtuelle organisasjoner og liknende samarbeidsformer.

NOTES ON AUTHORS

Jens Petter Berg (<j.p.berg@jus.uio.no>; born 1952) has the degree of cand. jur from the University of Oslo (1980). He has worked as an administrative officer in the Ministry of Finance and as Assistant Director at the Oslo Tax Office. Since 1992 he has been attached to the NRCCL, where he is now finalising his doctoral project, "Taxation at what cost? Legal limitations on the tax authorities' processing of information on taxpayers – with special emphasis on limitations set by core rights, human rights and data protection rights".

Jon Bing (<jon.bing@jus.uio.no>) is professor and former head of the NRCCL. He has the degrees of dr. juris (University of Oslo, 1982), dr. juris hon. causae (Stockholm University, 1997), dr. juris hon. causae (Copenhagen University, 1998). Amongst numerous engagements, he is chair of the Data Protection Tribunal in Norway and Visiting Professor at King's College, London. His main fields of research are privacy/data protection law, intellectual property rights and private international law.

Lee A. Bygrave (<lee.bygrave@jus.uio.no>; <http://folk.uio.no/lee/>) was awarded the degree of dr. juris at the University of Oslo in 2000. In addition, he has a B.A.(Hon.s) and LL.B.(Hon.s) from the Australian National University, Canberra. He is presently postdoctoral research fellow at the NRCCL, where he works primarily on consumer and privacy/data protection issues connected with e-commerce.

Stephen K. Karanja (<s.k.karanja@jus.uio.no>; <http://folk.uio.no/stephenk/>) is a doctoral research fellow. He has an LL.B.(Hon.s) from the University of Nairobi, Kenya and an M.A. (ESST) from the University of Oslo. The main focus of his research is legal issues concerning border control, surveillance, privacy and exchange of information within the framework of the Schengen system.

Dag Wiese Schartum (<d.w.schartum@jus.uio.no>; <http://folk.uio.no/dags/>) works at the Section for Information Technology and Administrative Systems (SITAS) (<http://www.afin.uio.no/>) which is linked to the NRCCL. He was awarded the degree of dr. juris in 1993 and became professor in 1997. He has been in charge of SITAS since its inception in 1994. Schartum works particularly on issues concerned with privacy/data protection, automation of legal decision-making, ICT and transparency, together with issues dealing with the development and administration of sets of rules.

Susan Schiavetta (<susan.schiavetta@jus.uio.no>) is a doctoral research fellow. She has a B.A.(Hon.s) in European Business Law from the University of Abertay Dundee, Scotland and an LL.M. (with distinction) in Information Technology and Telecommunications Law from the University of Strathclyde, Glasgow. She is currently working within the area of Online Dispute Resolution for her dr. juris degree.

Olav Torvund (<olav.torvund@jus.uio.no>; <http://www.torvund.net/>) is professor and current head of the NRCCL. He is also the chairman of the board for InterMedia (<http://www.intermedia.uio.no/>). He has the degree of dr. juris from the University of Oslo (1993). He works primarily on electronic transactions, intellectual property and contract law.

Emily M. Weitzenböck (<emily.weitzenboeck@jus.uio.no>; <http://folk.uio.no/emilyw/>) is a researcher with an LL.M. from the University of Southampton, England and an LL.D. from the University of Malta. She works primarily on corporate and contractual legal issues related to dynamic, networked organisations such as virtual organisations.